# AZ-500:
# Azure Security Engineer Associate

by Christopher Nett


# Connect with me!

Get discounted courses, updates and industry insights

My Website

Azure Newsletter

Cybersecurity Newsletter

Social Media

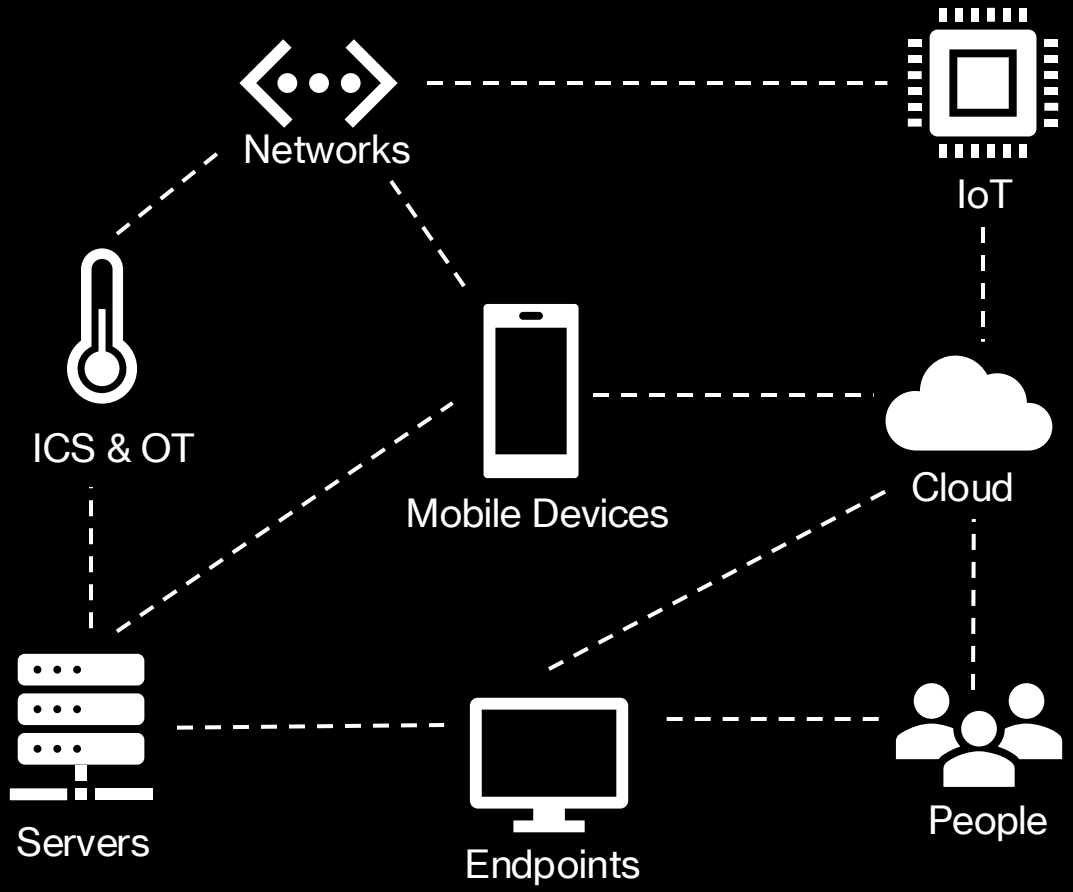
LinkedIn

X

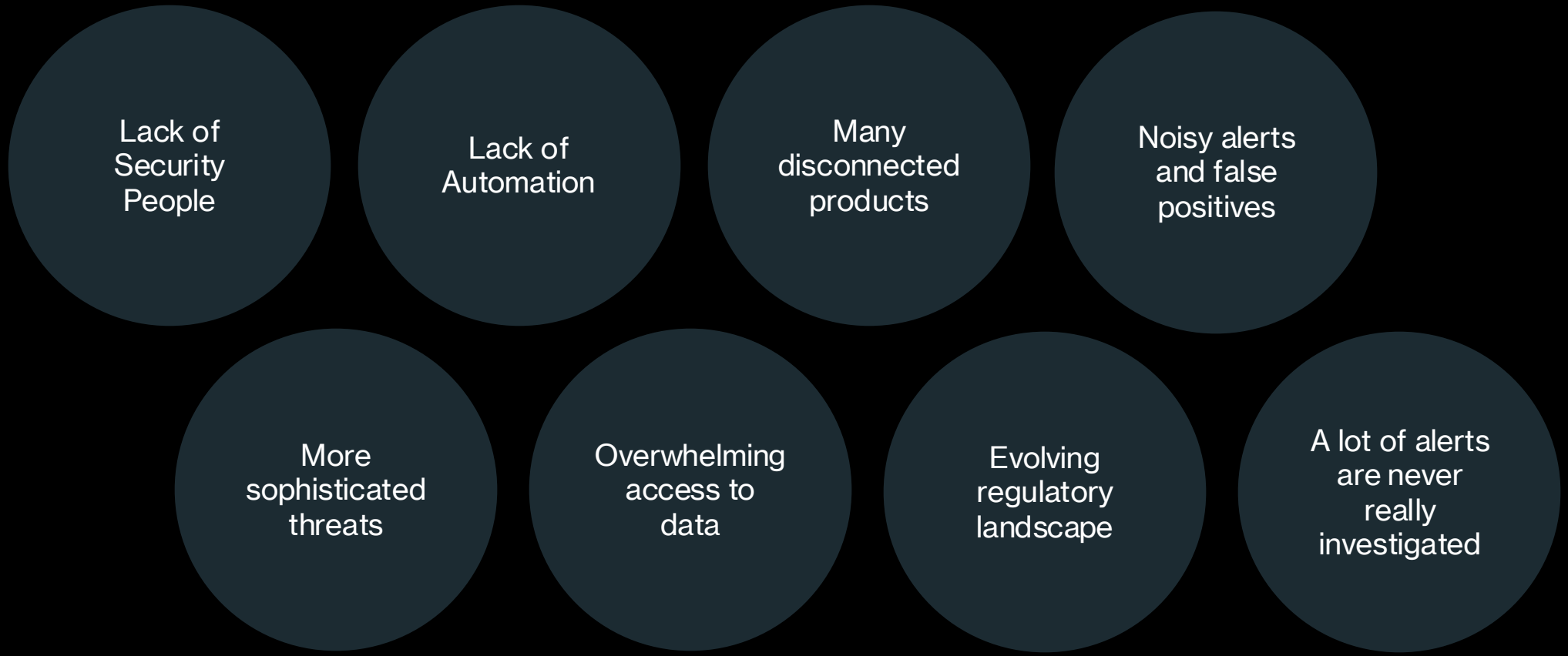
Bluesky

Threads

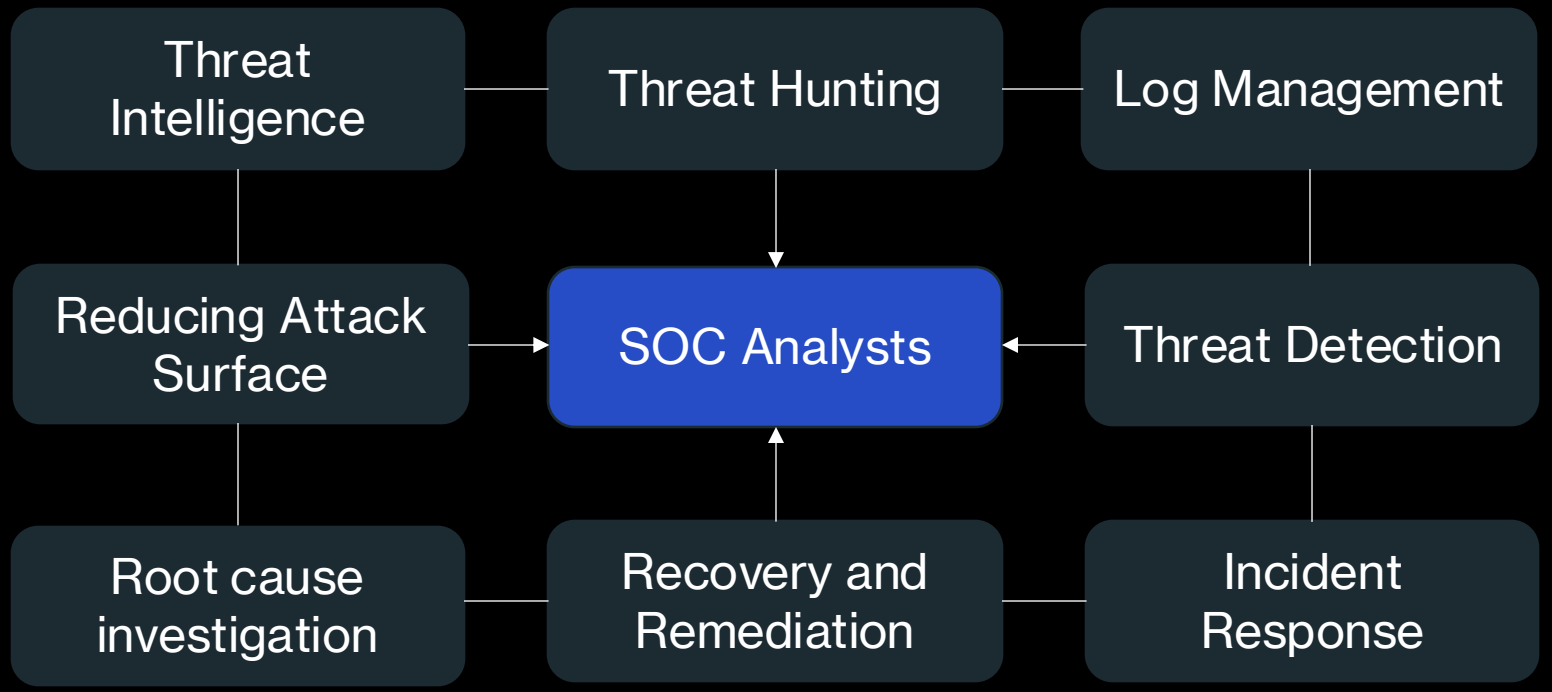
# It is a complex world we live in




# Cyber Security Challenges



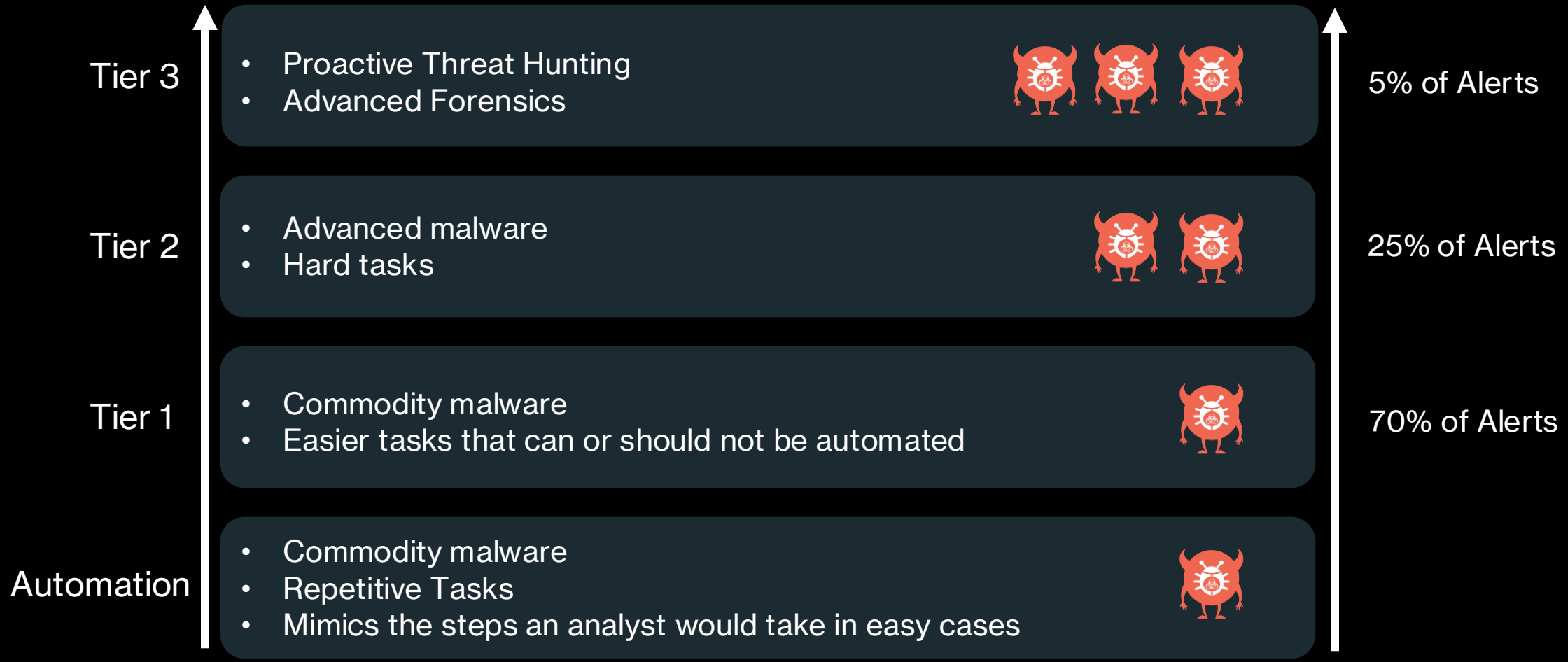
# What is a Security Operations Center (SOC)?






Source: What is a security operations center (SOC)? | Microsoft Security

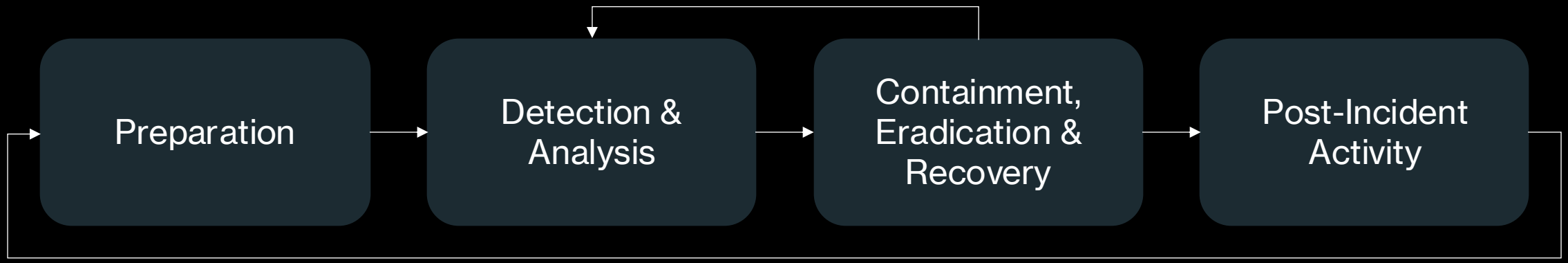
# SOC Model




Christopher Nett

Source: What is a security operations center (SOC)? | Microsoft Security

# Cyber Security Incident Response Process




NIST 800-61: Computer Security Incident Handling Guide



Source: Computer Security Incident Handling Guide (nist.gov)

# EDR, XDR, SIEM & SOAR

| | | |
|---|---|---|
| EDR | • Endpoint Detection and Response<br>• Behavior monitoring for endpoints | Defender for Endpoint |
| XDR | • Extended Detection and Response<br>• Behavior monitoring beyond the endpoint | Defender XDR<br>Defender for Cloud |
| SIEM | • Security Information & Event Management<br>• Centralized collection, correlation and analysis of logs | Sentinel |
| SOAR | • Security Orchestration, Automation & Response<br>• Automates incident response procedures | Sentinel +<br>Azure Logic Apps |

Christopher Nett

Source: What is a security operations center (SOC)? | Microsoft Security

# Blue and Red Teaming

- Security Monitoring
- Incident Response
- Forensics
- Threat Hunting

- Vulnerability Assessments
- Penetration Testing
- Social Engineering
- Simulate adversary TTPs

Christopher Nett

# Purple Teaming

Blue and Red collaborate to improve security posture

Collaborative simulation of adversary TTPs

Drastic upskilling of both teams

# Intelligence, Threat Intelligence and CTI




Source: What is Cyber Threat Intelligence? (cisecurity.org)

# Cyber Threat Intelligence (CTI) 

What is Cyber Threat Intelligence?

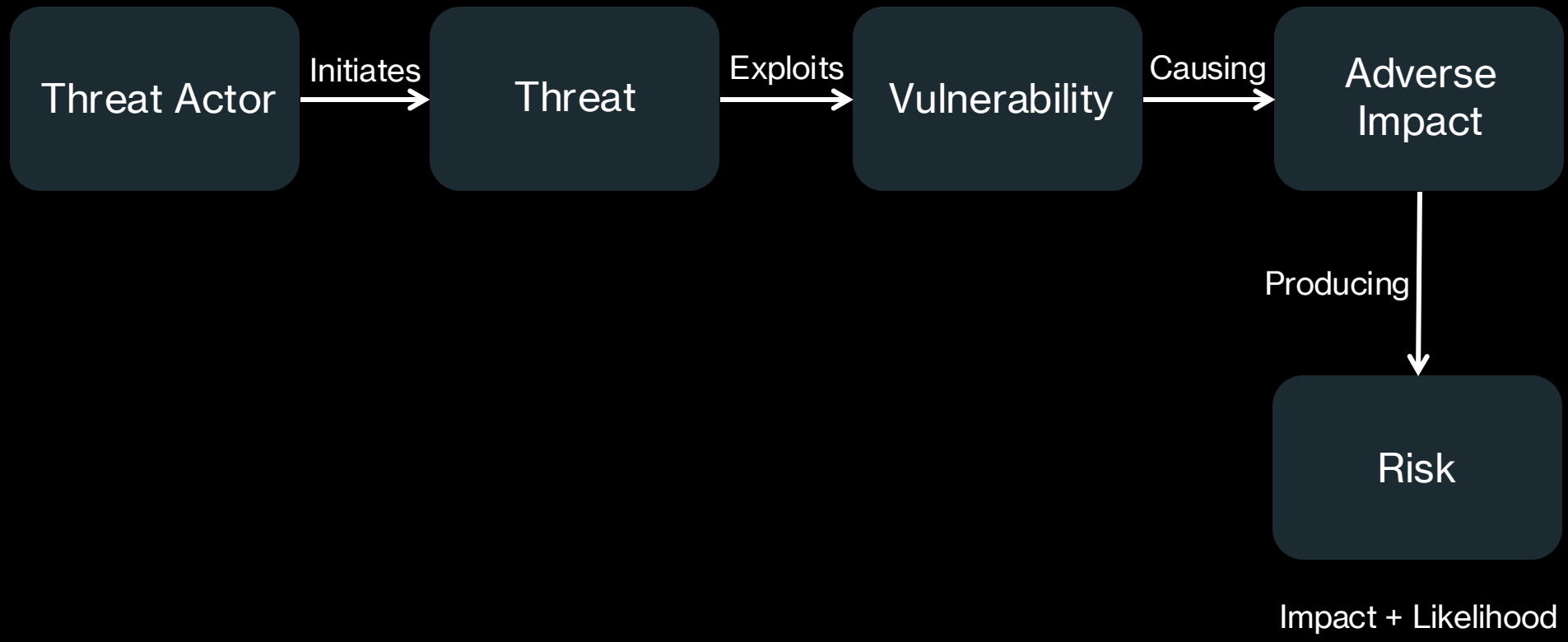
“Cyber Threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect critical assets of the enterprise.”

**Enabling Threat-Informed-Defense**



Source: What is Cyber Threat Intelligence? (cisecurity.org)

# Threat, Vulnerability & Risk






Source: Security and Privacy Controls for Information Systems and Organizations (nist.gov)

# Threat-Informed-Defense

- What is the mission of my organization?
- What threat actors are interested in my organizations industry?
- What are the motivations of those threat actors?
- What TTPs are those threat actors using?
- How can I detect and protect my organization against those TTPs?

# Tactics, Techniques and Procedures

- Tactics: The high-level description of the behavior and strategy of a threat actor.
- Techniques: These are the non-specific guidelines and intermediate methods that describe how a tactic action can be realized.
- Procedures: These refer to the sequence of actions performed using a technique to execute on an attack tactic. The procedure involves detailed descriptions activities.

Reconnaissance

Scanning

Vulnerability Scanning



Source: What Are TTPs? Tactics, Techniques & Procedures Explained | Splunk

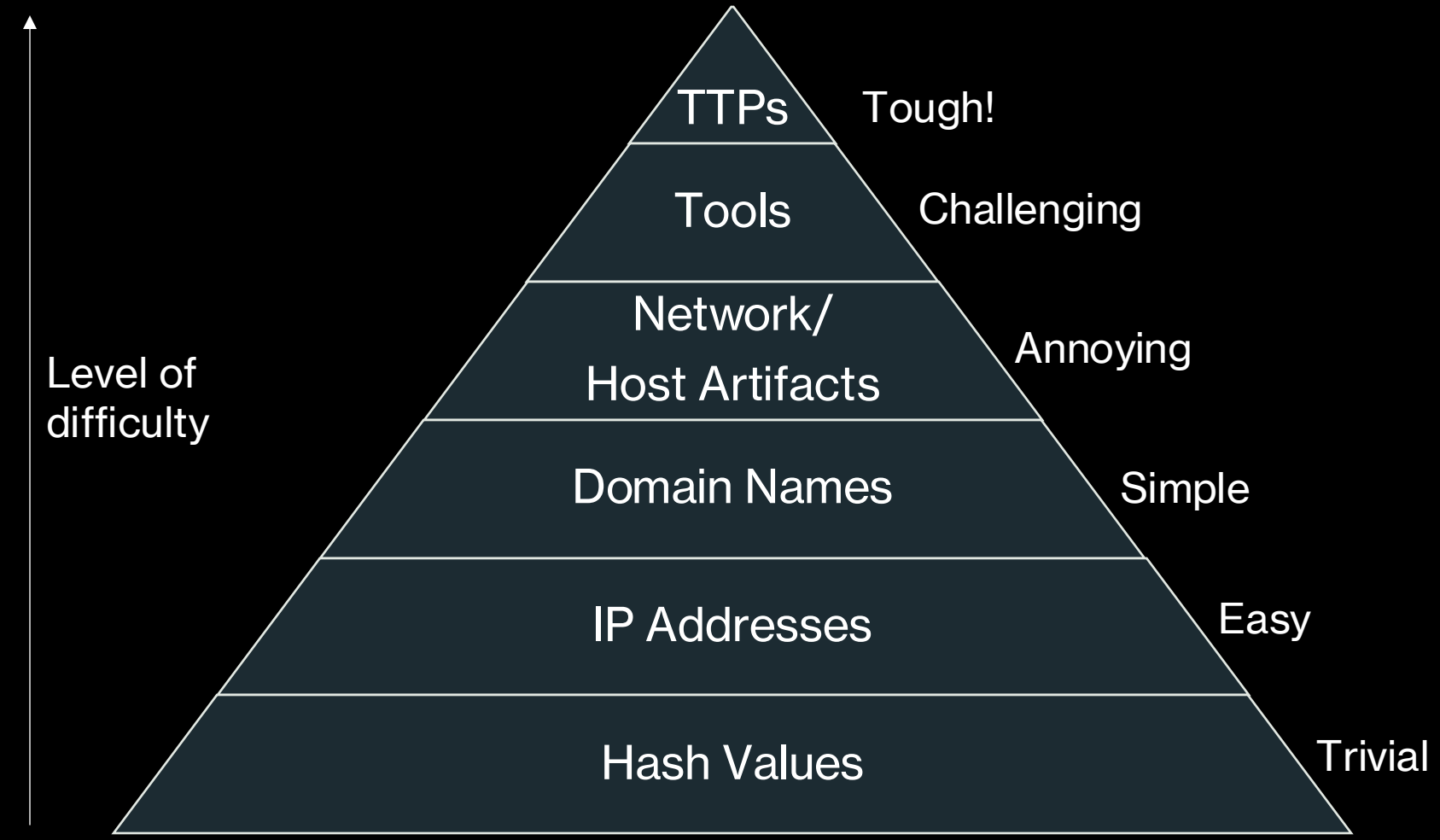
# IOCs and IOAs

- IOC: An Indicator of Compromise (IOC) is evidence on a system that indicates that the security of the network has been breached.
- IOA: Indicators of attack (IOA) focus on detecting the intent of what an attacker is trying to accomplish and its behavior, regardless of the malware or exploit used in an attack.




Source: IOA vs IOC: Understanding the Differences - CrowdStrike

# Pyramid of Pain




Christopher Nett

Source: Enterprise Detection & Response: The Pyramid of Pain (detect-respond.blogspot.com)

# What is Threat Hunting?

Threat Hunting is the practice of proactively searching for cyber threats that are lurking undetected in your environment.

There are two Threat Hunting Models:

1) Intelligence-based Hunting: Leverage IOCs, hash values, IP addresses, domain names or host artifacts
2) Hypothesis-based Hunting: Hunt based on IOAs and TTPs of adversaries



Source: What is threat hunting? | IBM)

# CTI Sources

Enterprise




OSINT


Social Media

# What is a Vulnerability?

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.



Source: vulnerability - Glossary | CSRC (nist.gov)

# Common Vulnerabilities and Exposures (CVE)

- Led by MITRE
- Every newly discovered vulnerability is assigned a CVE ID in the form of CVE-yyyy-xxxx
- Includes a vulnerability description, data sources as well as the official vendor announcement

# Common Vulnerabilities and Exposures (CVE)

- CVE-2009-2935
- Google V8, as used in Google Chrome before 2.0.172.43, allows remote attackers to bypass intended restrictions on reading memory, and possibly obtain sensitive information or execute arbitrary code in the Chrome sandbox, via crafted JavaScript.
- CVSS Version 2.0 Score: 10.0



https://nvd.nist.gov/vuln/detail/CVE-2009-2935

# Common Vulnerability Scoring System (CVSS)

- Evaluates the severity of the vulnerability from 1-10
- Considers the CIA triad but also other factors

CVSSv2

| CVSS Score | Severity |
|---|---|
| 7.0 – 10.0 | High |
| 4.0 – 6.9 | Medium |
| 0.0 – 3.9 | Low |

CVSSv3

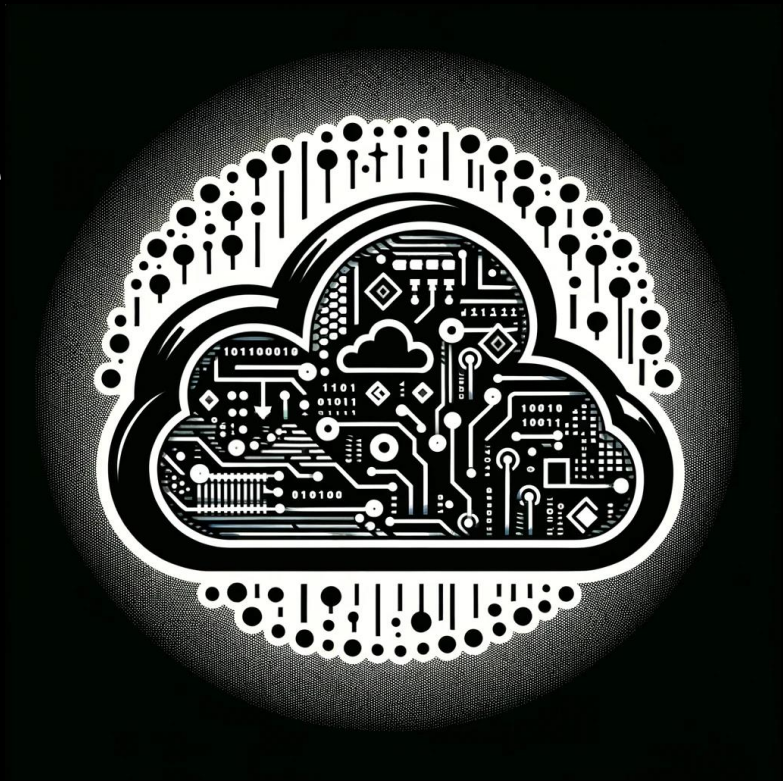
| CVSS Score | Severity |
|---|---|
| 9.0 – 10.0 | Critical |
| 7.0 – 8.9 | High |
| 4.0 – 6.9 | Medium |
| 0.1 – 3.9 | Low |
| 0 | None |



Source: https://nvd.nist.gov/vuln-metrics/cvss

# Cloud Computing Properties

- On-demand self service
- Broad network access
- Resource pooling
- Rapid elastic
- Measured service





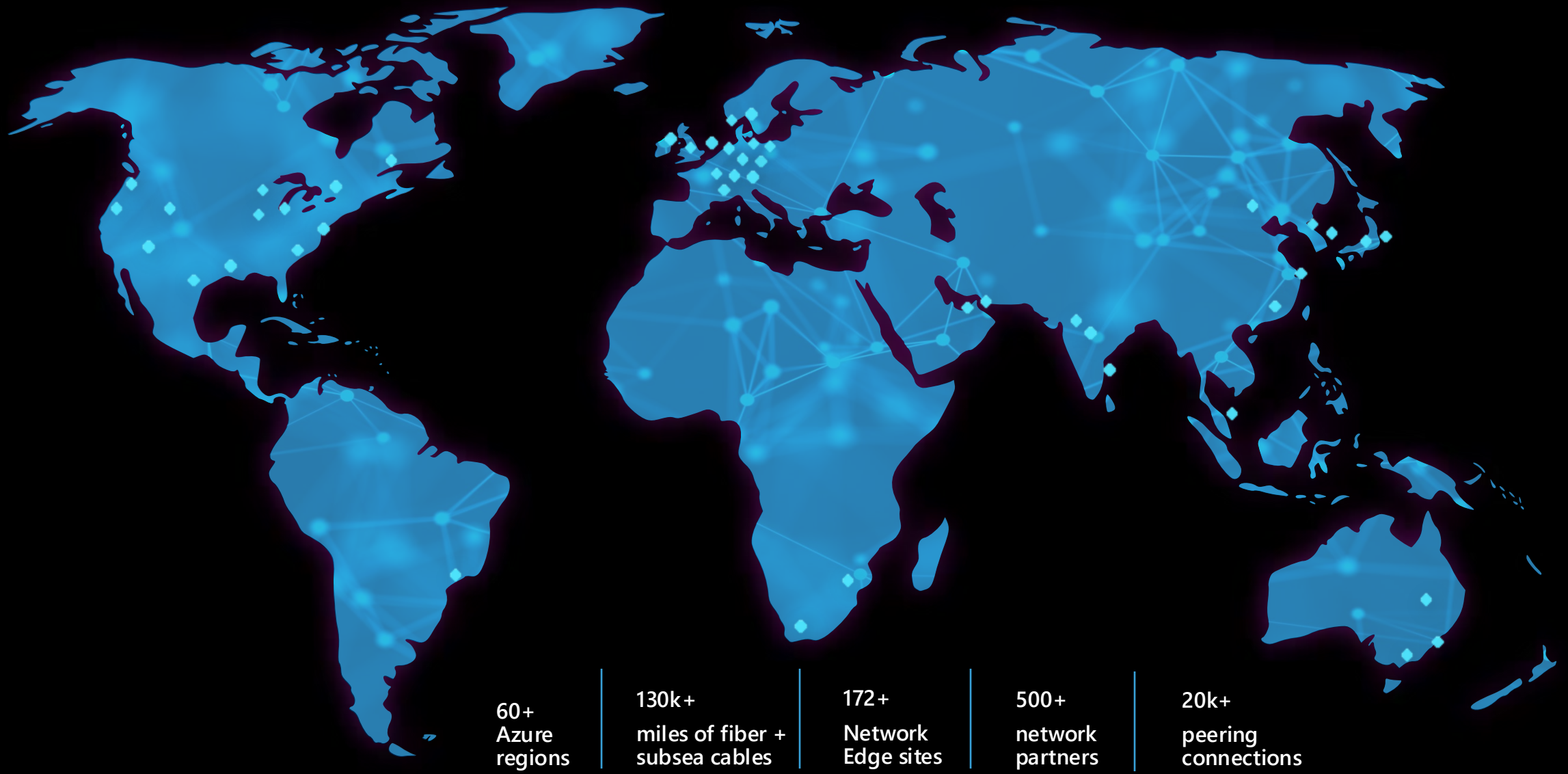
Source: nistspecialpublication800-145.pdf

# Public, Private, Multi & Hybrid Cloud


Christopher Nett

Source: nistspecialpublication800-145.pdf

# Azure Global Backbone



60+
Azure regions

130k+
miles of fiber + subsea cables

172+
Network Edge sites

500+
network partners

20k+
peering connections

Christopher Nett

Source: Global Network – Backbone Networking Infrastructure | Microsoft Azure

# Shared Responsibility in Azure

| Responsibility | On-prem | IaaS | PaaS | SaaS |
|---|---|---|---|---|
| Information and Data |  |  |  |  |
| Devices (Mobile and PCs) |  |  |  |  |
| Accounts and Identities |  |  |  |  |
| Identity and Directory Infrastructure |  |  |  |  |
| Applications |  |  |  |  |
| Network Controls |  |  |  |  |
| Operating System |  |  |  |  |
| Physical Hosts |  |  |  |  |
| Physical Network |  |  |  |  |
| Physical Datacenter |  |  |  |  |

Christopher Nett

Source: Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn

# Azure Subscription Types

## Free

- Free credits for 30 days
- Some services are free for 12 months

## Student

- Free credits for 12 months
- No credit card required

## Pay As You Go

- Pay for what you use
- Credit card required

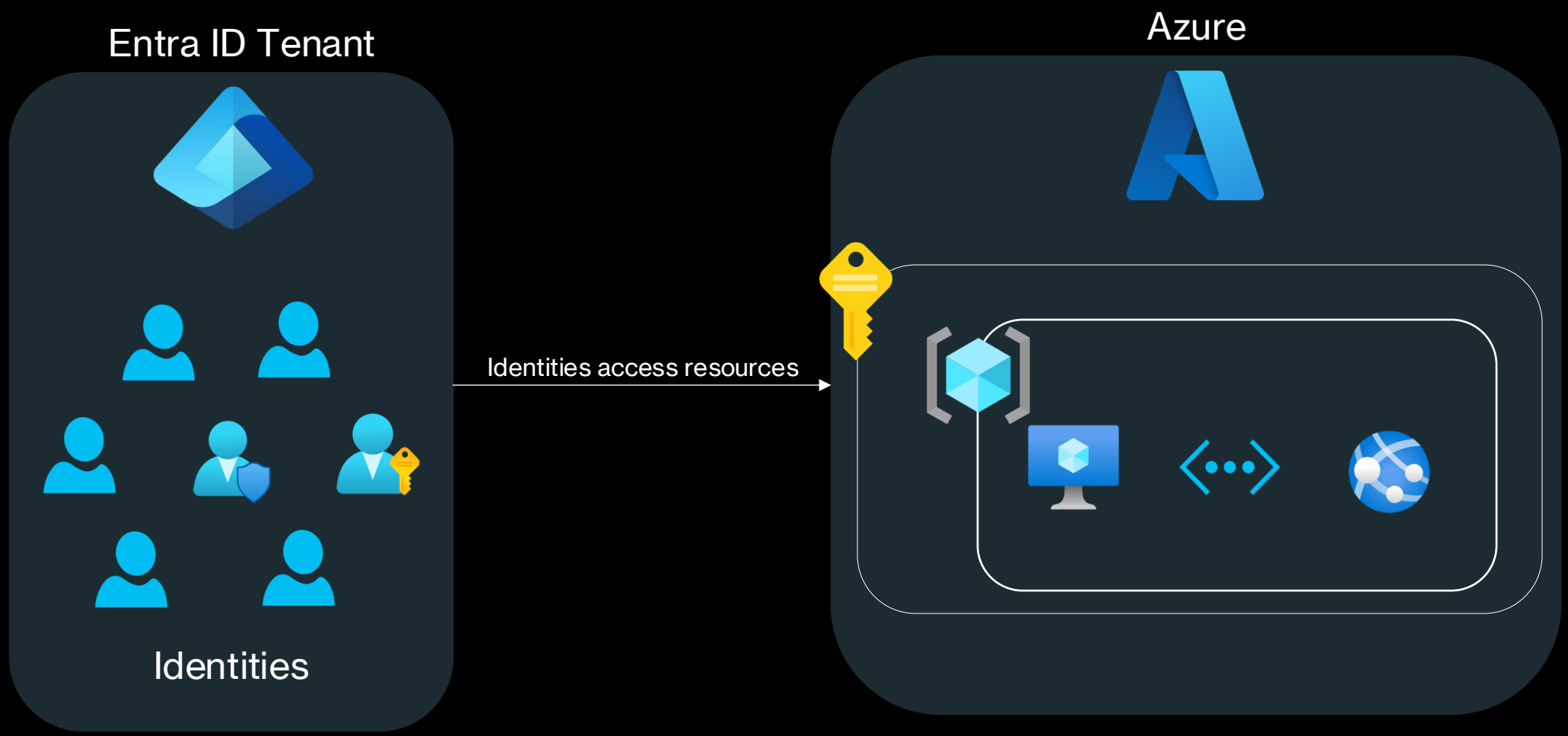
## Enterprise Agreement

- One consumption agreement for all Azure services
- Various different billing models



Source: Create Your Azure Free Account Today | Microsoft Azure

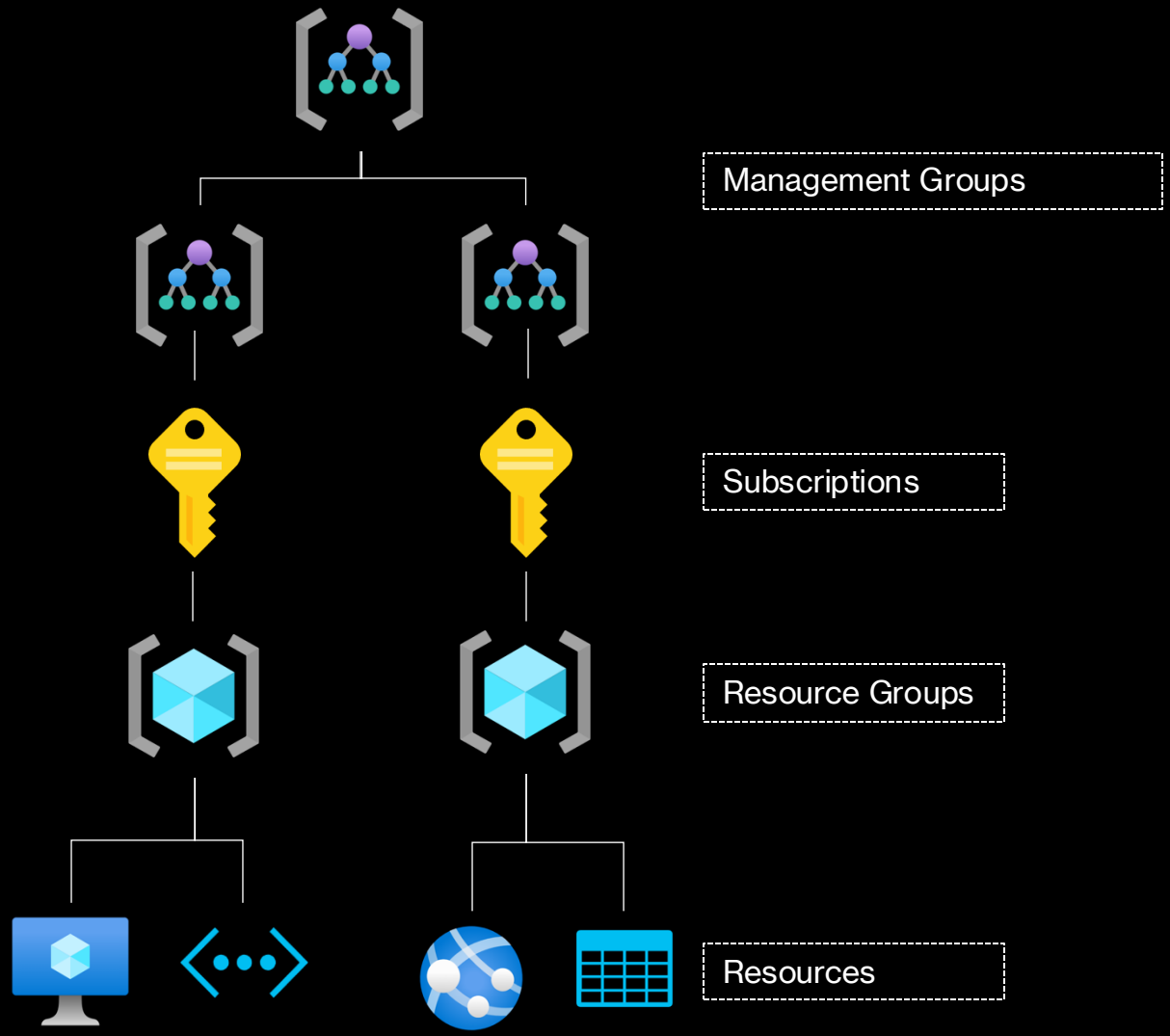
# Entra ID Tenants and Azure Subscriptions




Christopher Nett

Source: Microsoft Entra ID documentation - Microsoft Entra ID | Microsoft Learn

# Azure Resource Hierarchy




Christopher Nett

# What is Zero Trust?

- Zero Trust is a security strategy
- It is not a product or a service

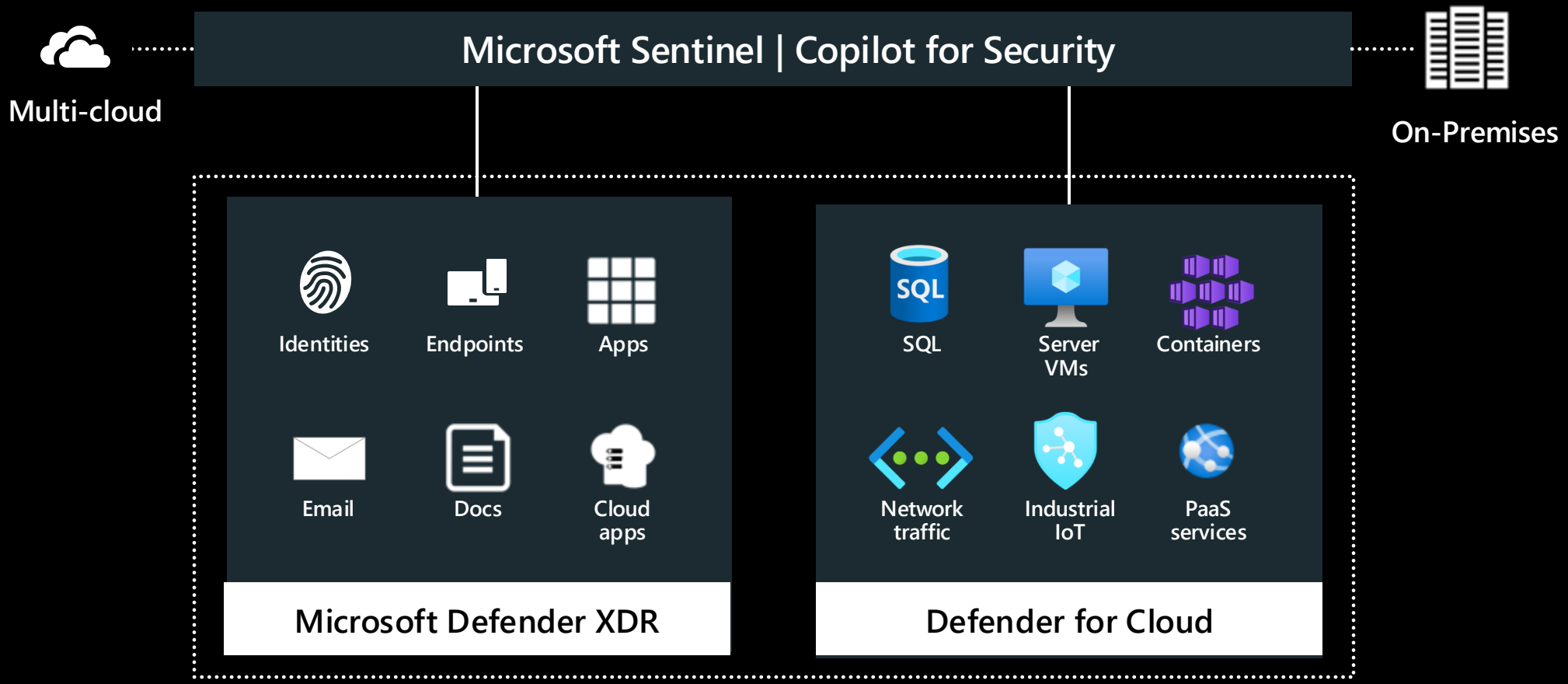
There are 3 core principles of Zero Trust:

1) Verify explicitly
2) Use least-privilege access
3) Assume breach




Source: Zero Trust Model - Modern Security Architecture | Microsoft Security

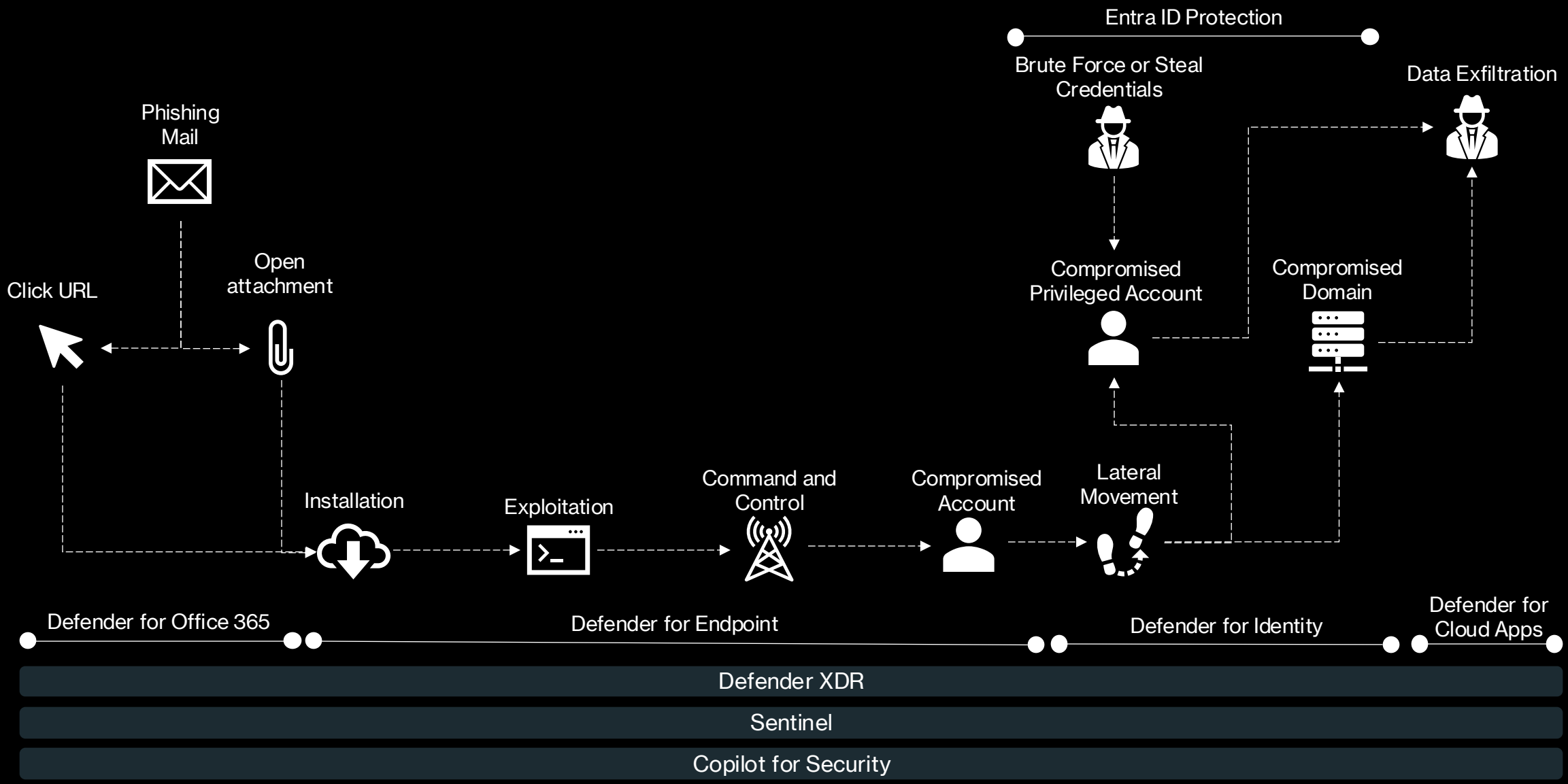
# The Microsoft Security Cosmos






Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn

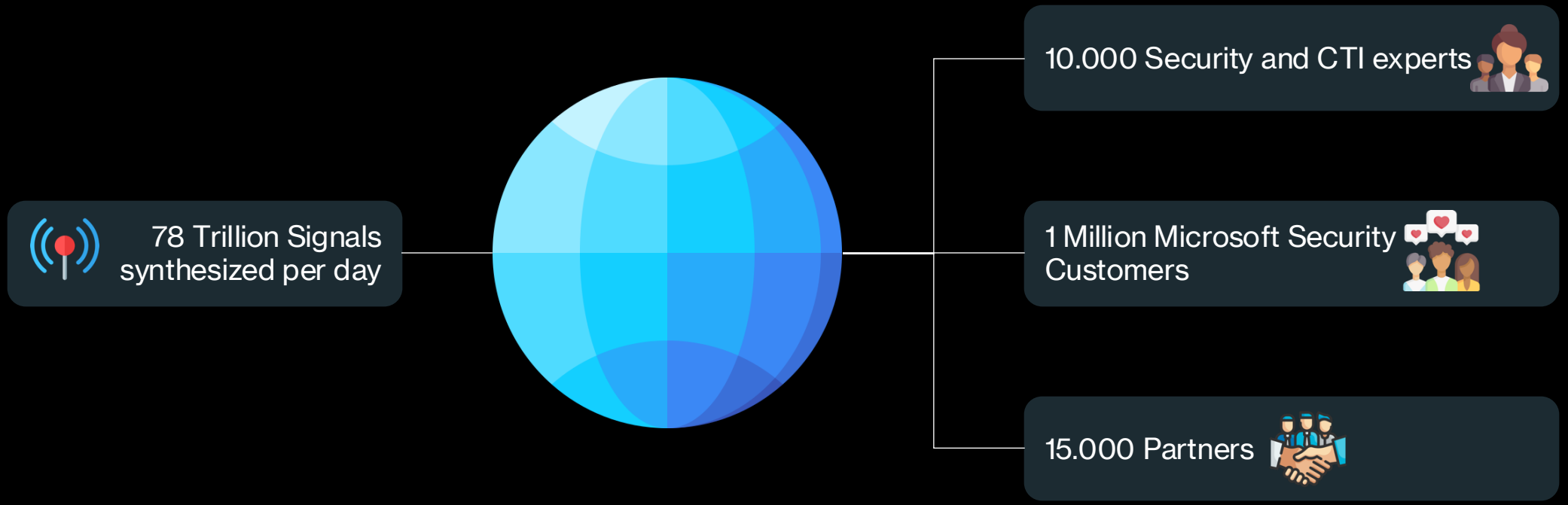
# Defending Across Attack Chains




Christopher Nett

Source: Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn

# Microsoft Cyber Threat Intelligence




Christopher Nett

Source: https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/

# Microsoft Entra

| Establish zero trust access controls | Secure access for employees | Secure access for customers & partners | Secure access in any cloud |
| --- | --- | --- | --- |
| Entra ID | Entra Private Access | Entra External ID | Entra Permissions Management |
| | Entra Internet Access | | Entra Workload ID |
| | Entra ID Governance | | |
| | Entra Verified ID | | |



Source: https://learn.microsoft.com/en-us/entra/fundamentals/what-is-entra

# Entra Licensing Overview

| Product | Free | Entra ID P1 | Entra ID P2 | Entra Suite |
|---|---|---|---|---|
| Entra ID | (X) | X | X | X |
| Entra ID Protection | | | X | X |
| Entra ID Governance | | (X) | (X) | X |
| Entra Verified ID | | (X) | (X) | X |
| Entra Internet Access | | | | X |
| Entra Private Access | | | | X |



Source: https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing#xed91694e453d4abe9215d635dae003fc

# Microsoft Entra ID Governance

| | |
|---|---|
| Market Challenge | Managing user identities, permissions and entitlements across various IT environments |
| Purpose | Ensuring that the right people have the right access to the right resources at the right time |
| Features | Govern the identity lifecycle |
| | Govern the access lifecycle |
| | Secure privileged access for administration |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview

# Microsoft Entra Verified ID

| | |
|---|---|
| Market Challenge | People don’t own their identity data and individuals lack visibility on how their data is used and how to get it back |
| Purpose | Confidently issue and verify workplace credentials, citizenship, education status, certifications and other identity attributes in a global ecosystem designed for more secure interaction between people & organizations |
| Features | Decentralized Identity |
| | Verified Credentials |
| | Interoperability and Standards Compliance |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/verified-id/decentralized-identifier-overview

# Microsoft Entra External ID

| | |
|---|---|
| Market Challenge | Rapid increase of external identities that need to collaborate with customers, partners and employees |
| Purpose | A complete customer identity and access management (CIAM) solution that allows you to personalize and secure access to any application for customers and partners |
| Features | Flexible user onboarding and authentication |
| | B2B and B2C identity management |
| | Unified and scalable identity management |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/external-id/external-identities-overview

# Microsoft Entra Permissions Management (EPM)

| | |
|---|---|
| Market Challenge | There are over 40.000 permissions that can be granted across Azure, AWS and GCP. Identities are only using 1% of permissions granted. |
| Purpose | A cloud infrastructure entitlement management (CIEM) product that provides visibility and control over permissions for any identity and any resource in Azure, AWS and GCP. |
| Features | Visibility of permissions across Azure, AWS and CGP. |
| | Permission control and enforcement |
| | Automated permissions monitoring |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/permissions-management/overview

# Microsoft Entra Workload ID

| | |
|---|---|
| Market Challenge | The number of workload identities accessing critical infrastructure are increasing, now outnumbering human identities 10:1. |
| Purpose | A comprehensive set of features that helps secure adaptive access, detect and respond to compromised workload identities and simplify their lifecycle management |
| Features | Identity management for workloads |
| | Certificates and keyless authentication |
| | Automated lifecycle management |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/workload-id/workload-identities-overview

# Microsoft Entra Internet Access

| | |
|---|---|
| Market Challenge | Control web traffic with threat protection, content filtering and policy enforcement to ensure sage and productive internet usage for employees |
| Purpose | Secure access to all internet, SaaS and M365 apps and resources while protecting your organization against threats with an identity-centric secure web gateway |
| Features | Secure Web Gateway |
| | Zero-Trust based access |
| | Visibility and Analytics |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/global-secure-access/concept-internet-access

# Microsoft Entra Private Access

| | |
|---|---|
| Market Challenge | Simplify organizations network architecture to enhance security and reduce operational complexities by converging multiple security and networking solutions into a unified cloud-based service |
| Purpose | Remove the risk and operational complexity of legacy VPNs while boosting user productivity. Quickly and securely connect remote users from any device and any network to private apps: on-premises and across clouds |
| Features | Zero-Trust network access (ZTNA) |
| | Seamless access to private resources |
| | Real-time access monitoring and policy enforcement |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/global-secure-access/concept-private-access

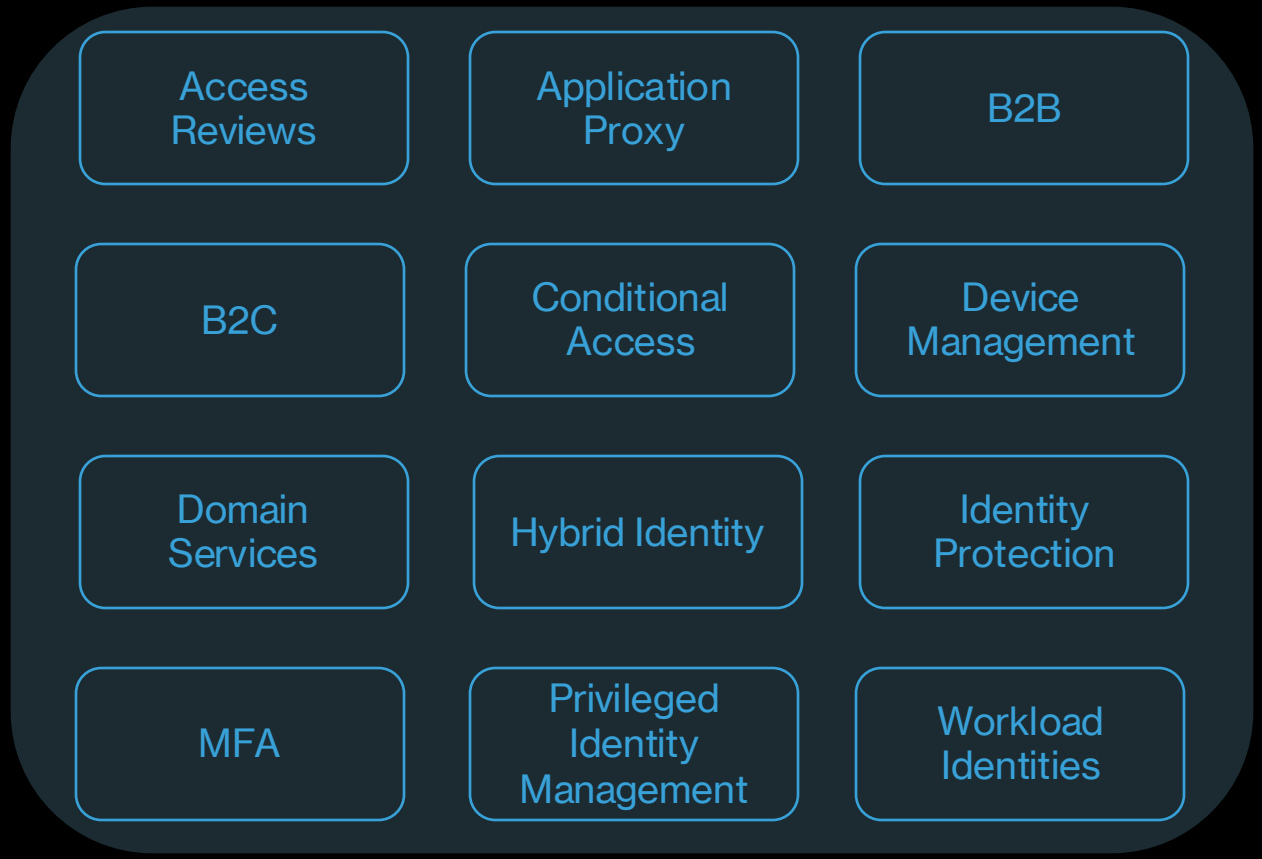
# Entra ID Overview

- Microsoft Entra ID is a cloud-based identity and access management service and provider that your employees can use to access external resources.
- Example resources include Microsoft 365, the Azure portal, and thousands of other SaaS applications and cloud services.
- Microsoft Entra ID also helps them access internal resources like apps on your corporate intranet, and any cloud apps developed for your own organization.



Source: https://learn.microsoft.com/en-us/entra/fundamentals/whatis

# Microsoft Entra ID






Source: https://learn.microsoft.com/en-us/entra/fundamentals/what-is-entra

# Entra ID Licensing

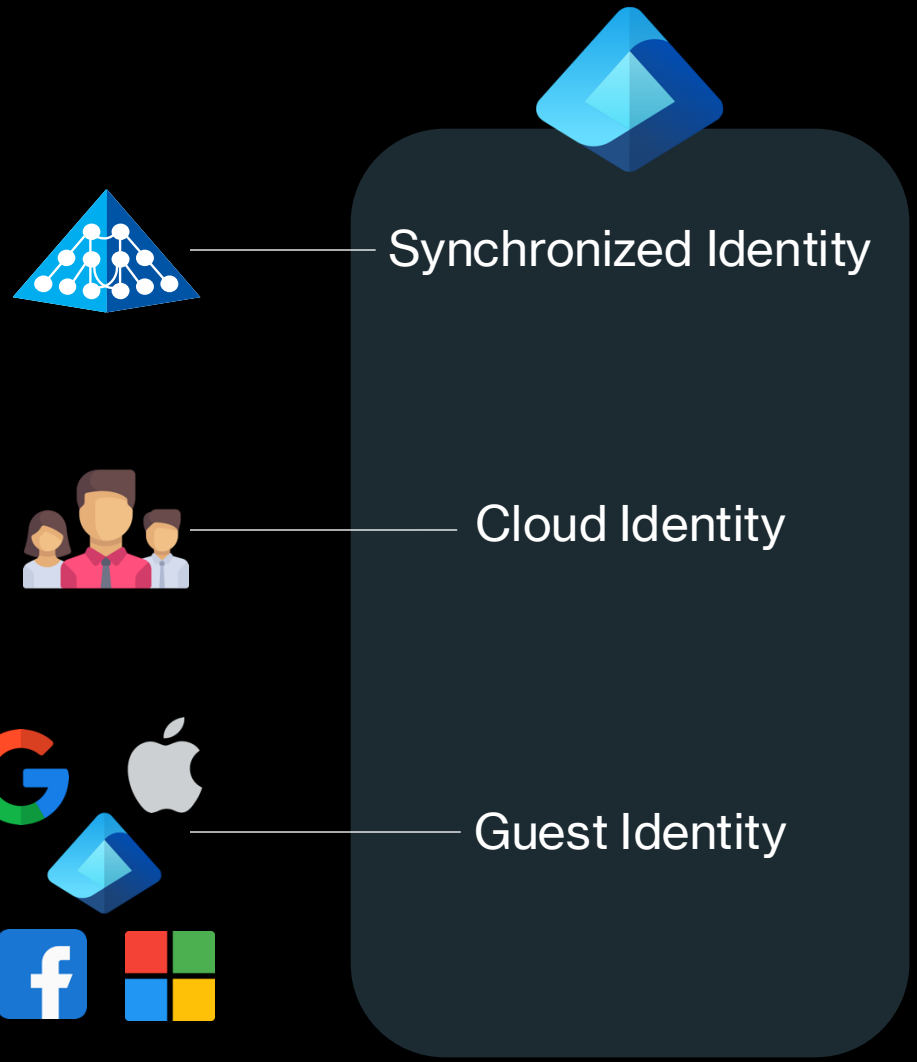
| Free | Entra ID P1 | Entra ID P2 | Entra ID Governance |
|---|---|---|---|
| Cloud authentication | Conditional Access | Identity Protection | Identity governance dashboard |
| SSO | Dynamic Group Membership | PIM | Lifecycle workflows |
| B2B | App Proxy | | |
| Passwordless | | | |



Source: Microsoft Entra Plans and Pricing | Microsoft Security

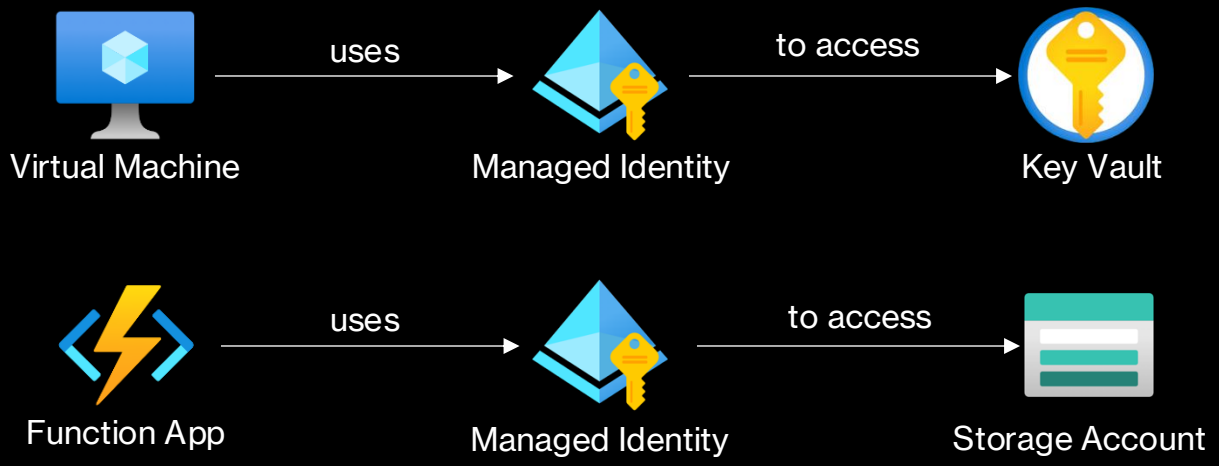
# Entra ID User Identities

- Allows humans to access enterprise resources
- Can be created in the cloud or on-premises
- Can be synchronized
- Supports username and password and MFA
- Stores properties such as:
  - Name = John Robbins
  - Office = Seattle



# Managed Identities (MI)

- Provides an identity to an Azure resource
- You don’t need to manage credentials as AuthN is managed by Azure
- You can use managed identities to authenticate to any Azure resource
- There are two types:
  - System assigned managed identity
  - User assigned managed identity






Source: Managed identities for Azure resources - Microsoft Entra ID | Microsoft Learn

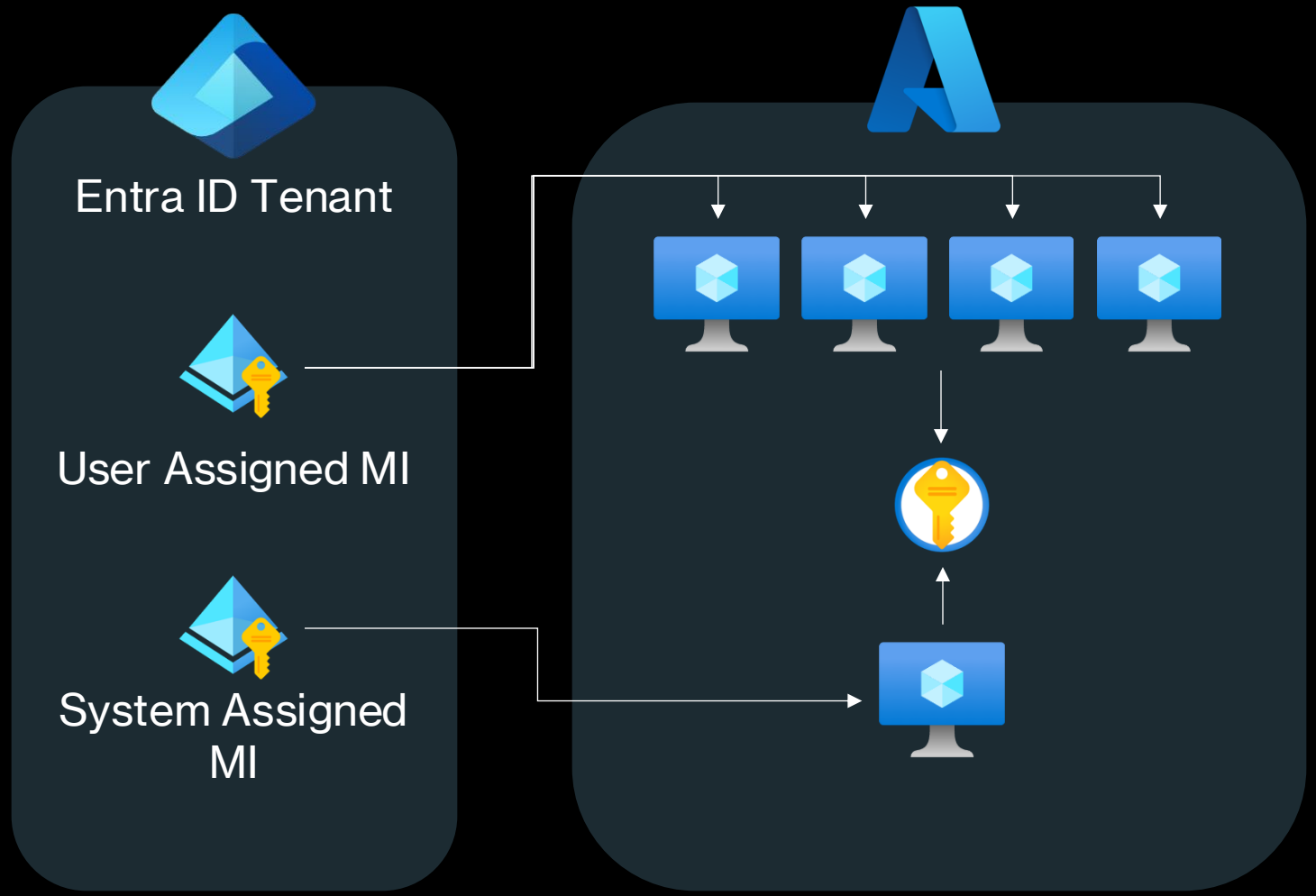
# System Assigned vs. User Assigned MI

| Property | System-assigned MI | User-assigned MI |
|---|---|---|
| Creation | Created with an Azure resource | Created as a stand-alone Azure resource |
| Lifecycle | Shared life cycle with the Azure resource | Independent life cycle |
| Deletion | When the parent resource is deleted, the managed identity is deleted as well | Must be explicitly deleted |
| Sharing across Azure resources | It can only be associated with a single Azure resource | The same user-assigned MI can be associated with more than one Azure resource |



Source: Managed identities for Azure resources - Microsoft Entra ID | Microsoft Learn

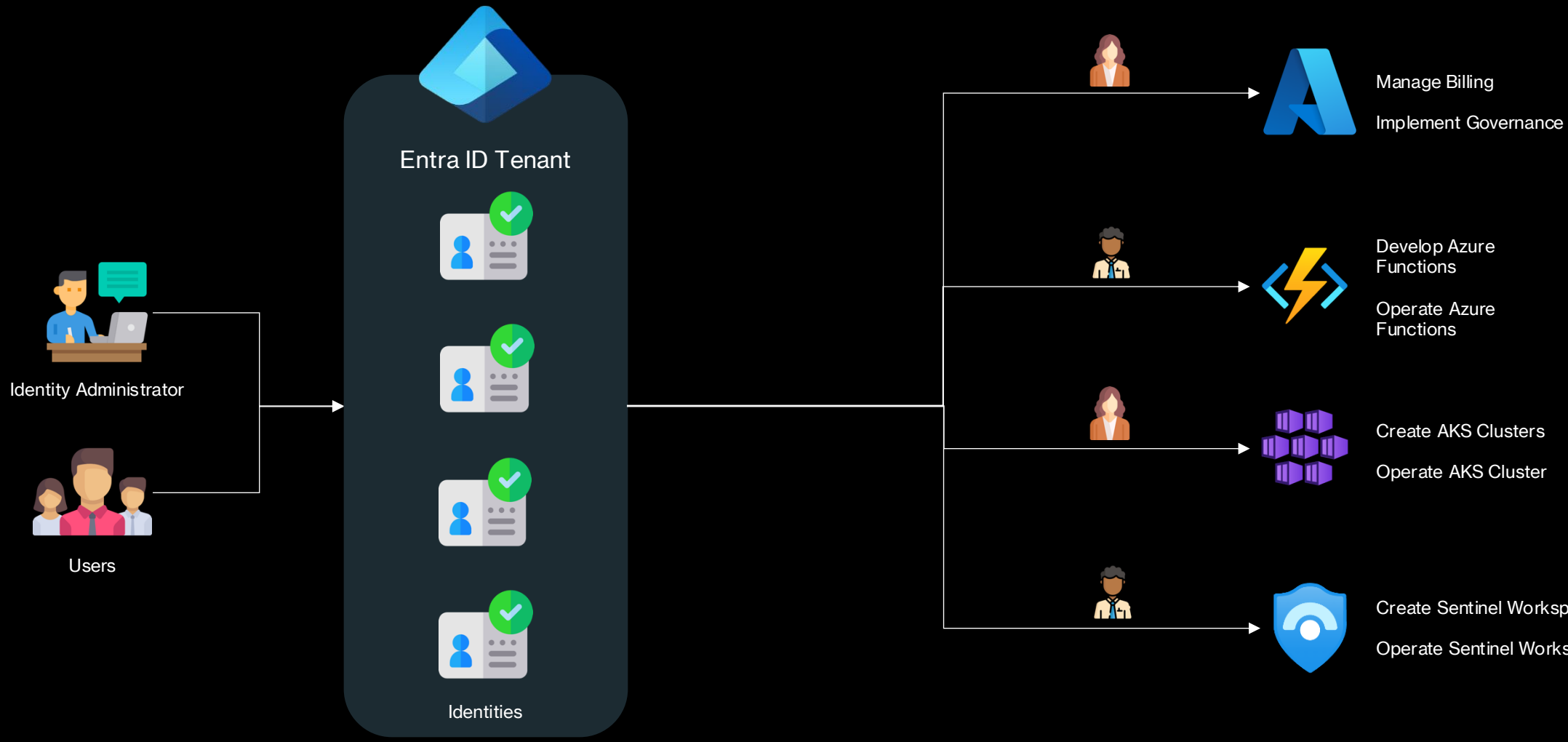
# System Assigned vs. User Assigned MI






Source: Managed identities for Azure resources - Microsoft Entra ID | Microsoft Learn

# Entra ID Groups – Why do we need groups?




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/fundamentals/concept-learn-about-groups

# Entra ID Groups - Features

Administration

Entra ID groups provide centralized management for organizing and controlling user access to resources and roles within an organization.

Security

Entra ID groups enhance security by enabling role-based access control (RBAC) and applying policies to group members for secure resource access.

Automation

Entra ID groups support automation by allowing dynamic group memberships based on predefined rules, simplifying user and access management.

Self-Service

Entra ID groups offer self-service features, allowing users to request group membership or manage their own group access without administrator intervention.

Christopher Nett

Source:

# Entra ID Groups – Group Types

## Security Groups 

- Used to manage user and computer access to shared resources.
- For example, you can create a security group so that all group members have the same set of security permissions.
- Members of a security group can include users, devices, service principals, and other groups (also known as nested groups), which define access policy and permissions.
- Owners of a security group can include users and service principals.

## Microsoft 365 Groups 

- Provides collaboration opportunities by giving group members access to a shared mailbox, calendar, files, SharePoint sites, and more.
- This option also lets you give people outside of your organization access to the group.
- Members of a Microsoft 365 group can only include users.
- Owners of a Microsoft 365 group can include users and service principals.



Source: https://learn.microsoft.com/en-us/entra/fundamentals/concept-learn-about-groups#group-types

# Entra ID Groups – Membership Types

## Assigned

- Assigned: Lets you add specific users as members of a group and have unique permissions.

## Dynamic

- Lets you use dynamic membership rules to automatically add and remove members.
- If a member's attributes change, the system looks at your dynamic group rules for the directory to see whether the member meets the rule requirements (is added), or no longer meets the rules requirements (is removed).

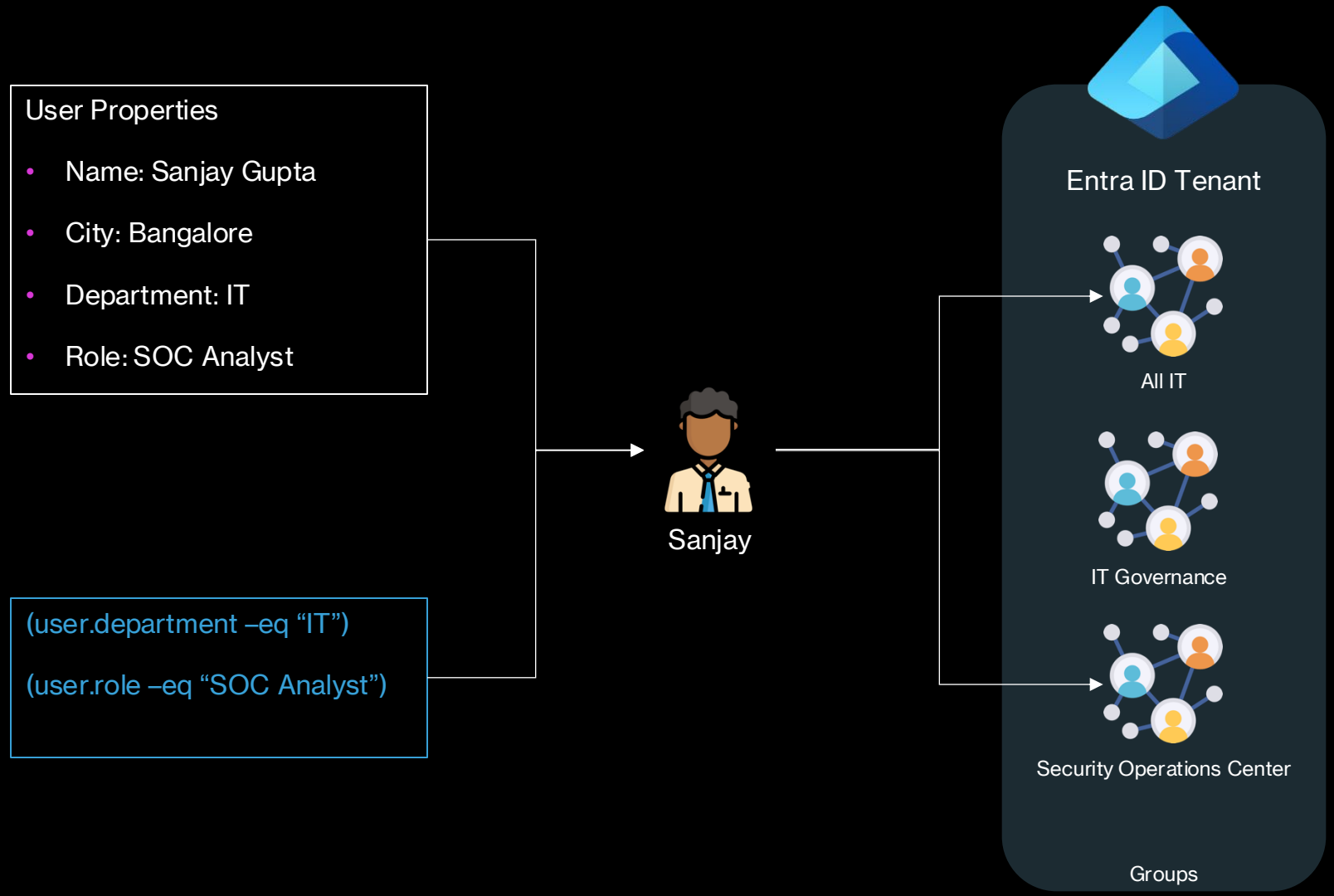
## Dynamic Device

- Lets you use dynamic group rules to automatically add and remove devices.
- If a device's attributes change, the system looks at your dynamic group rules for the directory to see whether the device meets the rule requirements (is added), or no longer meets the rules requirements (is removed).



Source: https://learn.microsoft.com/en-us/entra/fundamentals/concept-learn-about-groups#group-types

# Entra ID Dynamic Groups




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/fundamentals/concept-learn-about-groups#membership-types

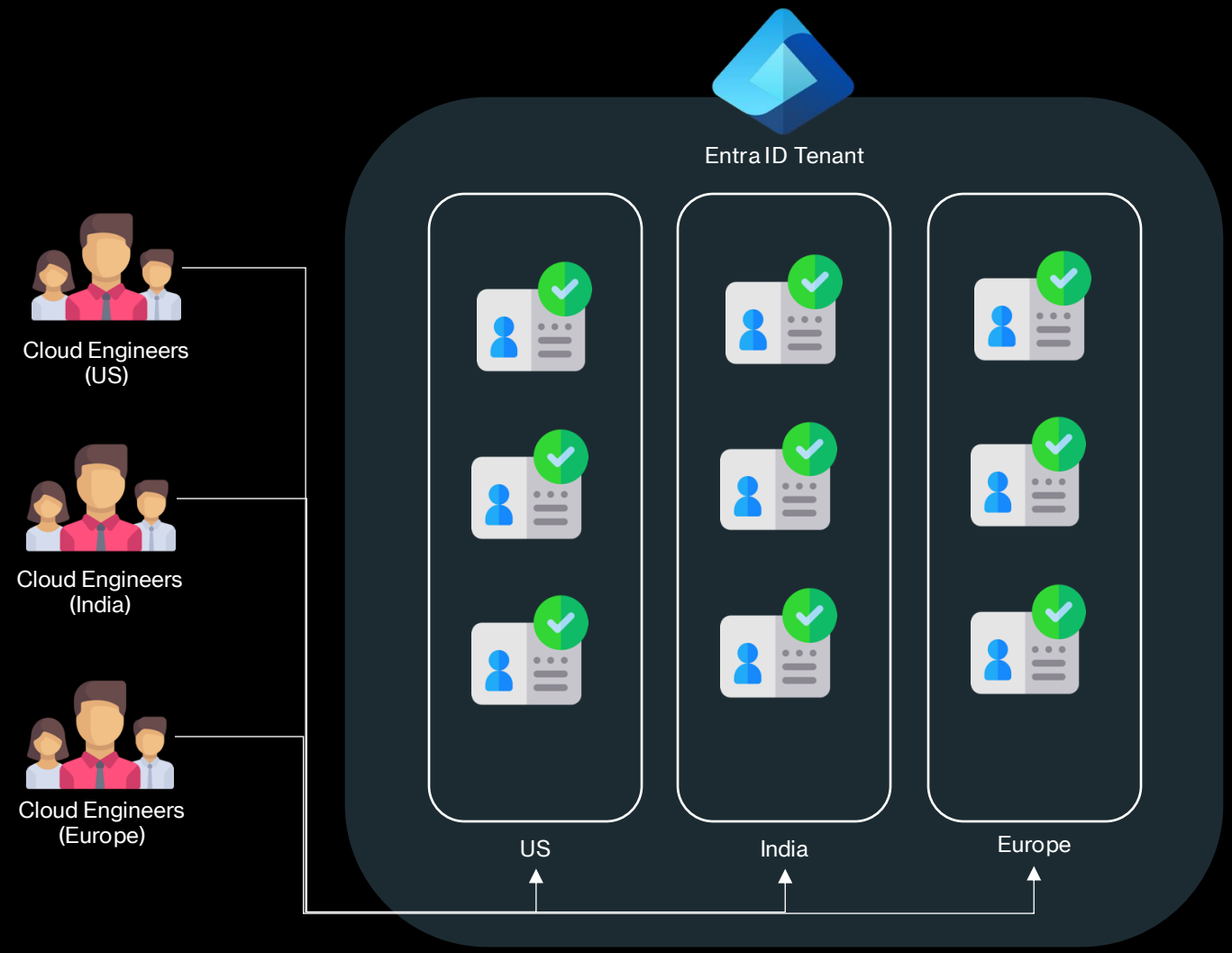
# Entra ID Administrative Units

- Administrative units restrict permissions in a role to any portion of your organization that you define.
- You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.
- Note that if you assign a role to a user that is not a member of an administrative unit, the scope of the role is the entire tenant.
- Users can be members of multiple administrative units. For example, you might add users to administrative units by geography and division; Megan Bowen might be in the "Seattle" and "Marketing" administrative units.



Source: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units

# Entra ID Administrative Units (AUs)



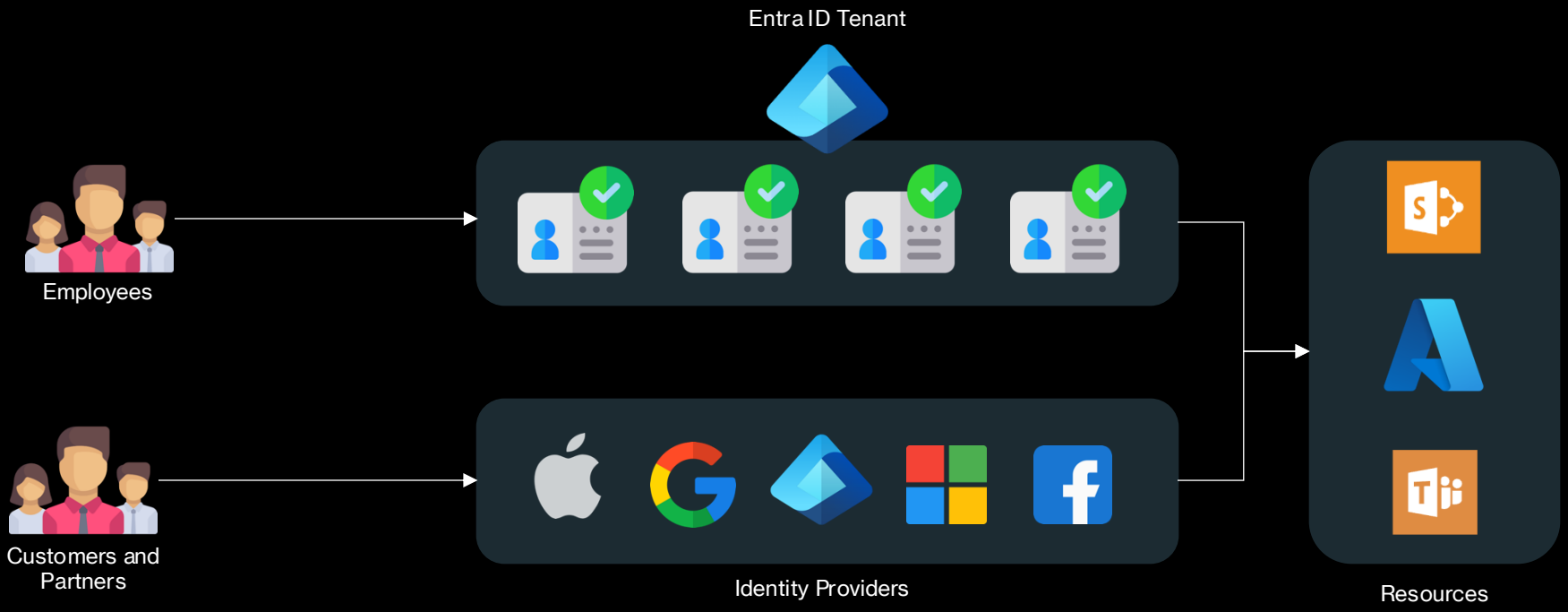

## Properties

- Simplifies the assignment of Entra ID permissions to objects within Entra ID itself
- Allows Entra ID objects to exist in multiple Aus simultaneously
- As with groups, membership can be assigned or dynamic
- Can include users, devices and security groups
- Require at least P1 licenses
- No nesting of AUs within Aus
- Permissions do not apply to members of the security groups



Source: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units

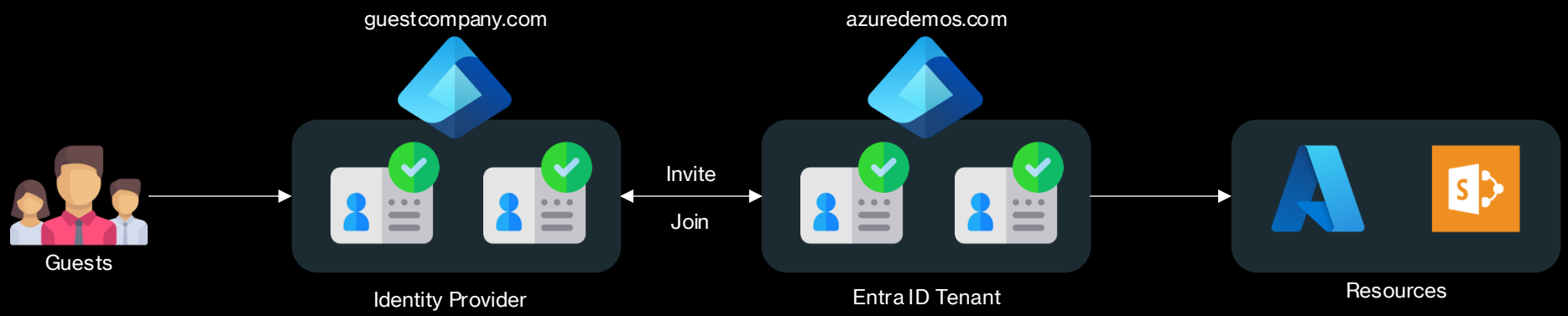
# Entra ID External Identities






Source: https://learn.microsoft.com/en-us/entra/external-id/external-identities-overview

# Entra ID External Identities – B2B Collaboration

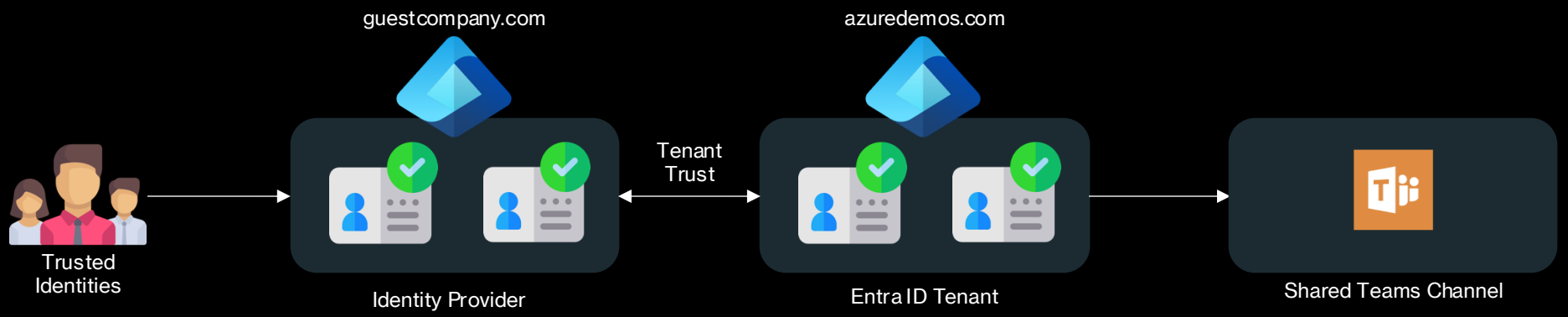



- External collaboration settings define the actual access and restrictions for invites
- azuredemos.com → Your Entra ID tenant where resources shall be shared with guests
- guestcompany.com → Guest identities from other IDPs



Source: https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b

# Entra ID External Identities – B2B Direct Connect

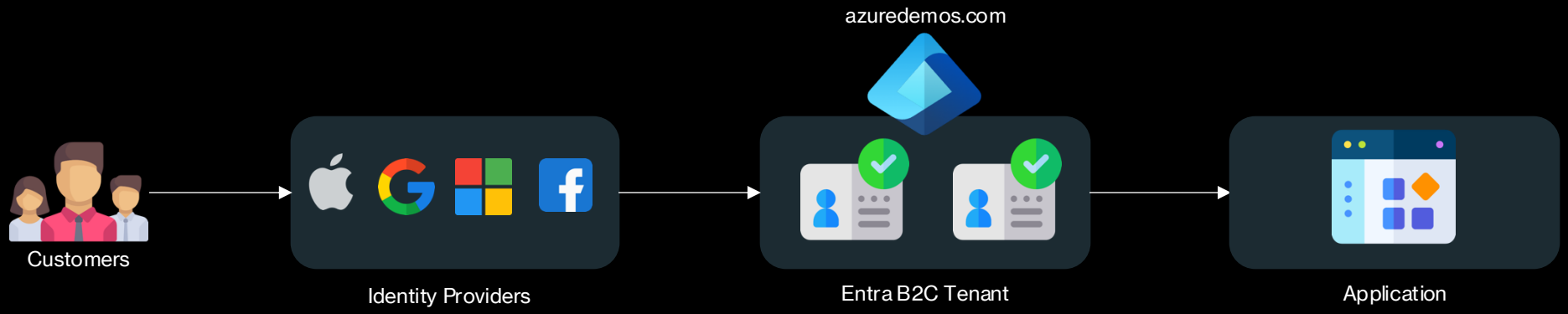



- Mutual trust between Entra tenants
- No guest identities required
- Cross-tenant settings define the access and trust level between organizations



Source: https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b

# Entra ID External Identities – B2C



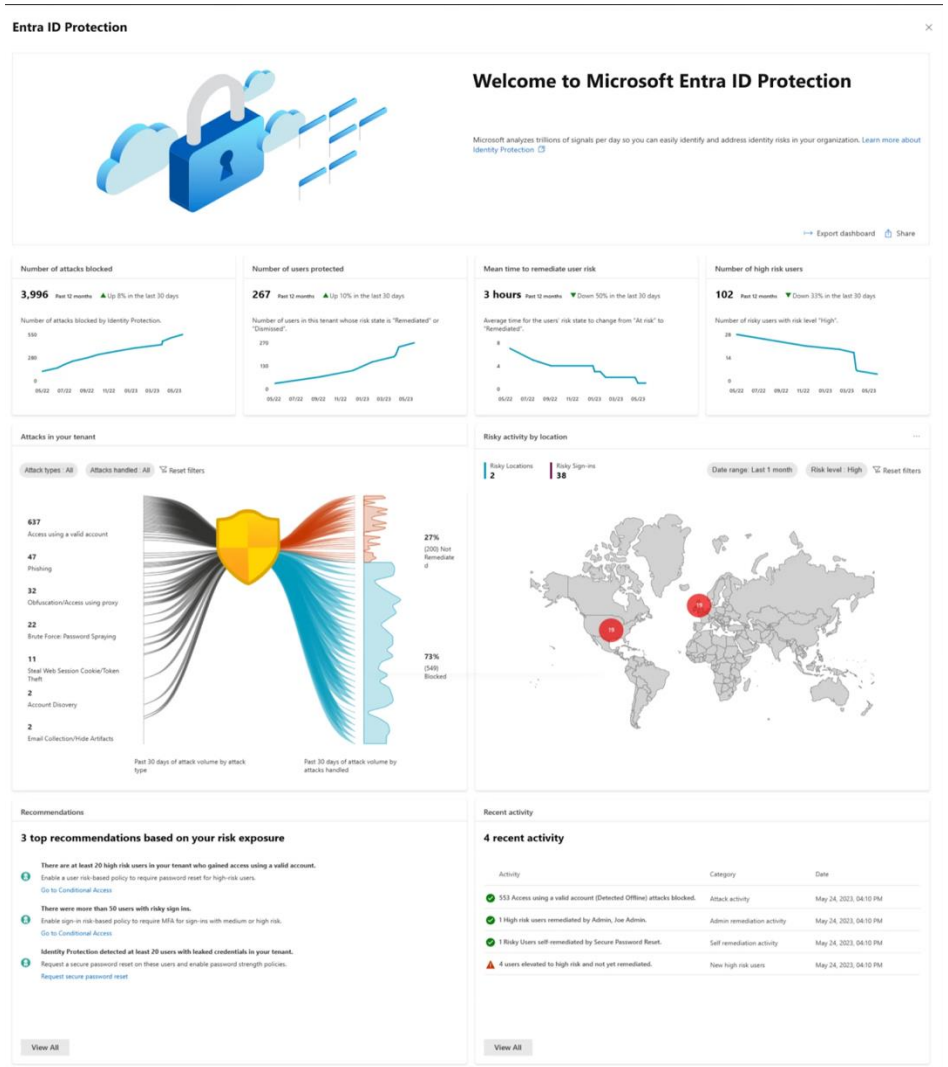

- B2C tenant provides identity services for the application
- Branding, sign-up experience, etc. can be customized



Source: https://learn.microsoft.com/en-us/entra/external-id/external-identities-overview

# Entra ID Protection

- Prevent identity compromise
- Enforce policies
- Seamlessly integrate




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

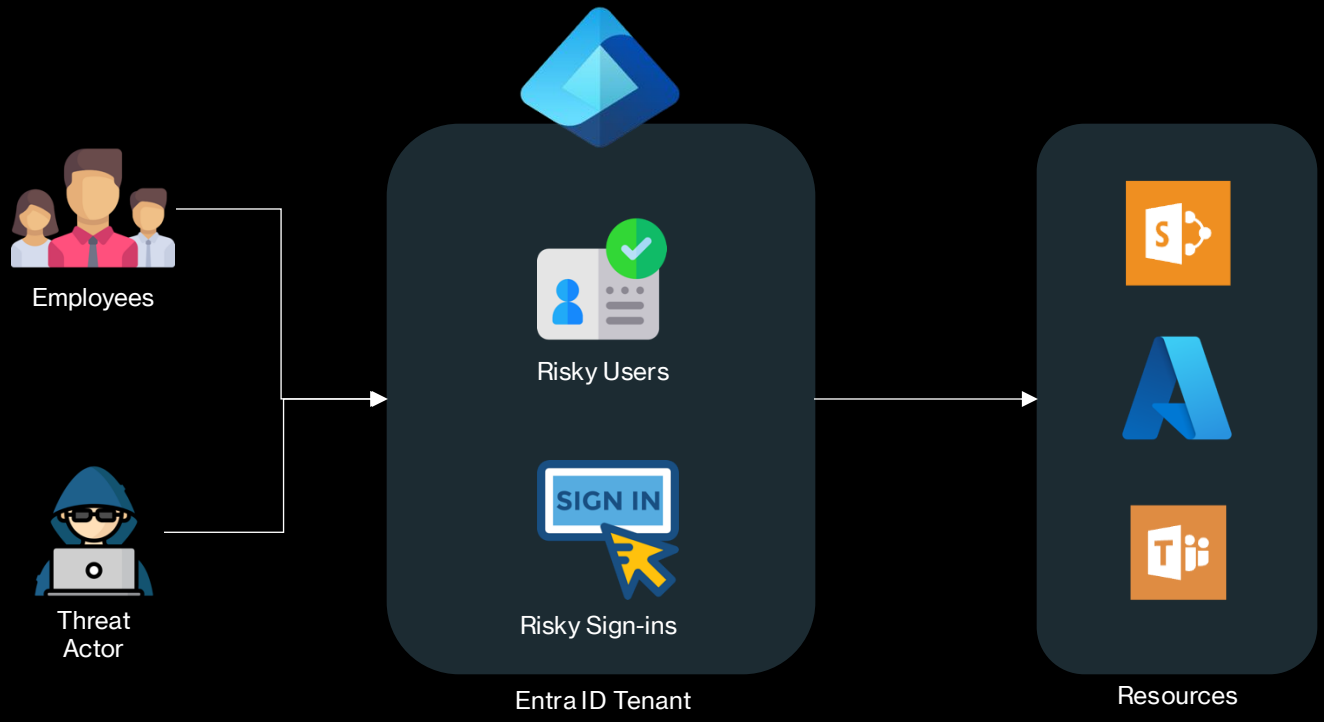
# Entra ID Protection

- Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks.
- These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation.
- Microsoft continually adds and updates detections in our catalog to protect organizations. These detections come from our learnings based on the analysis of trillions of signals each day from Active Directory, Microsoft Accounts, and in gaming with Xbox. This broad range of signals helps Identity Protection detect risky behaviors like:
  - Anonymous IP address usage
  - Password spray attacks
  - Leaked credentials
  - and more...
- During each sign-in, Identity Protection runs all real-time sign-in detections generating a sign-in session risk level, indicating how likely the sign-in is compromised. Based on this risk level, policies are then applied to protect the user and the organization



Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

# Entra ID Protection




Properties

User Risk:

- Monitors identities for risks
- Can be leveraged for actions, e.g. block access, or password change

Sign-in Risk:

- Monitors sign-ins for risks
- Can be leveraged to block access or require MFA



Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

# Entra ID Protection

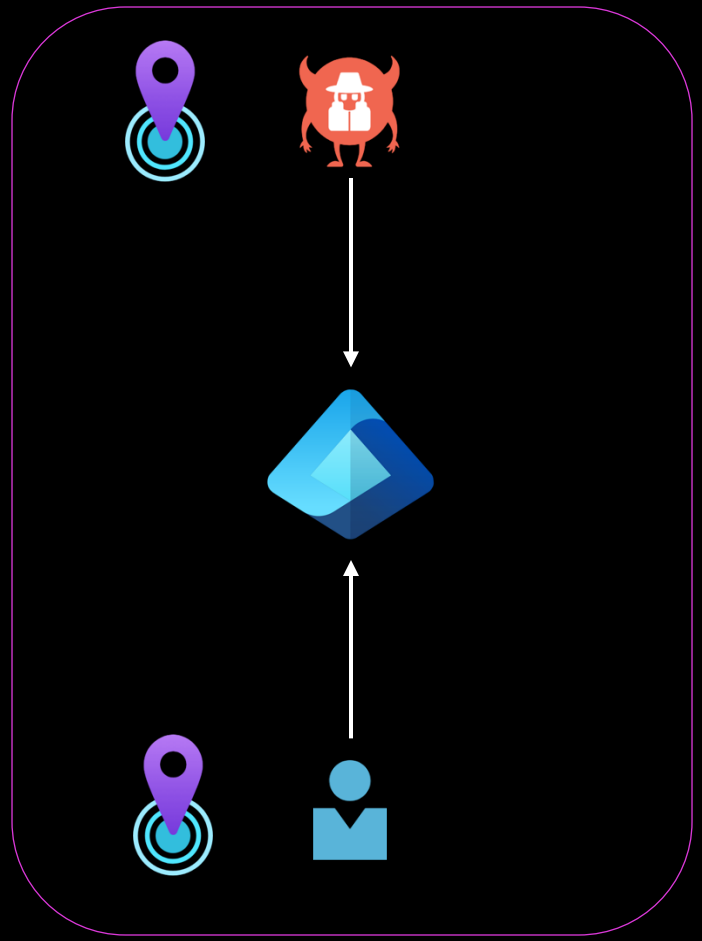
| Risk Detection | Detection Type |
|---|---|
| Atypical travel | Offline |
| Anomalous Token | Offline |
| Anomalous Token | Real-time or Offline |
| Suspicious browser | Offline |
| Unfamiliar sign-in properties | Real-time |
| Malicious IP address | Offline |
| Suspicious inbox manipulation rules | Offline |
| Password spray | Offline |
| Impossible travel | Offline |
| New country | Offline |
| Activity from anonymous IP address | Offline |
| Suspicious inbox forwarding | Offline |
| Mass Access to Sensitive Files | Offline |
| Verified threat actor IP | Real-time |
| Additional risk detected | Real-time or Offline |
| Anonymous IP address | Real-time |
| Admin confirmed user compromised | Offline |
| Microsoft Entra threat intelligence | Real-time or Offline |

# Entra ID Protection – Atypical Travel

## Description

- Two sign-ins in geo-distant locations
- At least one location is atypical for the user
- Obvious false positive such as VPNs are ignored by the detection
- Requires a learning of at least 14 days or 10 logins

## Flow



## Investigation

True Positive

- Mark sign-in as compromised
- Invoke password reset
- Block user if attacker has access to reset password or perform MFA and reset password

False Positive

- Dismiss alert if user is associated with the IP
- Dismiss Alert if user is expected to travel
- Dismiss alert if IP is from a sanctioned VPN

Christopher Nett

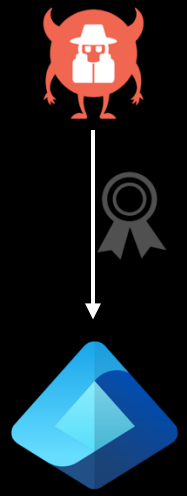
Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

# Entra ID Protection – Anomalous Token

## Description

- Indicates abnormal characteristics in a token, e.g. unusual token lifetime
- Covers session and refresh tokens

## Flow



## Investigation

True Positive

- Mark sign-in as compromised
- Invoke password reset
- Block user if attacker has access to reset password or perform MFA and reset password

False Positive

- Allow user to self-remediate with a conditional access risk policy
- Let an admin confirm sign-in as safe



Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

# Entra ID Protection – Suspicious Browser

## Description

- Anomalous behavior based on suspicious sign-in activity
- E.g. sign-in from different countries with the same browser
- E.g. TOR exit nodes

## Flow

## Investigation

True Positive

- Mark sign-in as compromised
- Invoke password reset
- Block user if attacker has access to reset password or perform MFA and reset password and tokens

False Positive

- Allow user to self-remediate with a conditional access risk policy
- Let an admin confirm sign-in as safe



Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

# Entra ID Protection – Unfamiliar Sign-in Properties

## Description

- Considers past sign-in history to look for anomalous sign-ins
- Stores information about previous sign-ins, and triggers a risk detection when a sign-in occurs with properties that are unfamiliar to the user
- Properties can include IP, ASN, location, device, browser, and tenant IP subnet

## Flow

IP
ASN
Location
Device
Browser
Tenant IP

## Investigation

**True Positive**

- Mark sign-in as compromised
- Invoke password reset
- Block user if attacker has access to reset password or perform MFA and reset password and tokens

**False Positive**

- Allow user to self-remediate with a conditional access risk policy
- Let an admin confirm sign-in as safe



Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

# Entra ID Protection

- Policies are configured on Entra ID tenant level
- Only one of each policy can be configured (user risk, sign-in risk)
- Entra ID protection should be combined with Conditional Access Policies



Source: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

# Entra ID Authentication Methods

| | | |
|---|---|---|
|   | Password | A secret string of characters known only to the user, used to authenticate identity. |
|  | SMS | A text message sent to the user's phone with a one-time code for authentication. |
|  | Voice | Authentication by receiving or sending a one-time code through a phone call. |
|  | Oauth Tokens | A secure token issued by an authorization server to allow access without revealing user credentials. |
|  | Microsoft Authenticator | A mobile app that generates time-based one-time passcodes or sends push notifications for multi-factor authentication. |
|  | Windows Hello for Business | A passwordless authentication system using biometrics (like facial recognition or fingerprints) and a PIN tied to a specific device. |
|  | FIDO2 Key | A physical security key used for passwordless authentication through public key cryptography. |
|  | Certificate-based Authentication | Authentication using digital certificates to verify a user's identity based on a trusted certificate authority. |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

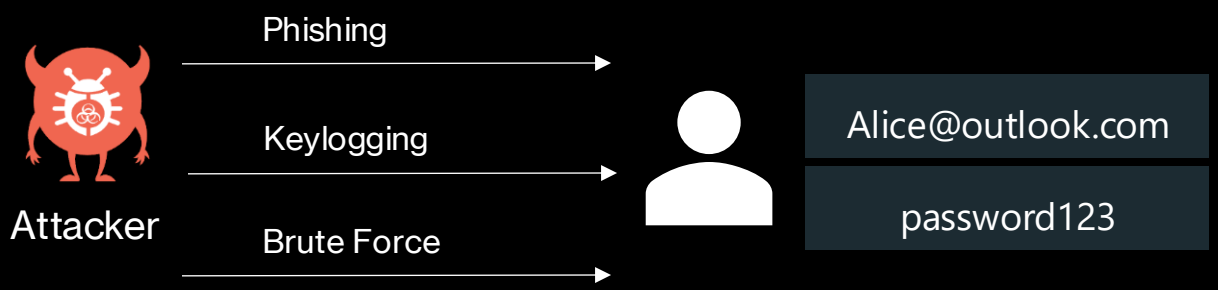
# Entra ID Authentication Methods

| AuthN Method | Passwordless | MFA | SSPR |
|---|---|---|---|
| Password | | X | X |
| SMS | | X | X |
| Voice | | X | X |
| OAuth Tokens | | X | X |
| Microsoft Authenticator | X | X | |
| Windows Hello for Business | X | X | |
| FIDO2 Key | X | X | |
| Certificate-based AuthN | X | X | |



Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

# Attacks on Passwords




20% of help desk calls are related to password resets

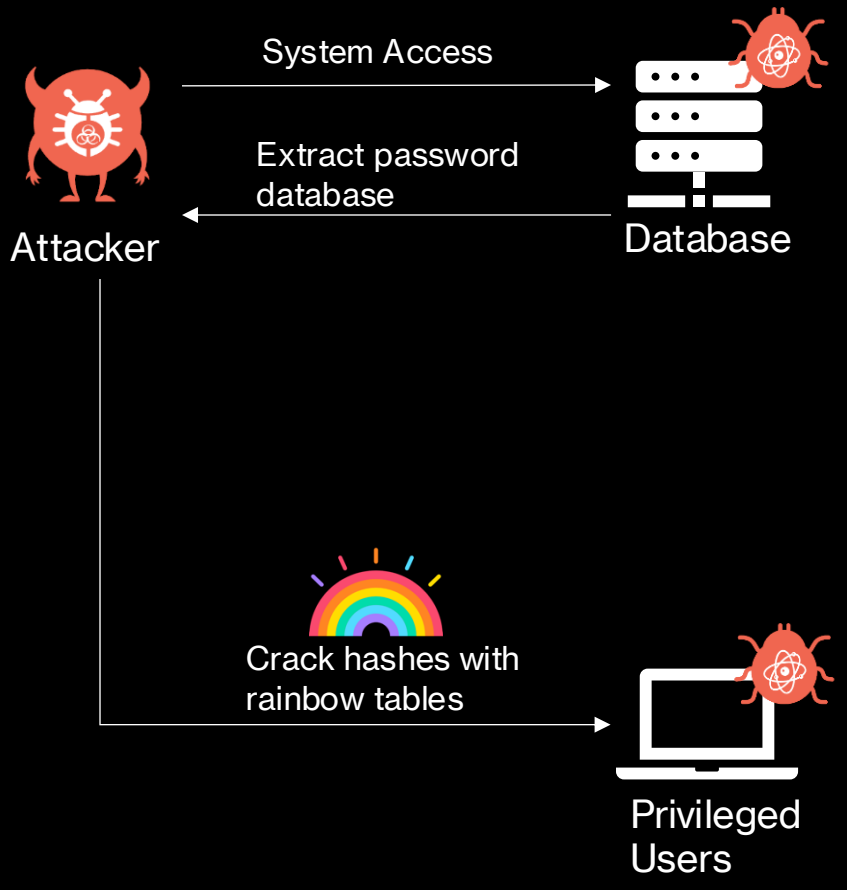
85% of breaches leveraged passwords

72% of passwords are reused across multiple accounts



Source: Lateral movement security alerts - Microsoft Defender for Identity | Microsoft Learn

# Attacks on Passwords



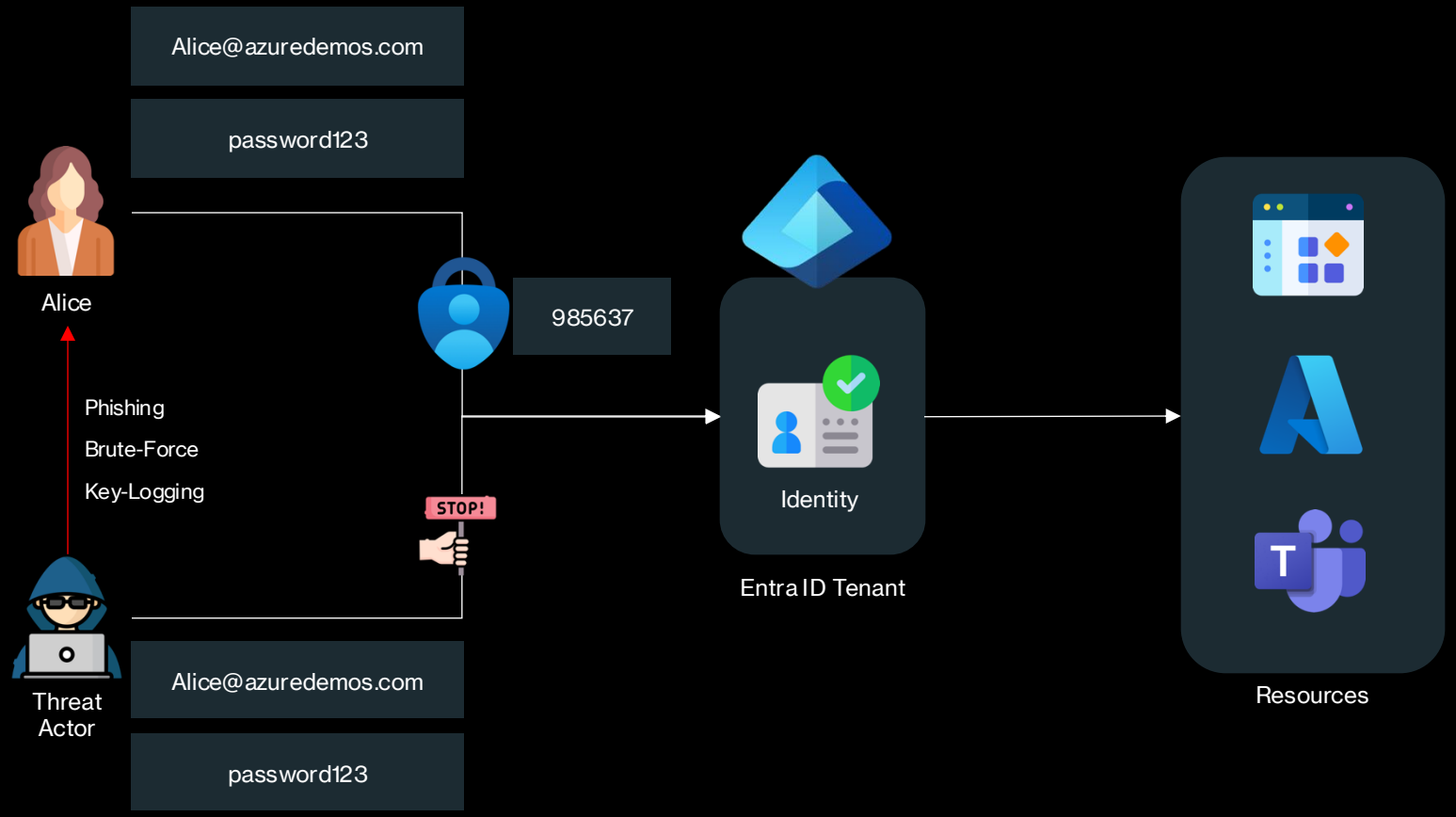

Rainbow Table

| String | MD5 Hash |
|---|---|
| test | 098f6bcd4621d373cade4e832627b4f6 |
| password123 | afc285bebb3dd733796cb06db01cd59a |
| administrator | 1f5836c5d50a072987b907b0f27d3cda |



Source: Lateral movement security alerts - Microsoft Defender for Identity | Microsoft Learn

# Entra ID MFA

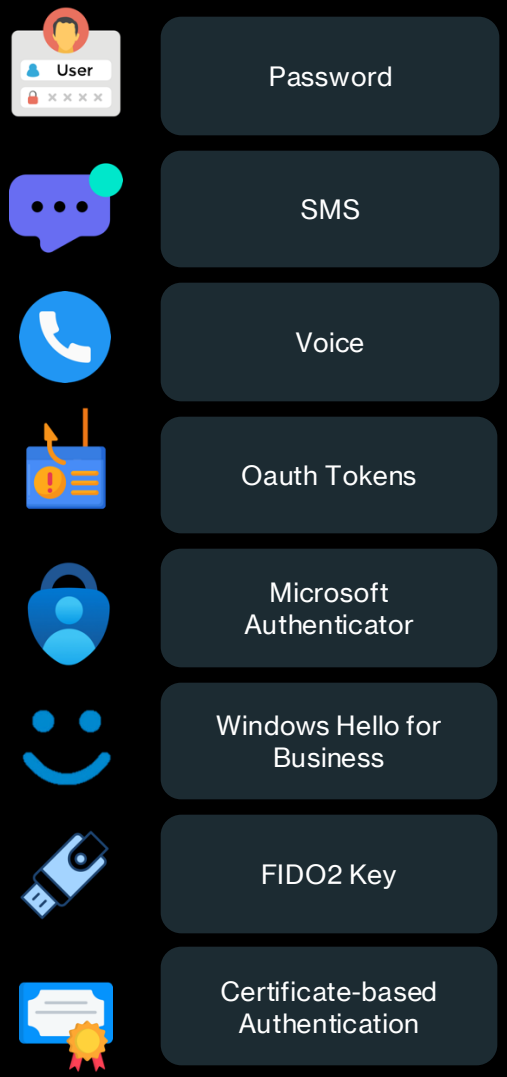


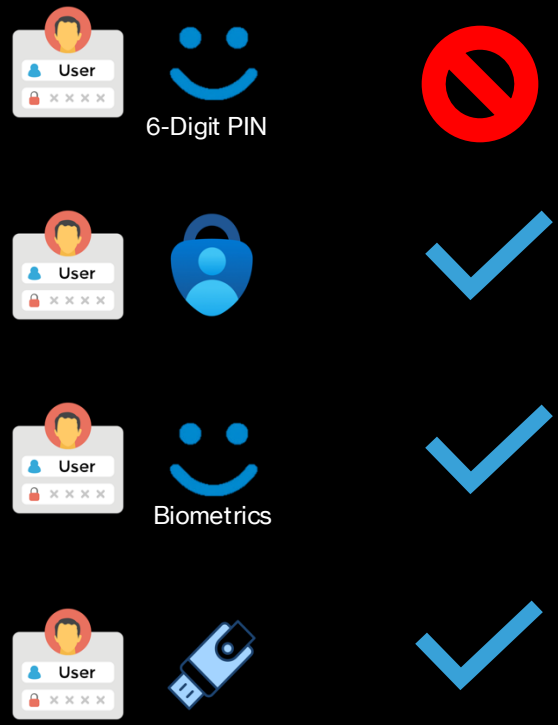

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

# Entra ID MFA

- Something you know
- Something you have
- Something you are

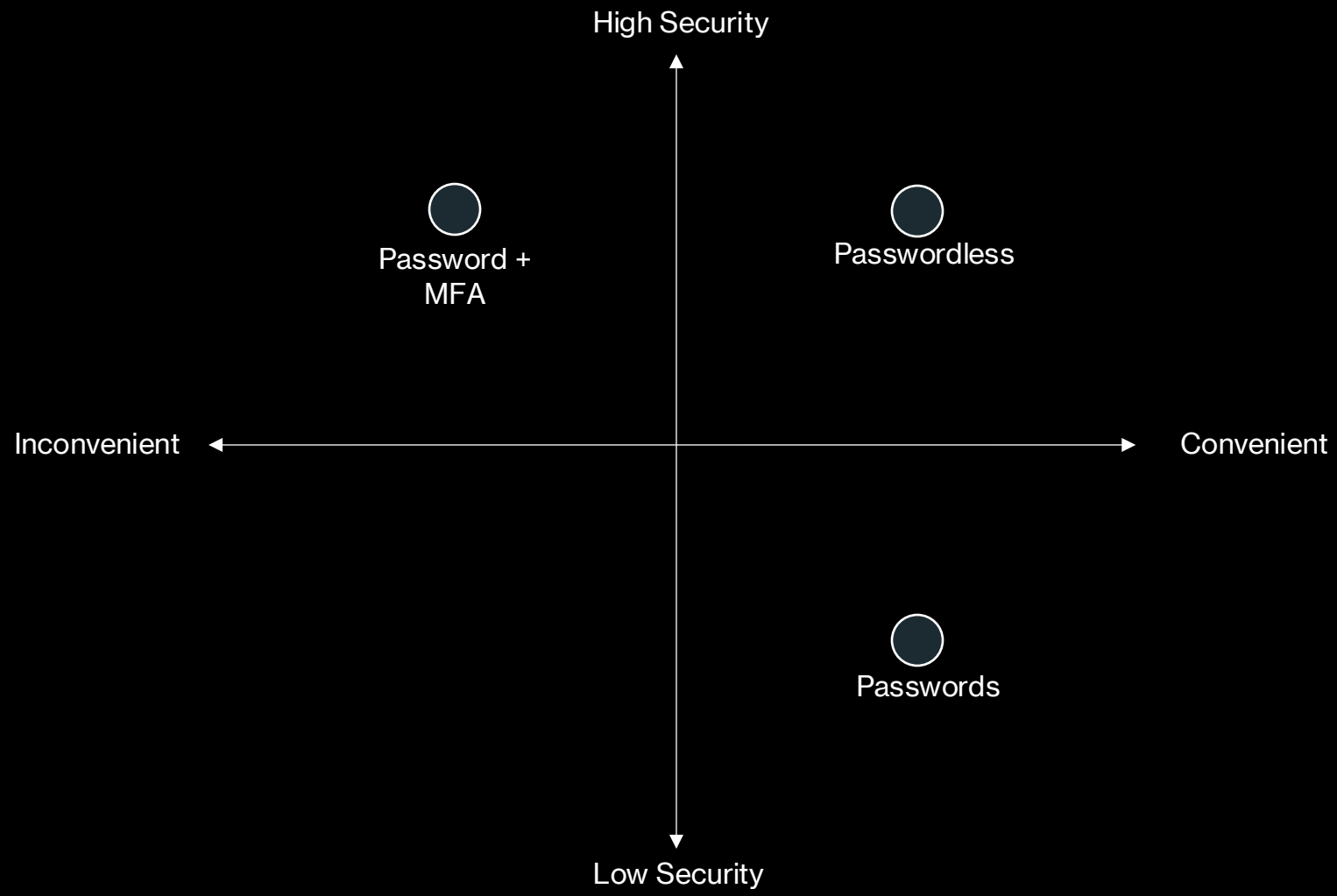





Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

# Password + MFA?






Source: Microsoft Entra passwordless sign-in - Microsoft Entra ID | Microsoft Learn

# Authentication Options

## Bad: Password

123456

qwerty

password

iloveyou

Password1

## Good: Password +

SMS

Voice

## Better: Password +

Oauth tokens

Certificates

## Best: Passwordless

Windows Hello

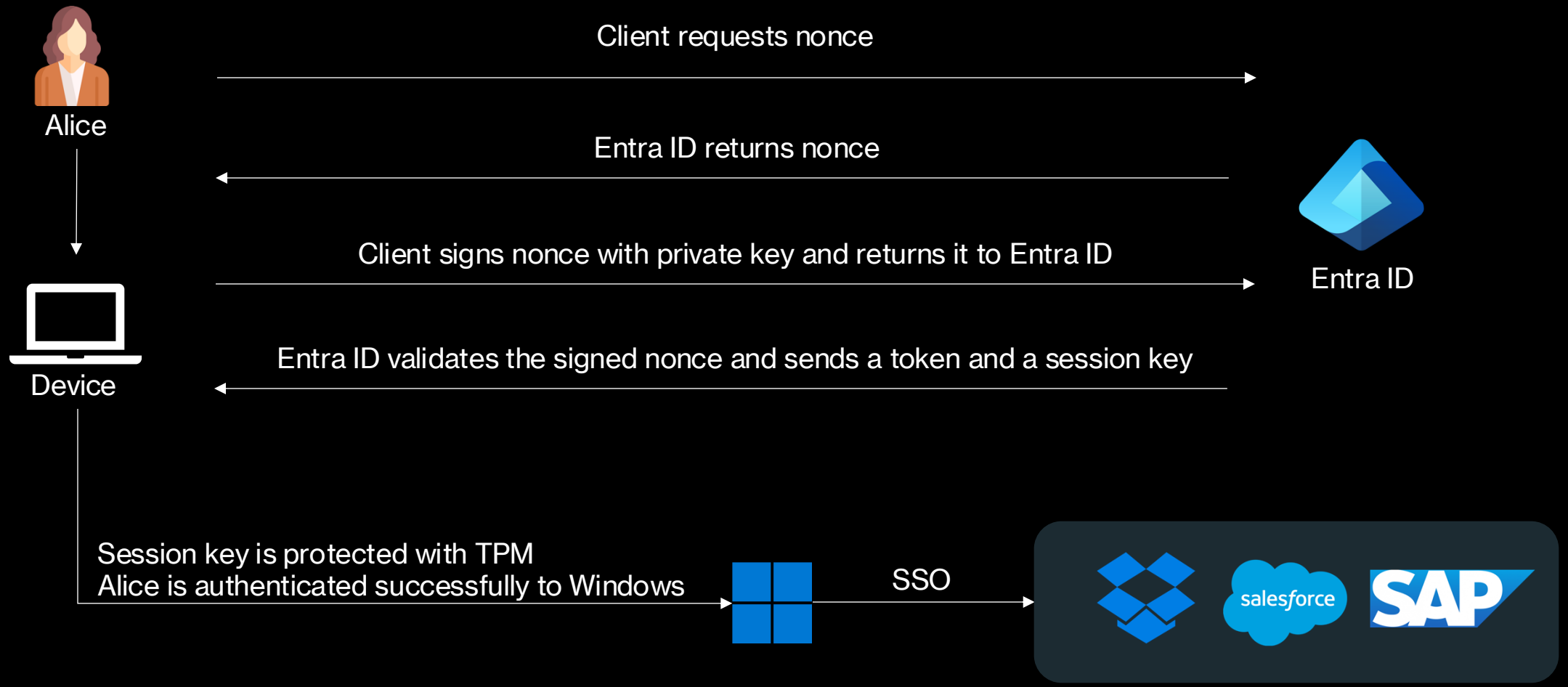
FIDO2 security key

Microsoft Authenticator



Source: Passwordless authentication | Microsoft Security

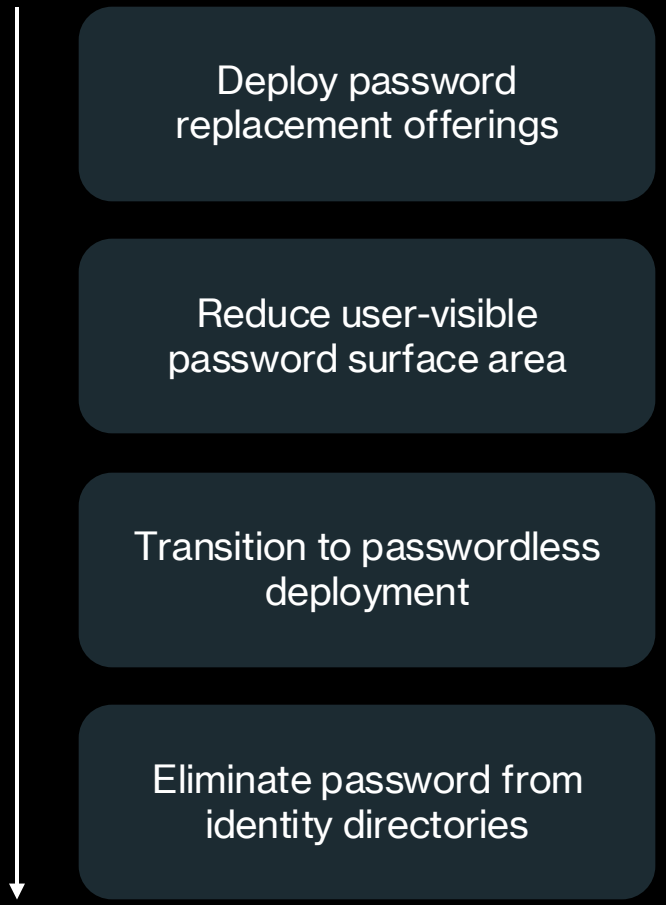
# Passwordless - Windows Hello for Business






Source: Microsoft Entra passwordless sign-in - Microsoft Entra ID | Microsoft Learn

# Passwordless




| AuthN Method | Passwordless |
|---|---|
| Password | |
| SMS | |
| Voice | |
| Microsoft Authenticator | X |
| Windows Hello for Business | X |
| FIDO2 Key | X |
| Certificate-based AuthN | X |



Source: Microsoft Entra passwordless sign-in - Microsoft Entra ID | Microsoft Learn

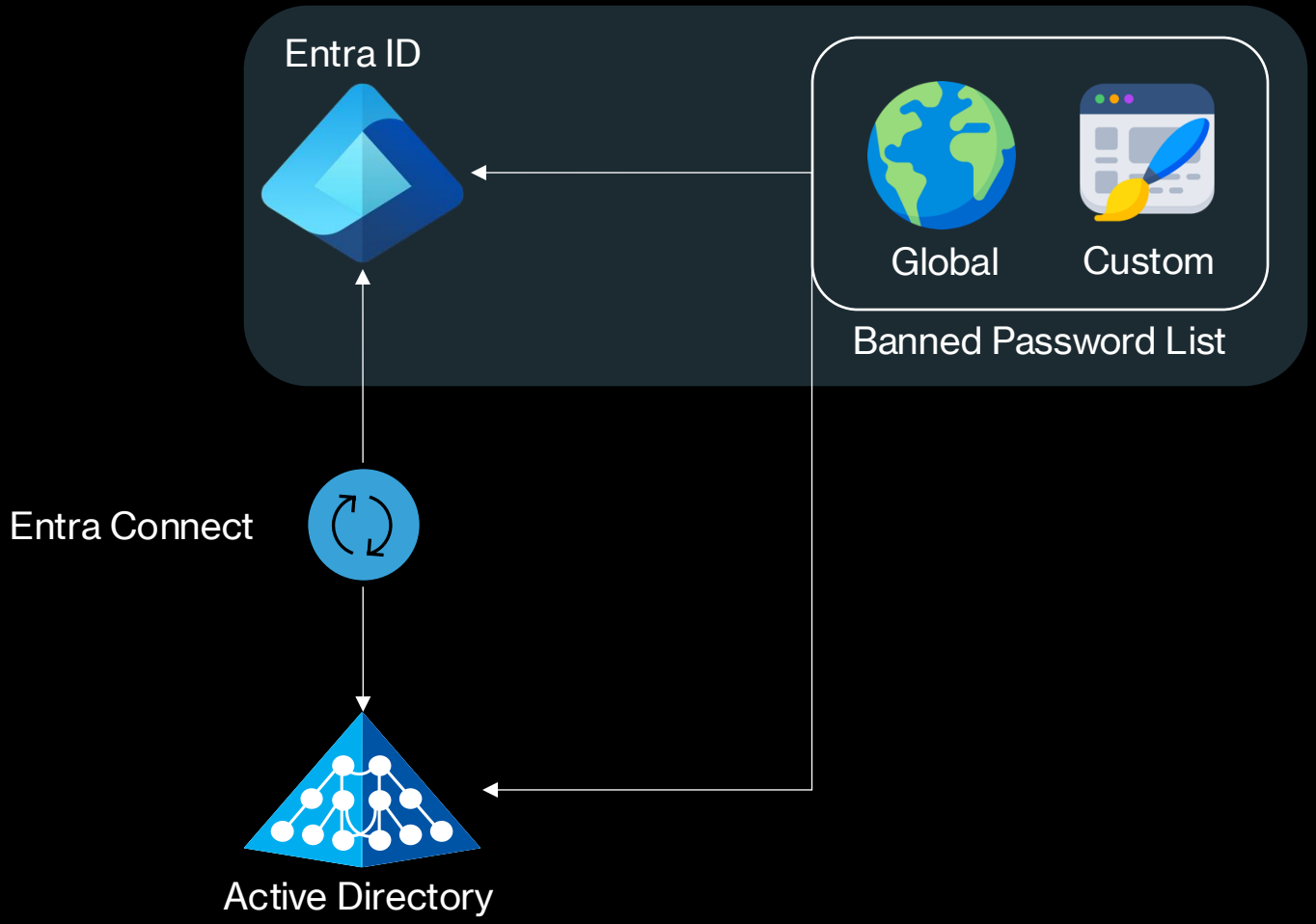
# Entra ID - Password Protection

- **Smart Password Policies:** Entra ID Password Protection prevents the use of common, weak, or compromised passwords by enforcing global and custom password ban lists to strengthen account security.
- **Real-Time Password Validation:** It checks passwords in real-time during user creation or password changes, ensuring users cannot set passwords that are easily guessable or previously breached.
- **Protection Across Hybrid Environments:** The service extends password protection to both cloud and on-premises environments, ensuring consistent password security across all connected systems.



Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad

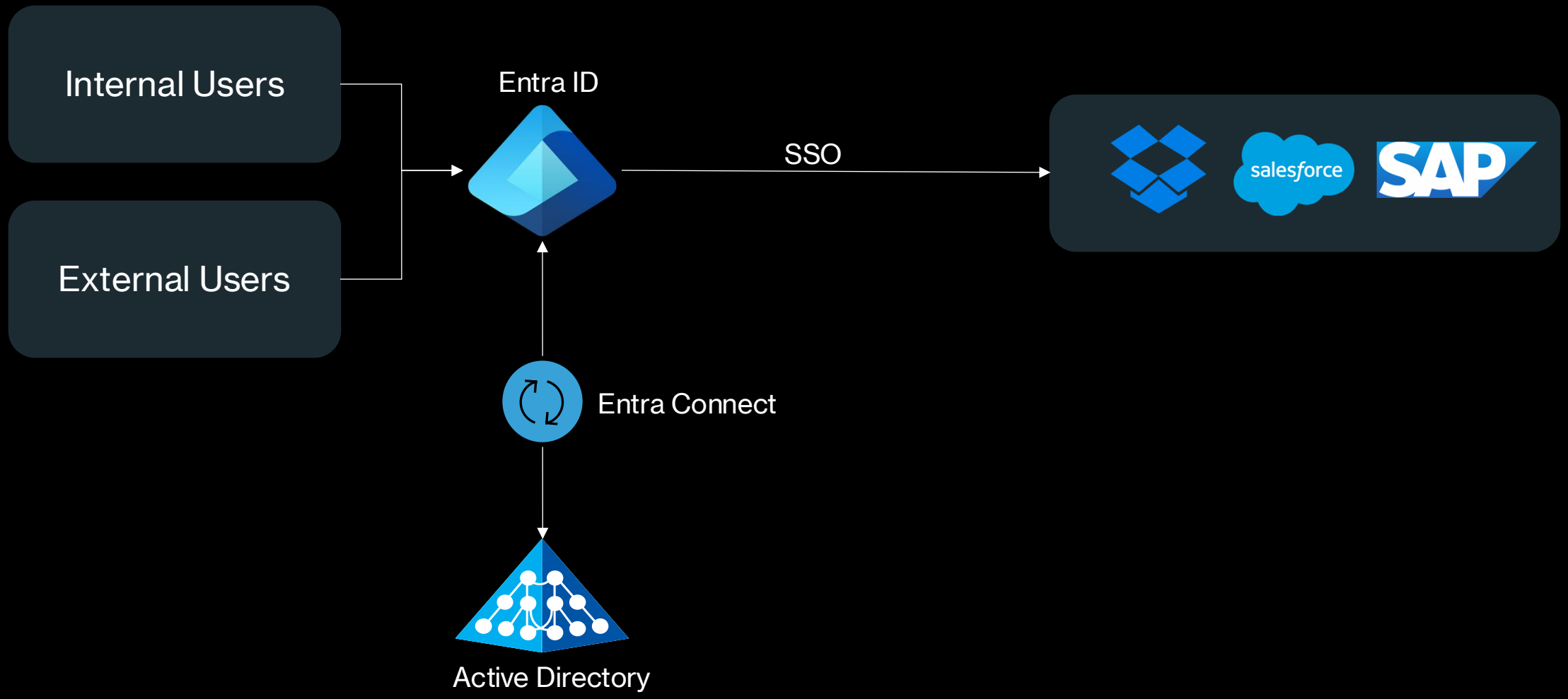
# Entra ID - Password Protection






Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad

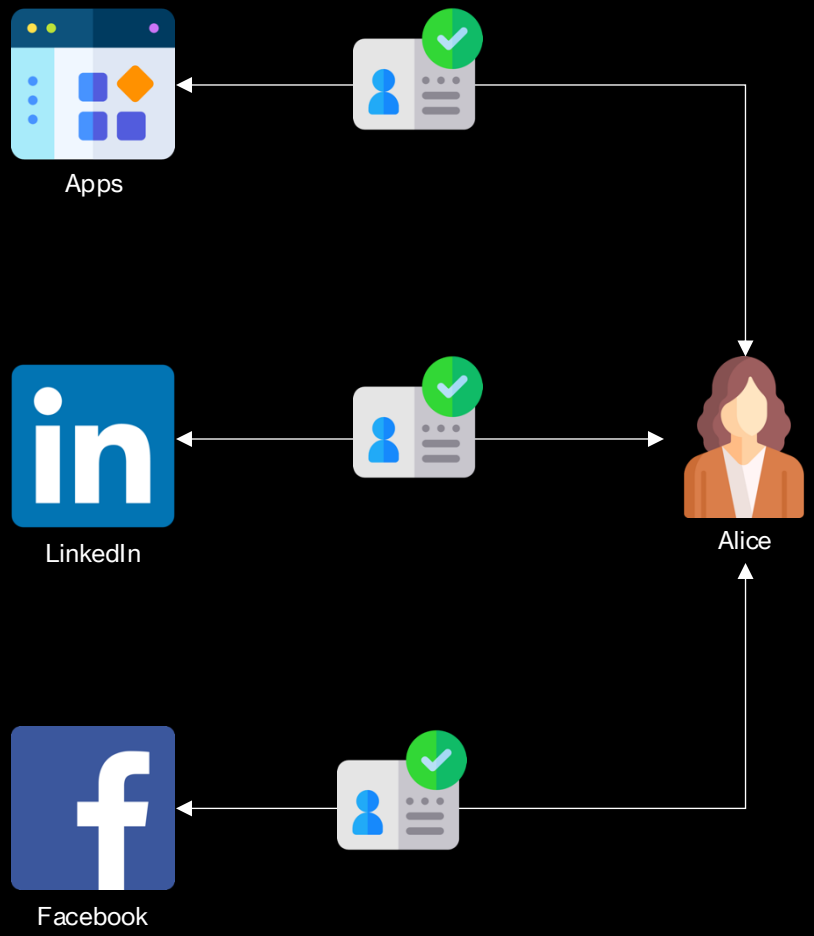
# Single Sign-On (SSO)






Source: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/add-application-portal-setup-sso

# Microsoft Entra Verified ID

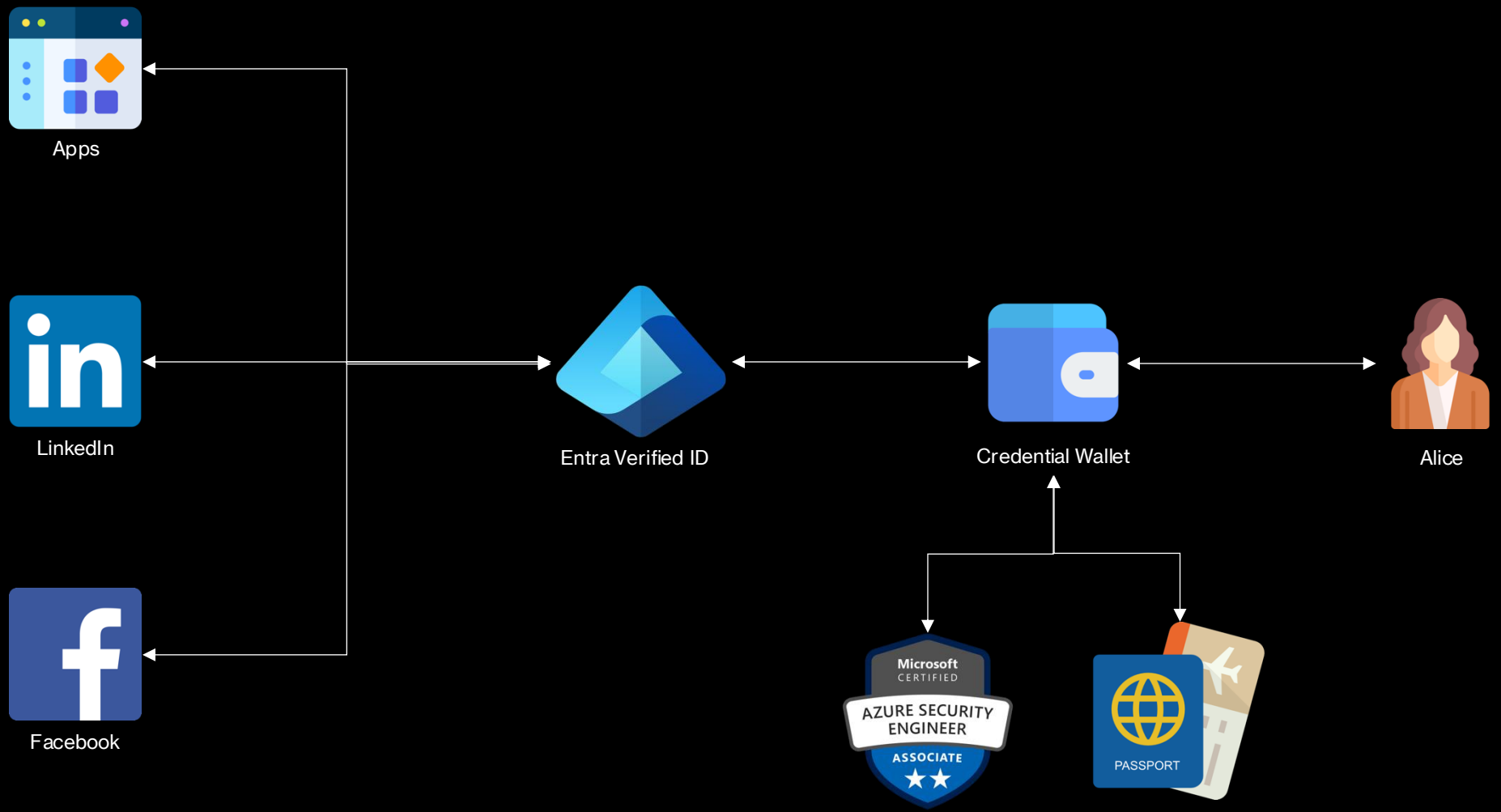



- Is the identity of the person correct?
- Is the work history correct?
- Is the person actually certified?



Source: https://learn.microsoft.com/en-us/entra/verified-id/decentralized-identifier-overview

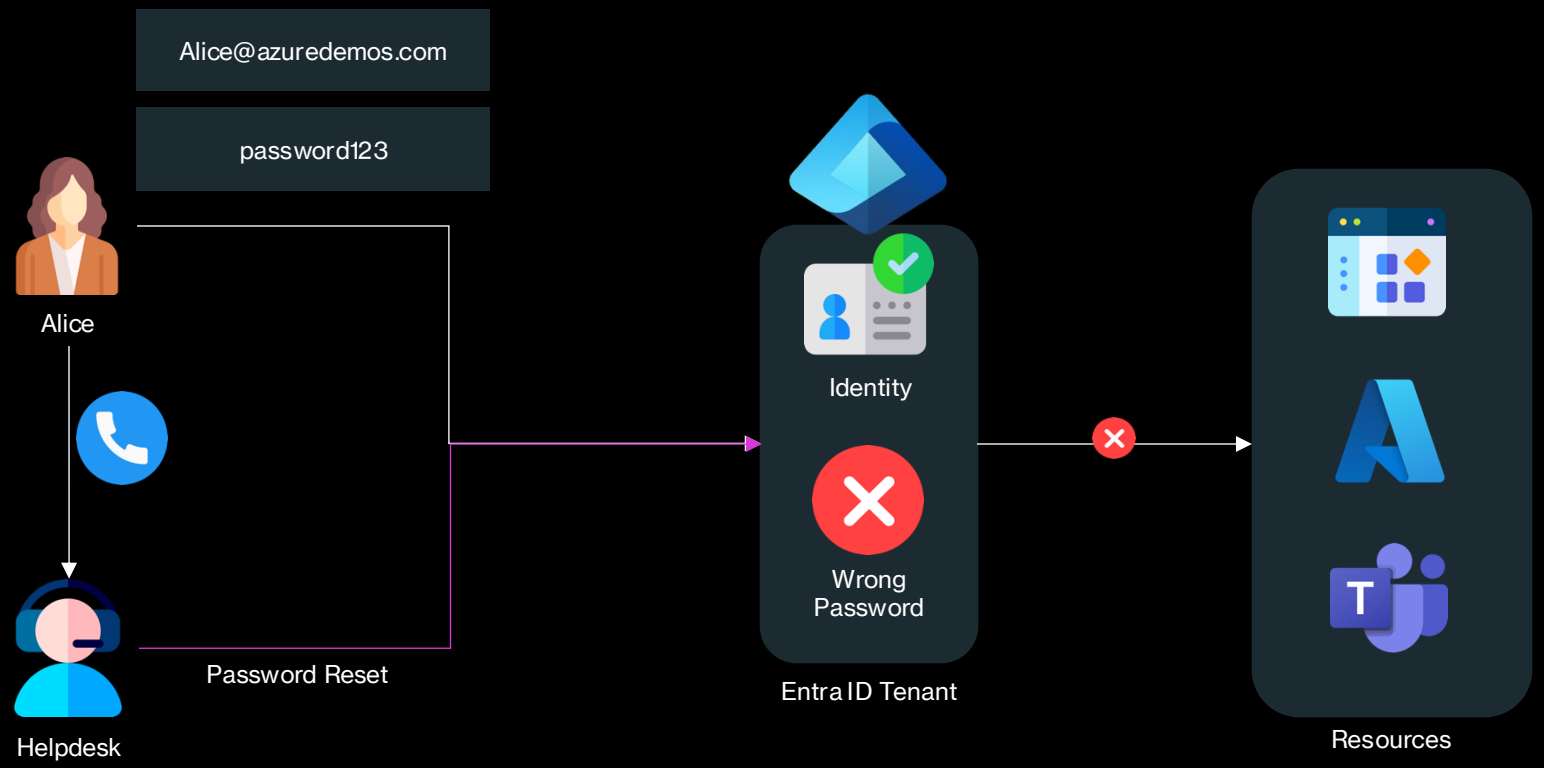
# Microsoft Entra Verified ID




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/verified-id/decentralized-identifier-overview

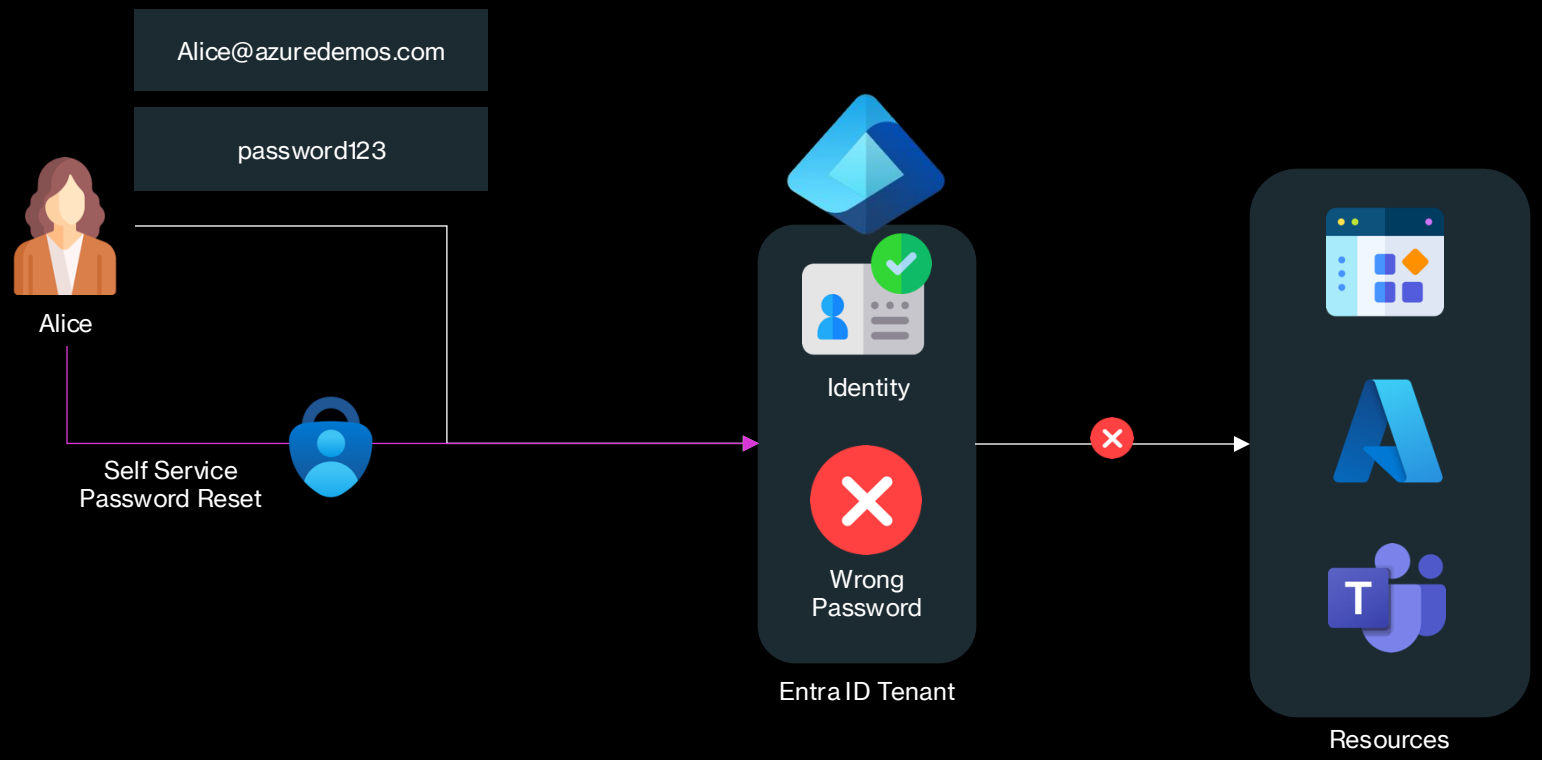
# Self-Service Password Reset (SSPR)




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

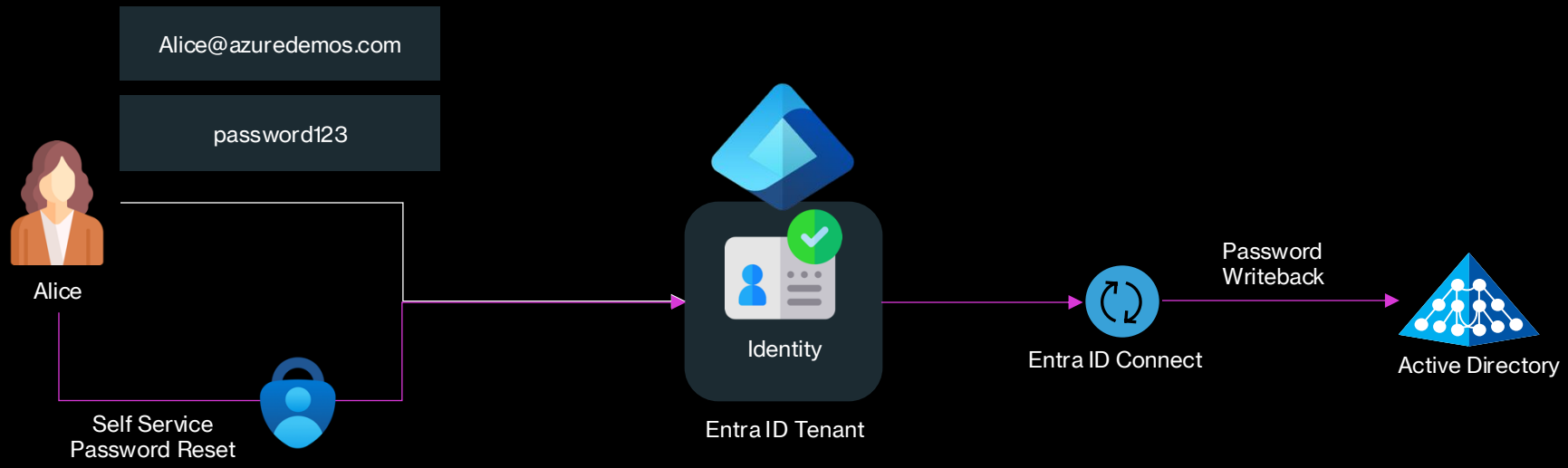
# Self-Service Password Reset (SSPR)




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

# Self-Service Password Reset (SSPR)






Source: https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

# Self-Service Password Reset (SSPR) – Key Benefits

- **Manage cost.** SSPR reduces IT support costs by enabling users to reset passwords on their own. It also reduces the cost of time lost due to lost passwords and lockouts.
- **Intuitive user experience.** It provides an intuitive one-time user registration process that allows users to reset passwords and unblock accounts on-demand from any device or location. SSPR allows users to get back to work faster and be more productive.
- **Flexibility and security.** SSPR enables enterprises to access the security and flexibility that a cloud platform provides. Administrators can change settings to accommodate new security requirements and roll these changes out to users without disrupting their sign-in.
- **Robust auditing and usage tracking.** An organization can ensure that the business systems remain secure while its users reset their own passwords. Robust audit logs include information of each step of the password reset process. These logs are available from an API and enable the user to import the data into a Security Incident and Event Monitoring (SIEM) system of choice.



Source: https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

# Entra Connect

Core Features:

- Password hash synchronization - A sign-in method that synchronizes a hash of a users on-premises AD password with Microsoft Entra ID.
- Pass-through authentication - A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.
- Federation integration - Federation is an optional part of Microsoft Entra Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
- Synchronization - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.
- Health Monitoring - Microsoft Entra Connect Health can provide robust monitoring and provide a central location in the Microsoft Entra admin center to view this activity.



Source: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-azure-ad-connect

# Entra Connect

Entra Connect Sync:

- A tool that synchronizes on-premises Active Directory with Microsoft Entra ID for hybrid identity management.
- It ensures users have a unified identity across on-premises and cloud environments, enabling seamless access to resources.
- Legacy on-premises deployment of the identity synchronization

Entra Connect Cloud Sync:

- A lightweight cloud-based service that syncs on-premises directory identities to Microsoft Entra ID without the need for full on-premises infrastructure.
- It is ideal for simplifying identity management and scaling across distributed environments with minimal infrastructure.
- Modern cloud-native identity synchronization that is managed in the cloud.

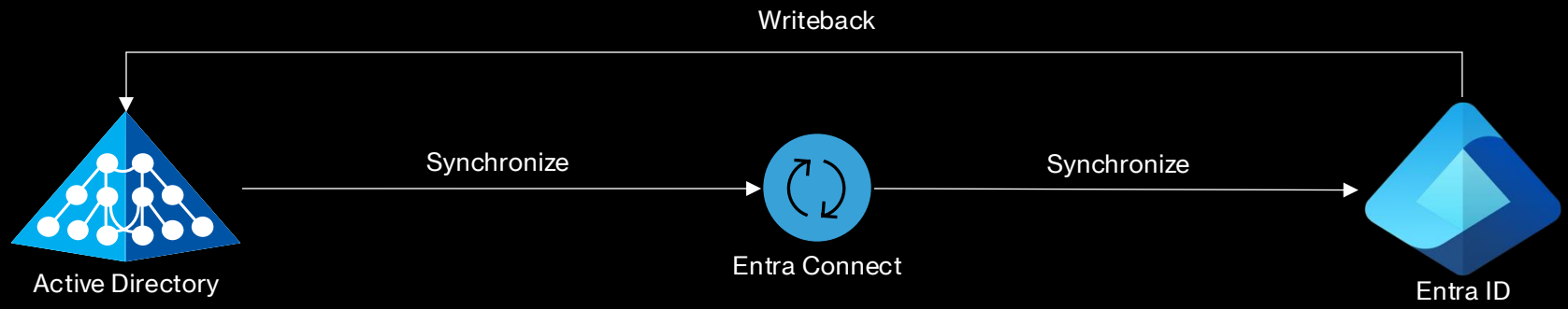
Entra Connect Health:

- A monitoring tool that provides insights into the health and performance of identity synchronization and authentication systems.
- It delivers alerts, analytics, and reports to ensure the availability and security of hybrid identity environments.



Source: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-azure-ad-connect

# Entra Connect






Source: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad

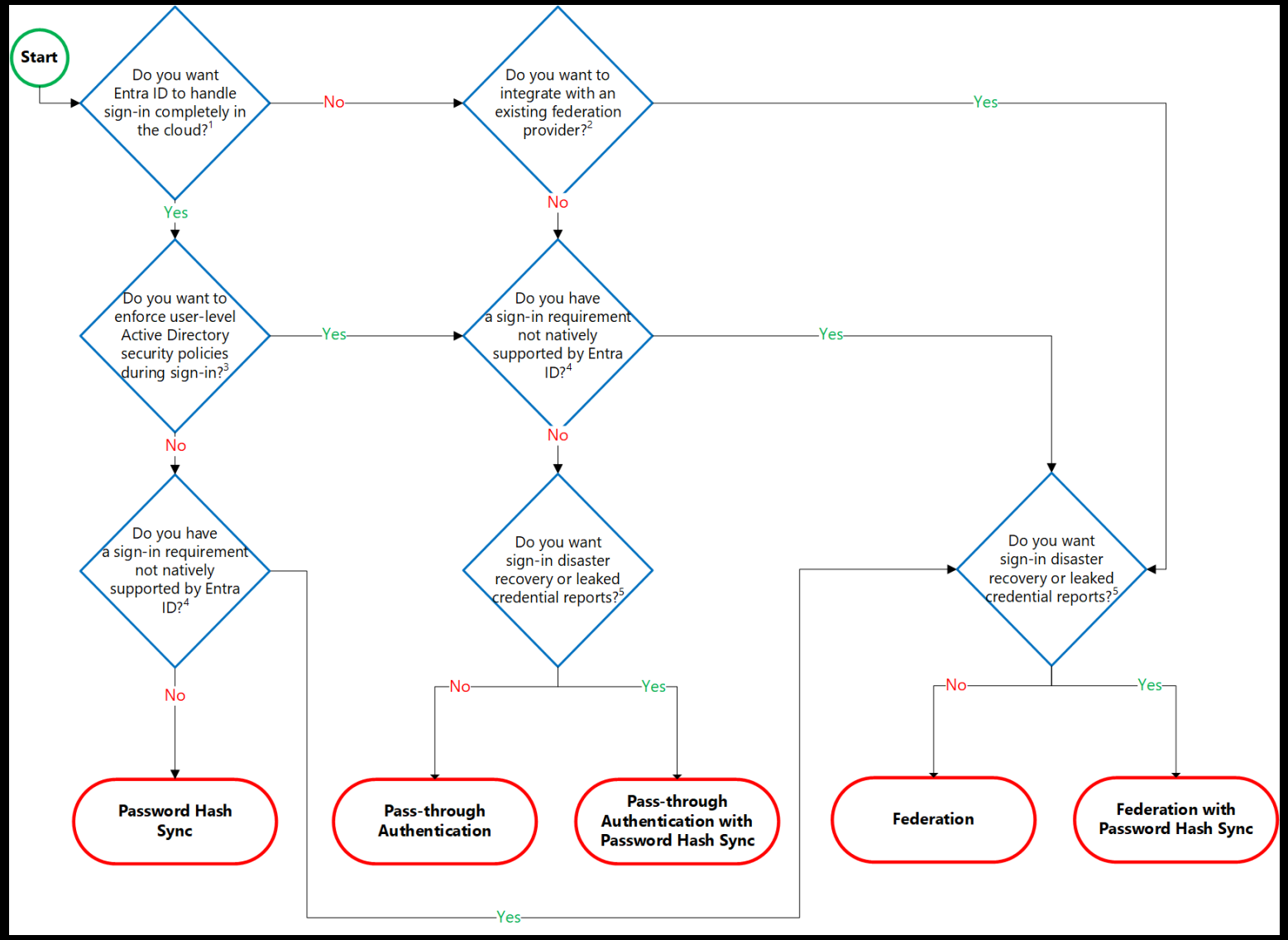
# Entra Connect

| Feature | Connect Sync | Cloud Sync |
|---|---|---|
| Synchronize single/multiple AD forest | x | x |
| Synchronize multiple disconnected AD forests | x | x |
| Lightweight agent installation model | | x |
| Multiple active agents for high availability | | x |
| Support for user objects | x | x |
| Support for group objects | x | x |
| Support for contact objects | x | x |
| Support for device objects | x | |
| Support for Password Hash Sync | x | x |
| Support for Pass-Through Authentication | x | |
| Support for federation | x | x |
| Seamless Single Sign-on | x | x |



Source: https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync#comparison-between-microsoft-entra-connect-and-cloud-sync

# Hybrid Authentication




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn

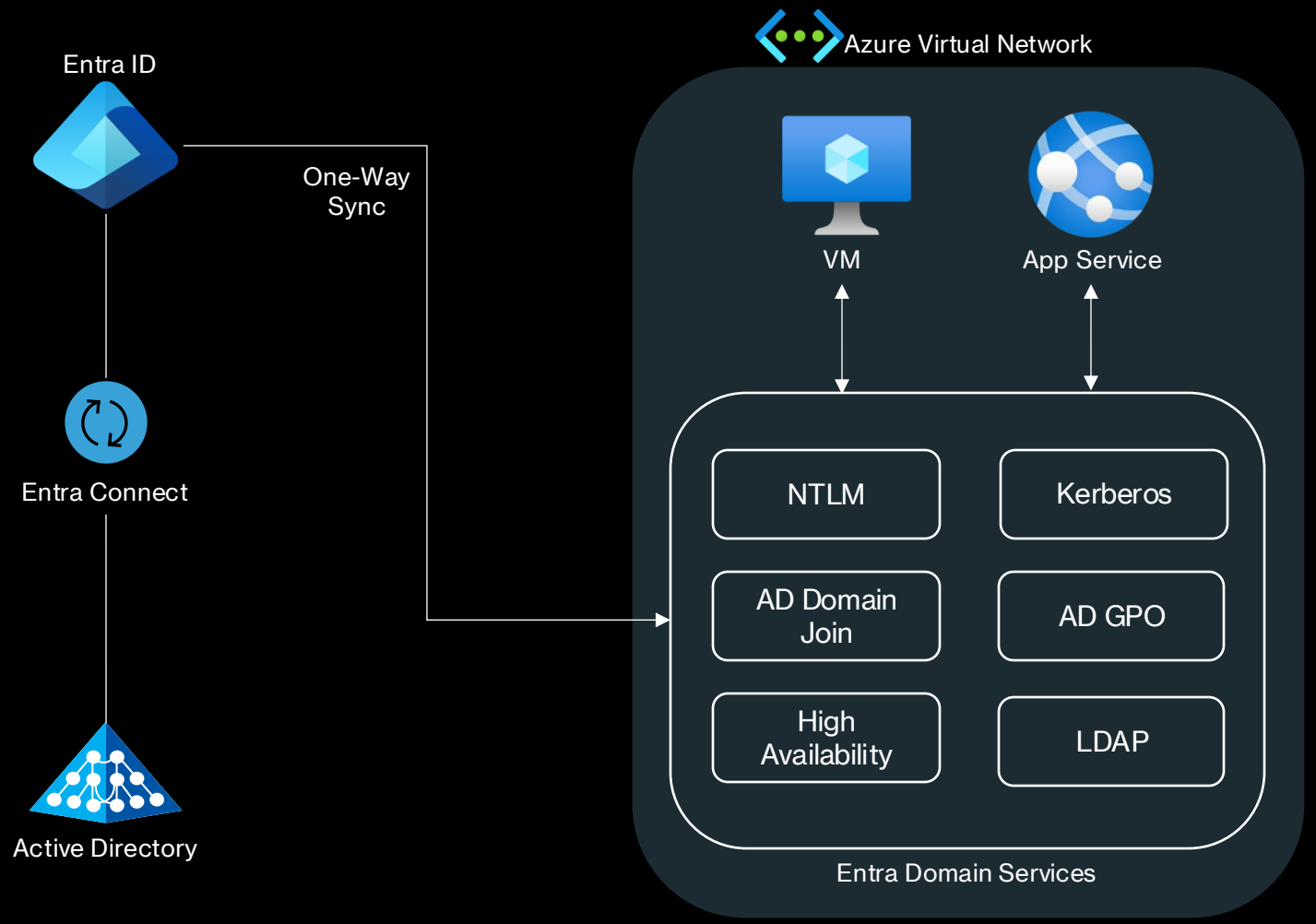
# Entra Domain Services

- Microsoft Entra Domain Services provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.
- A Domain Services managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.
- Domain Services integrates with your existing Microsoft Entra tenant. This integration lets users sign in to services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.



Source: https://learn.microsoft.com/en-us/entra/identity/domain-services/overview

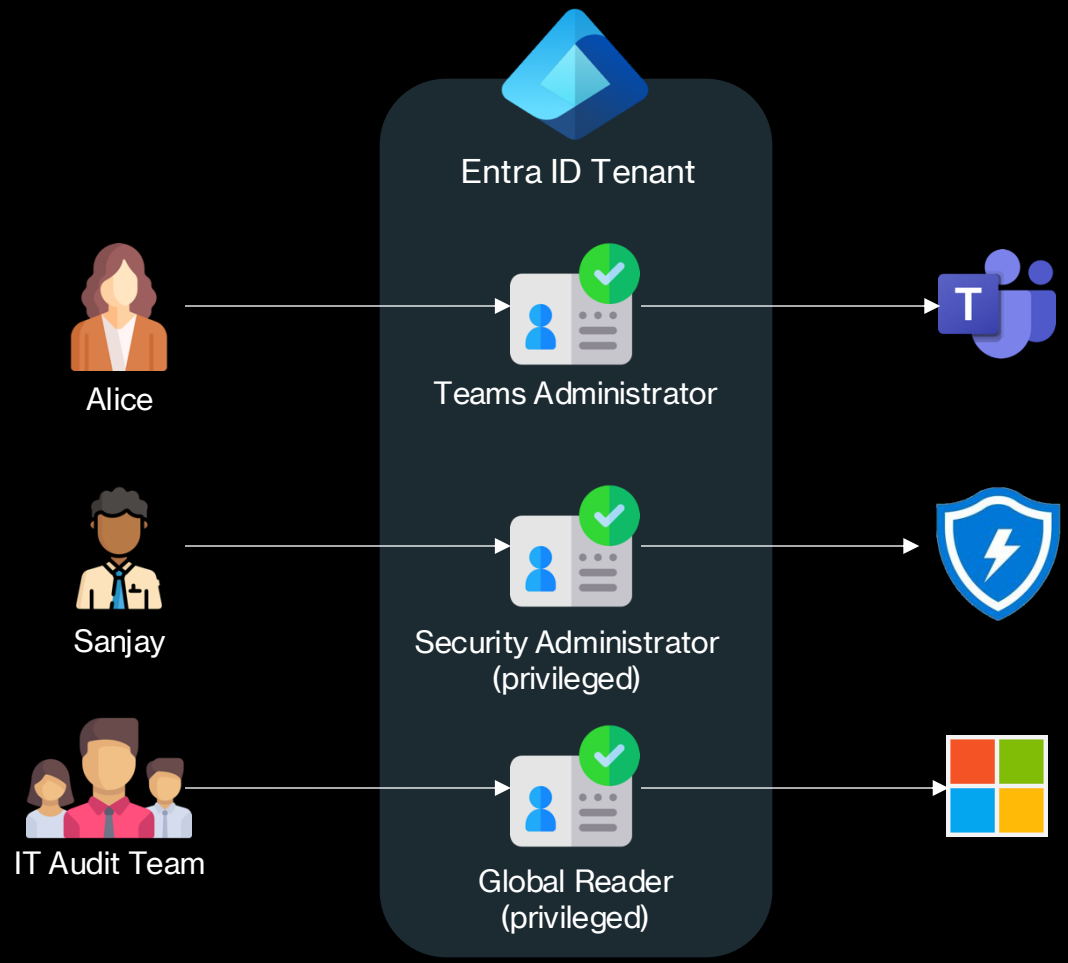
# Entra Domain Services




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/identity/domain-services/overview

# Entra ID Roles




- The **Teams Administrator** role allows users to manage Microsoft Teams settings, policies, and configurations, including meeting settings, messaging policies, and user management.
- They can also troubleshoot Teams-related issues and monitor service health, but they cannot modify users in Entra ID

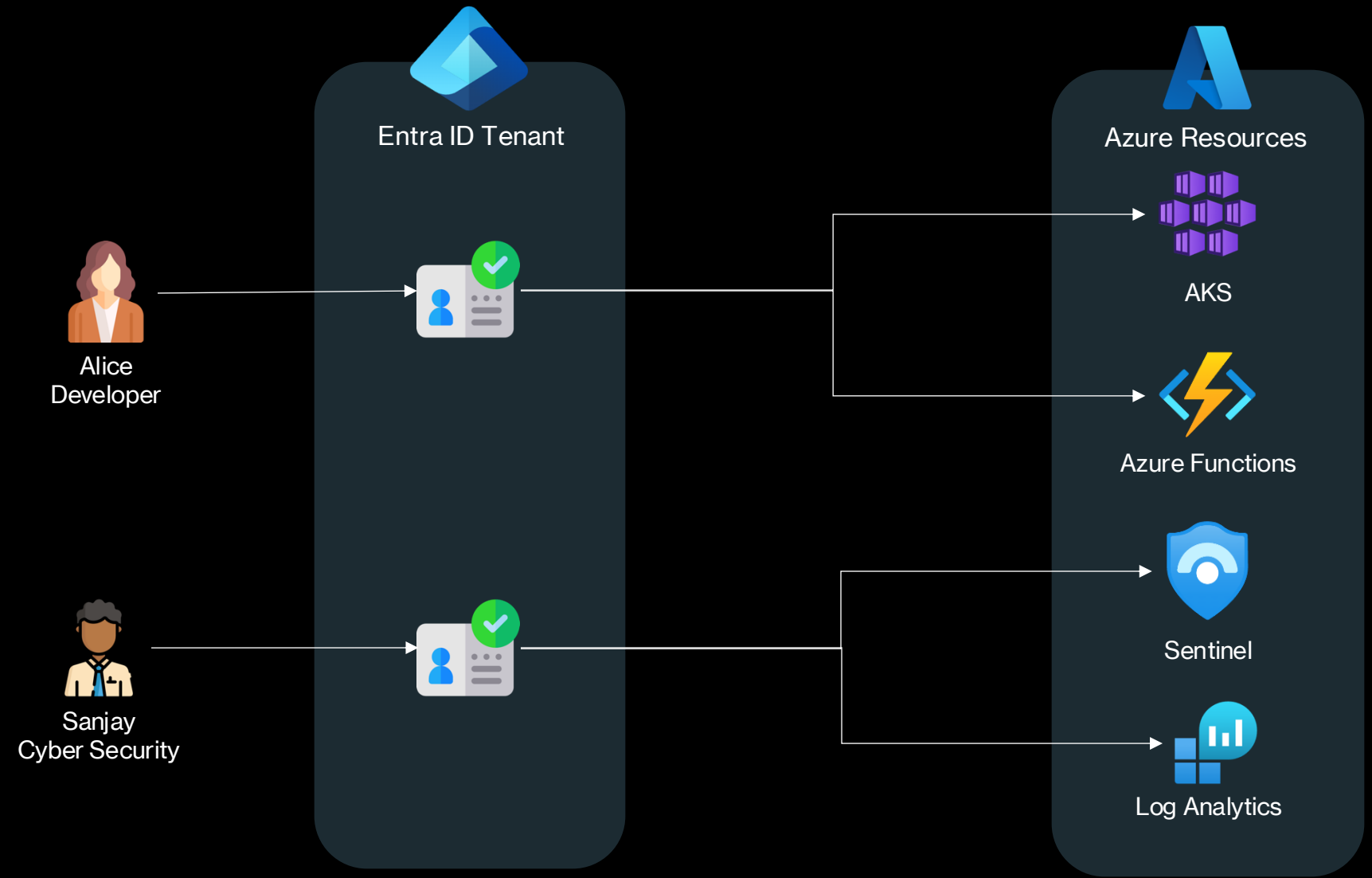
- The **Security Administrator** role grants the ability to manage security-related features, such as monitoring security reports, configuring security policies (like Conditional Access), and managing security alerts across the organization.
- They can also access sensitive data in security tools, such as Microsoft Defender XD, Sentinel or Defender for Cloud.

- The **Global Reader** role provides read-only access to all settings and resources across Microsoft 365, Azure, and Entra ID, without the ability to make any changes.
- It's useful for audits, reporting, and viewing configurations without the risk of accidental modifications.



Source: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#all-roles

# Azure Role-Based Access Control (RBAC)




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure Role-Based Access Control (RBAC)

An Azure RBAC role assignment consists of three elements:

- Security Principal
- Role definition
- Scope



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC – Security Principles

- The Security Principal is the entity to which you want to assign the permissions. This can be:
  - **User**: An individual with a Microsoft account or Entra ID account.
  - **Security Group**: A collection of users in Entra ID.
  - **Service Principal**: A security identity used by applications or services to access specific resources.
  - **Managed Identity**: An automatically managed identity in Azure tied to a specific resource.
  - **Example**: If you want to grant access to a security analyst, that user is the **security principal**.



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC – Role Definition

- A Role Definition is a collection of permissions that defines what actions the security principal can perform on resources. Each role includes:
  - **Actions:** The specific permissions that are granted, such as read, write, delete, etc.
  - **NotActions:** Any actions that are explicitly denied.
  - **DataActions:** Permissions related to data access (specific to Azure Storage, SQL, etc.).
  - **AssignableScopes:** The scopes where the role can be assigned.
- You can leverage built-in roles or define your own custom roles.



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC – Role Definition

```
{
  "Name": "Azure Sentinel Contributor",
  "Description": "Can manage all aspects of Azure Sentinel except access control
  "Actions": [
    "Microsoft.OperationalInsights/workspaces/read",
    "Microsoft.OperationalInsights/workspaces/write",
    "Microsoft.SecurityInsights/*"
  ],
  "NotActions": [],
  "AssignableScopes": [
    "/subscriptions/{subscription-id}/resourceGroups/{resource-group-id}/provide
  ]
}
```

Key permissions for Sentinel:

- Microsoft.SecurityInsights/alertRules/* (Manage alert rules)
- Microsoft.SecurityInsights/incidents/* (Manage incidents)
- Microsoft.OperationalInsights/workspaces/* (Manage the connected Log Analytics workspace)



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

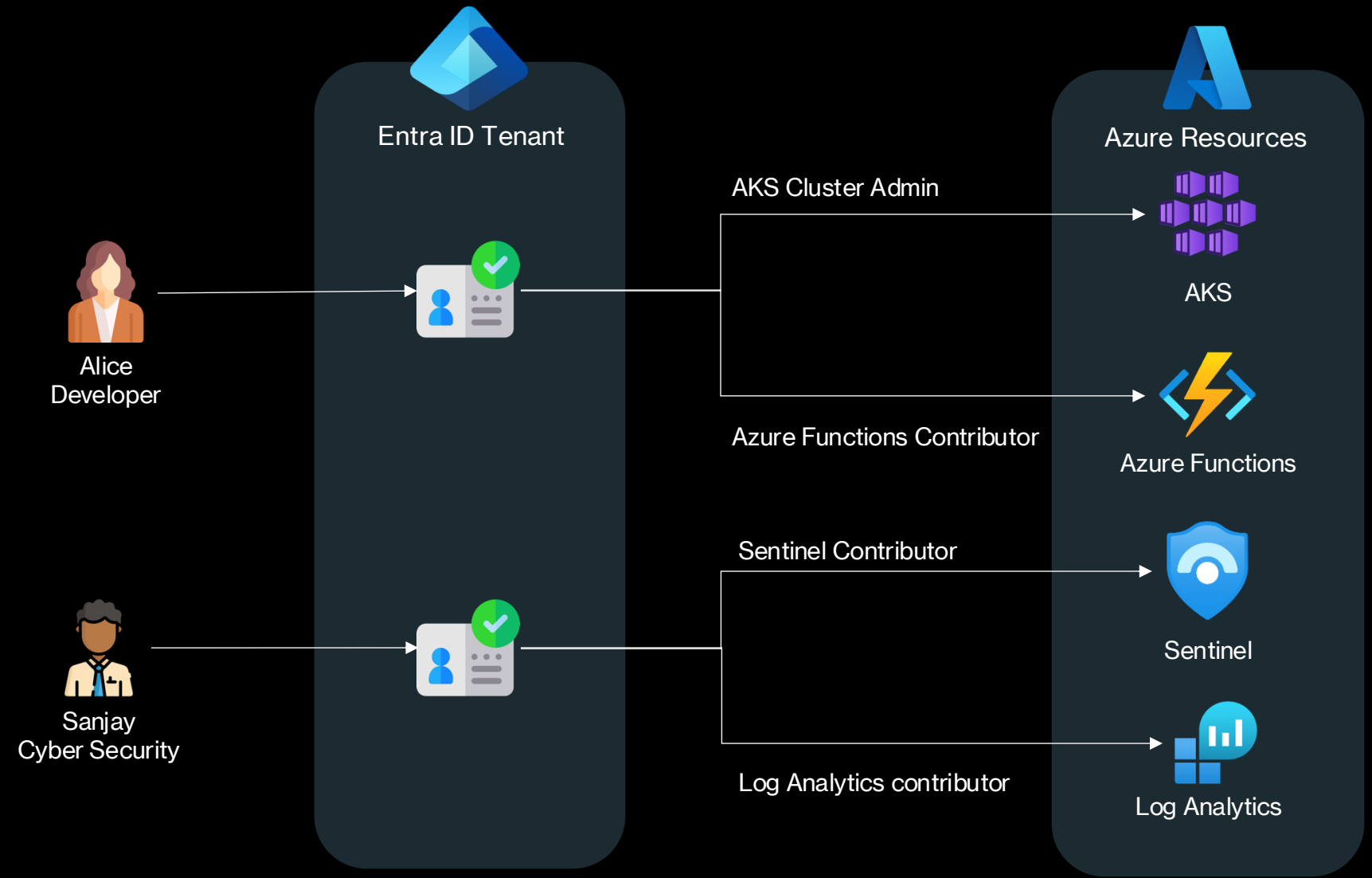
# Azure RBAC – Scope

- The Scope determines where the role applies. It defines the boundary where the security principal can access resources based on the assigned role. Scopes can be at different levels:
  - **Management Group:** Access applies across all resources in management group.
  - **Subscription:** Access applies across all resources in the subscription.
  - **Resource Group:** Access applies to all resources in a specific resource group.
  - **Resource:** Access applies to a specific resource, such as a Log Analytics workspace.



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure Role-Based Access Control (RBAC)




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC Custom Roles

- Custom RBAC roles come into play when you need more granular control over permissions, allowing you to define exactly what actions a user or group can perform on Azure resources. Custom roles allow you to:
  - Combine specific permissions from multiple built-in roles.
  - Tailor permissions to very specific tasks that built-in roles might not accommodate.
  - Avoid giving users more permissions than they need (following the principle of least privilege).



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC Custom Roles

- Imagine a **Security Operations Center (SOC)** for an organization that is responsible for monitoring, detecting, and responding to security incidents across the enterprise.
- Different teams within the SOC (such as threat hunters, incident responders, and SOC analysts) will need access to different sets of resources and actions in Azure, but the built-in roles may be too broad for their specific needs.
- To meet the needs of both teams while following the principle of least privilege, you can create custom roles for each team.



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC Custom Roles

The SOC Threat Hunter needs:

- Access to Sentinel Hunting queries.
- Ability to read security incidents but not manage them.
- No permissions to alter Sentinel configuration or automation rules.

```
{
  "Name": "SOC Threat Hunter",
  "IsCustom": true,
  "Description": "Role for SOC Threat Hunters to perform threat hunting in Senti
  "Actions": [
    "Microsoft.SecurityInsights/huntingQueries/read",
    "Microsoft.SecurityInsights/huntingQueries/results/read",
    "Microsoft.SecurityInsights/incidents/read",
    "Microsoft.OperationalInsights/queryResults/read",
    "Microsoft.OperationalInsights/workspaces/read"
  ],
  "NotActions": [
    "Microsoft.SecurityInsights/alertRules/write",
    "Microsoft.SecurityInsights/automationRules/write",
    "Microsoft.SecurityInsights/incidents/write"
  ],
  "AssignableScopes": [
    "/subscriptions/{subscription-id}/resourceGroups/{resource-group-id}/provide
  ]
}
```



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC Custom Roles

| | | |
|---|---|---|
|  | Granular Control | Custom RBAC allows you to define very specific permissions, ensuring that users only have access to exactly what they need, minimizing the risk of over-permissioning. |
|  | Tailored to Business Needs | It enables the creation of roles that match unique business or operational needs, which built-in roles may not address fully. |
|  | Enhanced Security and Compliance | By assigning least privilege access through custom roles, you improve security posture and ensure compliance with regulatory standards that mandate limited access. |
|  | Complexity in Management | Managing many custom roles across different users or groups can become complex, leading to potential confusion about who has access to what resources. |
|  | Maintenance Overhead | As your environment changes or grows, keeping custom roles updated with new services or permissions can require ongoing effort and updates. |
|  | Potential for Misconfiguration | Creating overly restrictive or permissive custom roles can lead to issues where users either can't perform their tasks or have more access than intended, which can introduce security risks. |

Christopher Nett

# Azure RBAC vs. Entra ID Roles - Scope

**Azure RBAC:** 

- Scope: Azure RBAC is primarily used to manage access to Azure resources such as virtual machines, storage accounts, databases, and networking components.
- Purpose: It controls who can perform actions like reading, writing, or managing specific resources in the Azure Resource Manager (ARM) environment.
- Example: Assigning a user the "Contributor" role to manage an Azure Virtual Machine.

**Entra ID Roles:** 

- Scope: Entra ID roles are used to manage access to directory-level features and services within Entra ID
- Purpose: These roles focus on identity and access management tasks like managing users, groups, applications, and directory settings.
- Example: Assigning a user the "Global Administrator" role to manage user accounts and groups in Entra ID.



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC vs. Entra ID Roles – Resource Targets

**Azure RBAC:** 

- Targets Azure resources like databases, VMs, networking resources, and storage within a specific subscription or resource group.
- It defines actions such as read, write, delete for specific Azure services.

**Entra ID Roles:** 

- Targets identity-related resources within the Entra ID tenant, such as users, groups, service principals, policies, and roles.
- Defines permissions related to managing user identities, security policies, and authentication settings.



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

# Azure RBAC vs. Entra ID Roles – Resource Targets

| Feature | Azure RBAC | Entra ID Roles |
|---|---|---|
| Scope | Azure resources (VMs, Storage, etc.) | Identity management (users, groups) |
| Purpose | Manage access to Azure services | Manage Entra ID/AD directory features |
| Targeted Resources | Virtual machines, databases, etc. | Users, groups, applications, policies |
| Common Roles | Contributor, Reader, Owner | Global Admin, User Admin, Security Admin |
| Granularity | Resource-level permissions | Tenant-wide permissions |
| Common Use Case | Assign resource-specific permissions | Assign directory-wide administrative tasks |
| Where It's Used | Azure Subscription/Resource Groups | Entra ID |



Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview#how-azure-rbac-works

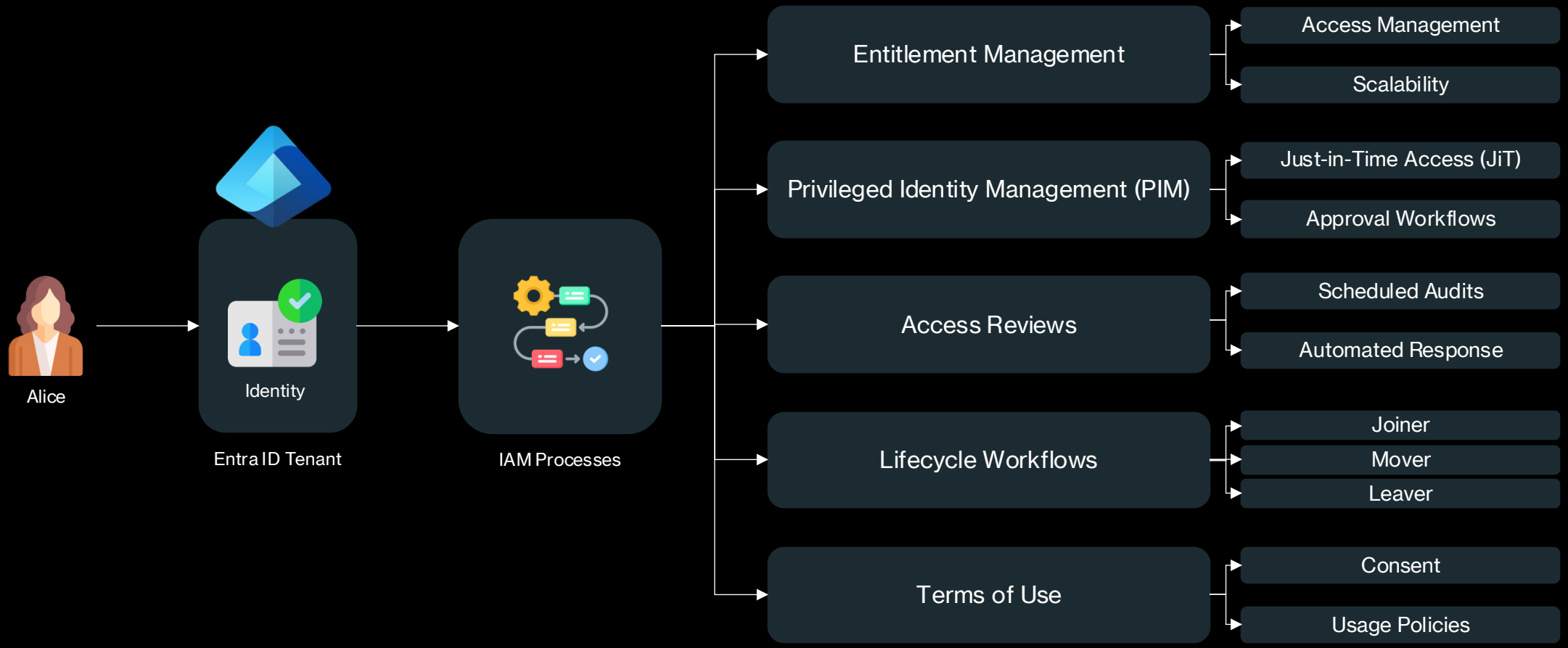
# Microsoft Entra ID Governance

| | |
|---|---|
| Market Challenge | Managing user identities, permissions and entitlements across various IT environments |
| Purpose | Ensuring that the right people have the right access to the right resources at the right time |
| Features | Govern the identity lifecycle |
| | Govern the access lifecycle |
| | Secure privileged access for administration |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview

# Entra ID Governance






Source: https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview

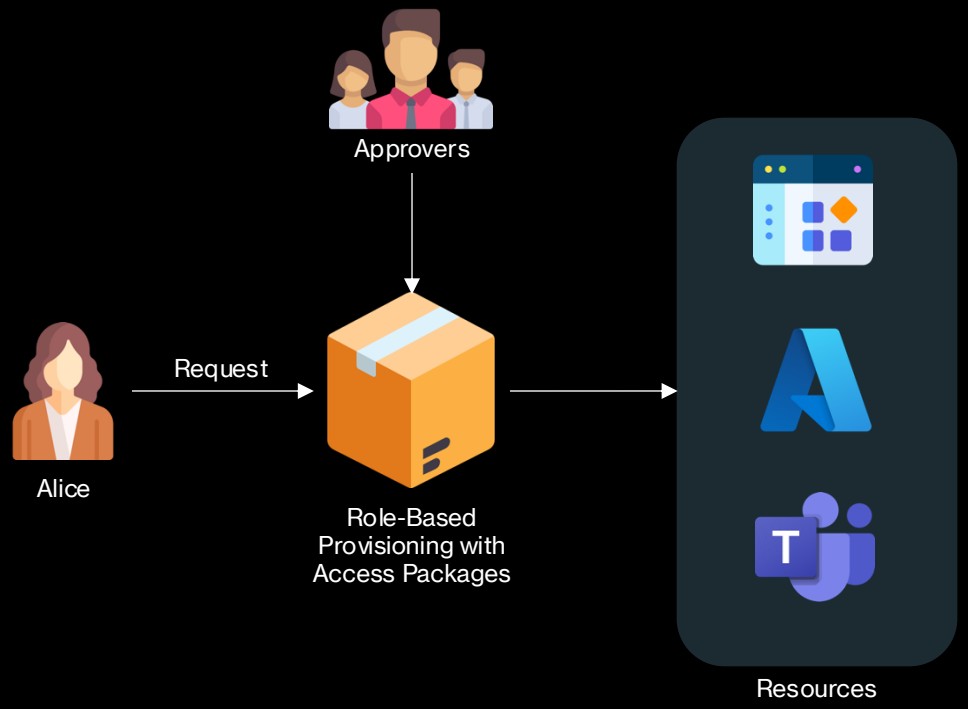
# Entra ID Entitlement Management

- Entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.
- People in organizations need access to various groups, applications, and SharePoint Online sites to perform their job.
- Managing this access is challenging, as requirements change. New applications are added or users need more access rights.
- This scenario gets more complicated when you collaborate with outside organizations. You might not know who in the other organization needs access to your organization's resources, and they won't know what applications, groups, or sites your organization is using.



Source: https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview

# Entra ID Entitlement Management




- Identities can be internal or external
- Collections are used to manage resources and access packages
- Licenses are required for for all reviewers, approvers and requestors



Source: https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview

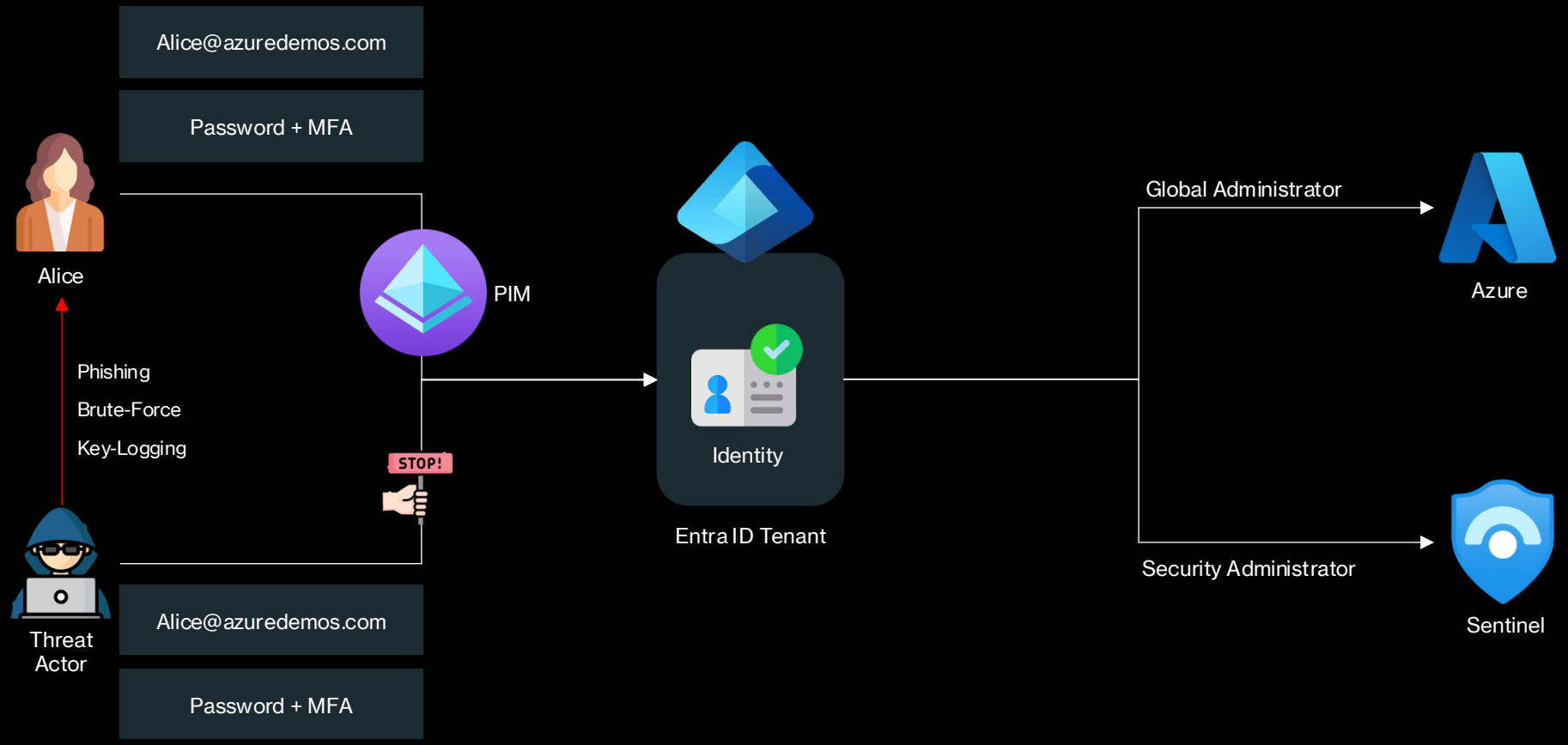
# Entra ID Privileged Identity Management (PIM)

- Privileged Identity Management (PIM) is a service in Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization.
- These resources include resources in Microsoft Entra ID, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.



Source: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

# Entra ID Privileged Identity Management (PIM)




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

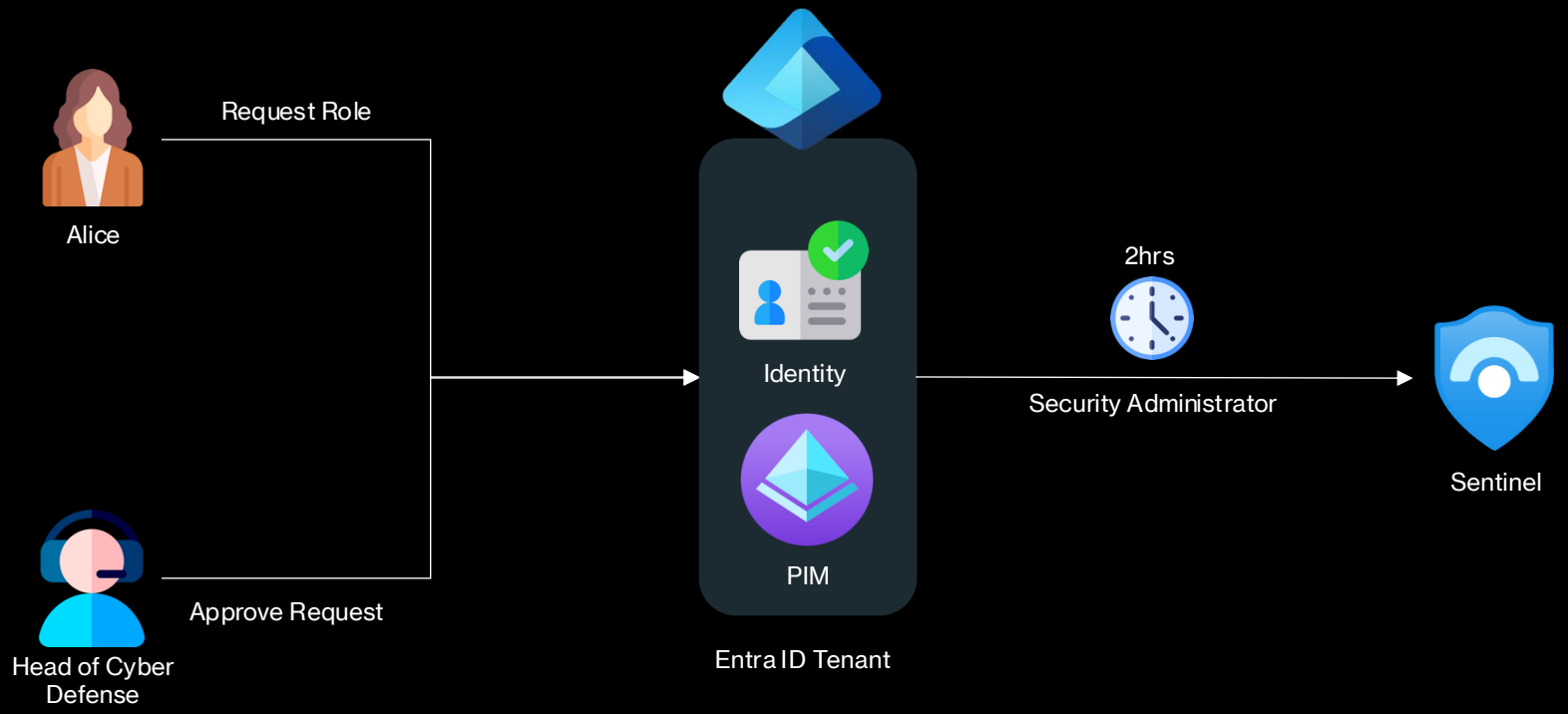
# Entra ID Privileged Identity Management (PIM)

- Provide **just-in-time privileged access** to Microsoft Entra ID and Azure resources
- Assign **time-bound access** to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multifactor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit
- Prevents removal of the last active **Global Administrator** and **Privileged Role Administrator** role assignments



Source: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

# Entra ID Privileged Identity Management (PIM)




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

# Entra ID Privileged Identity Management (PIM)

## Important Considerations

- **Just-in-Time Access:** Implement just-in-time (JIT) access to reduce exposure to security risks by granting elevated privileges only when needed, minimizing standing admin rights.
- **Approval Workflows:** Establish approval workflows for role activation to ensure that privileged access is granted only after appropriate oversight, adding a layer of security and accountability.
- **Time-Bound Role Assignments:** Use time-bound assignments to limit the duration of elevated privileges, ensuring that users only have access for a specific, predefined period.
- **Access Reviews and Auditing:** Regularly conduct access reviews and utilize detailed auditing capabilities to monitor who has privileged access, how often it’s used, and whether it's still necessary.
- **Security Alerts and Notifications:** Set up real-time alerts and notifications for key activities in PIM, such as role activation or suspicious behavior, to quickly detect and respond to potential security incidents.



Source: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

# Access Reviews 

- Access reviews in Microsoft Entra ID, part of Microsoft Entra, enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.
- User access can be reviewed regularly to make sure only the right people have continued access.
- Microsoft Entra ID enables you to collaborate with users from inside your organization, and with external users.
- Users can join groups, invite guests, connect to cloud apps, and work remotely from either their work or personal devices.
- The convenience of using self-service has led to a need for better access management capabilities.



Source: https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

# Access Reviews 

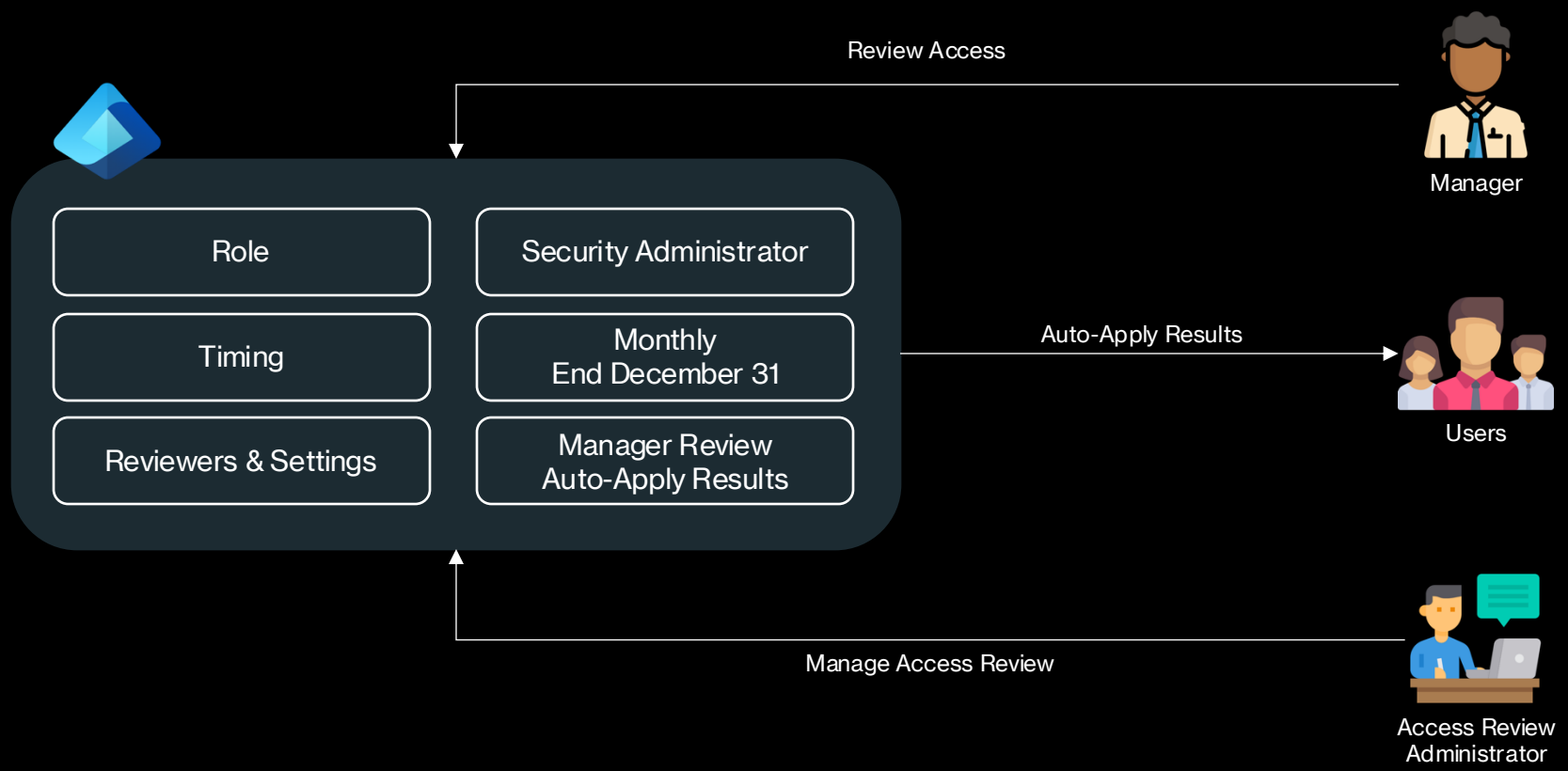
Why are access reviews important?

- As new employees join, how do you ensure they have the access they need to be productive?
- As people move teams or leave the company, how do you make sure that their old access is removed?
- Excessive access rights can lead to compromises.
- Excessive access right can also lead audit findings as they indicate a lack of control over access.
- You have to proactively engage with resource owners to ensure they regularly review who has access to their resources.



Source: https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

# Access Reviews




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

# Access Reviews

| | |
|---|---|
| Entra ID Roles | Review active and eligible assignments for Entra ID roles |
| Applications | Review internal and external guest user access to applications |
| Azure RBAC | Review active and eligible assignments for Azure RBAC roles |
| Teams and Groups | Review membership and guests for groups and teams |



Source: https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

# Microsoft Entra Permissions Management (EPM)

| | |
|---|---|
| Market Challenge | There are over 40.000 permissions that can be granted across Azure, AWS and GCP. Identities are only using 1% of permissions granted. |
| Purpose | A cloud infrastructure entitlement management (CIEM) product that provides visibility and control over permissions for any identity and any resource in Azure, AWS and GCP. |
| Features | Visibility of permissions across Azure, AWS and CGP |
| | Permission control and enforcement |
| | Automated permissions monitoring |

Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/permissions-management/overview

# Entra Permissions Management

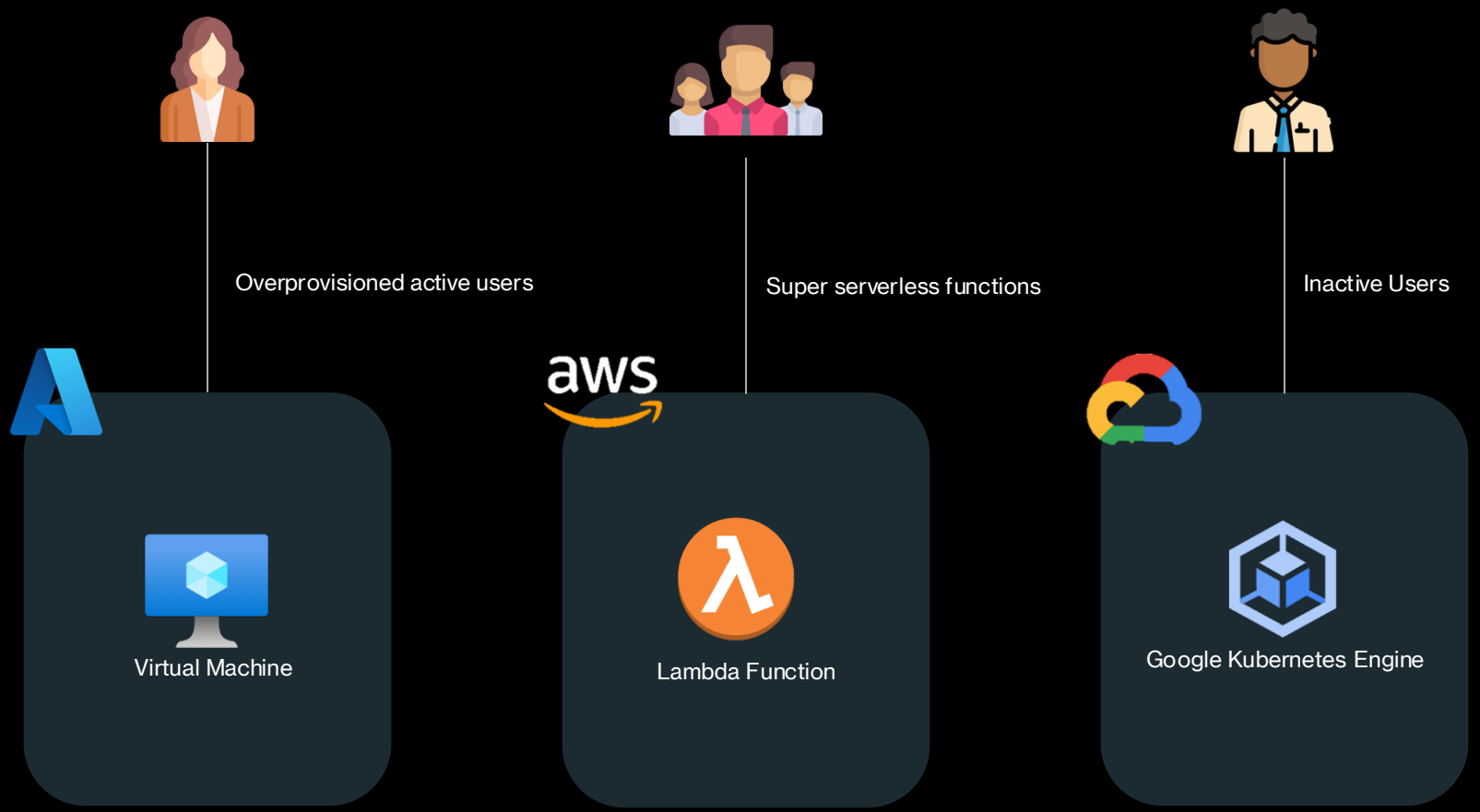
Organizations have to consider permissions management as a central piece of their Zero Trust security to implement least privilege access across their entire infrastructure:

- Organizations are increasingly adopting multicloud strategy and are struggling with the lack of visibility and the increasing complexity of managing access permissions.
- With the growth of identities and cloud services, the number of high-risk cloud permissions is exploding, expanding the attack surface for organizations.
- IT security teams are under increased pressure to ensure access to their expanding cloud estate is secure and compliant.
- The inconsistency of cloud providers' native access management models makes it even more complex for Security and Identity to manage permissions and enforce least privilege access policies across their entire environment.



Source: https://learn.microsoft.com/en-us/entra/permissions-management/overview

# Entra Permissions Management




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/architecture/permissions-manage-ops-guide-alerts

# Entra Permissions Management

## Discover

You can assess permission risks by evaluating the gap between permissions granted and permissions used

- Cross-cloud permissions discovery
- Permission Creep Index (PCI
- Permission usage analytics

## Remediate

You can right-size permissions based on usage, grant new permissions on-demand, and automate just-in-time access for cloud resources

- Automated deletion of permissions unused for the past 90 days.
- Permissions on-demand:

## Monitor

You can detect anomalous activities with machine learning-powered (ML-powered) alerts and generate detailed forensic reports

- ML-powered anomaly detections.
- Context-rich forensic reports around identities, actions, and resources
- Get comprehensive visibility: Discover which identity is doing what, where, and when.
- Automate least privilege access:
- Unify access policies across infrastructure as a service (IaaS) platforms



Source: https://learn.microsoft.com/en-us/entra/permissions-management/overview

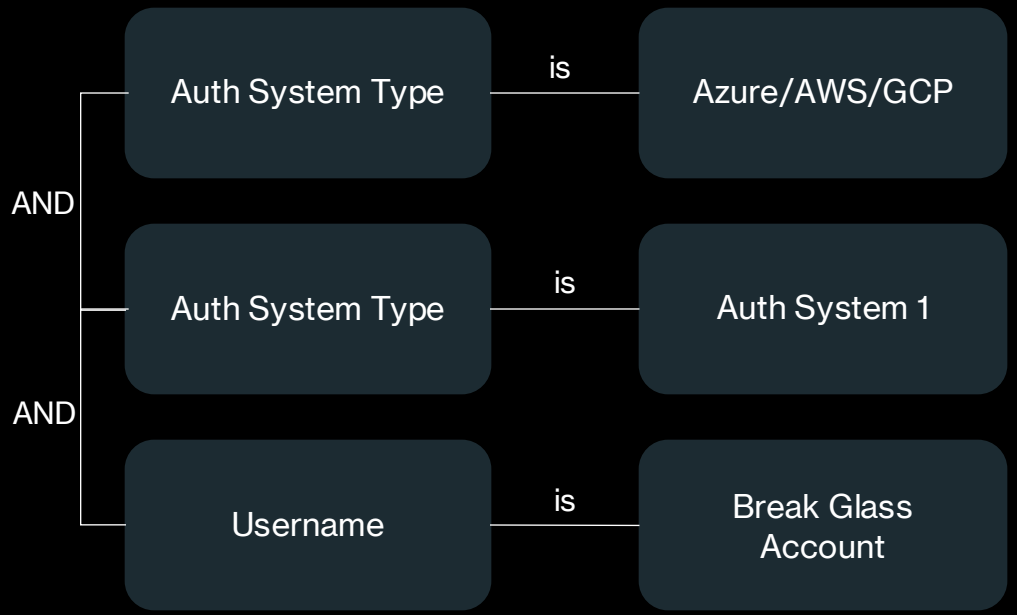
# Entra Permissions Management

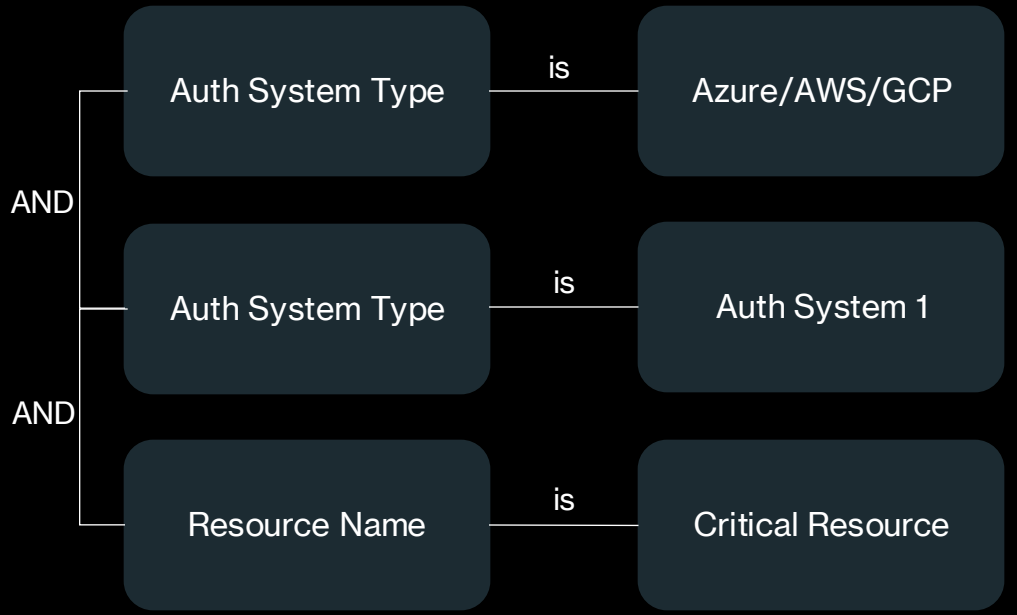
- There are four types of alerts:
  - Statistical anomaly
  - Rule-based anomaly
  - Permission analytics
  - Activity



Source: https://learn.microsoft.com/en-us/entra/architecture/permissions-manage-ops-guide-alerts

# Entra Permissions Management






Source: https://learn.microsoft.com/en-us/entra/architecture/permissions-manage-ops-guide-alerts

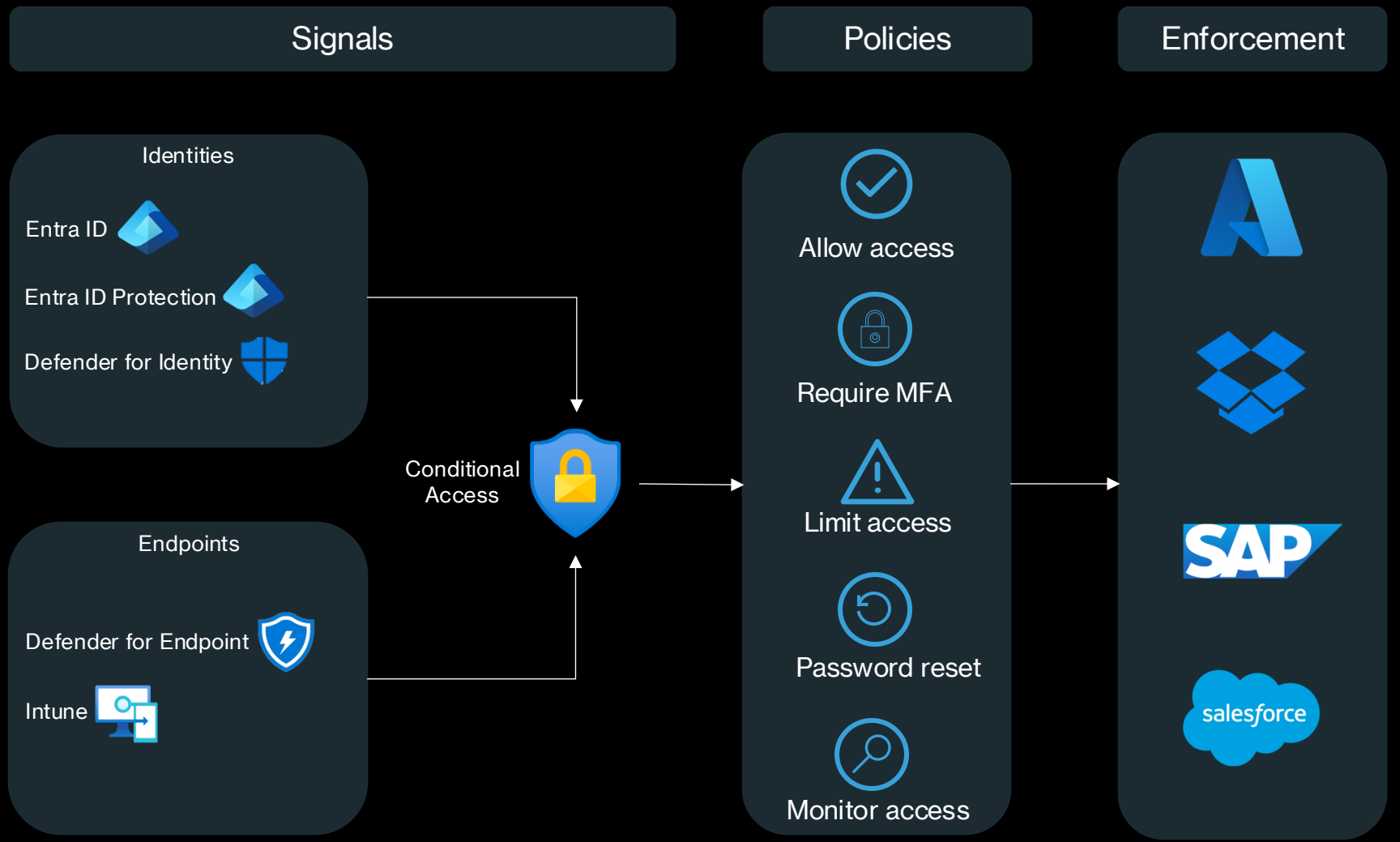
# Entra ID Conditional Access 

- Conditional Access is a feature of Microsoft Entra that enforces access controls based on user and device conditions.
- It evaluates signals like user location, device compliance, and risk levels before granting access to resources.
- Policies can be set to allow, block, or require additional authentication (e.g., MFA) based on specific conditions.
- Conditional Access helps secure access to cloud and on-premises resources by applying adaptive security measures.
- It enables organizations to implement a Zero Trust security model by ensuring only the right people and devices access critical data.



Source: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

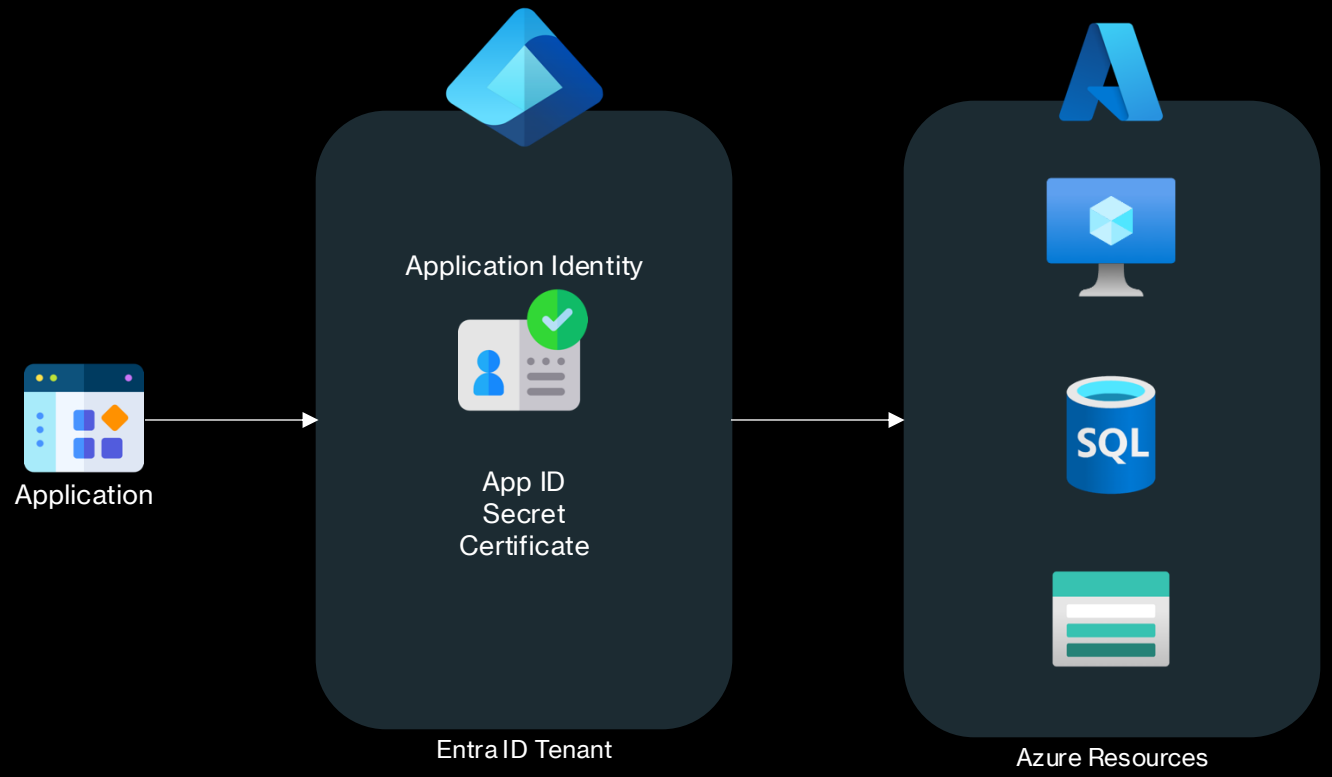
# Entra ID Conditional Access




Christopher Nett

Source: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

# Application Identities




Considerations:

- The application can be anywhere, even outside of Azure
- Applications must be registered within the Entra ID tenant
- Authentication can be done via secret or certificate



Source: https://learn.microsoft.com/en-us/entra/identity-platform/howto-create-service-principal-portal

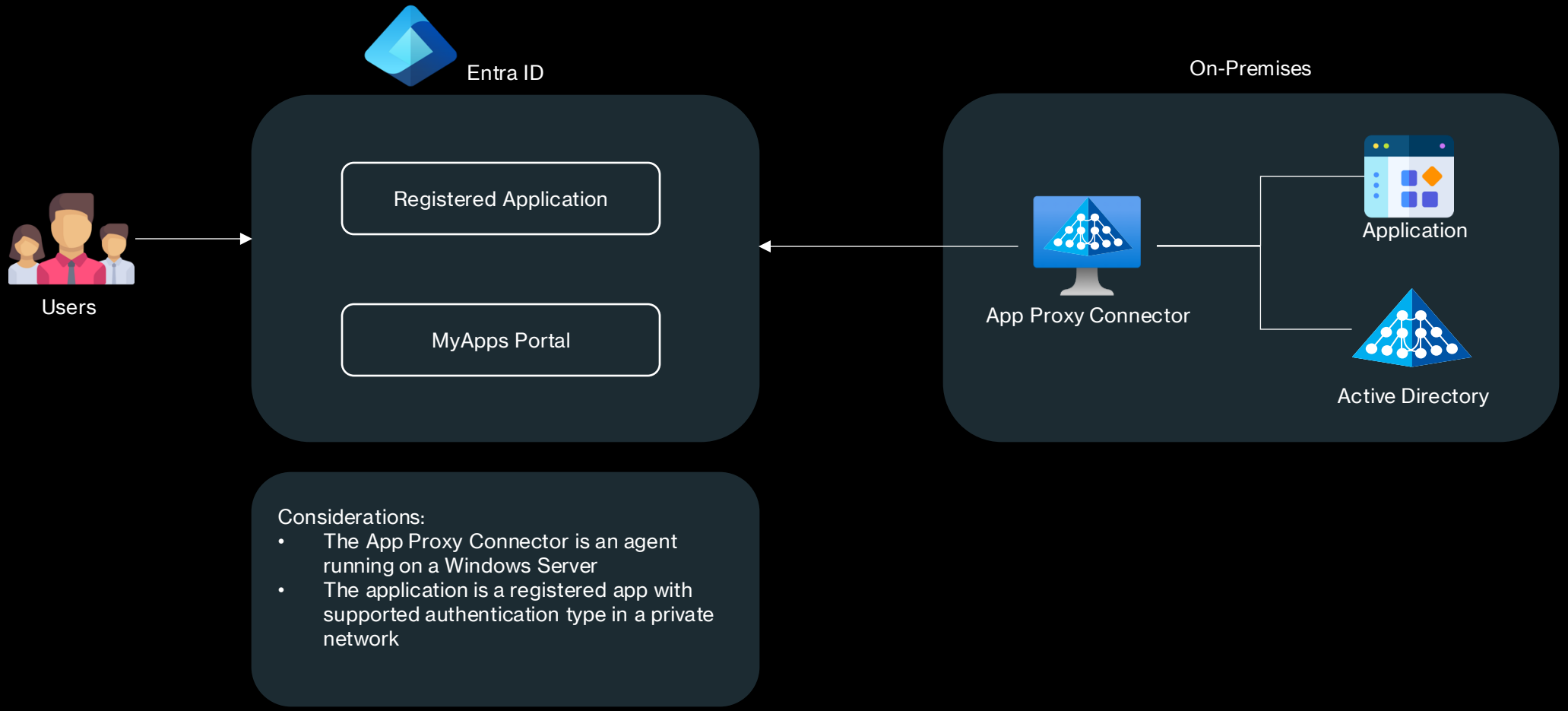
# Entra Application Proxy

- Microsoft Entra application proxy provides secure remote access to on-premises web applications.
- After a single sign-on to Microsoft Entra ID, users can access both cloud and on-premises applications through an external URL or an internal application portal.
- Microsoft Entra application proxy is:
  - **Simple to use**. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Microsoft Entra ID. You don't need to change or update your applications to work with application proxy.
  - **Secure**. On-premises applications can use Azure's authorization controls and security analytics. For example, on-premises applications can use Conditional Access and two-step verification. Application proxy doesn't require you to open inbound connections through your firewall.
  - **Cost-effective**. On-premises solutions typically require you to setup and maintain demilitarized zones (DMZs), edge servers, or other complex infrastructures. Application proxy runs in the cloud, which makes it easy to use. To use application proxy, you don't need to change the network infrastructure or install more appliances in your on-premises environment.



Source: https://learn.microsoft.com/en-us/entra/identity/app-proxy/overview-what-is-app-proxy

# Entra Application Proxy



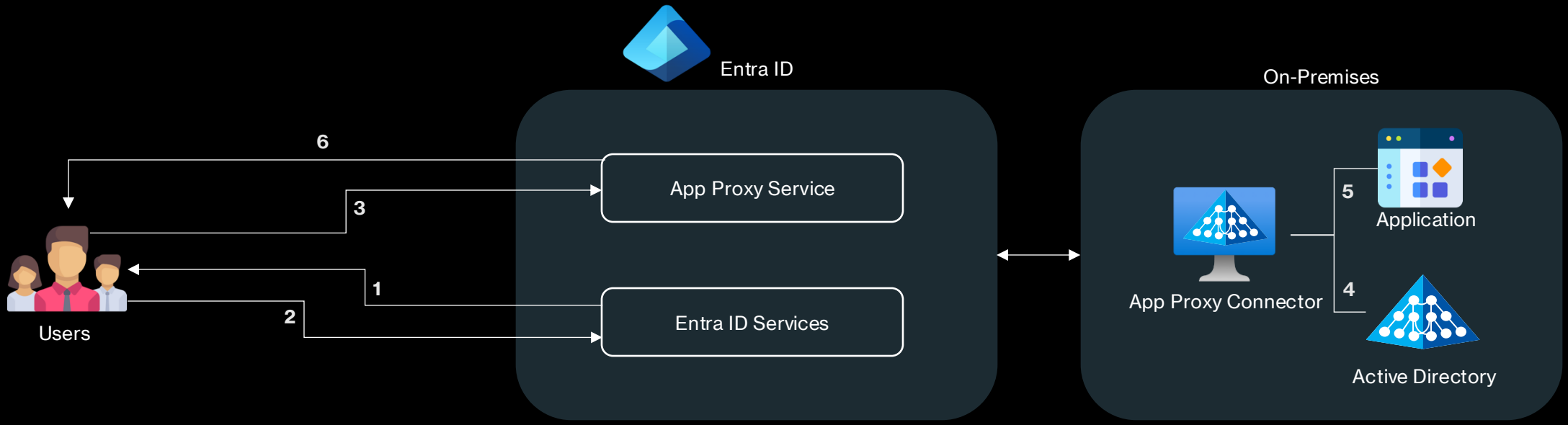

Considerations:

- The App Proxy Connector is an agent running on a Windows Server
- The application is a registered app with supported authentication type in a private network



Source: Remote access to on-premises apps - Microsoft Entra application proxy - Microsoft Entra ID | Microsoft Learn

# Entra Application Proxy




1. A user is directed to the Microsoft Entra sign-in page after accessing the application through an endpoint.
2. Microsoft Entra ID sends a token to the user's client device after a successful sign-in.
3. The client sends the token to the application proxy service. The service retrieves the user principal name (UPN) and security principal name (SPN) from the token. Application proxy then sends the request to the connector.
4. The connector performs single sign-on (SSO) authentication required on behalf of the user.
5. The connector sends the request to the on-premises application.
6. The response is sent through the connector and application proxy service to the user.



Source: Remote access to on-premises apps - Microsoft Entra application proxy - Microsoft Entra ID | Microsoft Learn

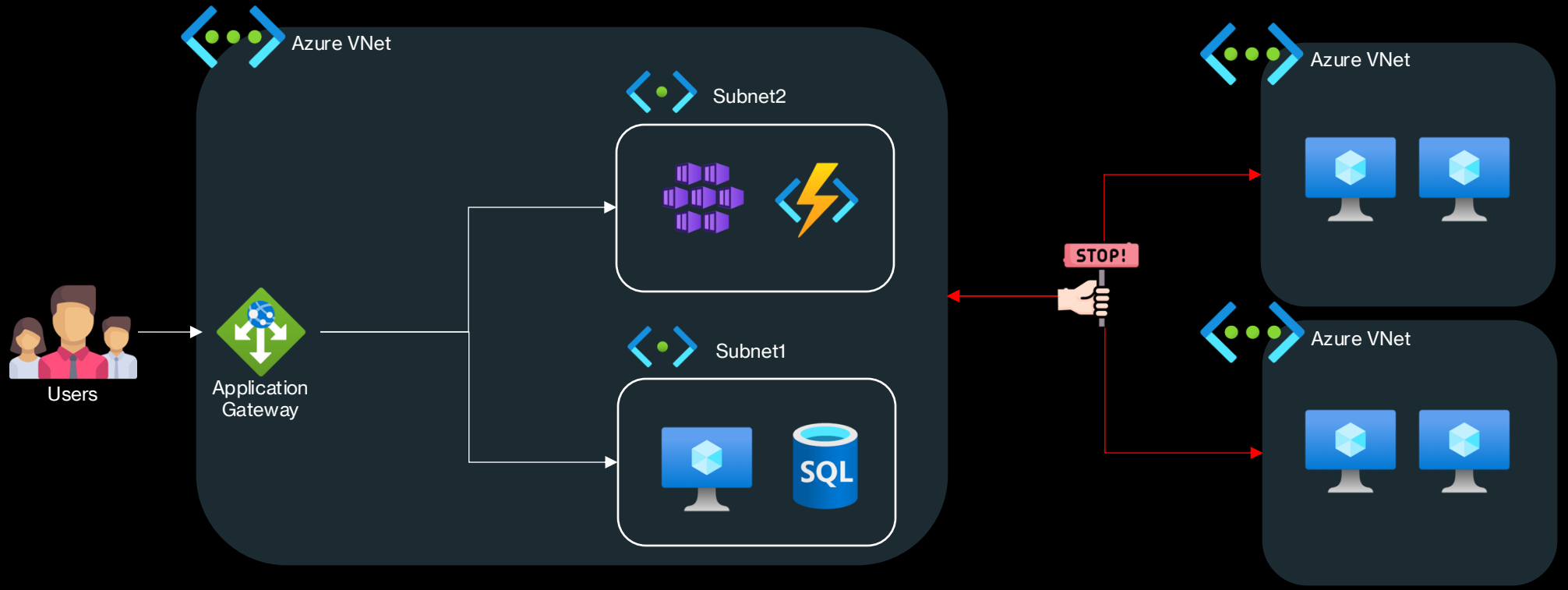
# Azure Virtual Networks (Vnets)

- Core Components of an Azure Vnet:
  - **Virtual Network:** An Azure Virtual Network (VNet) is a logically isolated network in the cloud where resources can securely communicate with each other, the internet, and on-premises networks.
  - **Subnets:** Subnets divide a VNet into smaller, manageable segments, each with its own range of IP addresses, allowing for more precise control of traffic flow and security.
  - **Network Interface:** A Network Interface (NIC) connects a virtual machine (VM) to a VNet, enabling communication within the network using a designated IP address.



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

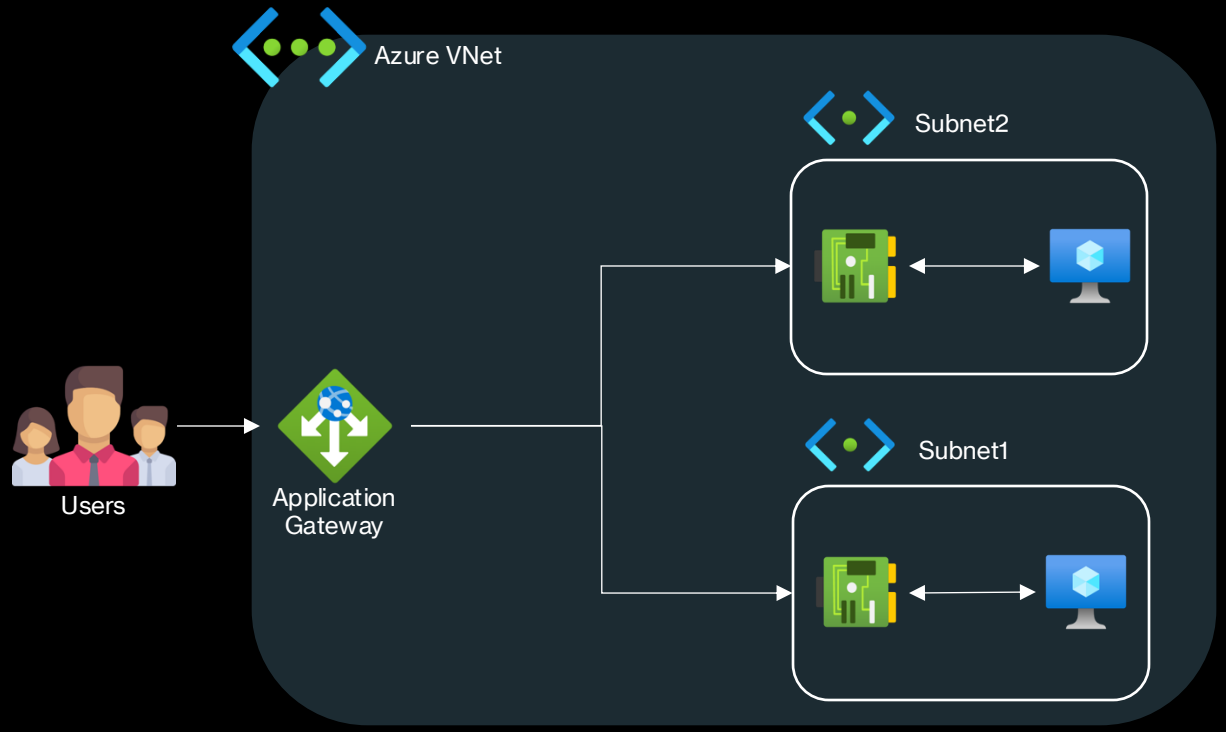
# Azure Virtual Networks (Vnets)






Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

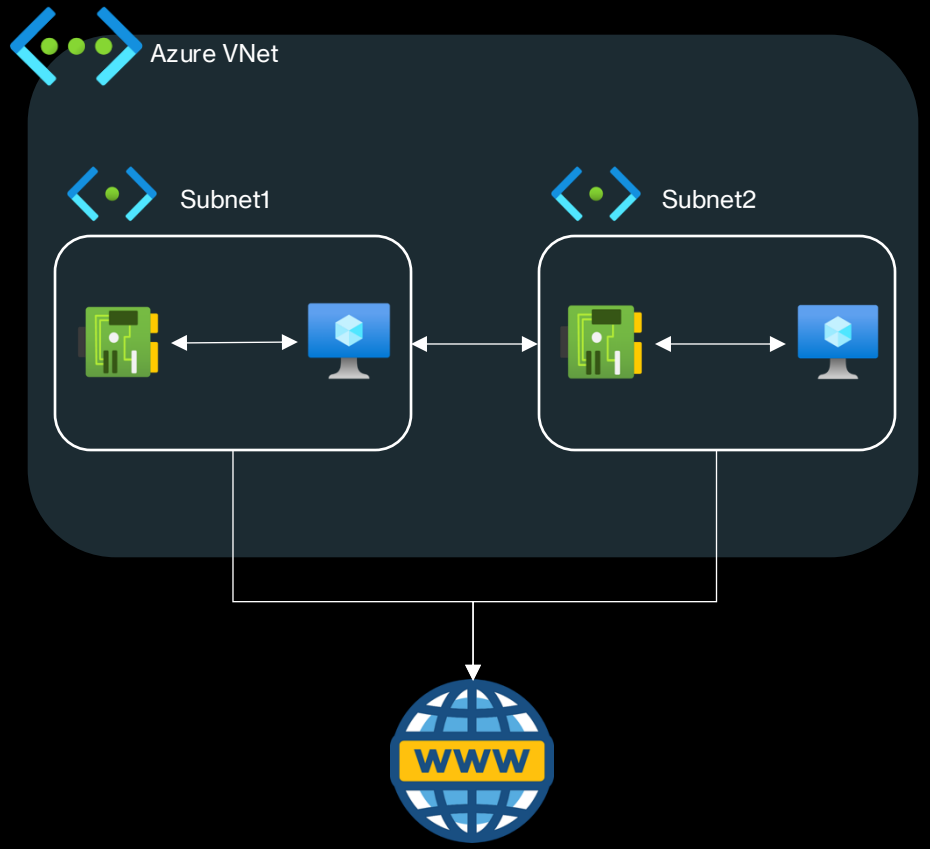
# Azure Virtual Networks (Vnets)






Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

# Azure Virtual Networks (Vnets) – Default Routes




Default Routes:

- Connectivity to the internet
- Connectivity between subnets
- Resource connectivity (e.g. VNet Peering, VPN, ...)



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

# Azure Virtual Networks (Vnets)

Further considerations:

- Protocols: TCP, UDP, ICMP and Unicast are supported.
- DNS: Azure provides DNS for you but you can also use custom DNS servers.
- IP Addressing: IPV4 and IPV6 are supported. IPV4 supports subnet ranges from /2 to /29, while IPV6 supports /64 subnets only.



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

# Network Security Groups (NSGs) 

- Filter inbound and outbound traffic
- Can be attached to a VM a subnet or both
- Based on a 5-Tuple:
  - Source IP Address
  - Destination IP Address
  - Source Port
  - Destination Port
  - Protocol (TCP or UDP)
- NSGs are stateful!



Source: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

# NSG Default rules

## Inbound

| Name | Priority | Source IP | Source Port | Destination IP | Destination Port | Protocol | Access |
|---|---|---|---|---|---|---|---|
| ALLOW VNET INBOUND | 65000 | VIRTUAL_NETWORK | * | VIRTUAL_NETWORK | * | * | ALLOW |
| ALLOW AZURE LOAD BALANCER INBOUND | 65001 | AZURE_LOADBALANCER | * | * | * | * | ALLOW |
| DENY ALL INBOUND | 65500 | * | * | * | * | * | DENY |

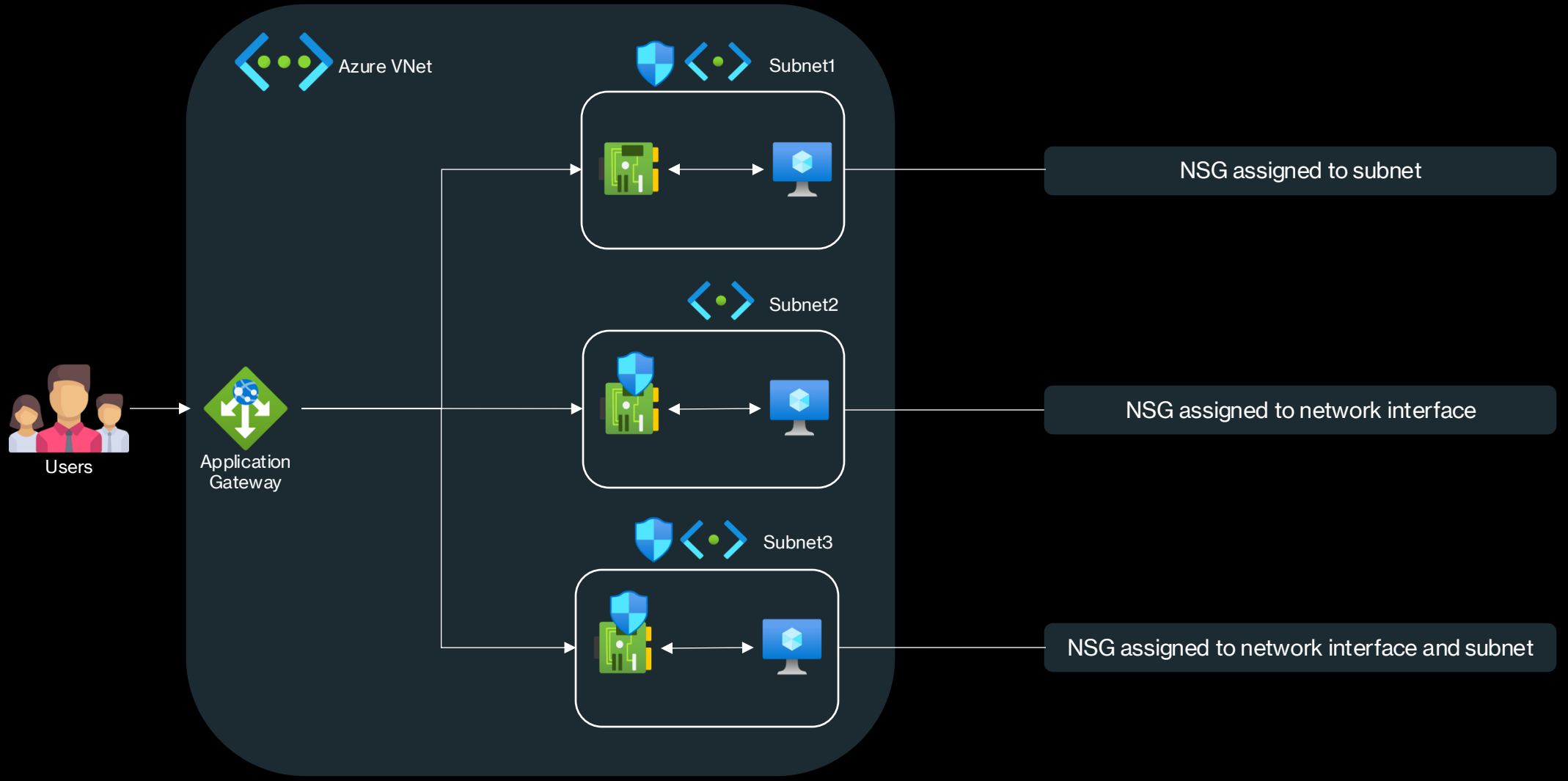
## Outbound

| Name | Priority | Source IP | Source Port | Destination IP | Destination Port | Protocol | Access |
|---|---|---|---|---|---|---|---|
| ALLOW VNET OUTBOUND | 65000 | VIRTUAL_NETWORK | * | VIRTUAL_NETWORK | * | * | ALLOW |
| ALLOW INTERNET OUTBOUND | 65001 | * | * | INTERNET | * | * | ALLOW |
| DENY ALL OUTBOUND | 65500 | * | * | * | * | * | DENY |



Source: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

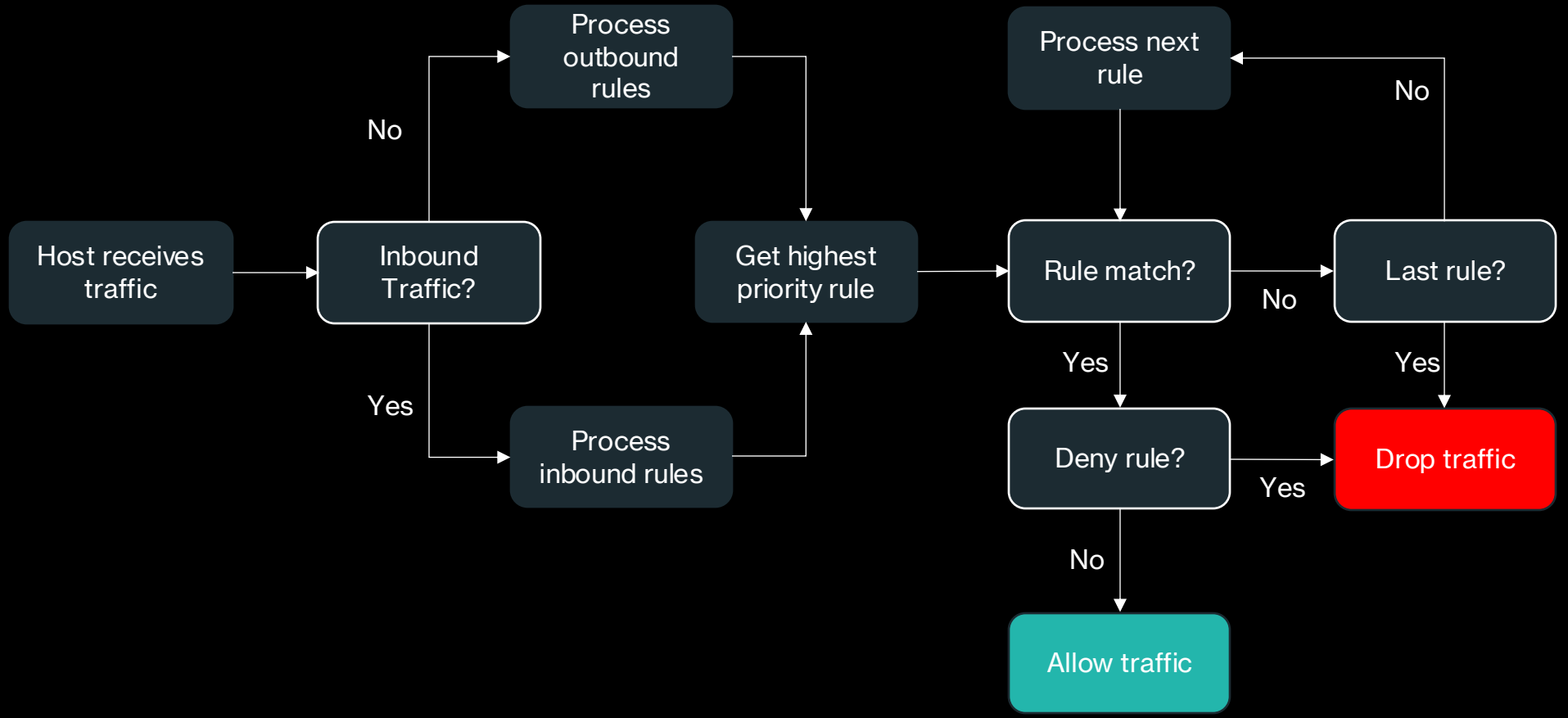
# Network Security Groups (NSGs)




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

# NSG Rule Processing

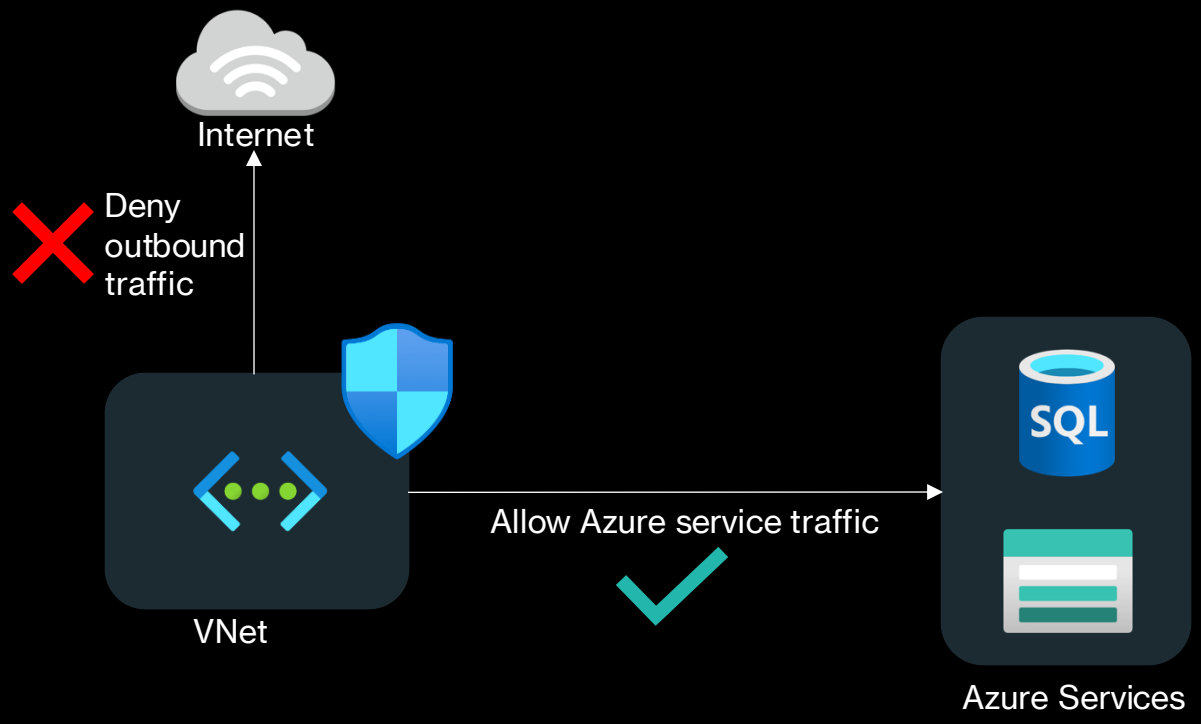





Source: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

# NSG Service Tags

- Restrict traffic to certain Azure services
- IPs for each tag are managed by Azure




| Action | Name | Source | Destination | Port |
|---|---|---|---|---|
| Allow | AllowStorage | **VirtualNetwork** | **Storage** | Any |
| Allow | AllowSQL | **VirtualNetwork** | **Sql.EastUS** | Any |
| Deny | DenyAllOutBound | Any | Any | Any |



Source: Azure service tags overview | Microsoft Learn

# Application Security Groups (ASGs) 

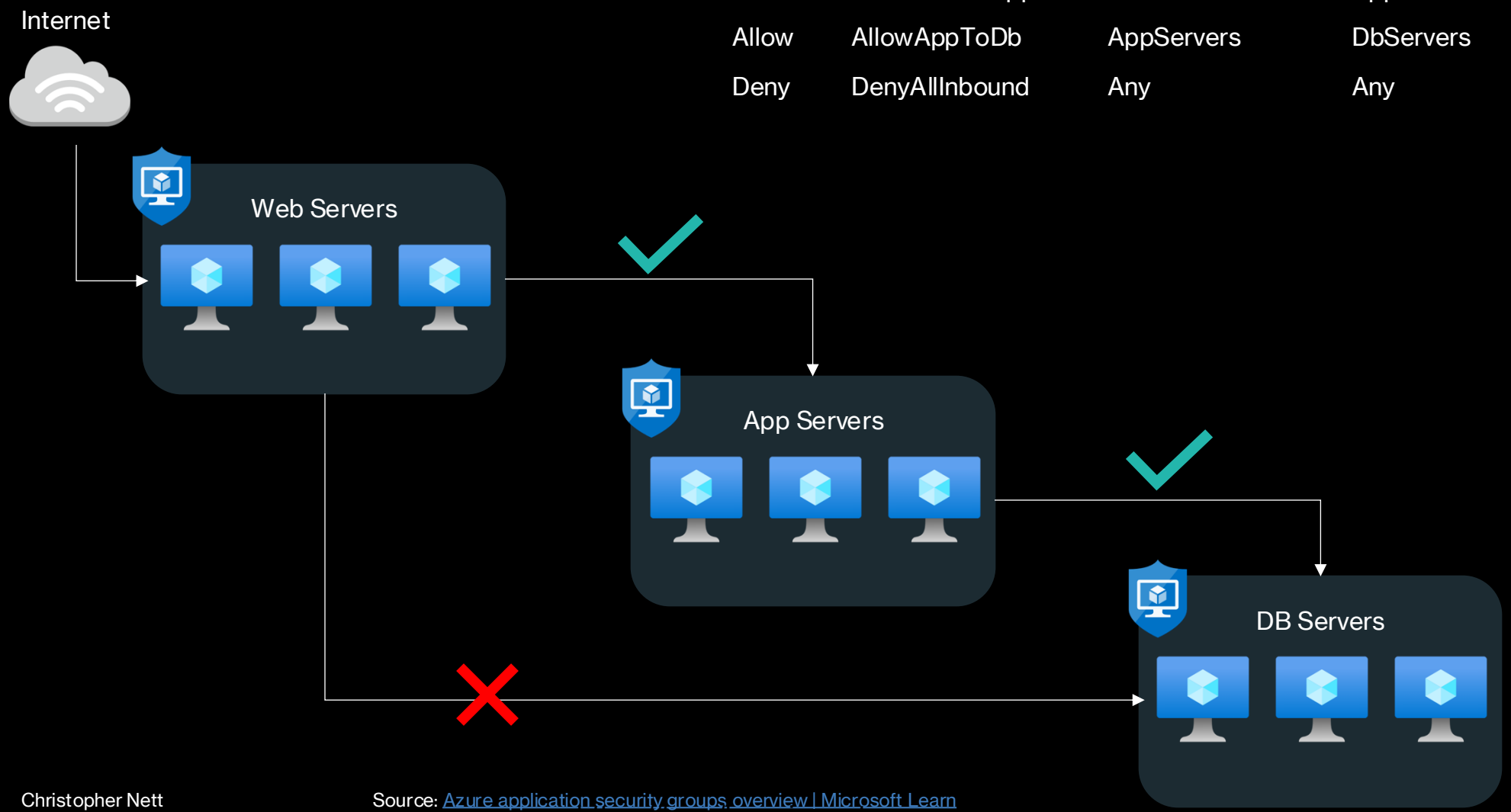
- **Granular Network Segmentation**: ASGs in Azure allow you to group VMs based on their application roles, enabling fine-grained network segmentation. You can easily manage and control network security by applying rules to specific groups of VMs rather than individual instances.
- **Simplified Rule Management**: ASGs simplify the management of NSGs by allowing you to create security rules that target entire groups of VMs instead of specifying individual IP addresses. This reduces the complexity and number of rules in NSGs.
- **Dynamic Scalability**: When new VMs are added to an ASG, they automatically inherit the security rules applied to that group. This dynamic scalability ensures that the security posture remains consistent as your application scales, without the need for manual updates to NSGs.
- **Enhanced Security Posture**: By using ASGs with NSGs, you can create more specific and targeted security rules. This leads to a stronger security posture, as you can define rules that are highly specific to the needs of particular applications or workloads, minimizing the attack surface.
- **Ease of Management and Maintenance**: ASGs provide an easier way to manage and maintain security rules as your infrastructure evolves. You can update security rules across multiple VMs by modifying the ASG, reducing the risk of errors and ensuring consistent security configurations.



Source: Azure application security groups overview | Microsoft Learn

# ASGs

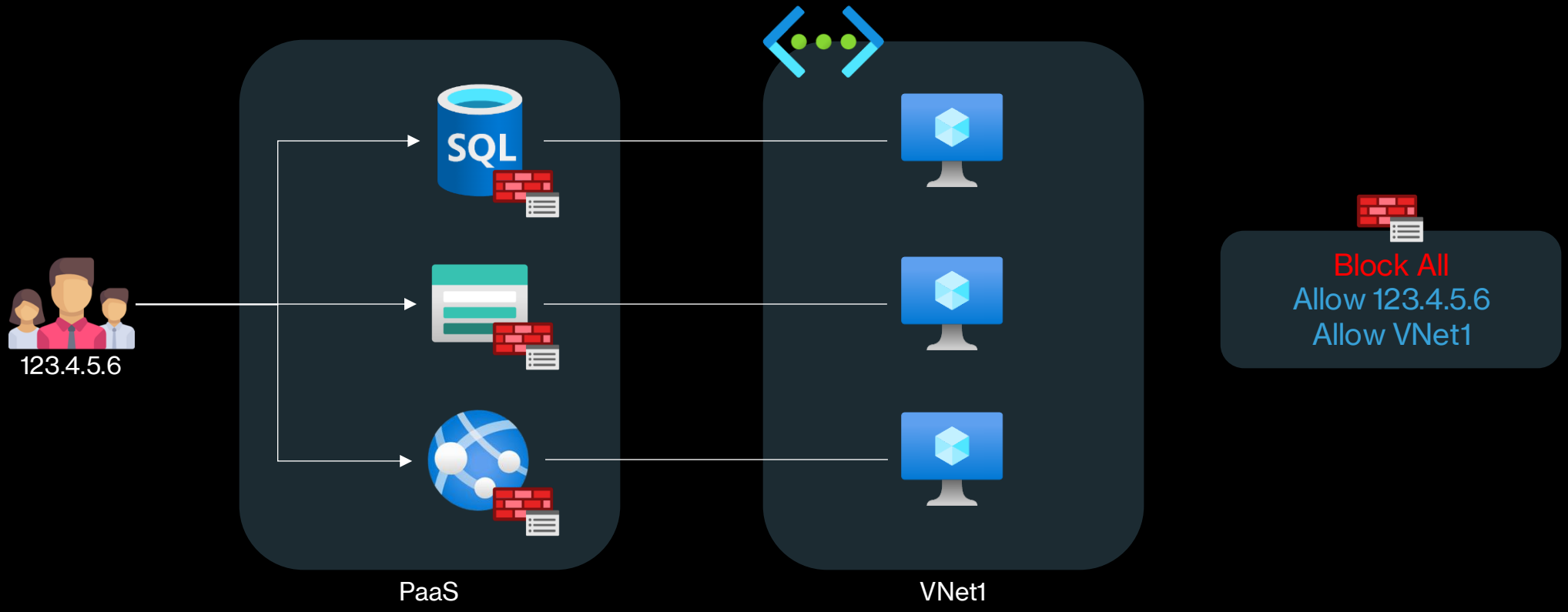
| Action | Name | Source | Destination | Port |
|---|---|---|---|---|
| Allow | AllowInternetToWeb | Internet | WebServers | 80,443 |
| Allow | AllowWebtoApp | WebServers | AppServers | 443 |
| Allow | AllowAppToDb | AppServers | DbServers | 1433 |
| Deny | DenyAllInbound | Any | Any | Any |




Christopher Nett

Source: Azure application security groups overview | Microsoft Learn

# Azure Resource Firewalls






Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

# Routing in Azure

- **System Routes**: Azure automatically creates default system routes for each subnet within a virtual network. These routes handle traffic within the virtual network, to the internet, or drop traffic if it falls within specific reserved IP address ranges. You cannot remove these system routes, but they can be overridden by custom routes.
- **Custom Routes**: Users can create custom (user-defined) routes to override the default system routes or to add additional routing rules. These routes allow more granular control over how traffic is directed within the network, such as routing traffic through a virtual appliance or a specific gateway.
- **Next Hop Types**: Azure uses different "next hop" types to determine the destination for network traffic. These include routing within the virtual network, routing to the internet, directing traffic to a virtual appliance (like a firewall), or dropping the traffic entirely (None). Custom routes allow specifying the next hop type, providing flexibility in traffic management.
- **Routing Priority and Selection**: When Azure routes outbound traffic, it selects the most specific route based on the longest prefix match. If multiple routes are available, Azure prioritizes user-defined routes first, followed by BGP routes, and finally system routes. System routes related to virtual networks and service endpoints may override more specific BGP routes.
- **Service Tags and Exact Match**: Azure allows the use of service tags in custom routes to represent groups of IP addresses associated with Azure services. This reduces complexity in managing IP address changes for services. When multiple routes have matching prefixes, Azure evaluates them in a specific order, giving preference to regional and top-level tags, followed by AzureCloud regional tags.



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

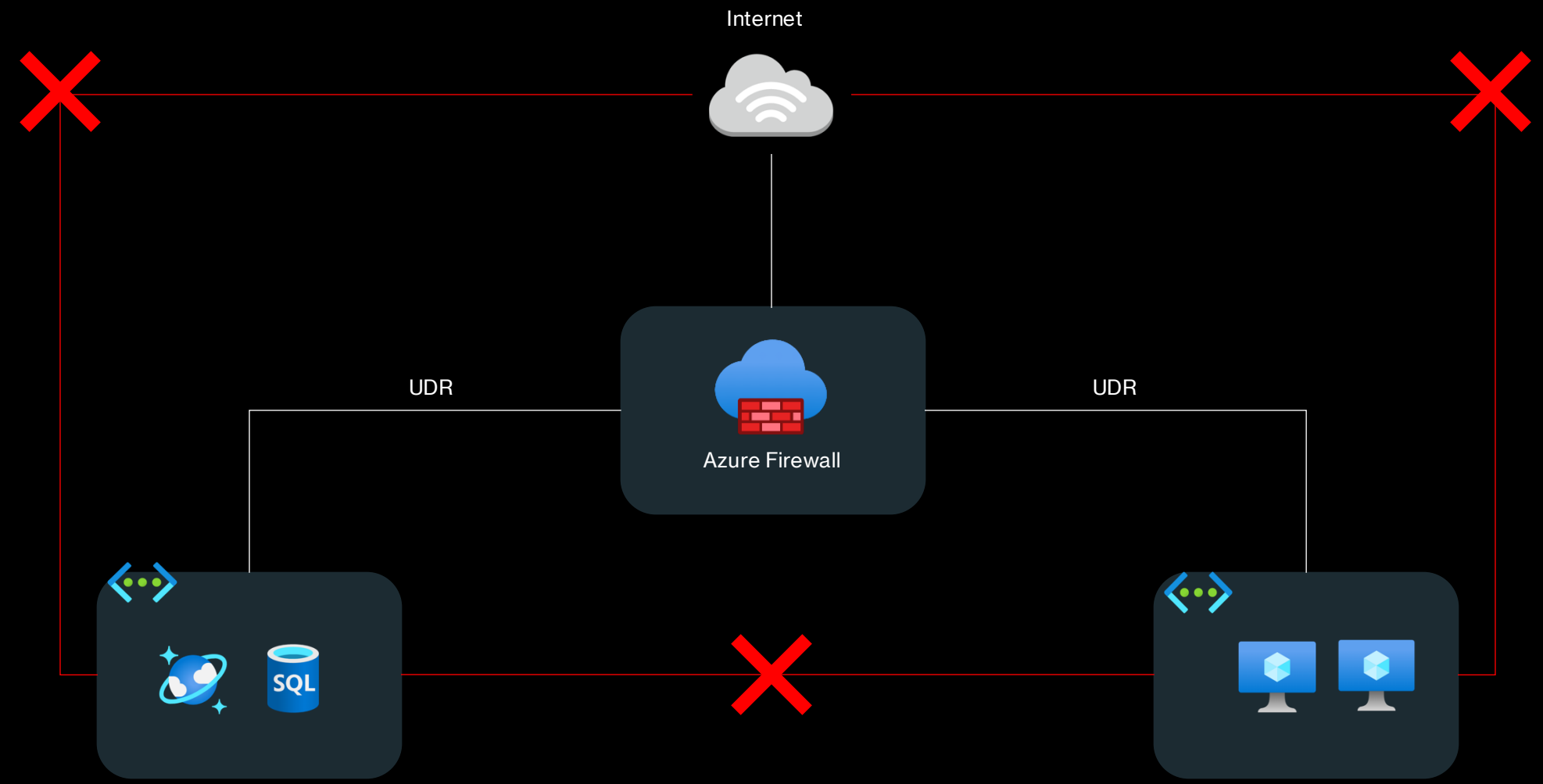
# User Defined Routing (UDR)

- **Customizable Traffic Flow:** UDRs in Azure allow you to customize the flow of network traffic within your virtual networks by specifying specific routing paths. This flexibility is crucial for implementing complex network architectures, such as forcing traffic through network security appliances or specific network virtual appliances (NVAs).
- **Enhanced Security Control:** UDRs enable you to direct traffic through security appliances like firewalls or intrusion detection systems, ensuring that all traffic is inspected and controlled according to your security policies. This adds an additional layer of security beyond standard Azure network configurations.
- **Optimized Network Performance:** By creating UDRs, you can optimize network performance by routing traffic through the most efficient paths. This is particularly useful in multi-tier architectures where different segments of your network might require specialized routing for optimal performance.
- **Avoid Default System Routes:** UDRs allow you to override Azure's default system routes, giving you the ability to create more specific routing rules. This is essential for scenarios where you need to prevent certain traffic from taking specific paths, such as avoiding internet exposure by routing through a private VPN connection.
- **Support for Hybrid and Multi-Cloud Architectures:** UDRs are critical in hybrid and multi-cloud environments, where traffic may need to be routed between on-premises networks and Azure, or between different cloud providers. By defining custom routes, you can ensure that traffic flows correctly across different environments while maintaining control and security.



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

# UDR






Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

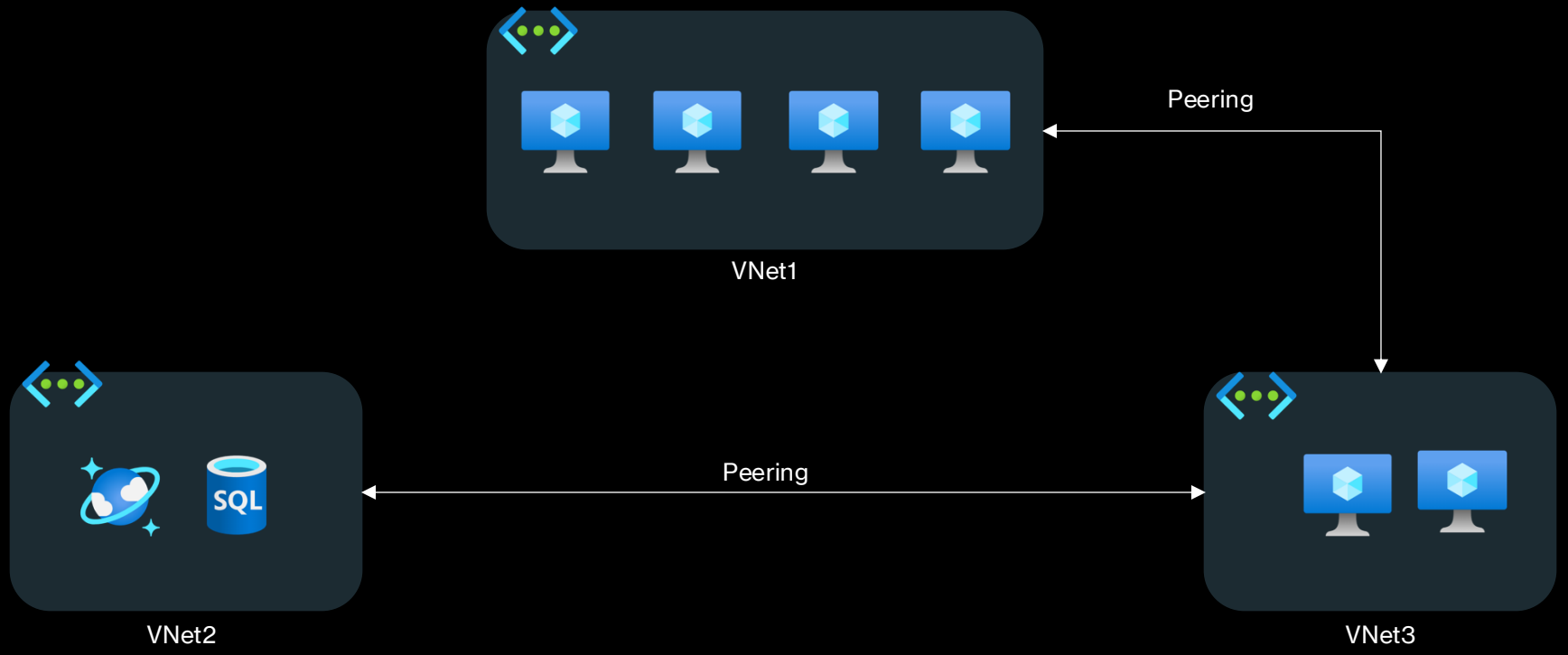
# VNet Peering

- **VNet Peering Overview**: VNet peering in Azure enables seamless connectivity between two virtual networks, allowing resources in different VNets to communicate with each other as if they were part of the same network. This connection is established using the Microsoft backbone network, ensuring low-latency and high-bandwidth communication.
- **Advantages - Low Latency and High Bandwidth**: VNet peering leverages Azure's internal backbone network, providing low-latency and high-bandwidth connections between peered VNets. This makes it ideal for scenarios where fast data transfer and communication between different virtual networks are required.
- **Advantages - Cost Efficiency**: Traffic between peered VNets is routed directly through Azure's backbone network without the need for an additional gateway or VPN, which can reduce costs associated with data transfer compared to traditional VPN connections.
- **Disadvantages - No Transitive Peering**: VNet peering does not support transitive peering, meaning if VNet A is peered with VNet B, and VNet B is peered with VNet C, VNet A cannot communicate directly with VNet C. This limitation may require additional peering connections or the use of a hub-and-spoke network topology. Peering is also not supported for overlapping IP ranges.
- **Disadvantages - Flat Networks**: VNet peering can lead to the creation of flat network architectures, where all resources within peered VNets can potentially communicate with each other. From a cybersecurity perspective, this lack of segmentation increases the risk of lateral movement by attackers within the network, making it more challenging to contain breaches and enforce security policies effectively.



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

# Vnet Peering




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

# VNet Peering

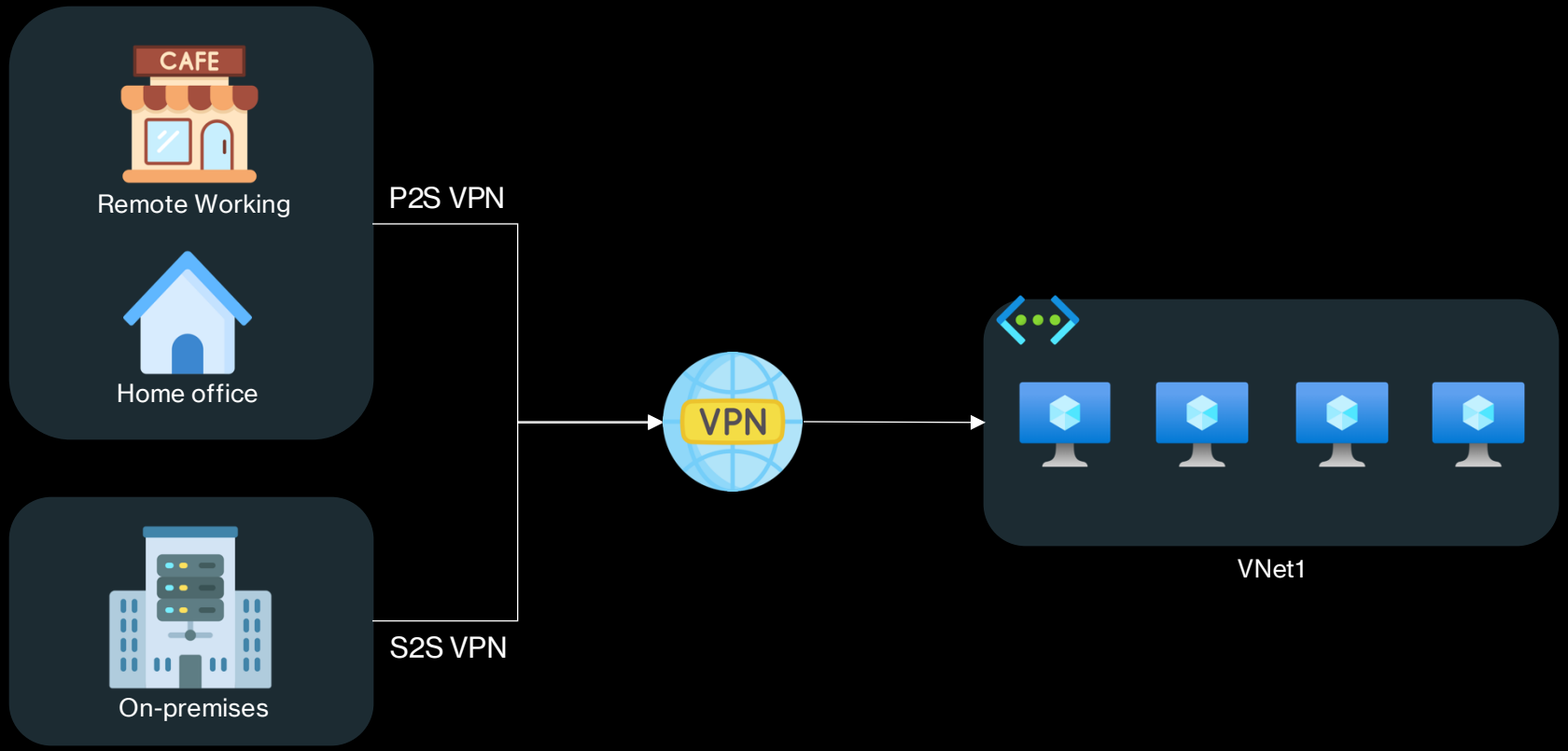
Important Considerations:

- Peering works across tenants/regions/subscriptions
- Peering is unsupported for overlapping IP ranges
- Transitive routing is not supported
- When you peer two VNets, two peers are created: one for each direction
- Peers support traffic forwarding
- System routes are automatically updated for connectivity purposes



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

# Virtual Private Networks (VPNs)






Source: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

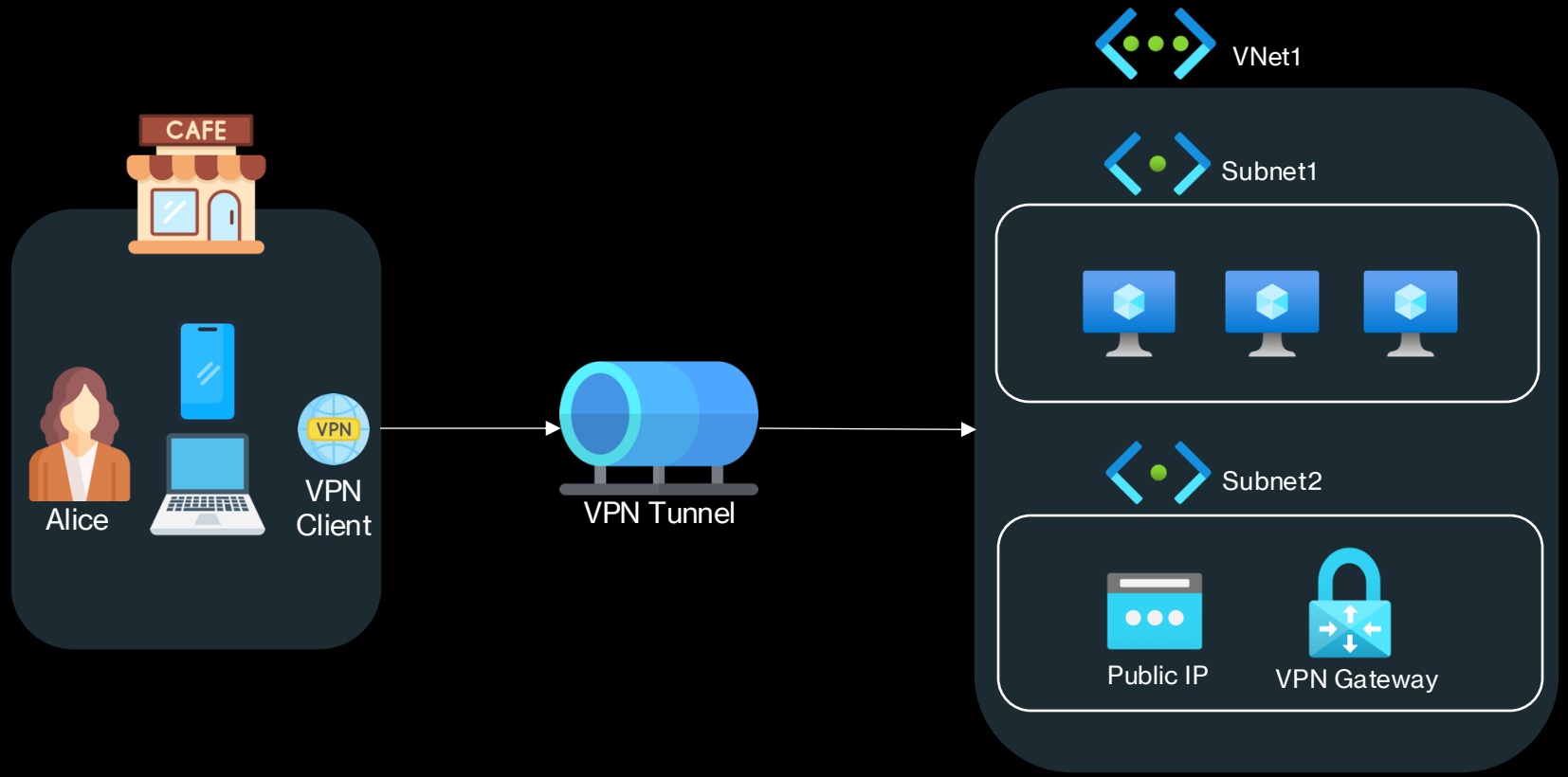
# Point-to-Site VPN (P2S)

- **Description:** Point-to-Site VPN allows individual clients (such as laptops or mobile devices) to securely connect to an Azure Virtual Network from remote locations. This is often used for remote workers or small-scale connections where only a few clients need access.
- **Authentication:** Supports native Azure certificate-based authentication, Azure Active Directory (Azure AD), and RADIUS (Remote Authentication Dial-In User Service).
- **Protocols Supported:** SSTP (Secure Socket Tunneling Protocol), OpenVPN, and IKEv2 (Internet Key Exchange version 2).
- **Scalability:** Ideal for small to medium-sized deployments with a limited number of clients.



Source: https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

# Point-to-Site VPN (P2S)






Source: https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

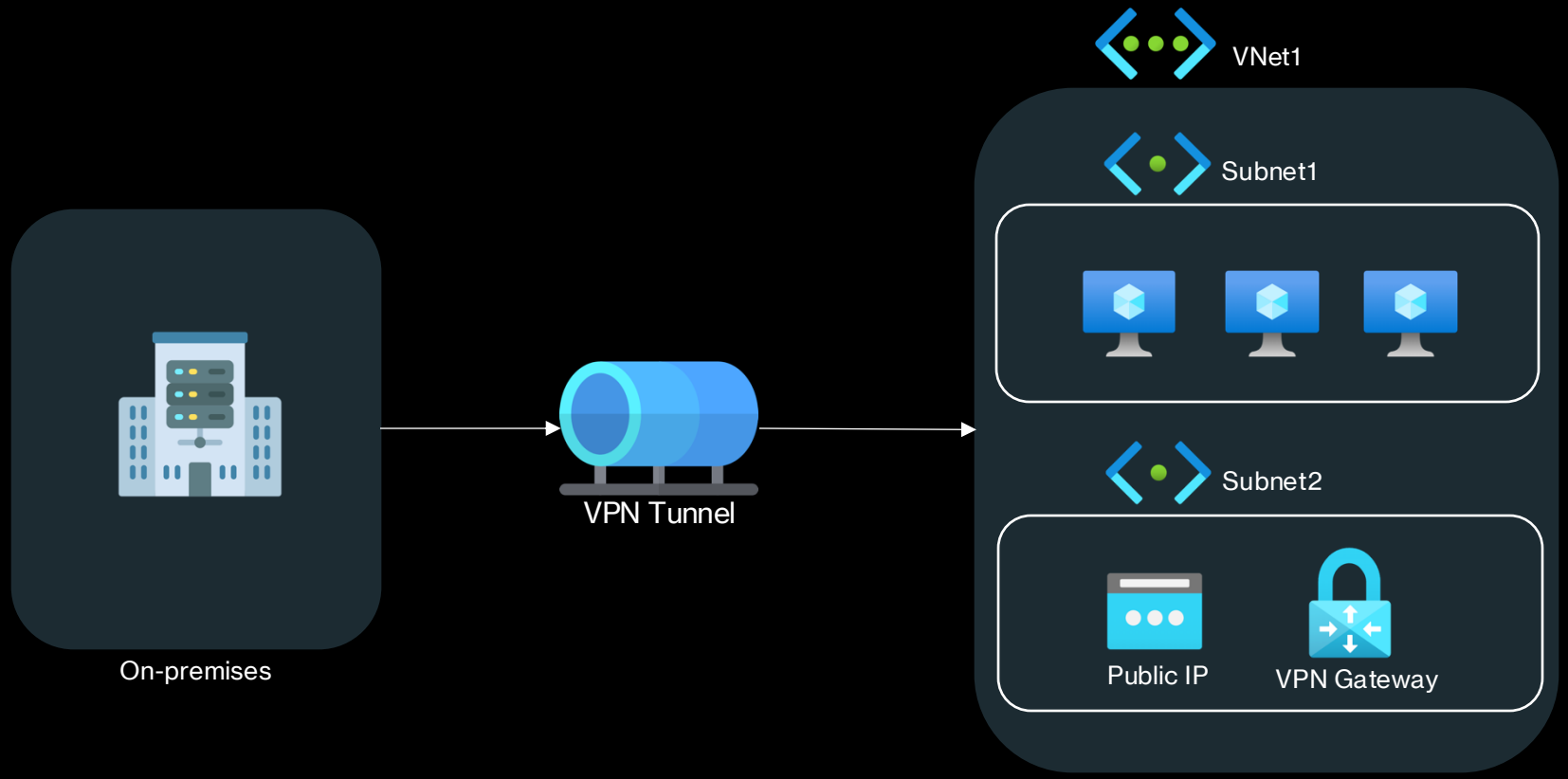
# Site-to-Site VPN (S2S)

- **Description:** Site-to-Site VPN is designed for connecting on-premises networks to Azure Virtual Networks over an IPsec/IKE (Internet Protocol Security/Internet Key Exchange) VPN tunnel. This is suitable for extending an on-premises network to Azure or for connecting multiple office locations to a centralized Azure VNet.
- **Authentication:** Uses a shared key (pre-shared key) for authentication between the on-premises VPN device and the Azure VPN gateway.
- **Scalability:** Supports multiple sites but is best suited for medium-sized enterprise environments where consistent and reliable connectivity is needed.
- **Gateway Types:** Supports both VPN gateway types (Policy-based and Route-based) with Route-based being the more flexible and scalable option.



Source: https://learn.microsoft.com/en-us/azure/vpn-gateway/design

# Site-to-Site VPN (S2S)






Source: https://learn.microsoft.com/en-us/azure/vpn-gateway/design

# ExpressRoute 

- ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider.
- With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.
- Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility.
- ExpressRoute connections offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet, because they don't go over the public Internet.



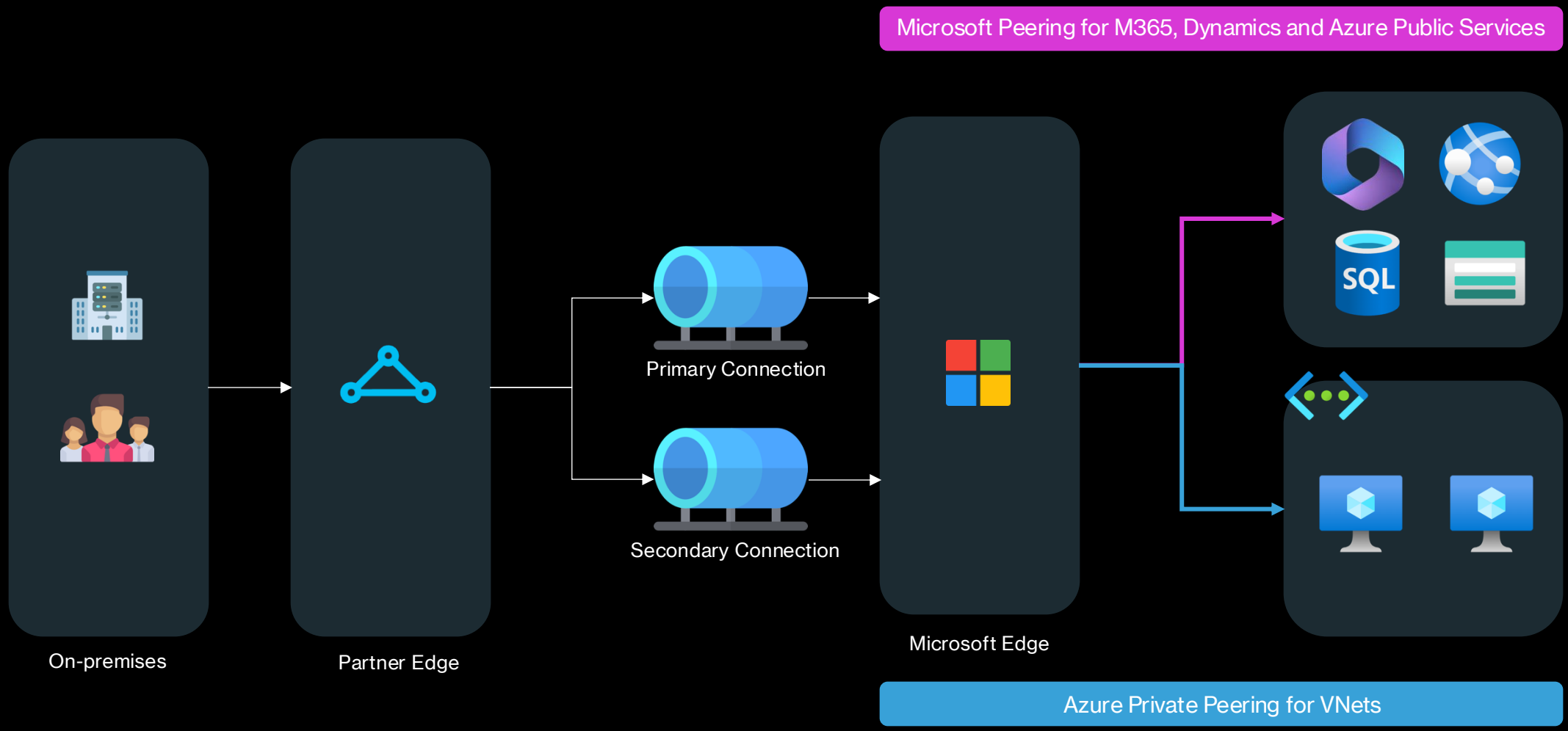
Source: https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction

# ExpressRoute 

Key Benefits:

- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on.
- Dynamic routing between your network and Microsoft via BGP.
- Built-in redundancy in every peering location for higher reliability.
- Connection uptime SLA.
- QoS support for Skype for Business.

# ExpressRoute




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction

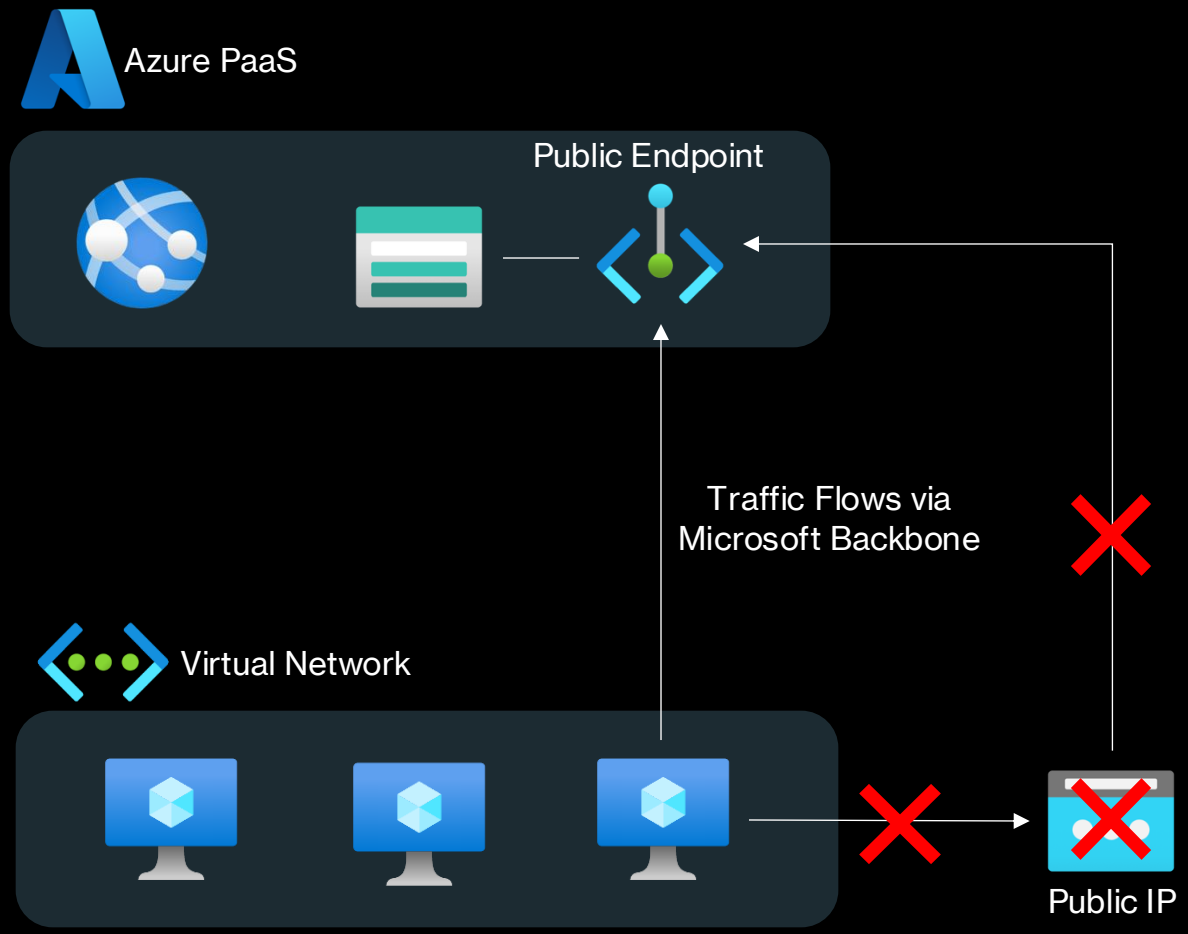
# Service Endpoints

- A Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network.
- Service endpoints allow you to secure your critical Azure service resources to only your virtual networks.
- Service Endpoints enable private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

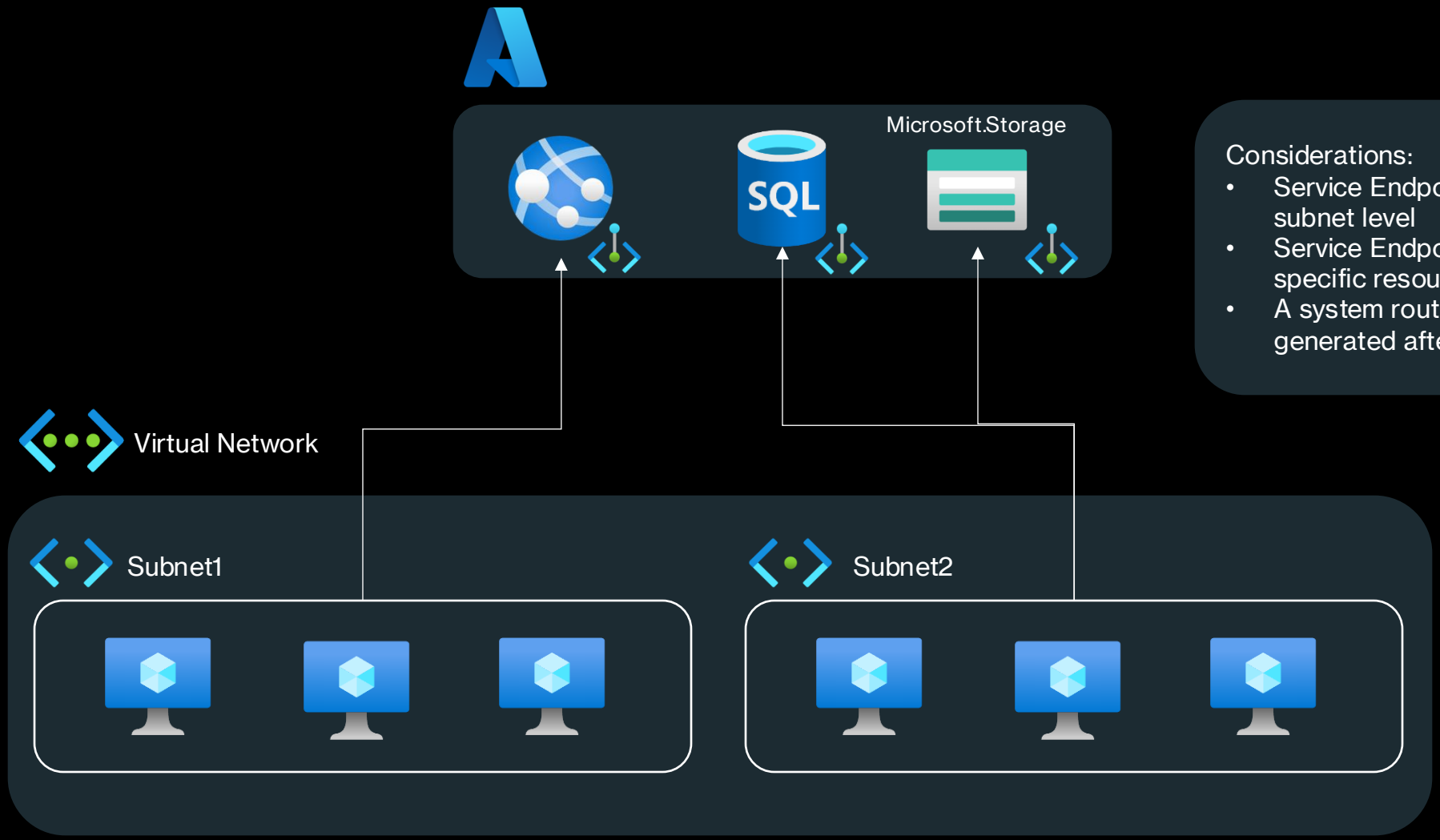
# Service Endpoints






Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

# Service Endpoints




Considerations:

- Service Endpoints are enabled on subnet level
- Service Endpoints are enabled for a specific resource provider
- A system route will automatically be generated after configuration



Source: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

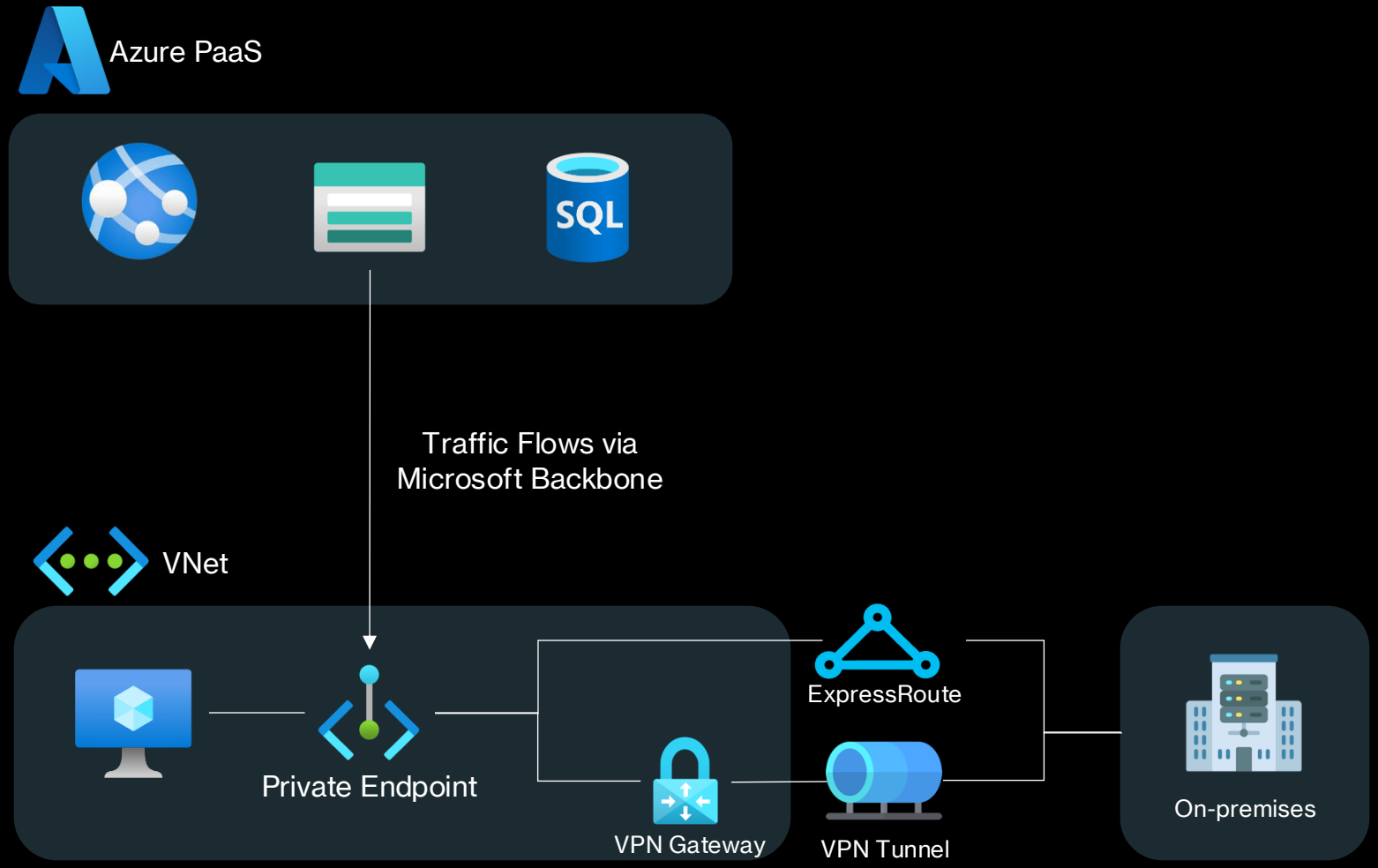
# Azure Private Link

- Azure Private Link enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.
- Traffic between your virtual network and the service travels the Microsoft backbone network.
- Exposing your service to the public internet is no longer necessary.
- You can create your own private link service in your virtual network and deliver it to your customers.



Source: https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

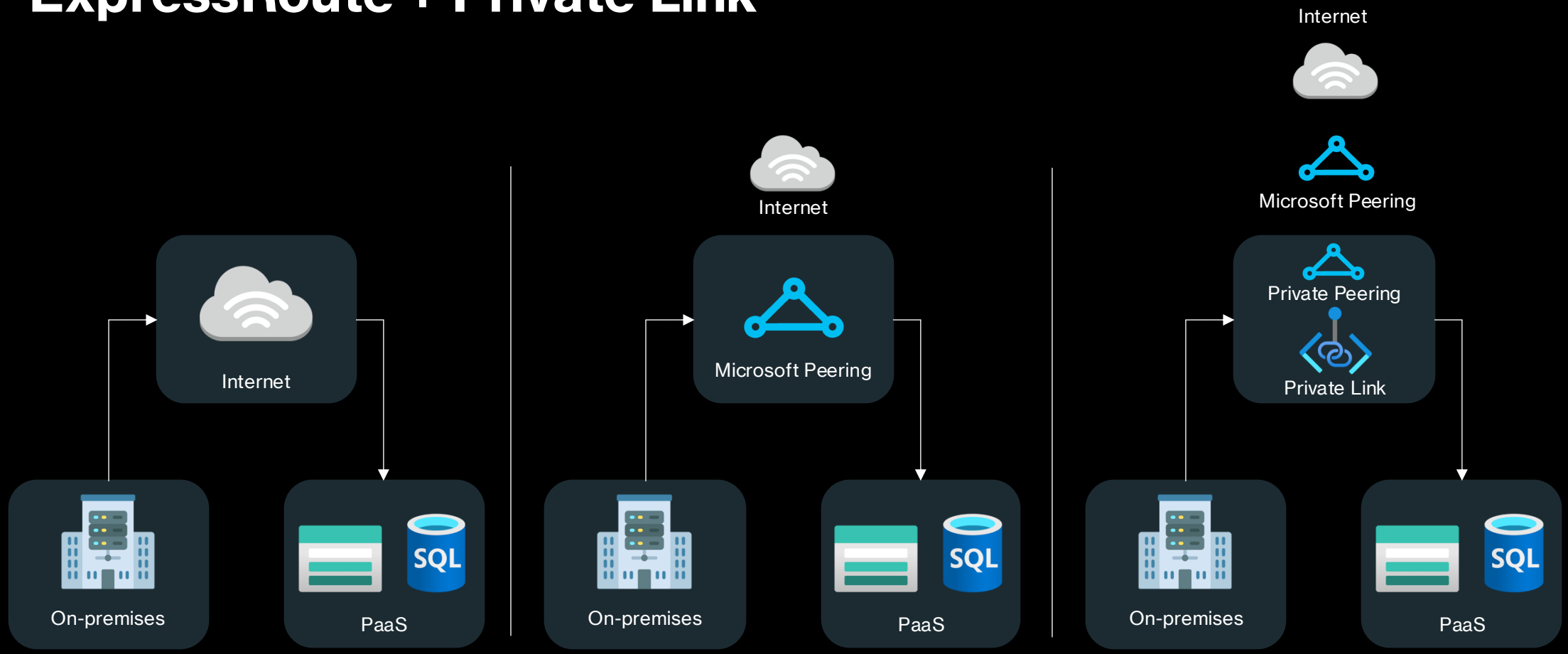
# Azure Private Link






Source: https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

# ExpressRoute + Private Link




- Traffic traverses the internet
- Secured using ACLs on public IPs
- On-prem Firewall open to Azure Public IPs

- Traffic stays within the Microsoft network
- Microsoft peering draws Microsoft public IP traffic
- On-prem Firewall open to Azure Public IPs

- Traffic is fully private traversing the Microsoft network
- No exposure of public IPs on either side
- On-prem Firewall only open to private

Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

# Azure App Service 

- Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends.
- You can develop in your favorite language, be it .NET, .NET Core, Java, Node.js, PHP, or Python.
- Applications run and scale with ease on both Windows and Linux-based environments.
- App Service adds Microsoft Azure to your application, including improved security, load balancing, autoscaling, and automated management.
- Additionally, you can take advantage of its DevOps capabilities, such as continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domains, and TLS/SSL certificates.
- With App Service, you pay for the Azure compute resources you use. The compute resources you use are determined by the App Service plan that you run your apps on.



Source: https://learn.microsoft.com/en-us/azure/app-service/overview

# Azure App Service

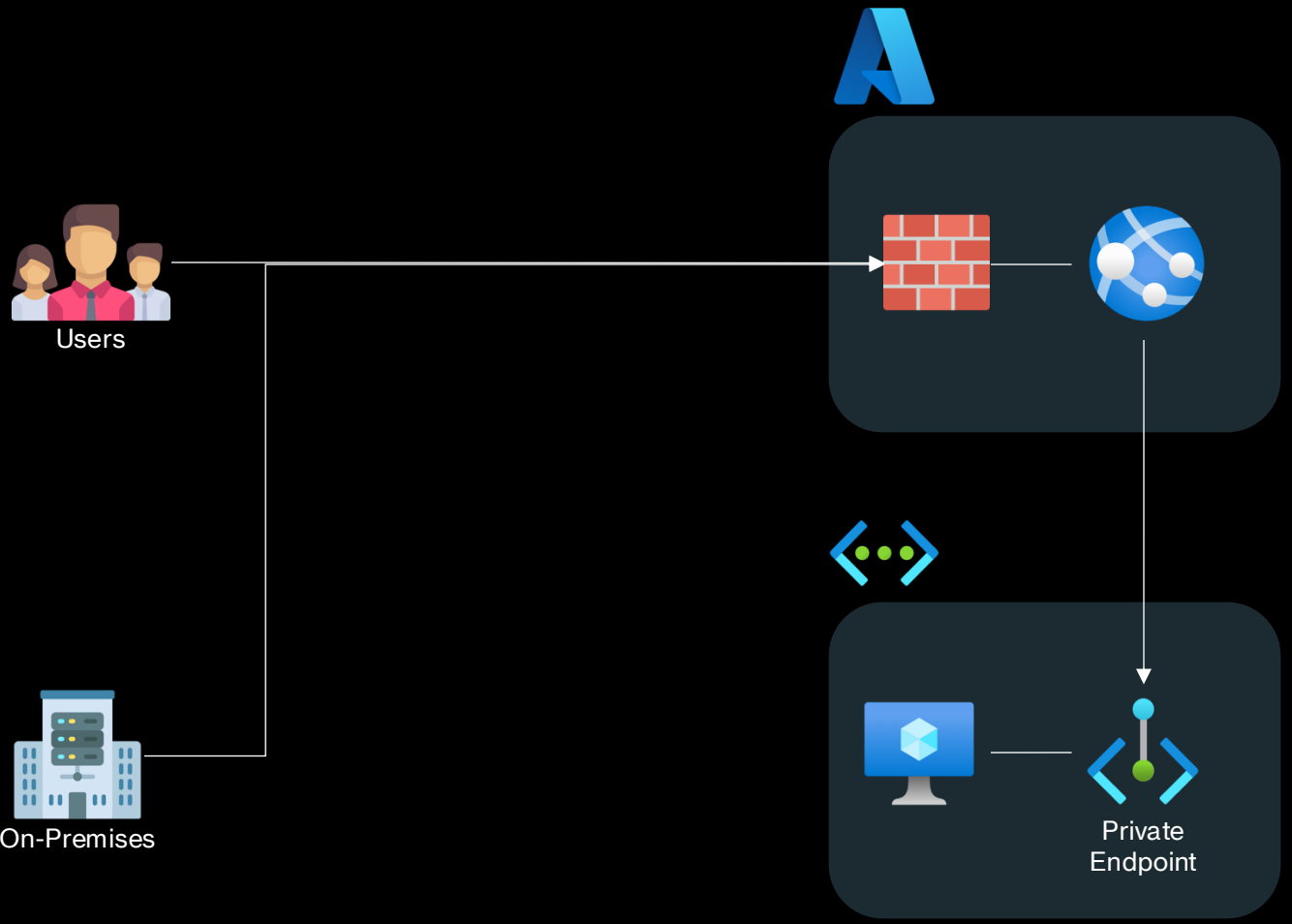

Considerations:

- App Service Plan: Defines the features and resources that are available to your app
- Apps reside in a runtime environment (the app services)
- An app service plan can support multiple app services



Source: https://learn.microsoft.com/en-us/azure/app-service/overview

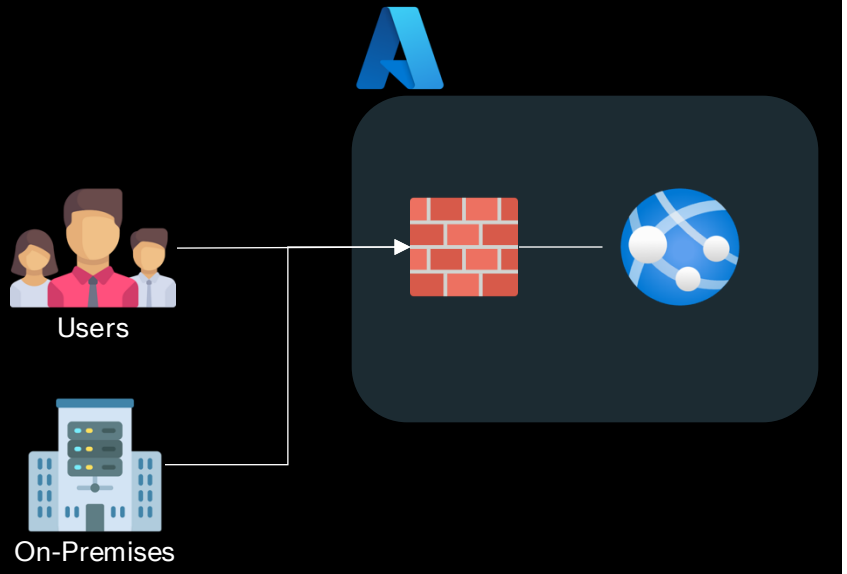
# Azure App Service

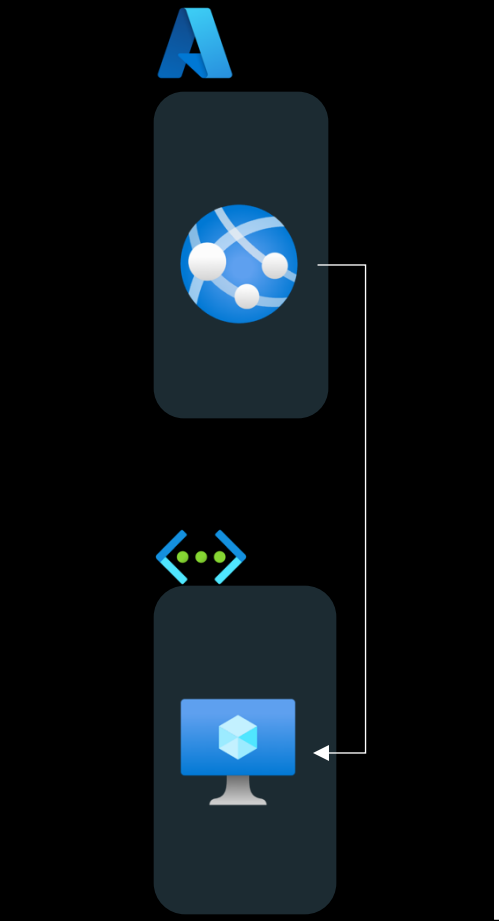


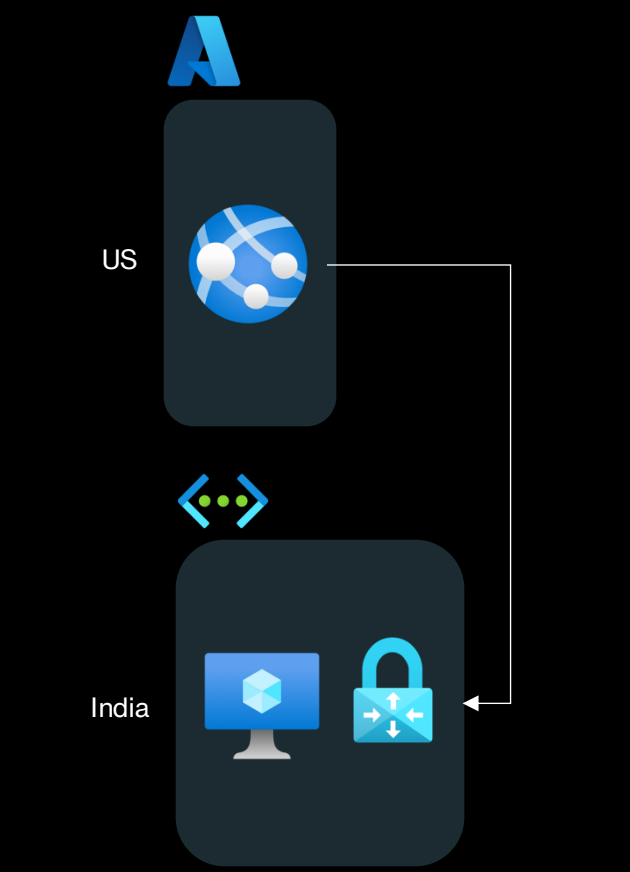



Source: https://learn.microsoft.com/en-us/azure/app-service/overview

# Azure App Service



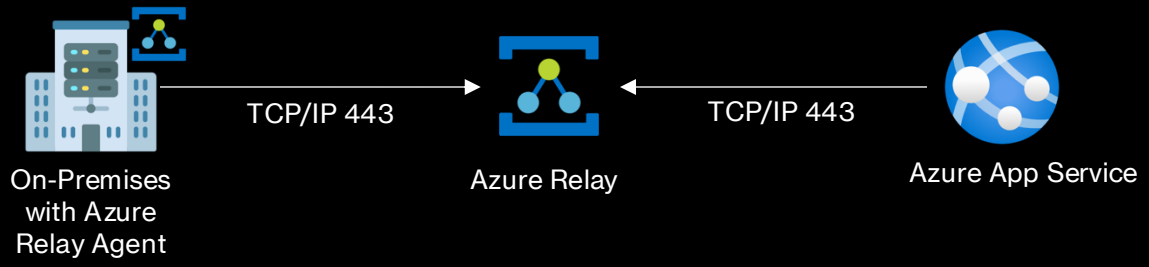




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/app-service/overview

# Azure App Service – Hybrid Connections




Considerations:

- Only outbound connectivity is required via TCP/IP 443



Source: https://learn.microsoft.com/en-us/azure/app-service/overview

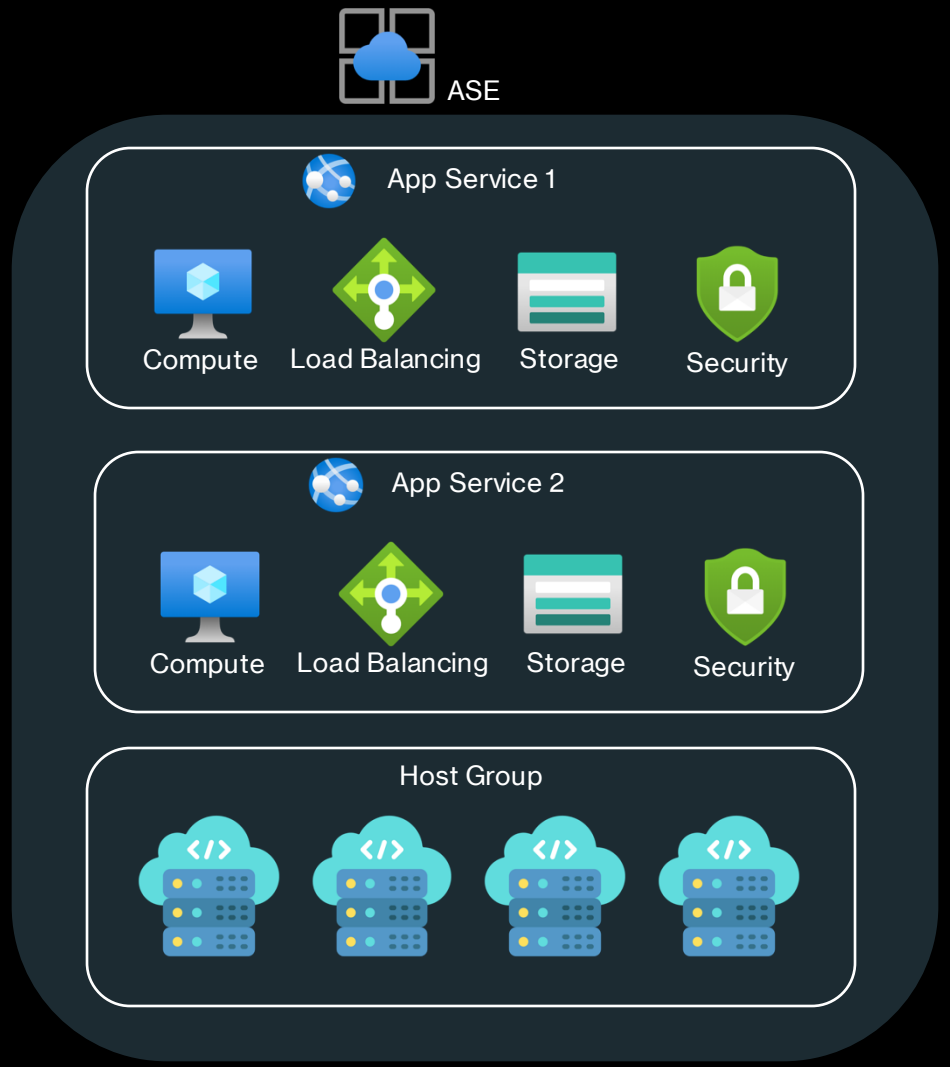
# Azure App Service Environment (ASE) 

- An App Service Environment is an Azure App Service feature that provides a fully isolated and dedicated environment for running App Service apps securely at high scale.
- Unlike the App Service public multitenant offering where supporting infrastructure is shared, with App Service Environment, compute is dedicated to a single customer.
- Supports hypervisor isolation by leveraging host groups
- Enabled network isolation through VNet integration



Source: https://learn.microsoft.com/en-us/azure/app-service/environment/overview

# Azure App Service Environment (ASE)




Considerations:

- Dedicated environment
- Can be deployed to a VNet and supports internal or external access
- Host Group: Runs ASE on hypervisors dedicated to you
- ASE deploys apps to an App Service Plan called isolated



Source: https://learn.microsoft.com/en-us/azure/app-service/environment/overview

# Azure Firewall 

- Cloud Native Firewall in Azure
- L3 to L7 Policies
- Integrated Microsoft CTI
- Integrated IDS/IPS
- URL and Web Content Filtering
- TLS Inspection



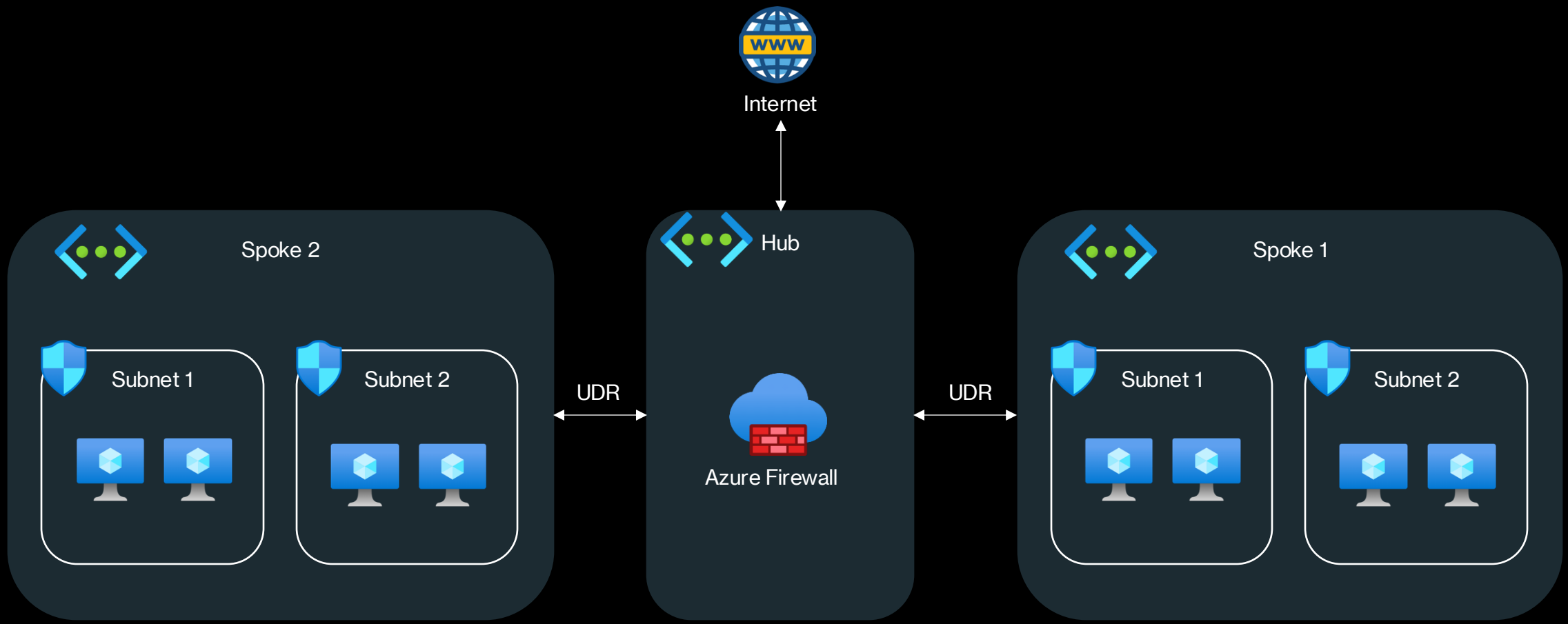
Source: https://learn.microsoft.com/en-us/azure/firewall/overview

# Azure Firewall


Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/firewall/overview

# Azure Firewall + Hub & Spoke




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/firewall/overview

# Azure Firewall SKUs

- Azure Firewall Premium is recommended to secure highly sensitive applications (such as payment processing). It supports advanced threat protection capabilities like malware and TLS inspection.
- Azure Firewall Standard is recommended for customers looking for Layer 3–Layer 7 firewall and needs autoscaling to handle peak traffic periods of up to 30 Gbps. It supports enterprise features like threat intelligence, DNS proxy, custom DNS, and web categories.
- Azure Firewall Basic is recommended for SMB customers with throughput needs of 250 Mbps.



Source: https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku

# Azure Firewall SKUs

| Feature Category | Feature | Firewall Basic | Firewall Standard | Firewall Premium |
|---|---|---|---|---|
| L3-L7 Filtering | Application level FQDN filtering | X | X | X |
| | Network level FQDN filtering | | X | X |
| | Stateful firewall (5 tuple) | X | X | X |
| | NAT (SNAT + DNAT) | X | X | X |
| Reliability & Performance | Availability Zones | X | X | X |
| | Built-in HA | X | X | X |
| | Cloud scalability | Up to 250 Mbps | Up to 30 Gbps | Up to 100 Gbps |
| | Fat flow support | N/A | 1 Gpbs | 10 Gpbs |
| Ease of Management | Central management via Firewall Manager | X | X | X |
| | Policy Analytics | X | X | X |
| Enterprise Integration | Full logging & SIEM integration | X | X | X |
| | Service tags and FQDN tags for policy management | X | X | X |
| | DevOps integration using REST/PS/CLI/Terraform | X | X | X |
| | Web content filtering | | X | X |
| | DNS Proxy + Custom DNS | | X | X |
| Advanced Threat Protection | Threat-Intelligence based filtering | Alert | X | X |
| | Inbound TLS termination (TLS reverse proxy) | | | Using AppGW |
| | Outbound TLS termination (TLS forward proxy) | | | X |
| | Fully managed IDPS | | | X |
| | URL filtering (full path, incl. TLS termination) | | | X |



Source: https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku

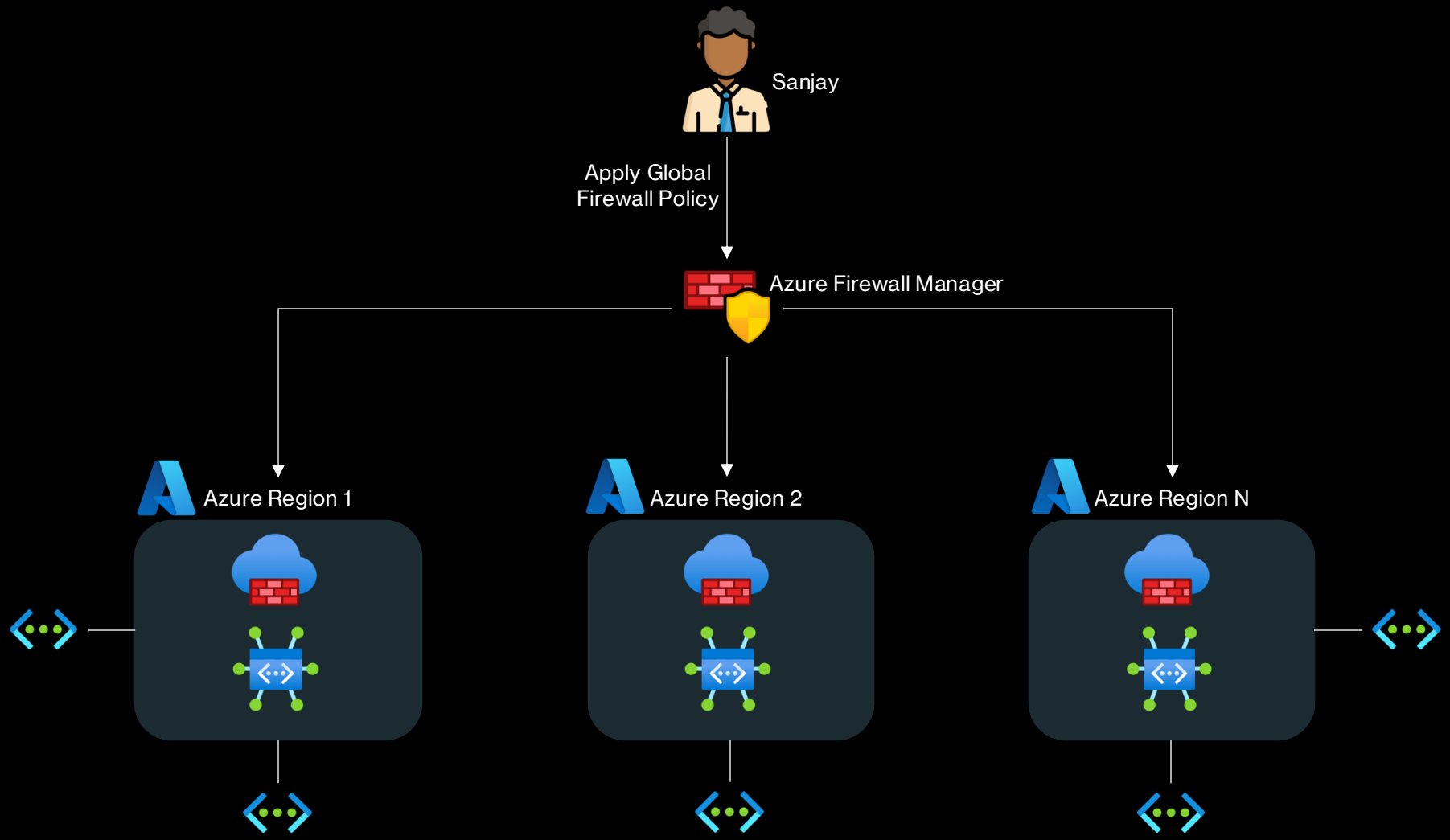
# Azure Firewall Manager 

- Azure Firewall Manager allows you to deploy and configure multiple Azure Firewall instances that span different Azure regions and subscriptions.
- Firewall Manager can provide security management for two network architecture types:
  - **Secured virtual hub:** An Azure Virtual WAN Hub is a Microsoft-managed resource that lets you easily create hub and spoke architectures. When security and routing policies are associated with such a hub, it's referred to as a secured virtual hub.
  - **Hub virtual network:** This is a standard Azure virtual network that you create and manage yourself. When security policies are associated with such a hub, it's referred to as a hub virtual networkYou can peer spoke virtual networks that contain your workload servers and services. You can also manage firewalls in standalone virtual networks that aren't peered to any spoke.



Source: https://learn.microsoft.com/en-us/azure/firewall-manager/overview

# Azure Firewall Manager




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/firewall-manager/overview

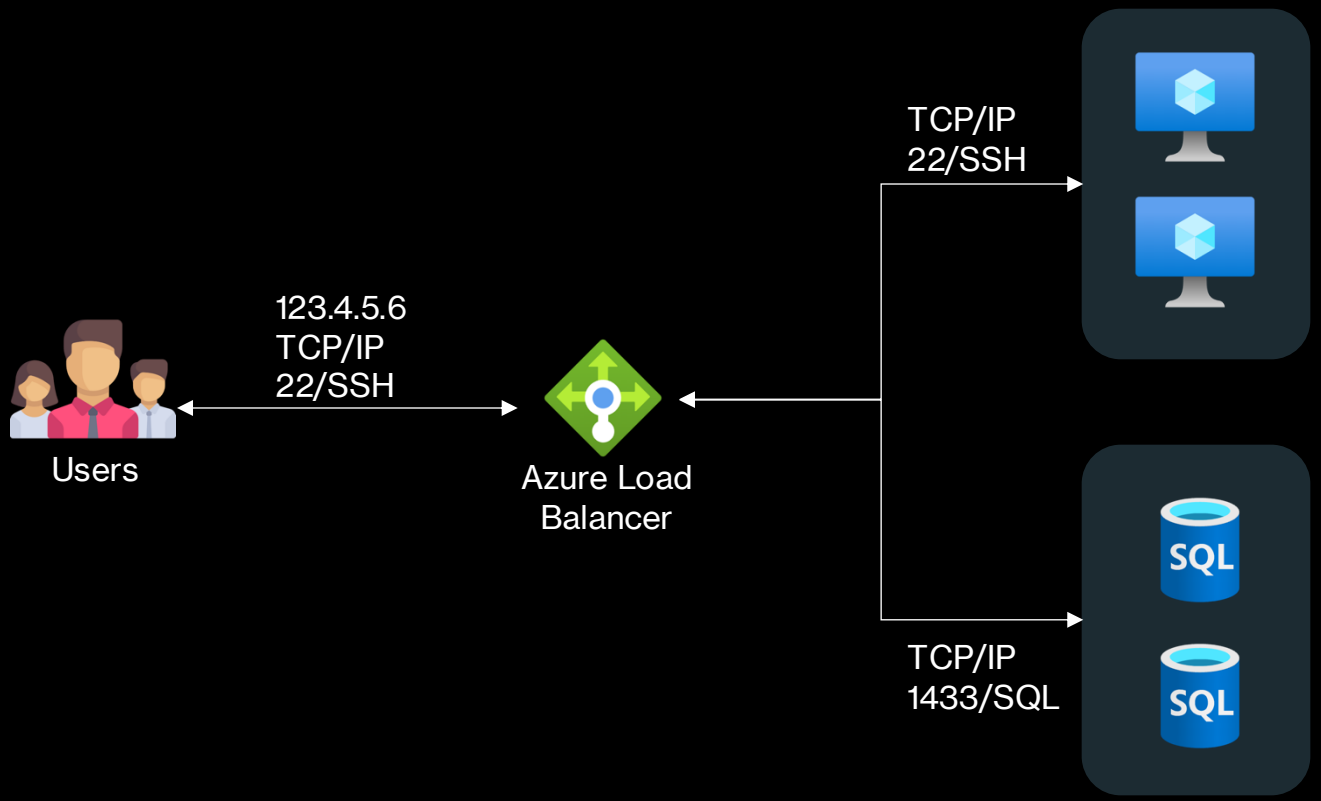
# Azure Load Balancer 

- Azure Load Balancer operates at layer 4.
- A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.
- An internal (or private) load balancer is used in scenarios where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.



Source: https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

# Azure Load Balancer






Source: https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

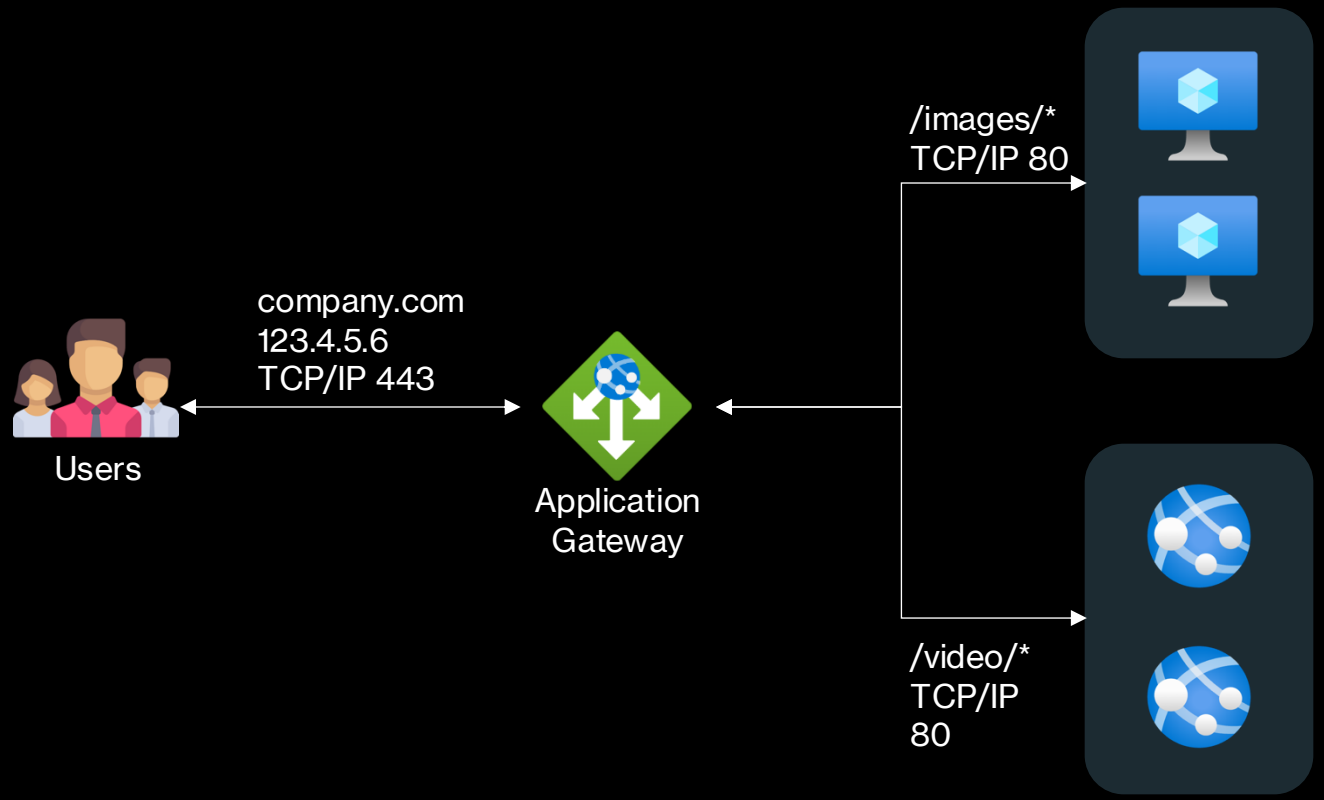
# Azure Application Gateway 

- Regional load balancing
- L7 load balancing
- TLS offloading
- Path-based routing
- Integrated autoscaling
- Multi-Site routing
- WAF attach



Source: What is Azure Application Gateway | Microsoft Learn

# Azure Application Gateway




**Rules**

Prioritized rules that combine settings together, e.g. by supporting path-based rules

**Frontend**

Allows the usage of public IP,  private IP or both

**Backend**

Supports multiple Azure services that are either public or private



Source: What is Azure Application Gateway | Microsoft Learn

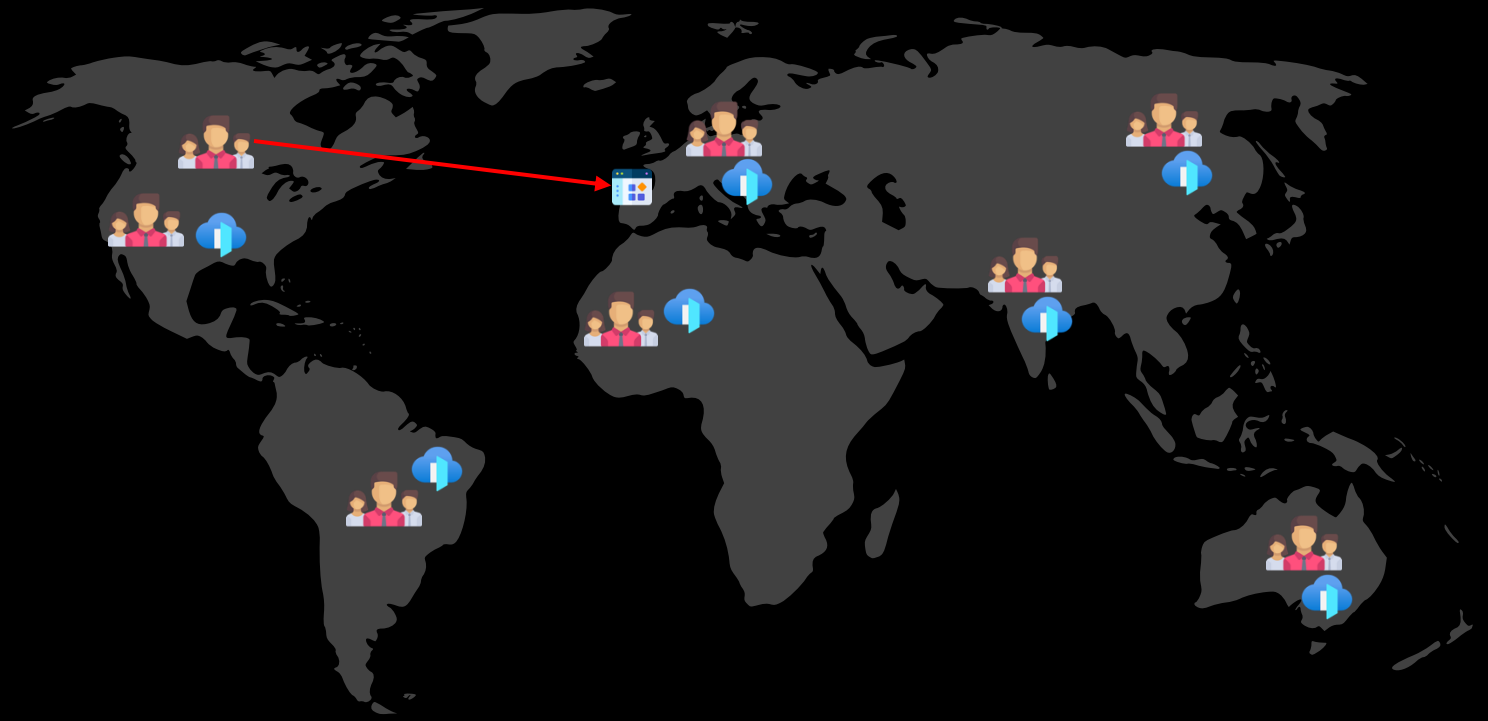
# Azure Front Door

- Global Load Balancing Service
- Content Delivery Network (CDN)
- Static & Dynamic Content Acceleration
- WAF, DDoS and Bot Manager Integration
- TLS Offloading
- Azure Managed Domains and TLS Certificates



Source: Azure Front Door | Microsoft Learn

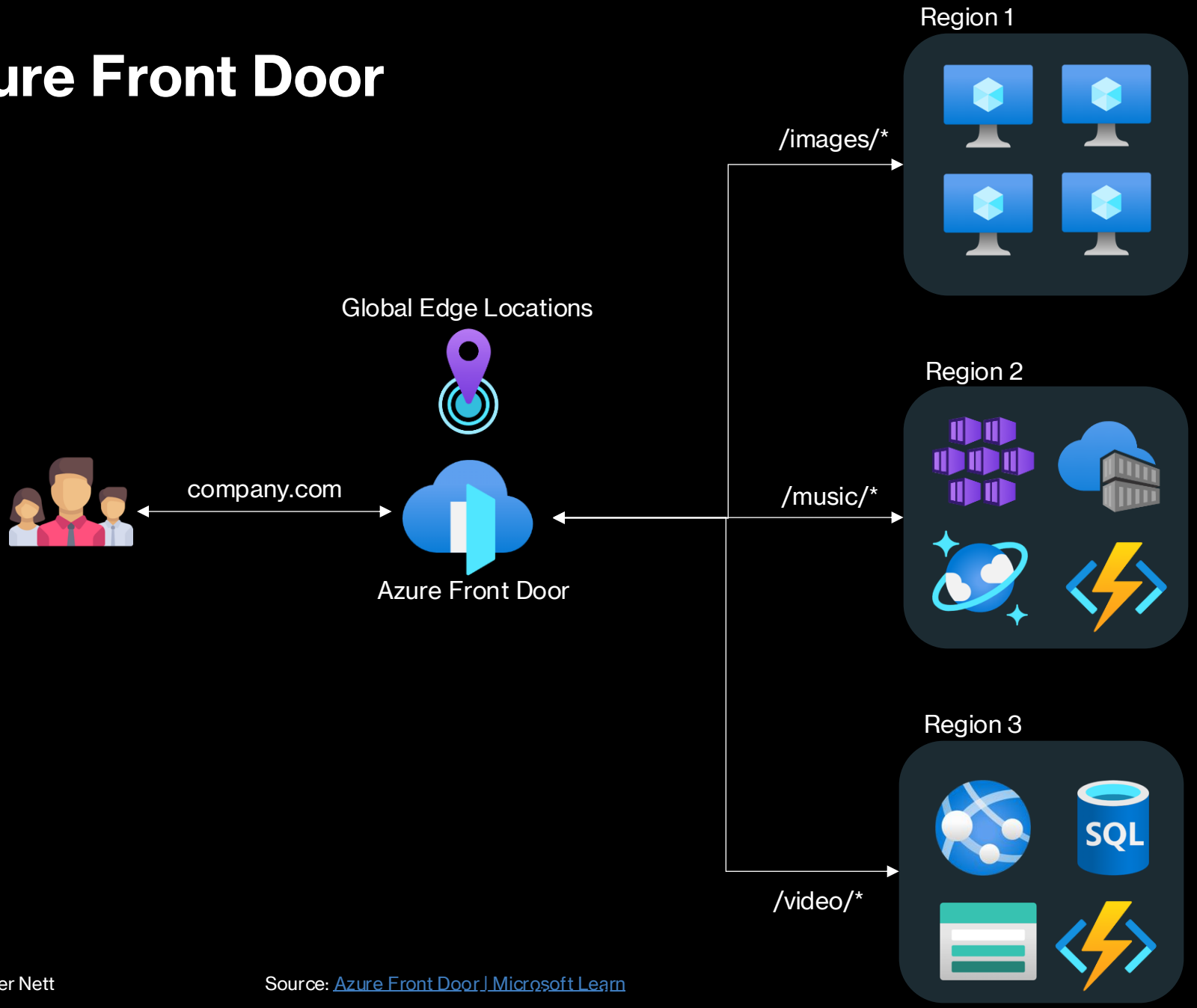
# Azure Front Door



Source: Global Network – Backbone Networking Infrastructure | Microsoft Azure

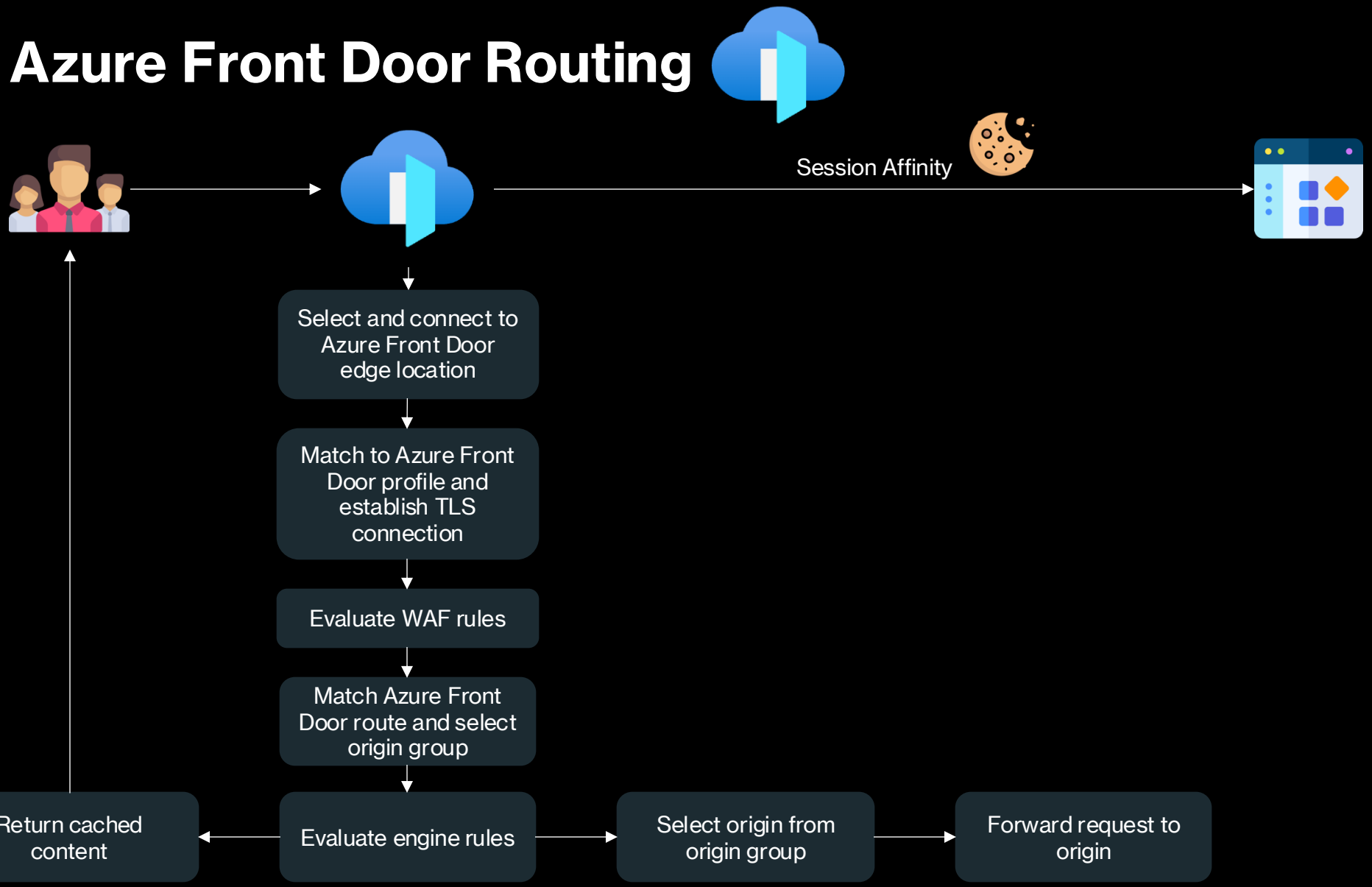
# Azure Front Door




Christopher Nett

Source: Azure Front Door | Microsoft Learn

# Azure Front Door Routing




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/frontdoor/front-door-routing-architecture?pivots=front-door-standard-premium

# Azure Front Door 

| Feature | Front Door Standard | Front Door Premium |
|---|---|---|
| Static file delivery | X | X |
| Dynamic site delivery | X | X |
| Custom comains | X | X |
| HTTPS support | X | X |
| Bring your own certificate | X | X |
| Path-based routing | X | X |
| Custom WAF rules | X | X |
| Microsoft managed WAF rules | | X |
| Bot protection | | X |
| DDoS Protection | X | X |
| Private Link connection to origin | | X |



Source: https://learn.microsoft.com/en-us/azure/frontdoor/front-door-cdn-comparison

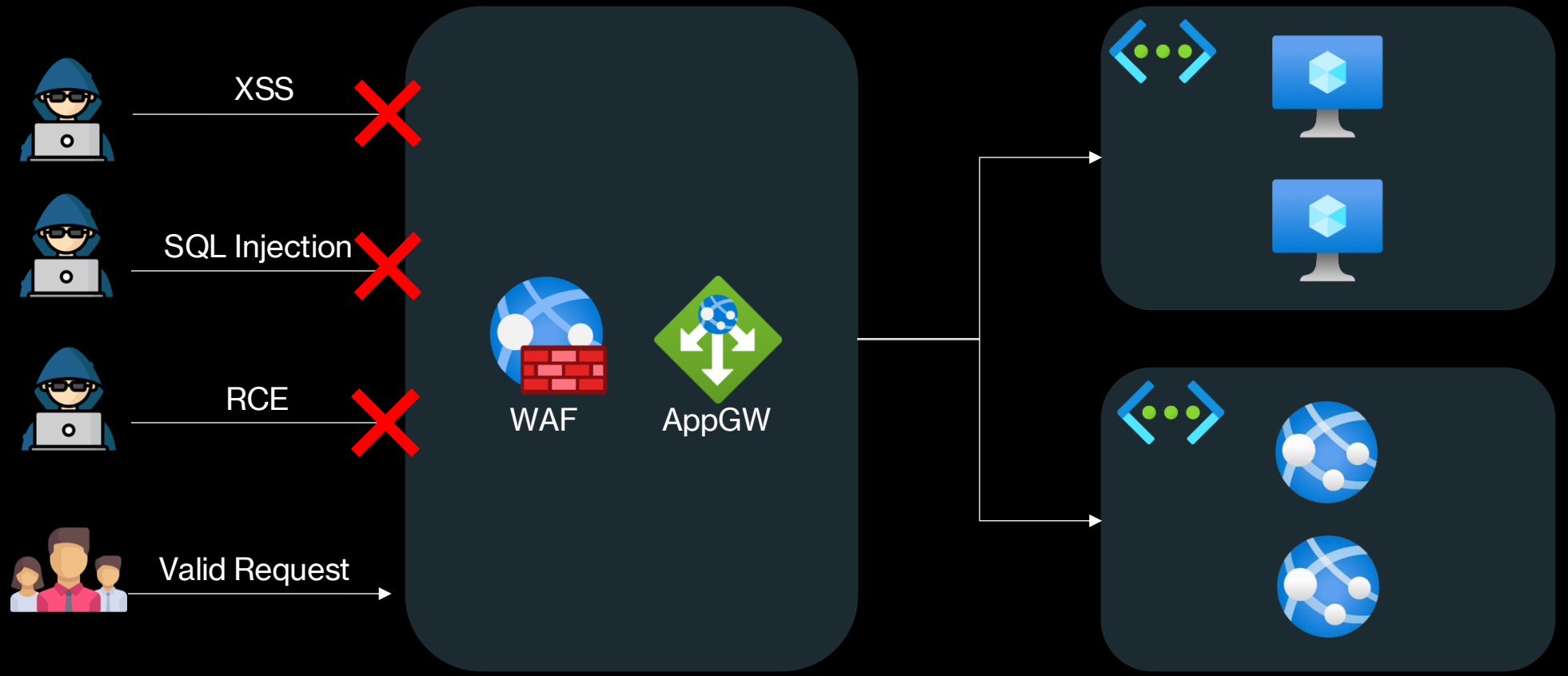
# Azure WAF 

- Azure Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities on Layer 7.
- Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities.
- Azure WAF can be deployed with Azure Application Gateway and Azure Front Door
- Microsoft provides managed WAF rulesets for e.g. the OWASP Top 10 or Bot Protection



Source: https://learn.microsoft.com/en-us/azure/web-application-firewall/overview

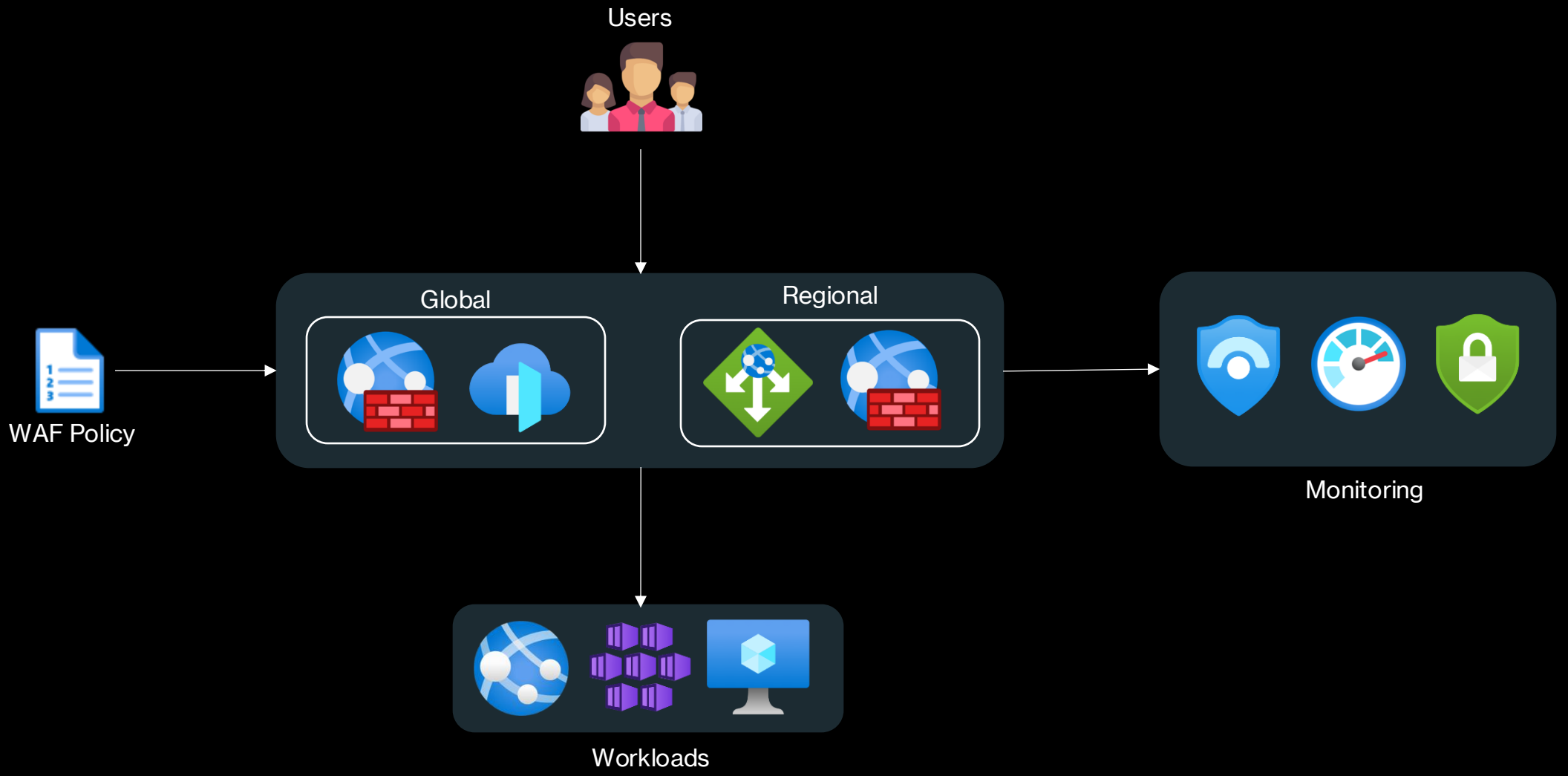
# Azure WAF






Source: What is Azure Web Application Firewall on Azure Application Gateway? - Azure Web Application Firewall | Microsoft Learn

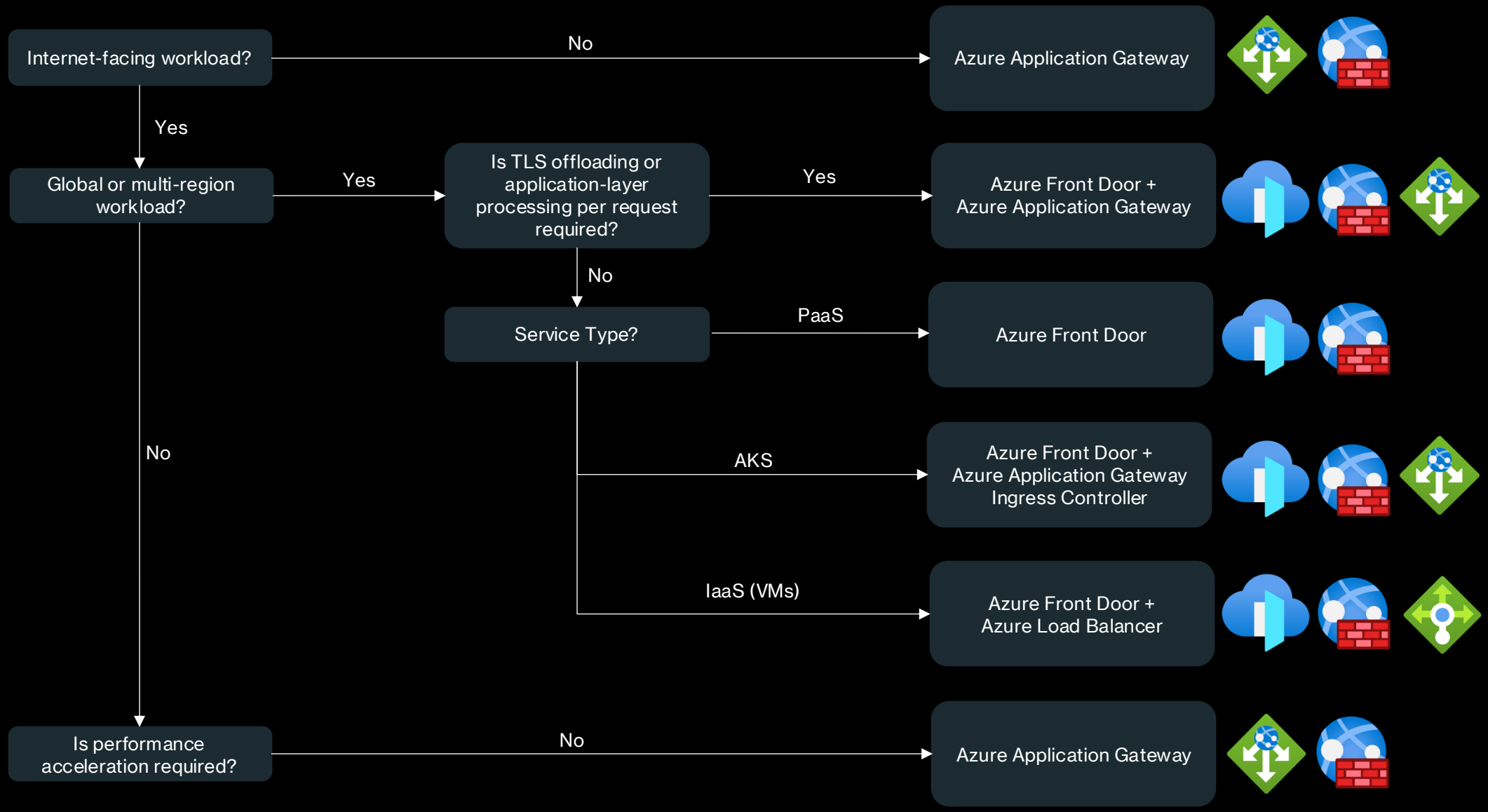
# Azure WAF






Source: https://learn.microsoft.com/en-us/azure/web-application-firewall/overview

# Azure WAF – Decision Flow




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

# Azure Web Application Firewall (WAF)

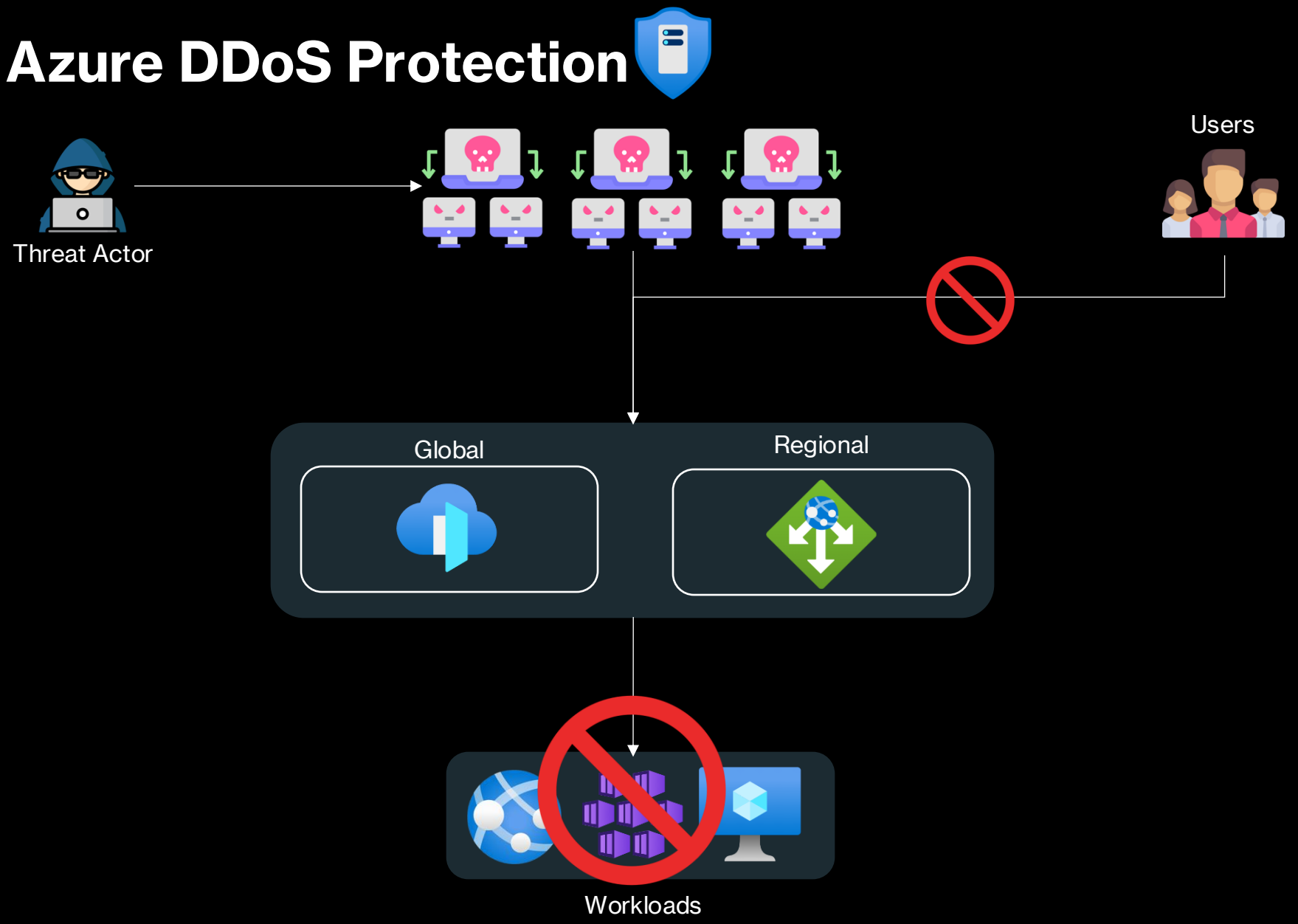
Core Features:

- Managed rulesets for e.g. OWASP Top 10
- Bot manager
- Custom WAF rules
- Json/XML parser
- Sentinel WAF solution
- Leverages Microsoft Threat Intelligence



Source: https://learn.microsoft.com/en-us/azure/web-application-firewall/overview

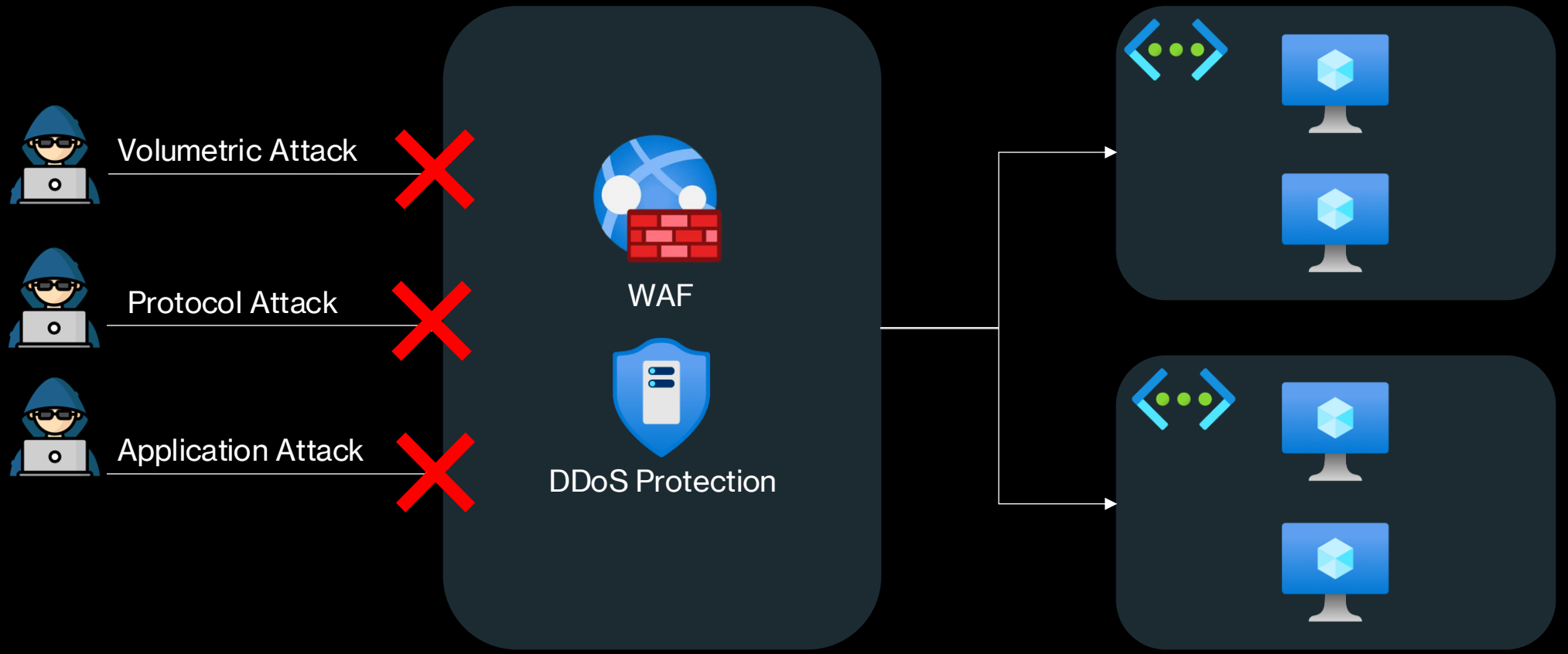
# Azure DDoS Protection




Christopher Nett

Source: Types of attacks Azure DDoS Protection mitigates | Microsoft Learn

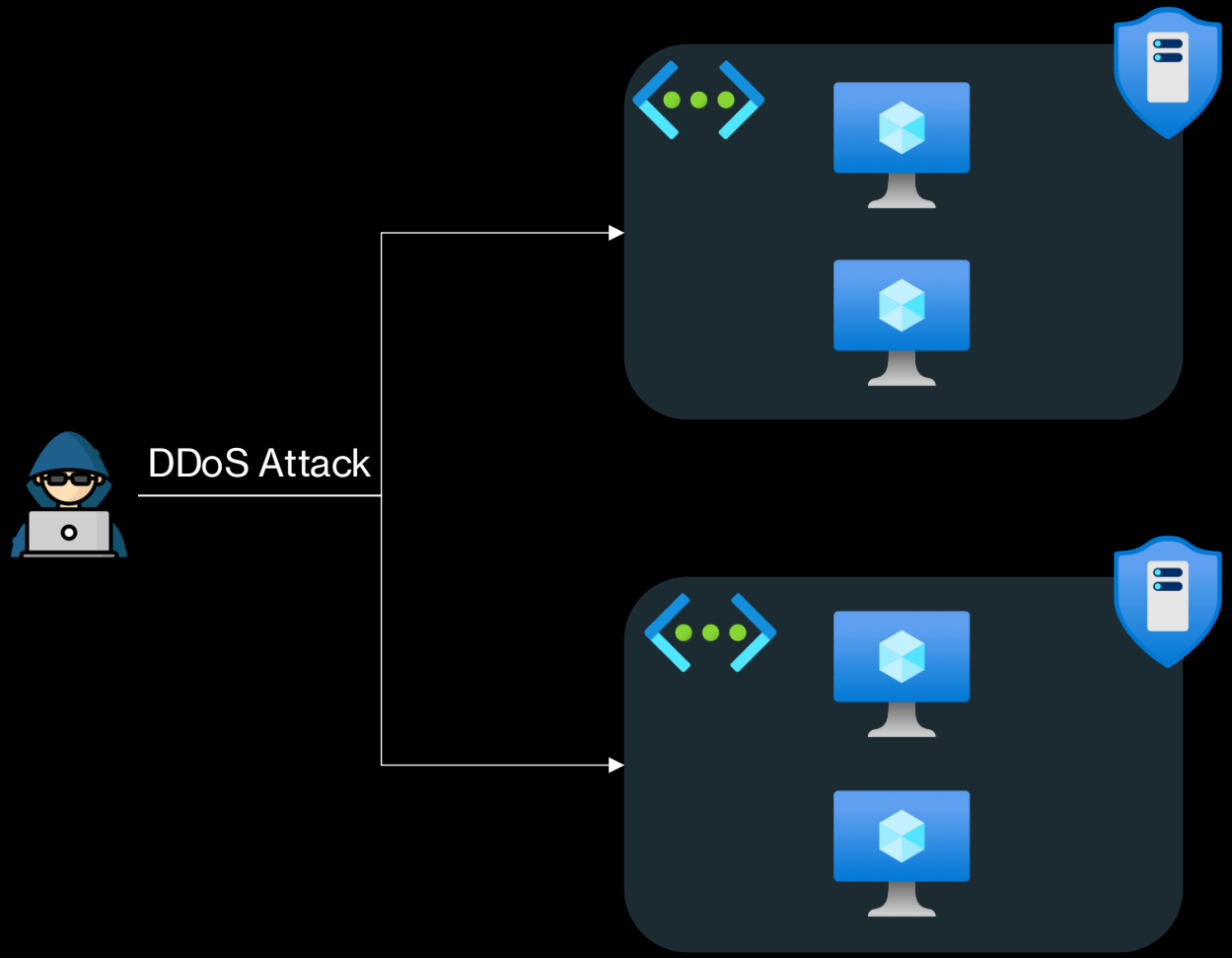
# Azure DDoS Protection – DDoS Attack Types






Source: Types of attacks Azure DDoS Protection mitigates | Microsoft Learn

# Azure DDoS Protection – Network Protection



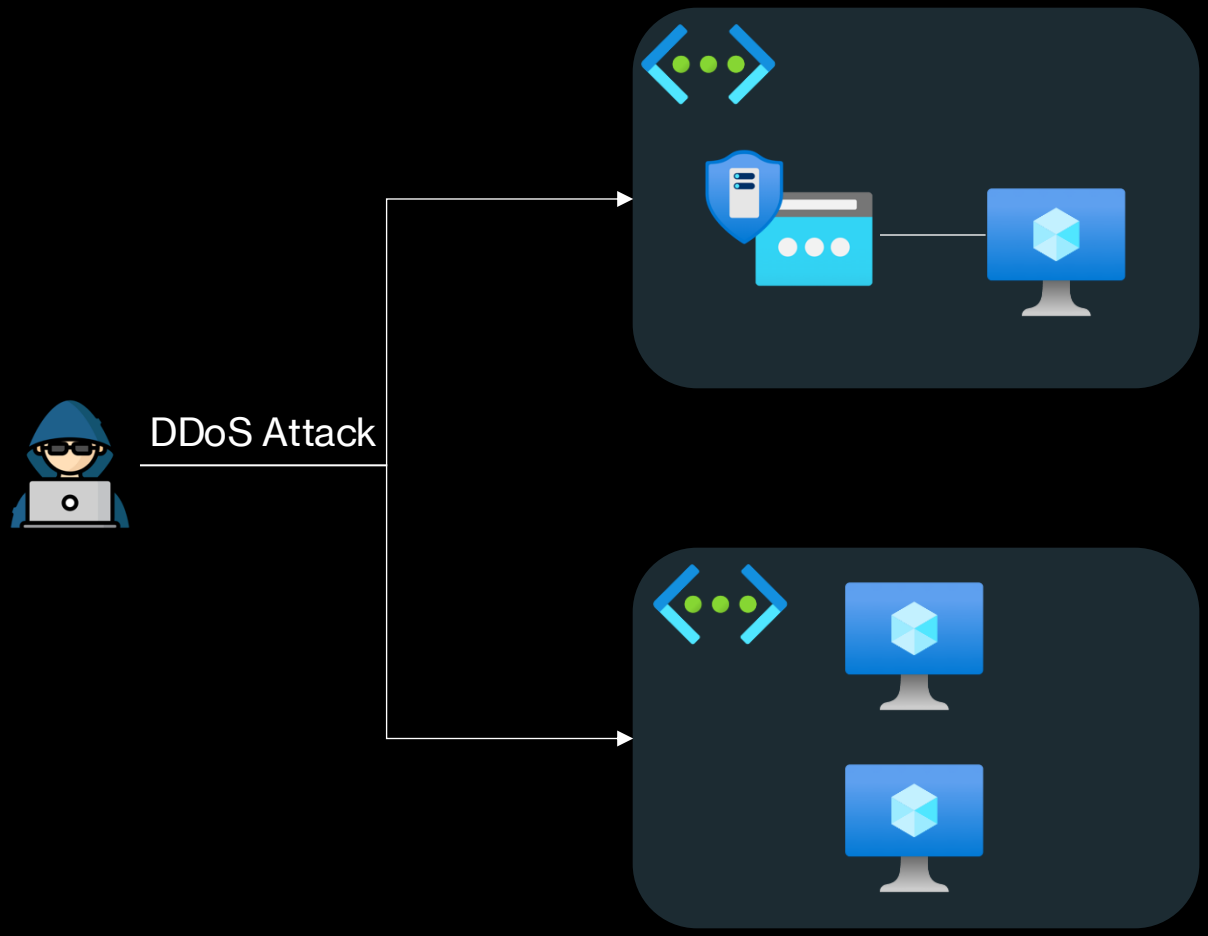

Considerations:

- Protects an entire VNet
- You can assign a network protection plan to multiple VNets
- You can use a single network protection plan across multiple subscriptions within the same tenant



Source: Types of attacks Azure DDoS Protection mitigates | Microsoft Learn

# Azure DDoS Protection – IP Protection




Considerations:

- Protects a public IP address
- You can use a single IP protection plan across multiple subscriptions within the same tenant



Source: Types of attacks Azure DDoS Protection mitigates | Microsoft Learn

# Azure DDoS Protection

| Feature | DDoS IP Protection | DDoS Network Protection |
|---|---|---|
| Active traffic monitoring & always on detection | Yes | Yes |
| L3/L4 Automatic attack mitigation | Yes | Yes |
| Automatic attack mitigation | Yes | Yes |
| Application based mitigation policies | Yes | Yes |
| Metrics & alerts | Yes | Yes |
| Mitigation reports | Yes | Yes |
| Mitigation flow logs | Yes | Yes |
| Mitigation policies tuned to customers application | Yes | Yes |
| Integration with Firewall Manager | Yes | Yes |
| Microsoft Sentinel data connector and workbook | Yes | Yes |
| Protection of resources across subscriptions in a tenant | Yes | Yes |
| Public IP Standard tier protection | Yes | Yes |
| Public IP Basic tier protection | No | Yes |
| DDoS rapid response support | Not available | Yes |
| Cost protection | Not available | Yes |
| WAF discount | Not available | Yes |
| Price | Per protected IP | Per 100 protected IP addresses |



Source: About Azure DDoS Protection tier Comparison | Microsoft Learn

# Azure DDoS Protection 

- **Always-on traffic monitoring:** Your application traffic patterns are monitored 24 hours a day, 7 days a week, looking for indicators of DDoS attacks. Azure DDoS Protection instantly and automatically mitigates the attack, once it's detected.
- **Adaptive real time tuning:** Intelligent traffic profiling learns your application's traffic over time, and selects and updates the profile that is the most suitable for your service. The profile adjusts as traffic changes over time.
- **DDoS Protection analytics, metrics, and alerting:** Azure DDoS Protection applies three auto-tuned mitigation policies (TCP SYN, TCP, and UDP) for each public IP of the protected resource, in the virtual network that has DDoS enabled. The policy thresholds are auto-configured via machine learning-based network traffic profiling. DDoS mitigation occurs for an IP address under attack only when the policy threshold is exceeded.



Source: https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

# Azure DDoS Protection 

- **Attack analytics:** Get detailed reports in five-minute increments during an attack, and a complete summary after the attack ends. Stream mitigation flow logs to Microsoft Sentinel or an offline security information and event management (SIEM) system for near real-time monitoring during an attack.
- **Attack metrics:** Summarized metrics from each attack are accessible through Azure Monitor.
- **Attack alerting:** Alerts can be configured at the start and stop of an attack, and over the attack's duration, using built-in attack metrics. Alerts integrate into your operational software like Microsoft Azure Monitor logs, Splunk, Azure Storage, Email, and the Azure portal.
- **Azure DDoS Rapid Response:** During an active attack, Azure DDoS Network Protection enabled customers have access to the DDoS Rapid Response (DRR) team, who can help with attack investigation during an attack and post-attack analysis.
- **Native platform integration:** Natively integrated into Azure. Includes configuration through the Azure portal. Azure DDoS Protection understands your resources and resource configuration.



Source: https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

# Azure DDoS Protection 

- **Turnkey protection:** Simplified configuration immediately protects all resources on a virtual network as soon as DDoS Network Protection is enabled. No intervention or user definition is required. Similarly, simplified configuration immediately protects a public IP resource when DDoS IP Protection is enabled for it.
- **Multi-Layered protection:** When deployed with a web application firewall (WAF), Azure DDoS Protection protects both at the network layer (Layer 3 and 4, offered by Azure DDoS Protection) and at the application layer (Layer 7, offered by a WAF). WAF offerings include Azure Application Gateway WAF SKU and third-party web application firewall offerings available in the Azure Marketplace.
- **Extensive mitigation scale:** All L3/L4 attack vectors can be mitigated, with global capacity, to protect against the largest known DDoS attacks.
- **Cost guarantee:** Receive data-transfer and application scale-out service credit for resource costs incurred as a result of documented DDoS attacks.



Source: https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

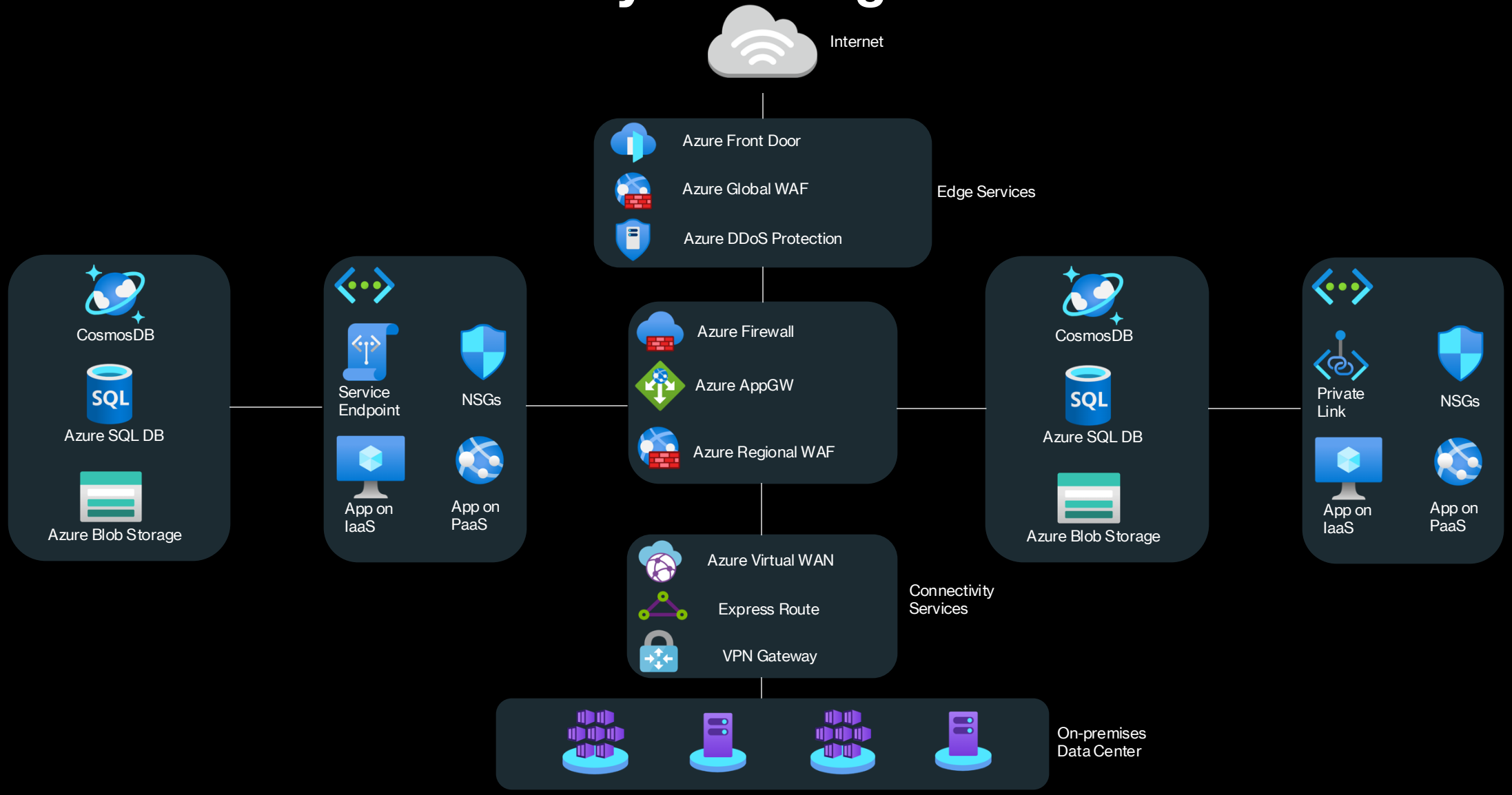
# Azure Traffic Manager 

- Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions.
- Traffic Manager also provides your public endpoints with high availability and quick responsiveness.
- Traffic Manager uses DNS to direct client requests to the appropriate service endpoint based on a traffic-routing method.
- Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure.
- Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models.
- Traffic Manager is resilient to failure, including the failure of an entire Azure region.



Source: https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

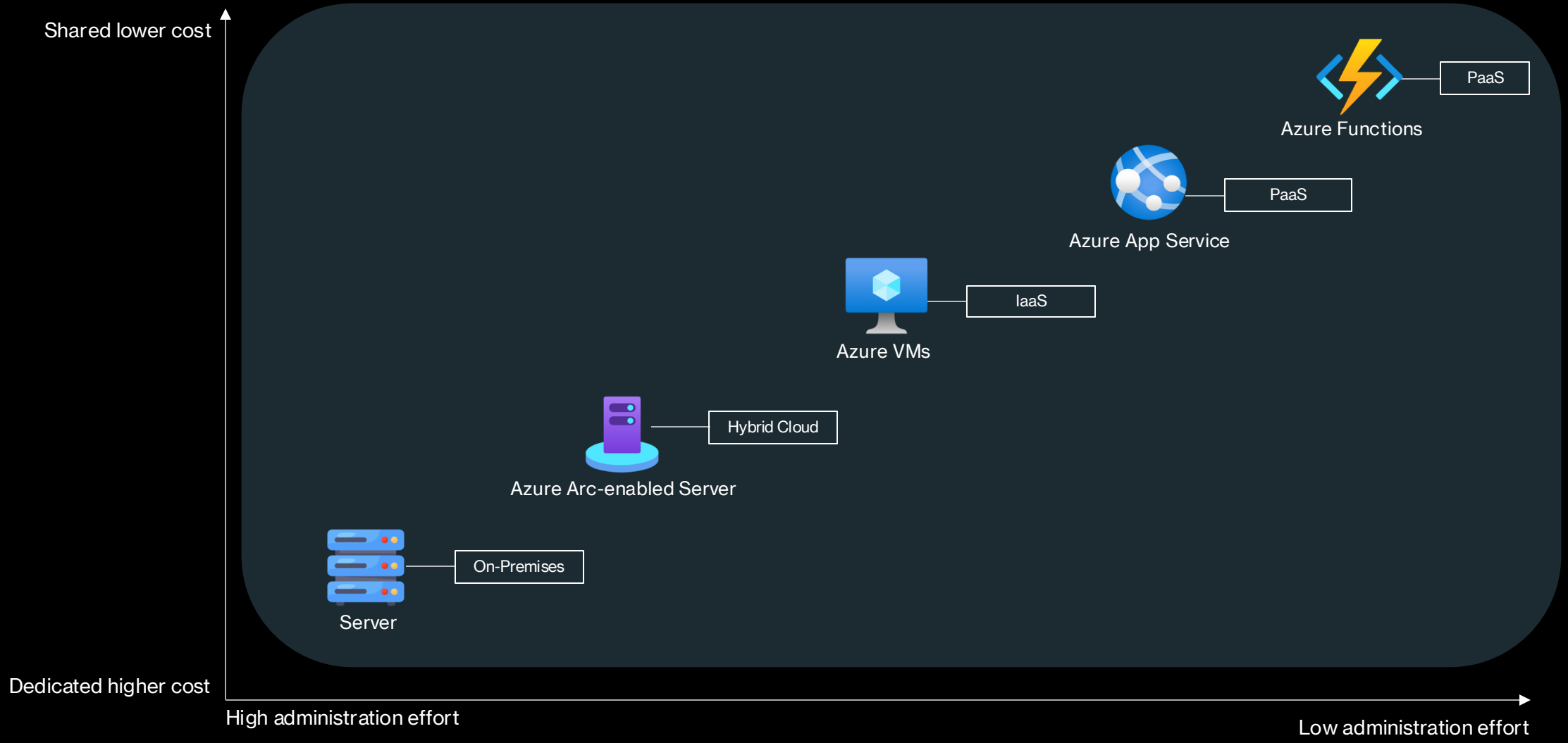
# Azure Network Security – The Big Picture




Christopher Nett

Source: [Network security concepts and requirements in Azure | Microsoft Learn]

# Azure Compute Services




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview?view=azuresql

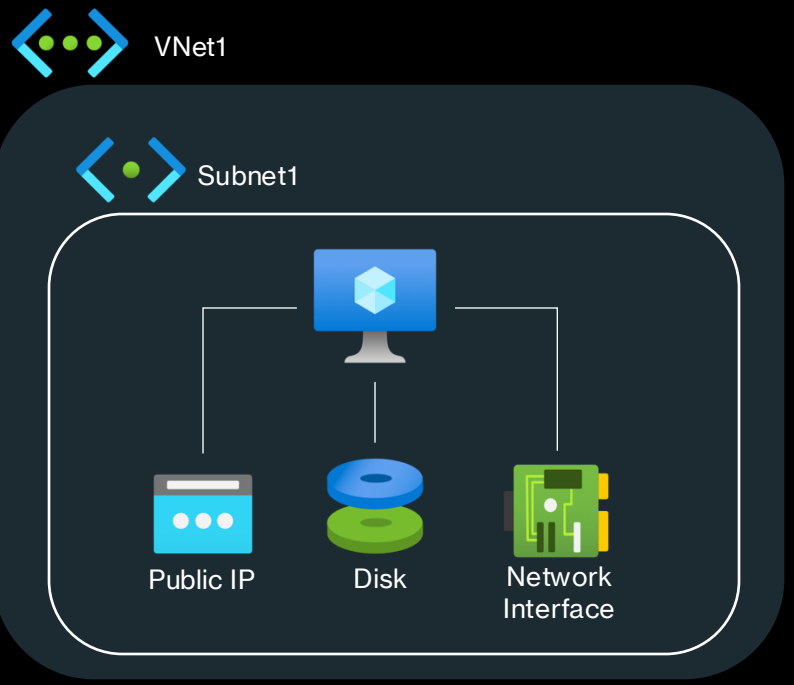
# Azure Virtual Machines (VMs) 

- Azure virtual machines (VMs) are one of several types of on-demand, scalable computing resources that Azure offers.
- Typically, you choose a virtual machine when you need more control over the computing environment than the other choices offer.
- An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it.
- However, you still need to maintain the virtual machine by performing tasks, such as configuring, patching, and installing the software that runs on it.



Source: https://learn.microsoft.com/en-us/azure/virtual-machines/overview

# Azure Virtual Machines (VMs)




Considerations:

- There are different VM types & SKUs for different use cases
- VMs require an Azure Vnet
- VMs require an OS disk



Source: https://learn.microsoft.com/en-us/azure/virtual-machines/overview

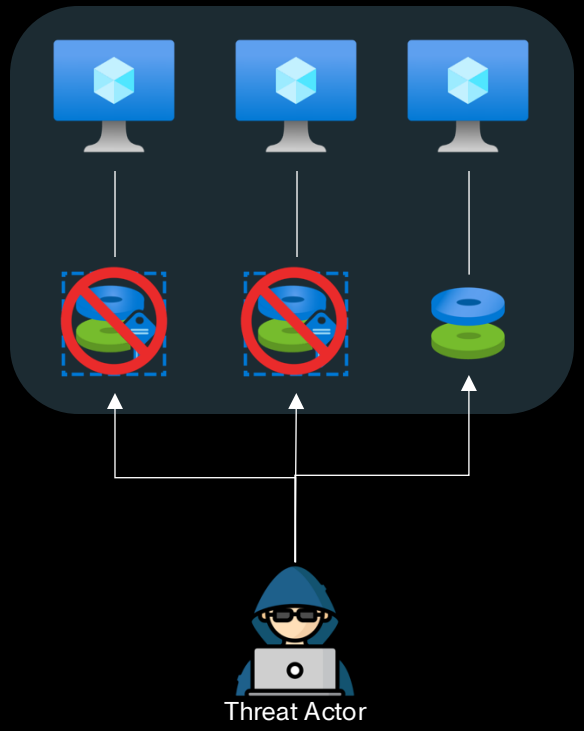
# Disk Encryption Options in Azure

- **Azure Disk Storage Server-Side Encryption** (also referred to as encryption-at-rest or Azure Storage encryption) is always enabled and automatically encrypts data stored on Azure managed disks (OS and data disks) when persisting on the Storage Clusters. When configured with a Disk Encryption Set (DES), it supports customer-managed keys as well. It doesn't encrypt temp disks or disk caches.
- **Encryption at host** is a Virtual Machine option that enhances Azure Disk Storage Server-Side Encryption to ensure that all temp disks and disk caches are encrypted at rest and flow encrypted to the Storage clusters.
- **Azure Disk Encryption** encrypts the OS and data disks of Azure virtual machines (VMs) inside your VMs by using the DM-Crypt feature of Linux or the BitLocker feature of Windows. ADE is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets, with the option to encrypt with a key encryption key (KEK).
- **Confidential disk encryption** binds disk encryption keys to the virtual machine's TPM and makes the protected disk content accessible only to the VM. The TPM and VM guest state is always encrypted in attested code using keys released by a secure protocol that bypasses the hypervisor and host operating system.



Source: https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview

# Azure Disk Encryption (ADE)



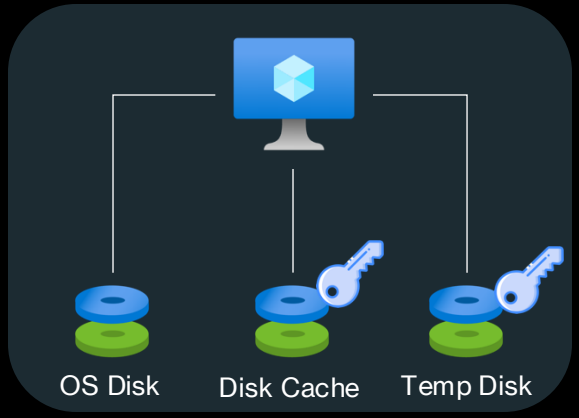

Considerations:

- All types and tiers of disks and VMs are supported for ADE, excluding ”Basic VMs” and “Ultra Disks”
- Azure Key Vault is used to store the encryption secret
- Windows: Bitlocker
- Linux: dm-crypt



Source: https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview

# Encryption at Host



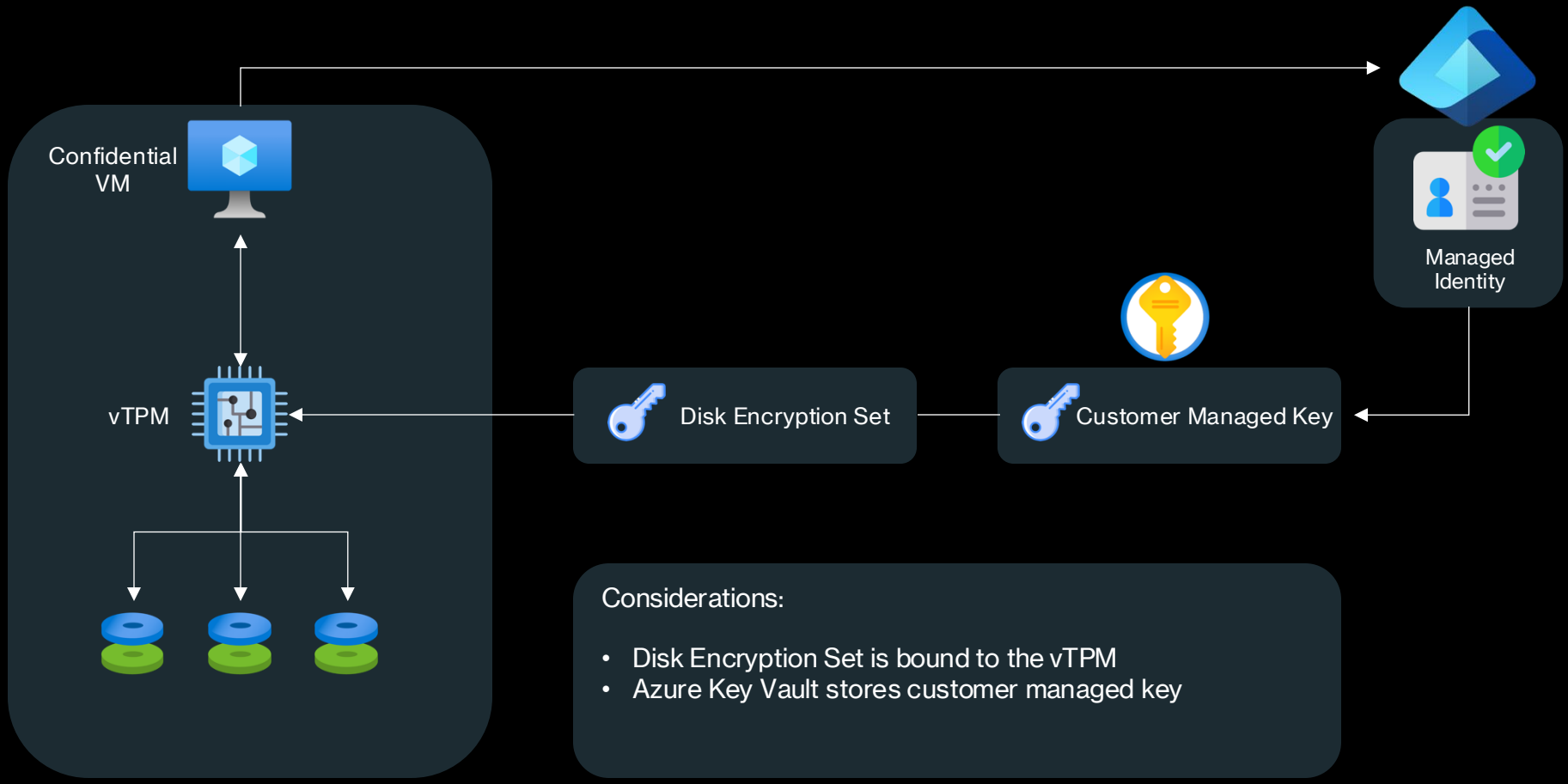

Considerations:

- Must be enabled at the subscription level first
- Protects the temp disks and disks caches of VMS without ADE
- Keys are stored in Azure Key Vault



Source: https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption#encryption-at-host---end-to-end-encryption-for-your-vm-data

# Confidential Disk Encryption






Source: https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview

# Azure Storage

| Azure Storage Types | |
|---|---|
| Blob Storage | A service for storing large amounts of unstructured data like text, images, and videos in scalable containers (blobs). |
| Azure Files | A fully managed cloud file share service that uses the standard SMB protocol, allowing shared file access across multiple virtual machines. |
| Queue Storage | A service designed for message queuing between application components, enabling asynchronous communication in distributed systems. |
| Table Storage | A NoSQL key-value store that allows for quick access to structured data with fast and scalable query support. |

Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-introduction

# Azure Storage

- An Azure Storage Account is a cloud-based service that provides scalable, highly available, and durable storage for various data types, including blobs, files, queues and tables.
- It acts as a unified container for multiple Azure storage services, enabling secure access, redundancy options, and data management features, all while supporting different storage tiers for cost and performance optimization.




Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview

# Azure Storage 

| Type of storage account | Supported storage services | Redundancy options | Usage |
|---|---|---|---|
| Standard general-purpose v2 | Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files | Locally redundant storage (LRS) / geo-redundant storage (GRS) / read-access geo-redundant storage (RA-GRS)<br><br>Zone-redundant storage (ZRS) / geo-zone-redundant storage (GZRS) / read-access geo-zone-redundant storage (RA-GZRS) | Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type. |
| Premium block blobs | Blob Storage (including Data Lake Storage[1]) | LRS<br><br>ZRS | Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency |
| Premium file shares | Azure Files | LRS<br><br>ZRS | Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares. |
| Premium page blobs | Page blobs only | LRS<br><br>ZRS | Premium storage account type for page blobs only. |



Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview

# Azure Storage

- Multiple Azure storage services can co-exist in the same storage account
- Storage services are built for public accessibility with public endpoints but you can also leverage private endpoints
- Storage accounts have properties:
  - Name
  - Performance
  - Type
  - Redundancy




Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-introduction

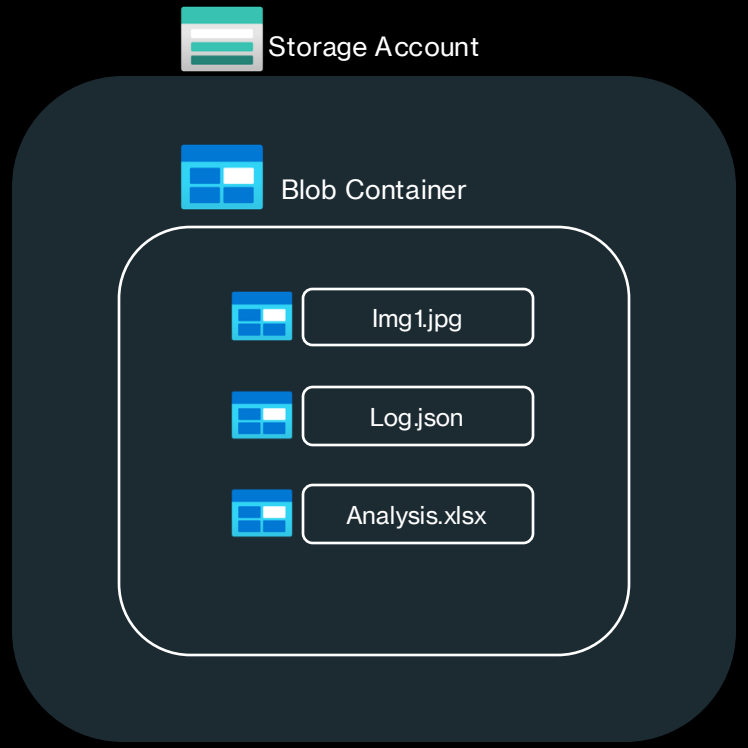
# Azure Blob Storage 

- Azure Blob Storage is Microsoft's object storage solution for the cloud. Blob Storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that doesn't adhere to a particular data model or definition, such as text or binary data.
- Blob Storage is designed for:
  - Serving images or documents directly to a browser.
  - Storing files for distributed access.
  - Streaming video and audio.
  - Writing to log files.
  - Storing data for backup and restore, disaster recovery, and archiving.
  - Storing data for analysis by an on-premises or Azure-hosted service.



Source: https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

# Azure Blob Storage




- Storage Account
  - Requires GPv2, BlockBlob or PageBlob
- Blob Container
  - The container for managing access to unstructured data
- Blobs
  - Blobs are the actual objects that are stored in the container

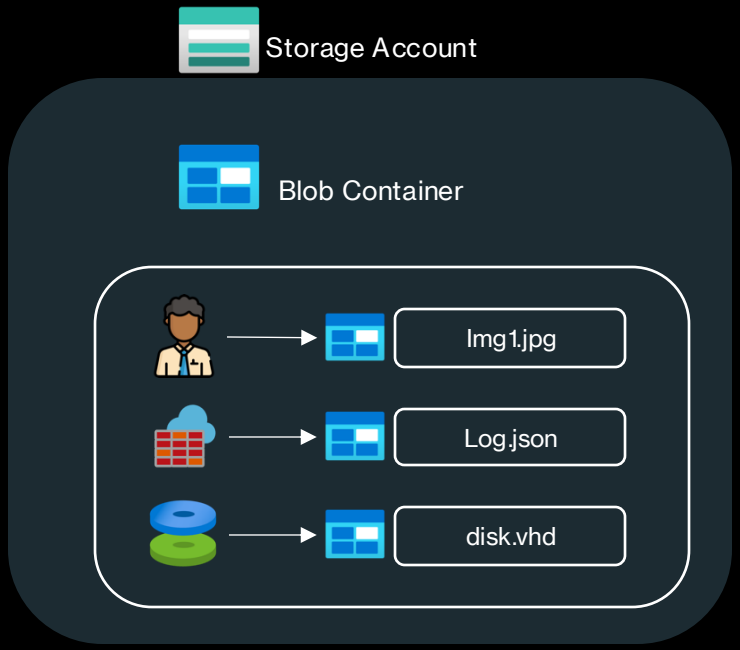


Source: https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

# Azure Blob Storage

Azure Storage supports three types of blobs:

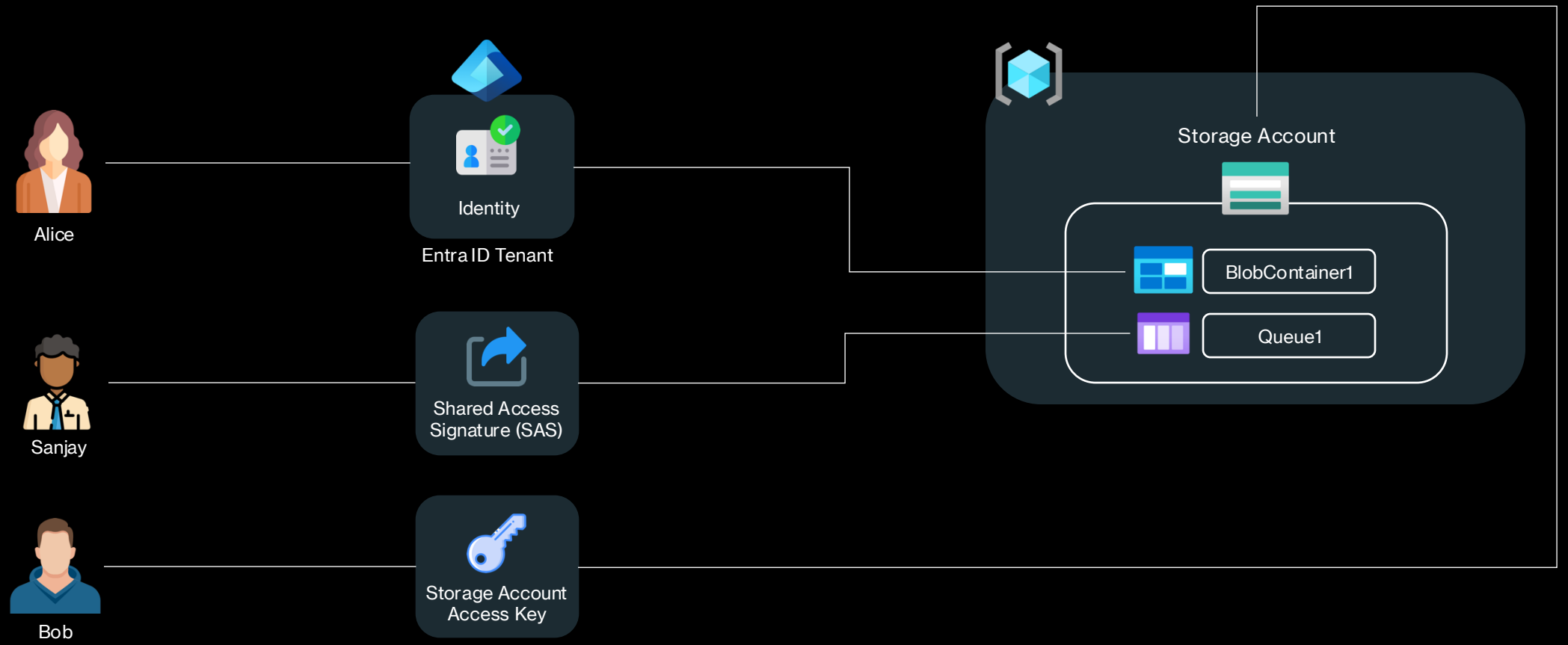
- Block blobs store text and binary data. Block blobs are made up of blocks of data that can be managed individually. Block blobs can store up to about 190.7 TiB.
- Append blobs are made up of blocks like block blobs, but are optimized for append operations. Append blobs are ideal for scenarios such as logging data from virtual machines.
- Page blobs store random access files up to 8 TiB in size. Page blobs store virtual hard drive (VHD) files and serve as disks for Azure virtual machines.






Source: https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

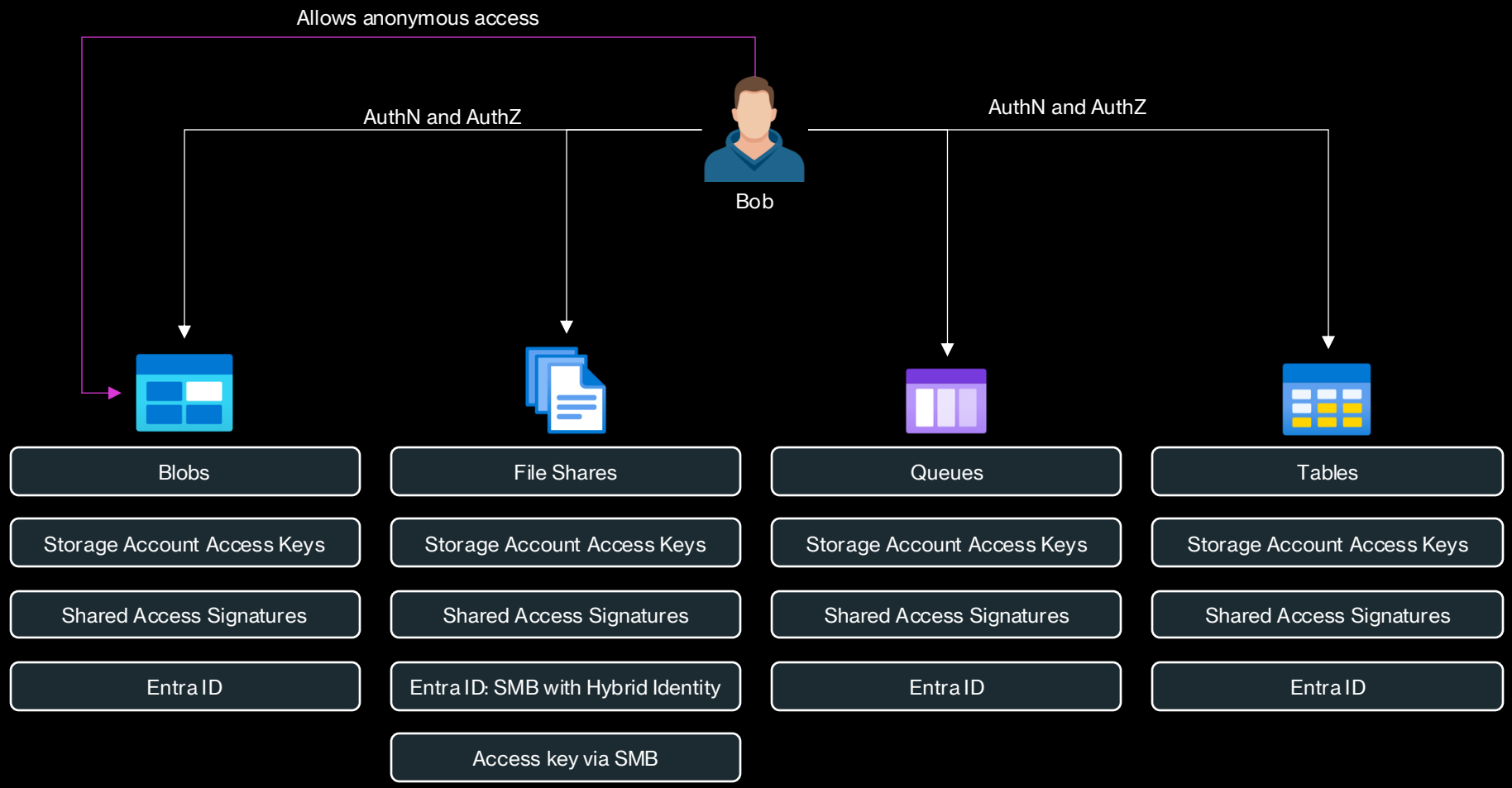
# AuthN and AuthZ for Azure Storage






Source: https://learn.microsoft.com/en-us/azure/storage/common/authorize-data-access?tabs=blobs

# AuthN and AuthZ for Azure Storage






Source: https://learn.microsoft.com/en-us/azure/storage/common/authorize-data-access?tabs=blobs

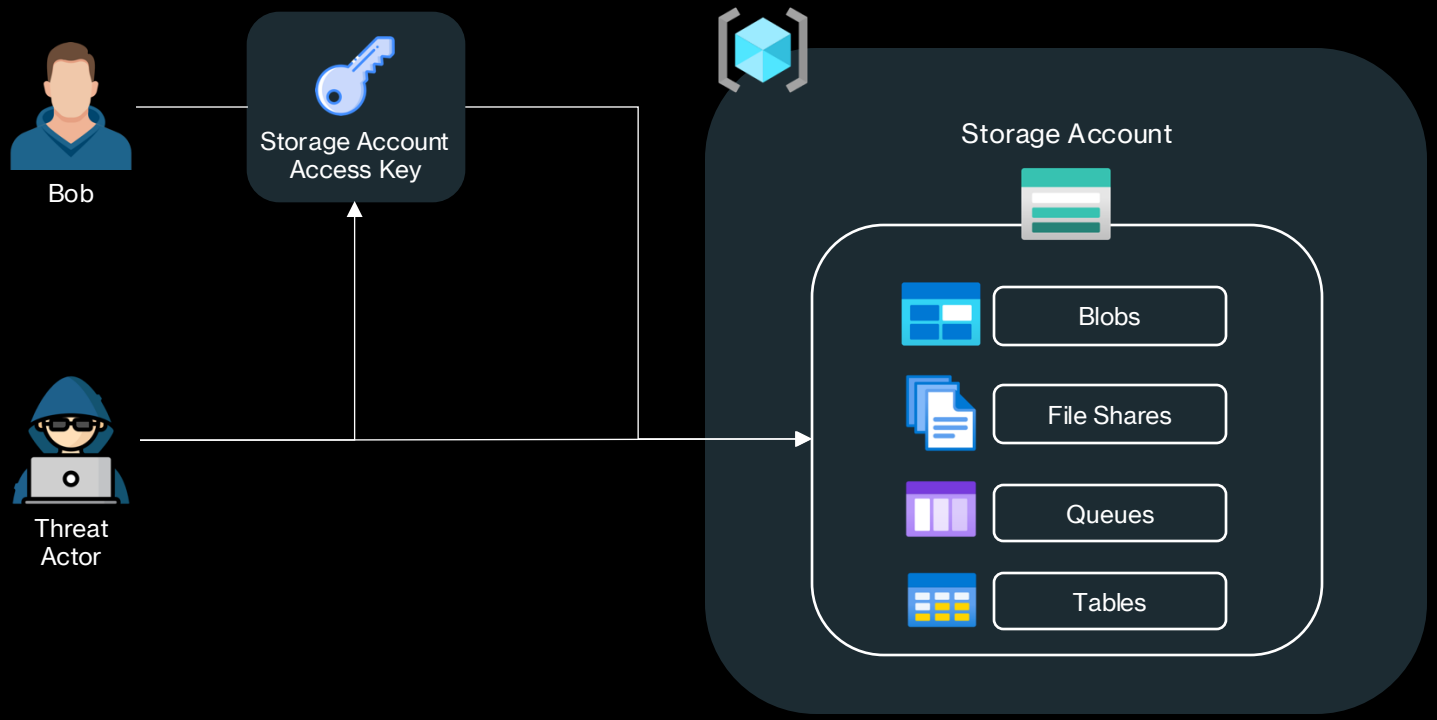
# Storage Account Access Keys

- When you create a storage account, Azure generates two 512-bit storage account access keys for that account. These keys can be used to authorize access to data in your storage account via Shared Key authorization, or via SAS tokens that are signed with the shared key.
- Microsoft recommends that you use Azure Key Vault to manage your access keys, and that you regularly rotate and regenerate your keys. Using Azure Key Vault makes it easy to rotate your keys without interruption to your applications. You can also manually rotate your keys.
- For optimal security, Microsoft recommends using Microsoft Entra ID with managed identities to authorize requests against blob, queue, and table data, whenever possible. Authorization with Microsoft Entra ID and managed identities provides superior security and ease of use over Shared Key authorization



Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal

# Storage Account Access Keys

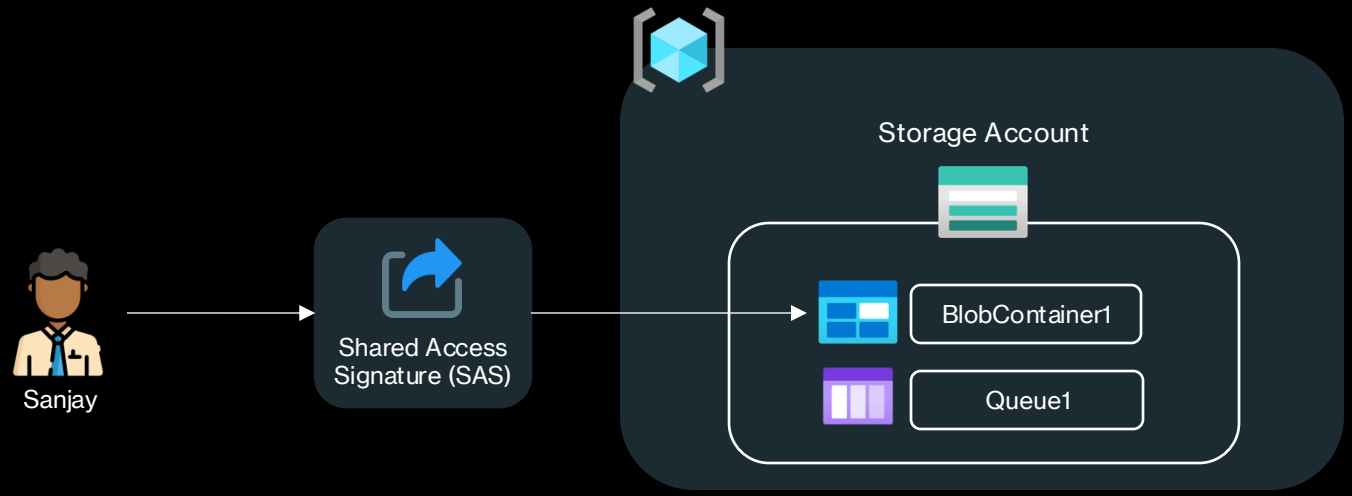





Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal

# Shared Access Signatures

- Azure Storage supports three types of shared access signatures:
  - User delegation SAS
  - Service SAS
  - Account SAS

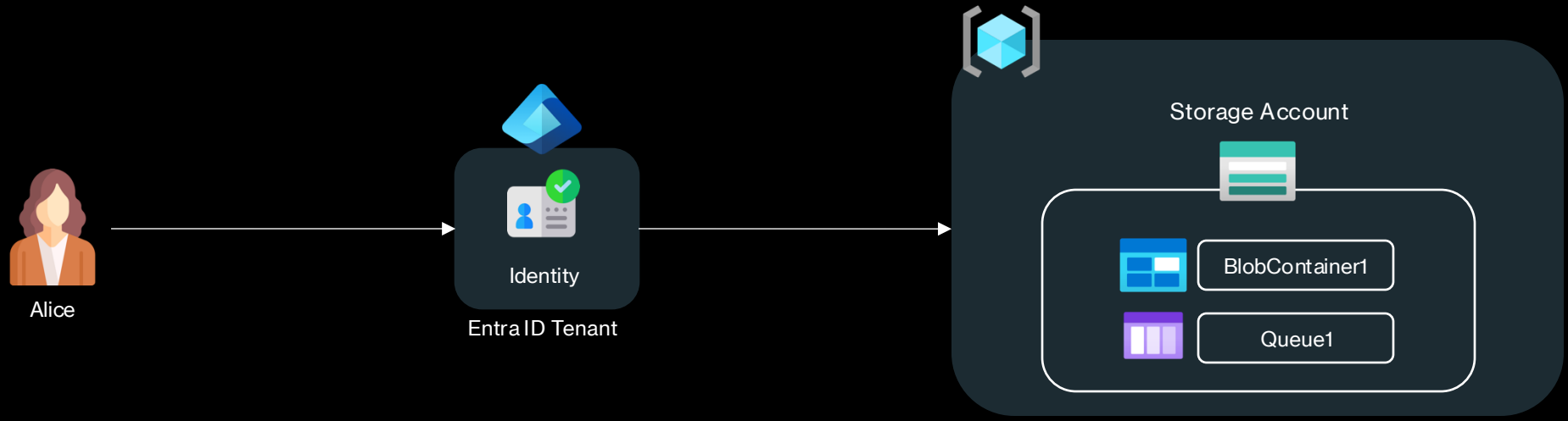



| User Delegation SAS | Service SAS | Account SAS |
| --- | --- | --- |
| • A user delegation SAS is secured with Microsoft Entra credentials and by the permissions specified for the SAS.<br>• A user delegation SAS applies to Blob storage only. | • A service SAS is secured with the storage account key.<br>• A service SAS delegates access to a resource in only one of the Azure Storage services: Blob storage, Queue storage, Table storage, or Azure Files. | • An account SAS is secured with the storage account key. An account SAS delegates access to resources in one or more of the storage services.<br>• All of the operations available via a service or user delegation SAS are also available via an account SAS. |



Source: https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview

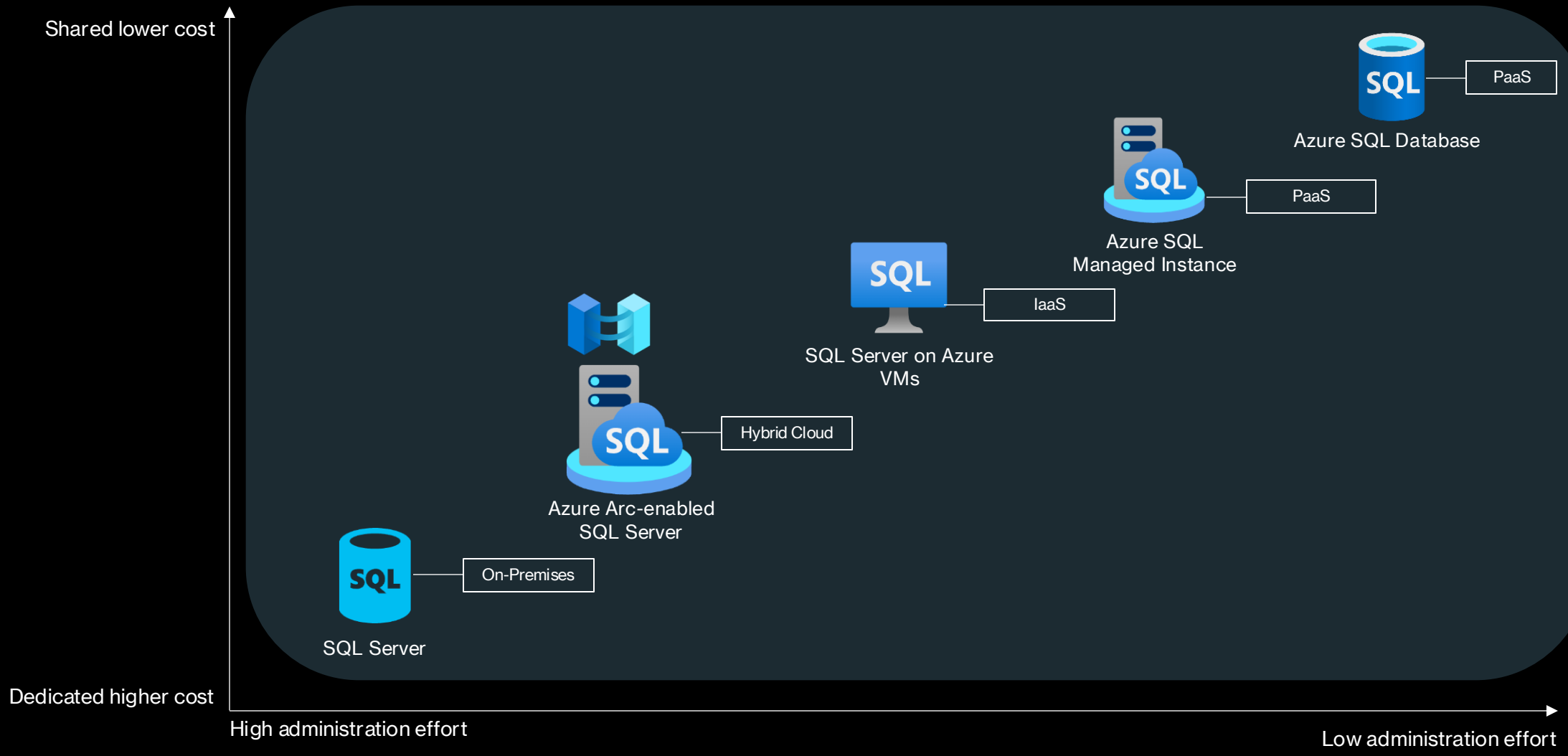
# Entra ID based Authentication






Source: https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory

# Azure SQL






Source: https://learn.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview?view=azuresql

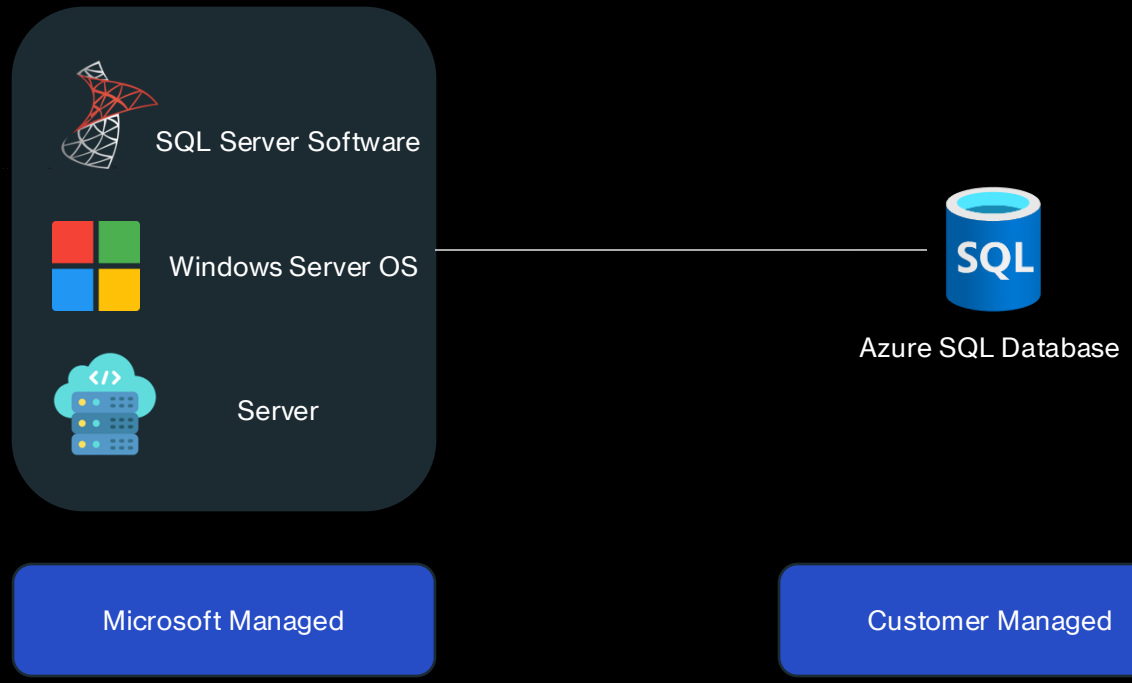
# Azure SQL Database 


- SQL Database is a fully managed service that has built-in high availability, backups, and other common maintenance operations.
- Microsoft handles all patching and updating of the SQL and operating system code. You don't have to manage the underlying infrastructure.



Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql

# Azure SQL Database






Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql

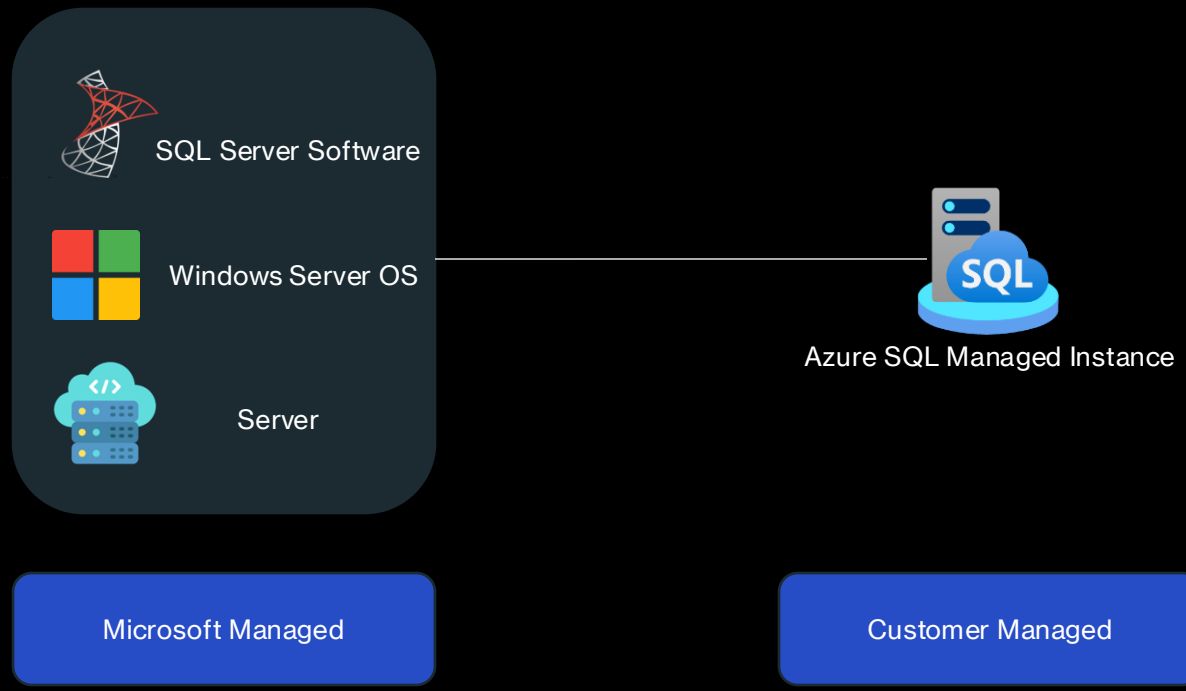
# Azure SQL Managed Instance 


- Azure SQL Managed Instance is a scalable cloud database service that's always running on the latest stable version of the Microsoft SQL Server database engine and a patched OS with 99.99% built-in high availability, offering close to 100% feature compatibility with SQL Server.
- PaaS capabilities built into Azure SQL Managed Instance enable you to focus on domain-specific database administration and optimization activities that are critical for your business while Microsoft handles backups.
- In addition, Microsoft handles patching and updating of the SQL and operating system code, which removes the burden on managing the underlying infrastructure.



Source: https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview?view=azuresql

# Azure SQL Managed Instance






Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql

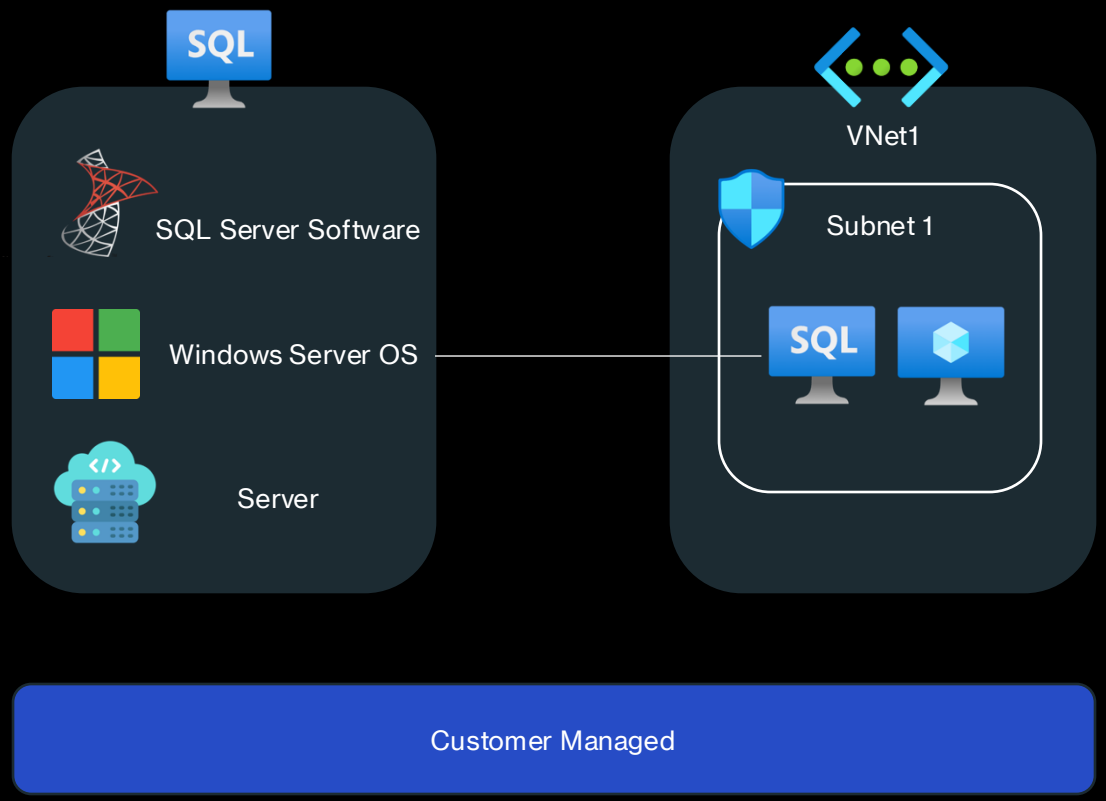
# SQL Server on Azure VMs 


- SQL Server on Azure Virtual Machines enables you to use full versions of SQL Server in the cloud without having to manage any on-premises hardware.
- SQL Server virtual machines (VMs) also simplify licensing costs when you pay as you go.
- Azure virtual machines run in many different geographic regions around the world. They also offer various machine sizes.
- The virtual machine image gallery allows you to create a SQL Server VM with the right version, edition, and operating system.
- This makes virtual machines a good option for many different SQL Server workloads.



Source: https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-on-azure-vm-iaas-what-is-overview?view=azuresql

# SQL Server on Azure VMs




- IaaS
- Full installation of SQL Server on the OS of the VM
- Responsibility for operations is with the customer
- Responsibility for backups and HA is with the customer



Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql

# Azure Arc-Enabled SQL Server 


- SQL Server enabled by Azure Arc extends Azure services to SQL Server instances hosted outside of Azure: in your data center, in edge site locations like retail stores, or any public cloud or hosting provider.
- Managing SQL Server through Azure Arc can also be configured for SQL Server VMs in Azure VMware Solution



Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql

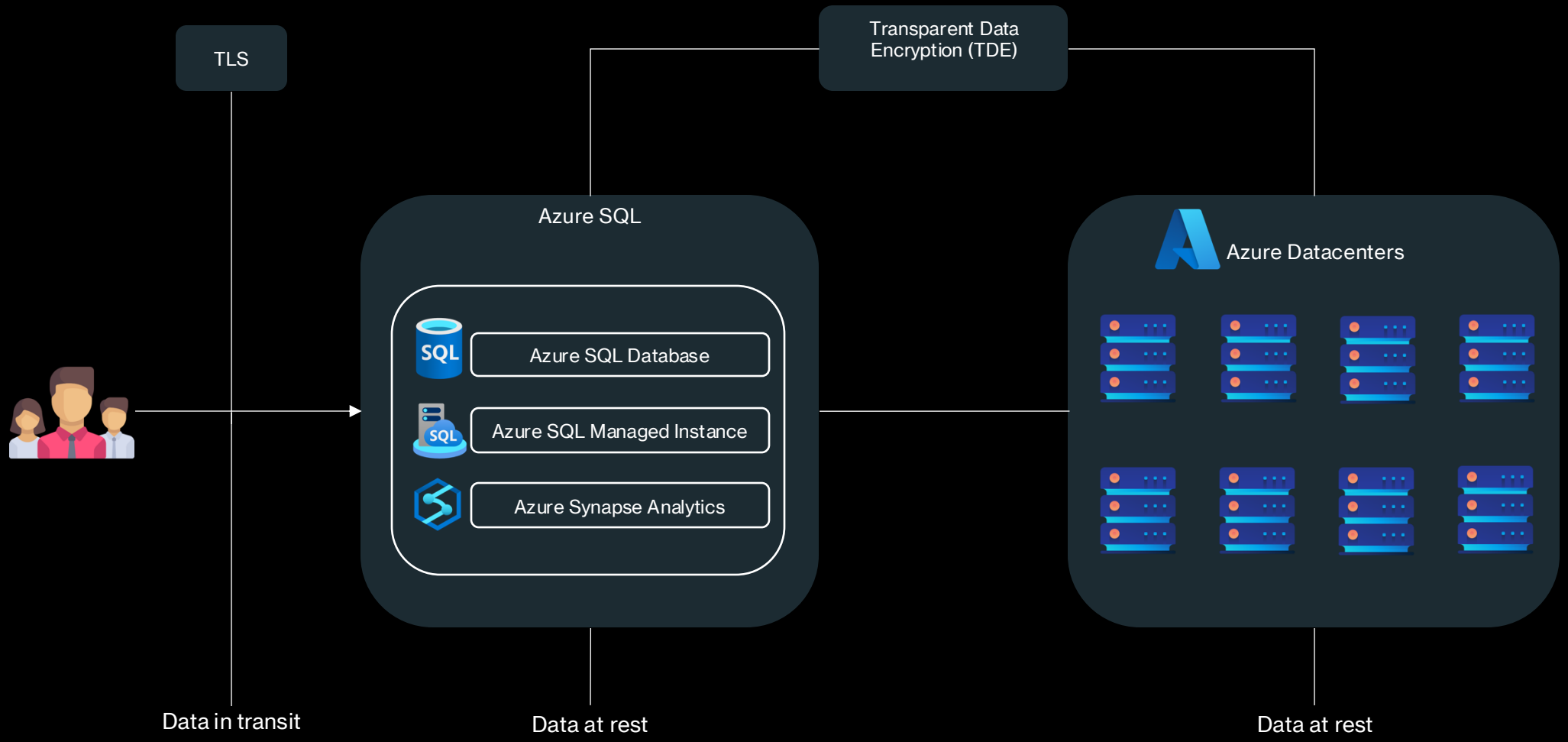
# Azure SQL Transparent Data Encryption (TDE)

- Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics against the threat of malicious offline activity by encrypting data at rest.
- It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.
- By default, TDE is enabled for all newly deployed Azure SQL Databases and must be manually enabled for older databases of Azure SQL Database.
- For Azure SQL Managed Instance, TDE is enabled at the instance level and newly created databases.
- TDE must be manually enabled for Azure Synapse Analytics.



Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?view=azuresql&tabs=azure-portal

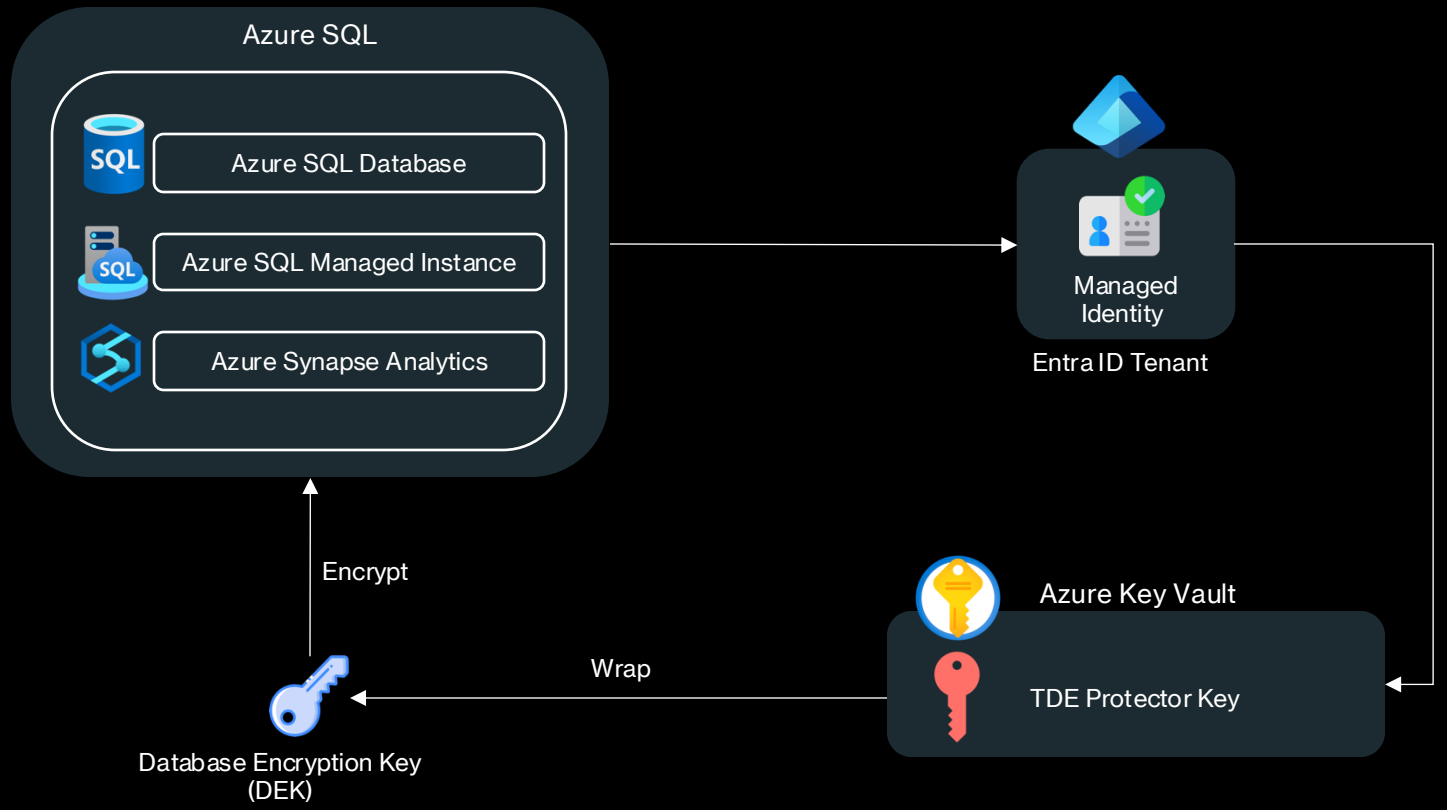
# Azure SQL Transparent Data Encryption (TDE)






Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?view=azuresql&tabs=azure-portal

# Azure SQL TDE – Key Management




Considerations:

- Applies to Azure SQL DB, Azure SQL Managed Instance and Azure Synapse Analytics
- DEK leverages AES-256
- Protector Key leverages RSA 3072
- A Managed Identity is required to access Azure Key Vault



Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?view=azuresql&tabs=azure-portal

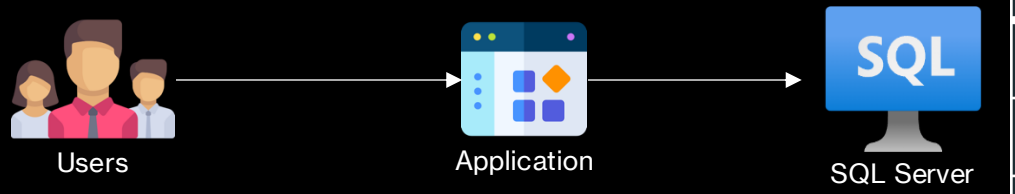
# Azure SQL Always Encrypted

- Always Encrypted and Always Encrypted with secure enclaves are features designed to safeguard sensitive information, including credit card numbers and national or regional identification numbers (such as U.S. social security numbers), in Azure SQL Database, Azure SQL Managed Instance, and SQL Server databases.
- It enables clients to encrypt sensitive data within client applications, ensuring that encryption keys are never exposed to the Database Engine.
- This provides a separation between those who own the data and can view it, and those who manage the data but should have no access: on-premises database administrators, cloud database operators, or other high-privileged unauthorized users.
- As a result, Always Encrypted allows customers to securely store their sensitive data in the cloud, reducing the risk of data theft by malicious insiders.
- Always Encrypted ensures that encryption is seamless for applications.
- On the client-side, Always Encrypted-enabled driver encrypts sensitive data before sending it to the Database Engine and automatically rewrites queries to maintain application semantics. It also automatically decrypts query results from encrypted database columns.

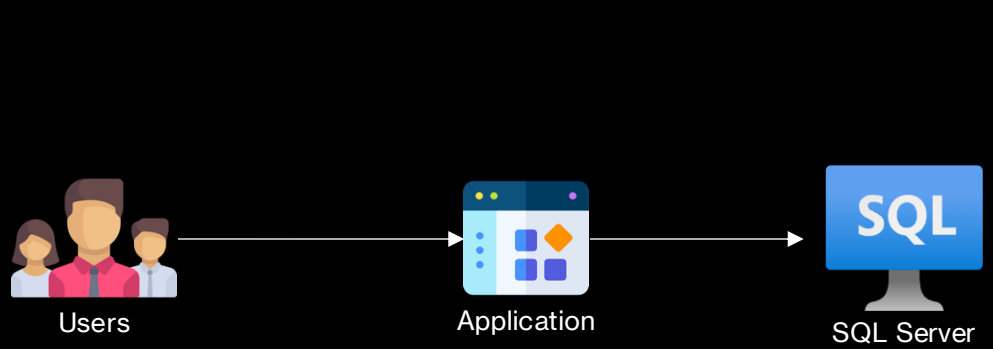


Source: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver16

# Azure SQL Always Encrypted




| ID | Credit Card Number | Expiry | Code |
|---|---|---|---|
| 123 | 1234-5678-1234-5678 | 01/2025 | 456 |
| 456 | 1234-5555-3333-2222 | 01/2026 | 789 |
| 789 | 1234-7777-8888-9999 | 01/2027 | 123 |

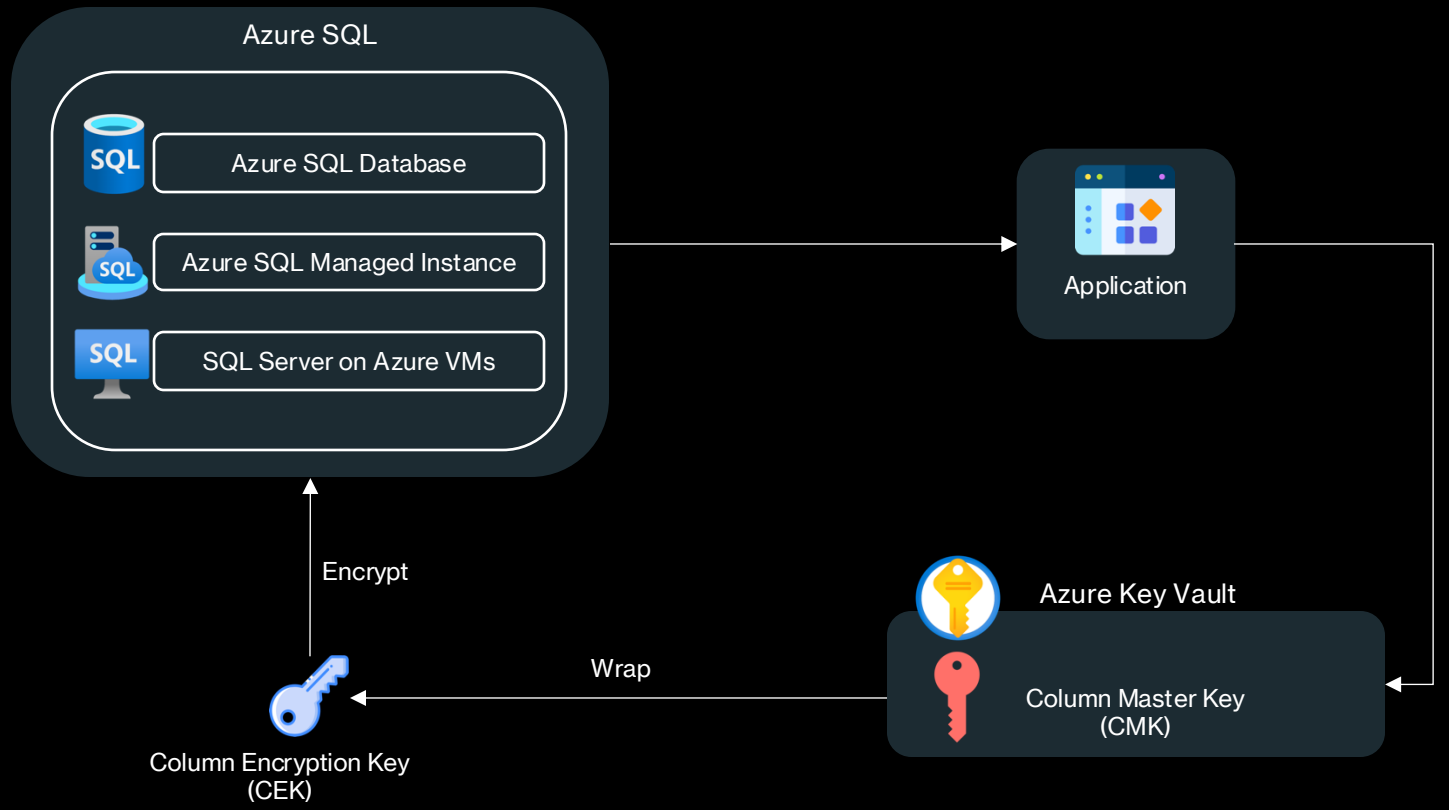



| ID | Credit Card Number | Expiry | Code |
|---|---|---|---|
| 123 | 0x01G0A1B2N6... | 01/2025 | 456 |
| 456 | 0x01F9M6H7E4... | 01/2026 | 789 |
| 789 | 0x01R4C5A9H1... | 01/2027 | 123 |



Source: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver16

# Azure SQL Always Encrypted




Considerations:

- Applies to Azure SQL DB, Azure SQL Managed Instance and SQL Server on Azure VMs
- You can encrypt one or more columns
- CMK must be stored in Azure Key Vault or a Windows Certificate Store



Source: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver16

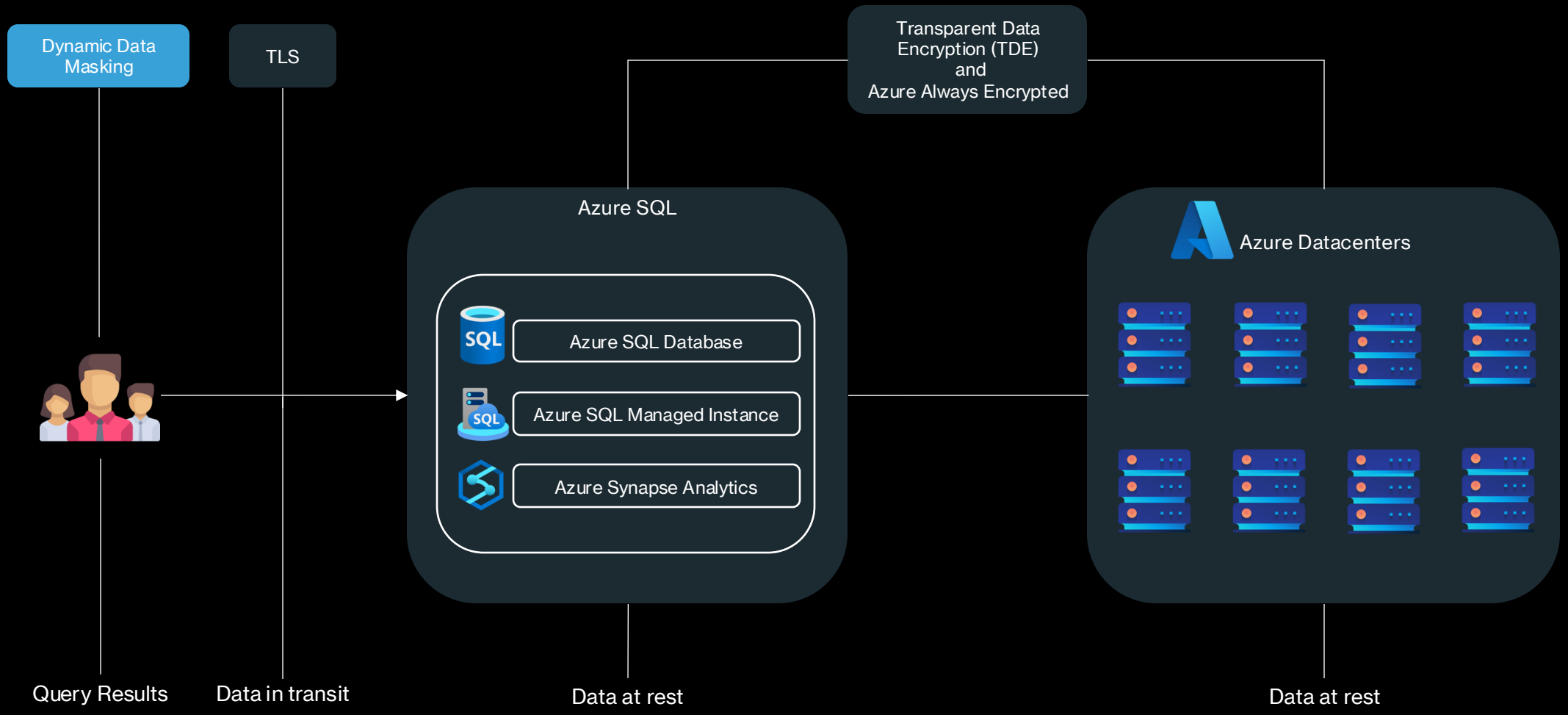
# Azure SQL Dynamic Data Masking

- Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics support dynamic data masking (DDM). Dynamic data masking limits sensitive data exposure by masking it to nonprivileged users.
- Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal effect on the application layer.
- It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database isn't changed.
- For example, a service representative at a call center might identify a caller by confirming several characters of their email address, but the complete email address shouldn't be revealed to the service representative.



Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

# Azure SQL Dynamic Data Masking

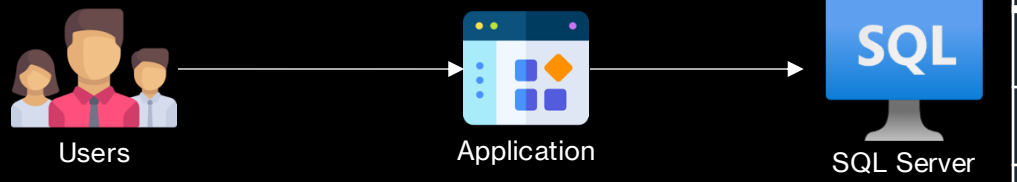





Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

# Azure SQL Dynamic Data Masking


| ID | Credit Card Number | Expiry | Code |
|---|---|---|---|
| 123 | 1234-5678-1234-5678 | 01/2025 | 456 |
| 456 | 1234-5555-3333-2222 | 01/2026 | 789 |
| 789 | 1234-7777-8888-9999 | 01/2027 | 123 |




| ID | Credit Card Number | Expiry | Code |
|---|---|---|---|
| 123 | XXXX-XXX-XXX-5678 | 01/2025 | 456 |
| 456 | XXXX-XXX-XXX-2222 | 01/2026 | 789 |
| 789 | XXXX-XXX-XXX-9999 | 01/2027 | 123 |



Source: https://learn.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

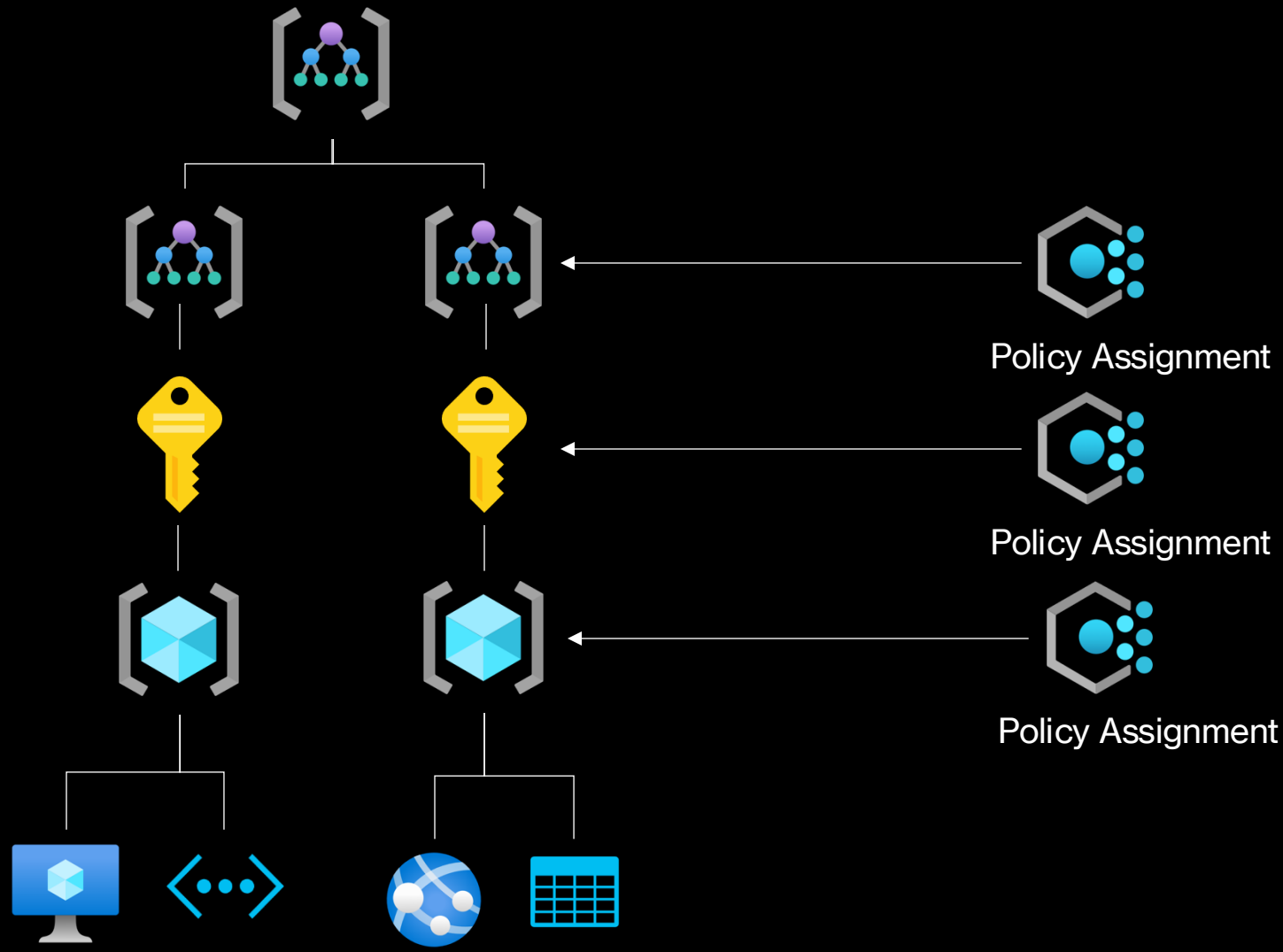
# Azure Policy

- An Azure Policy defines a desired configuration of an Azure resource
- Azure Policy evaluates resources and actions in Azure by comparing the properties of those resources to business rules.
- These business rules, described in JSON format, are known as policy definitions.
- To simplify management, several business rules can be grouped together to form a policy initiative (sometimes called a policySet).
- Defender for Cloud utilizes Azure Policy for all security recommendations
- Azure Policy examples in the context of security:
  - Enforce the deployment of defender for servers for all VMs
  - Audit whether an NSG is associated with a subnet
  - Deny resource creation if vulnerabilities are identified



Source: https://learn.microsoft.com/en-us/azure/governance/policy/overview

# Azure Policy



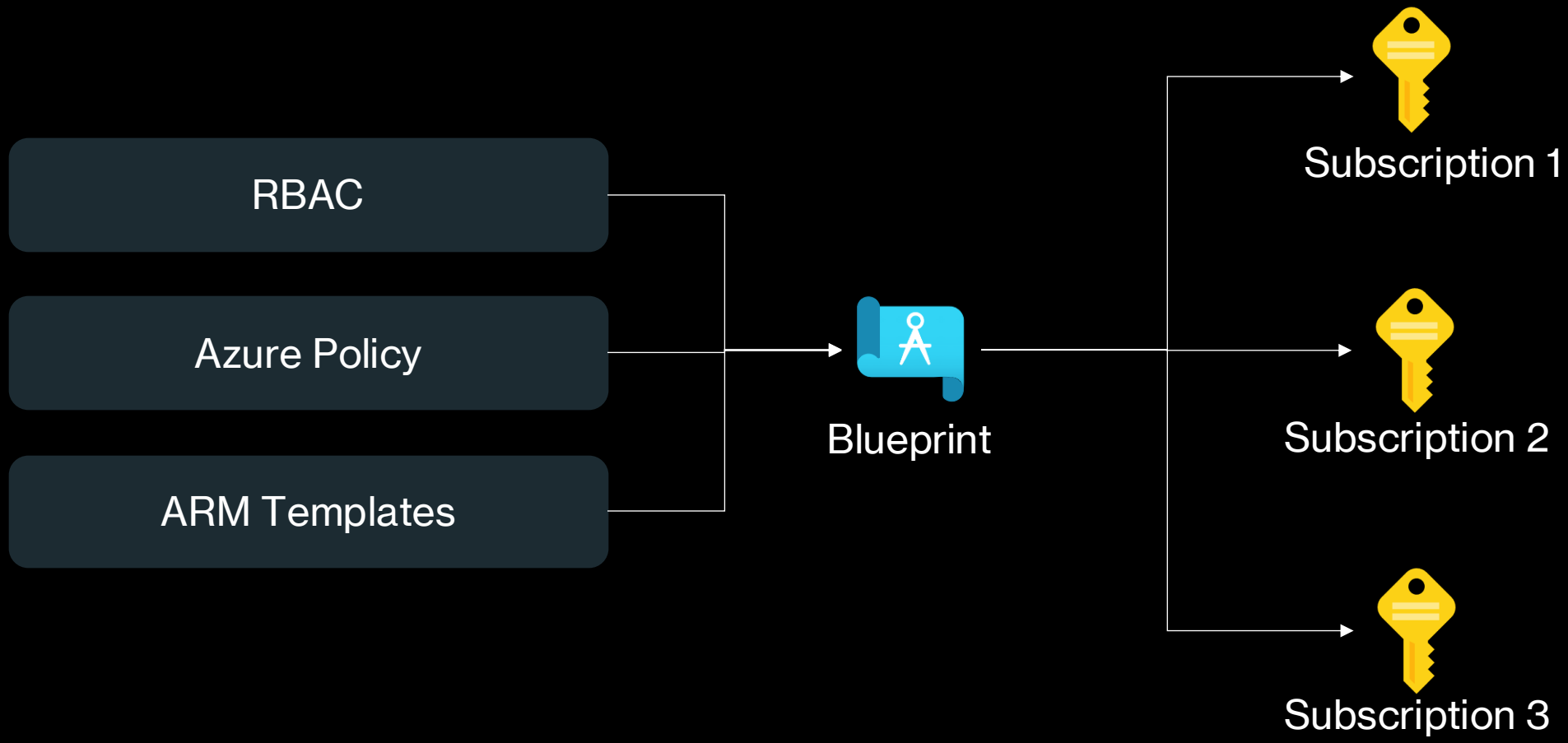
# Azure Policy Effects

- These effects are currently supported in a policy definition:
  - AddToNetworkGroup
  - Append
  - Audit
  - AuditIfNotExists
  - Deny
  - DenyAction
  - DeployIfNotExists
  - Disabled
  - Manual
  - Modify
  - Mutate



Source: Understand how effects work - Azure Policy | Microsoft Learn

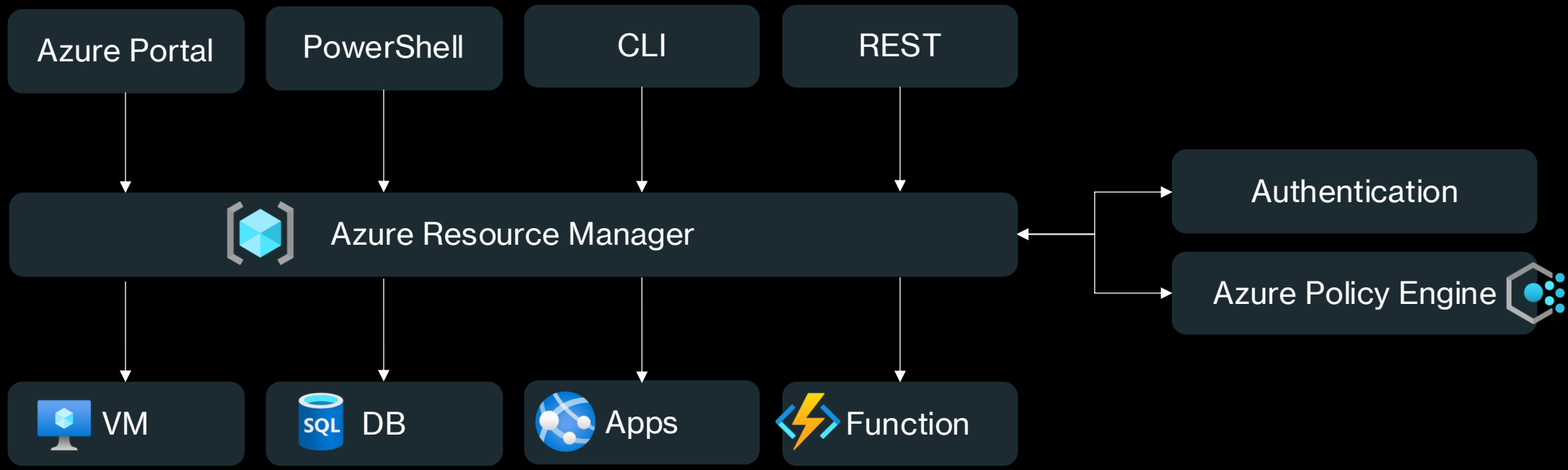
# Azure Blueprints






Source: https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

# Azure Resource Manager






Source: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview

# Azure Landing Zones

- An Azure landing zone is an environment that follows key design principles across eight design areas.
- These design principles accommodate all application portfolios and enable application migration, modernization, and innovation at scale.
- An Azure landing zone uses subscriptions to isolate and scale application resources and platform resources.
- Subscriptions for application resources are called application landing zones, and subscriptions for platform resources are called platform landing zones.



Source: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

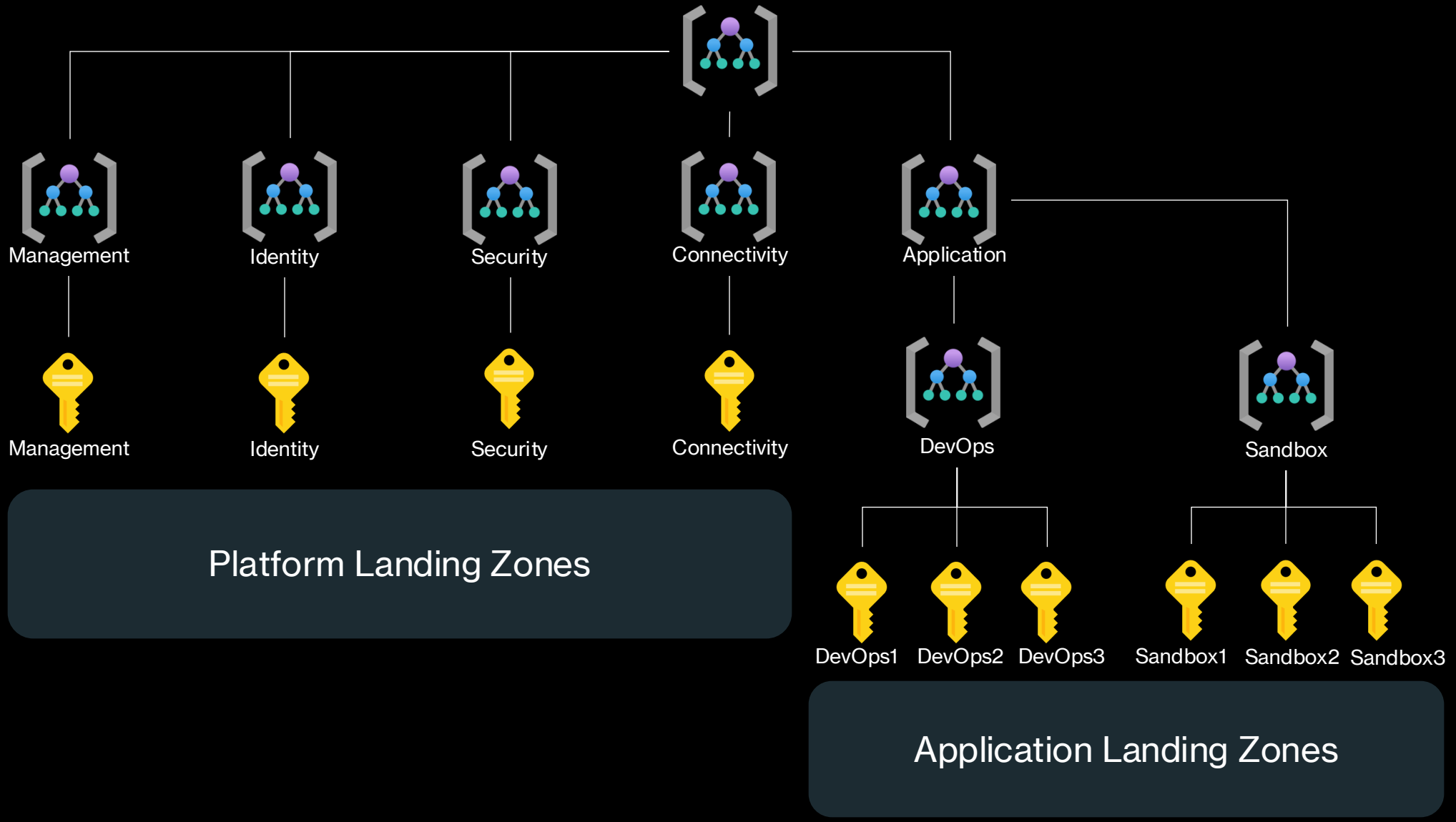
# Azure Landing Zones

- An Azure landing zone consists of platform landing zones and application landing zones.
- **Platform landing zone:** A platform landing zone is a subscription that provides shared services (identity, connectivity, management) to applications in application landing zones. Consolidating these shared services often improves operational efficiency. One or more central teams manage the platform landing zones.
- **Application landing zone:** An application landing zone is a subscription for hosting an application. You pre-provision application landing zones through code and use management groups to assign policy controls to them.



Source: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

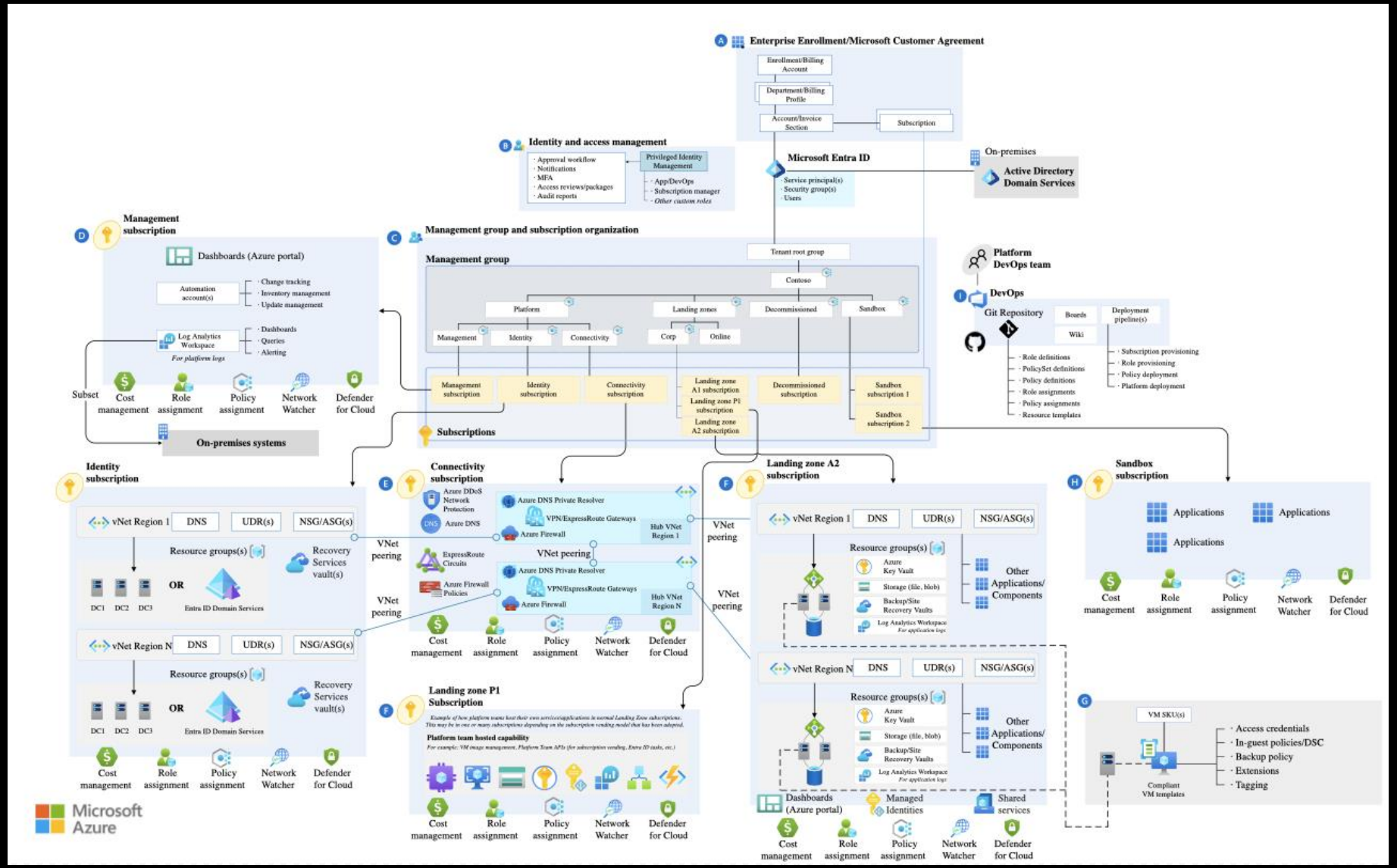
# Azure Landing Zones




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

# Azure Landing Zones




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

# Azure Key Vault

Certificates

Digital certificates used for cryptographic purposes.

Keys

Public and private keys used for cryptographic purposes.

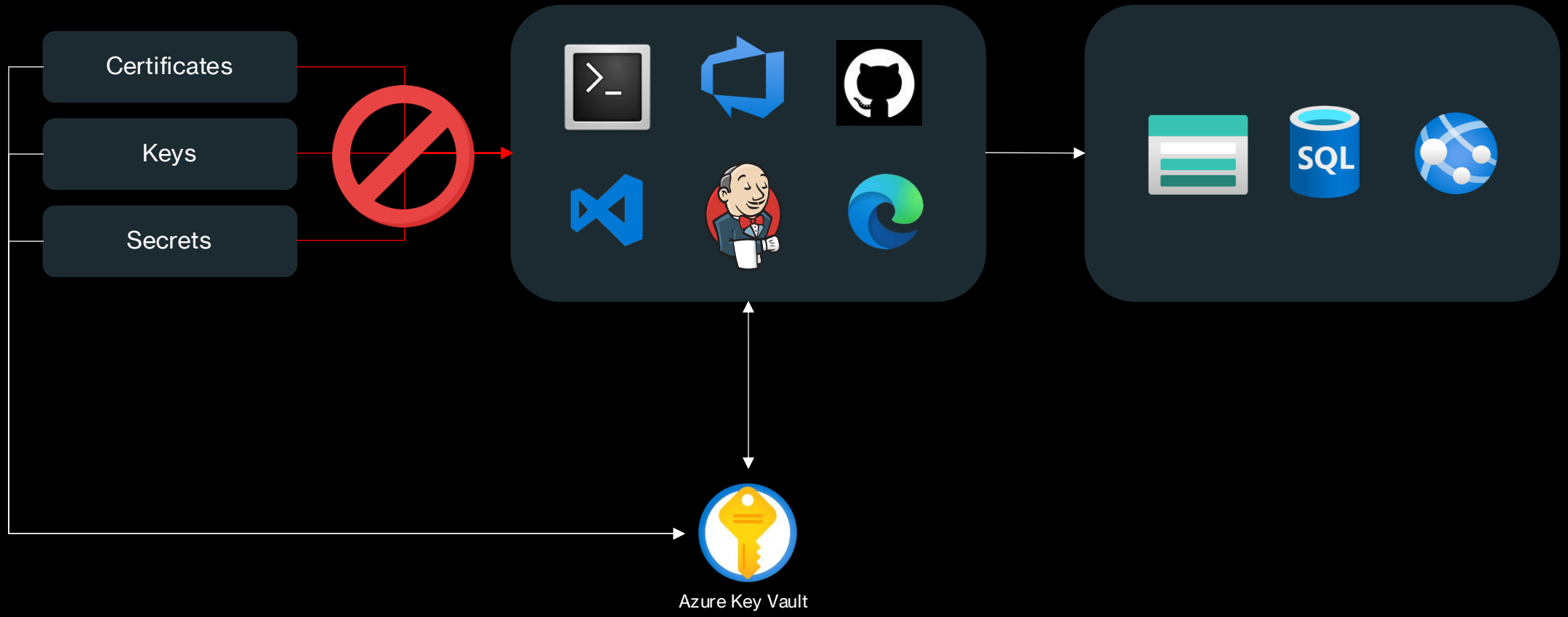
Secrets

Passwords, API keys and other secrets used for authentication.



Source: https://learn.microsoft.com/en-us/azure/key-vault/general/overview

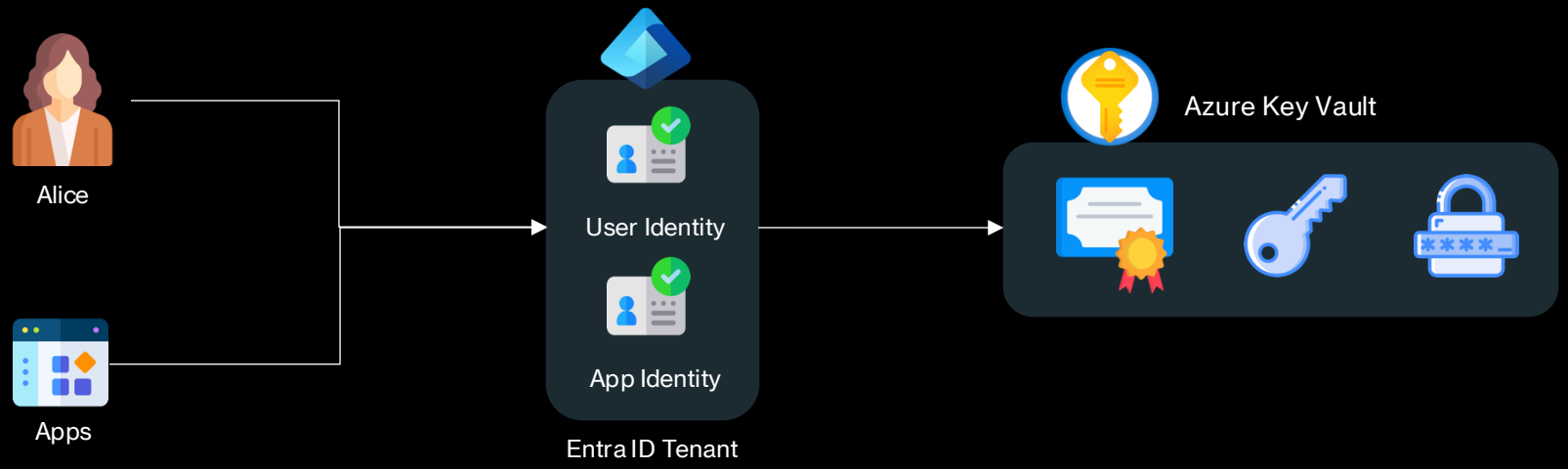
# Azure Key Vault






Source: https://learn.microsoft.com/en-us/azure/key-vault/general/overview

# AuthN and AuthZ in Azure Key Vault

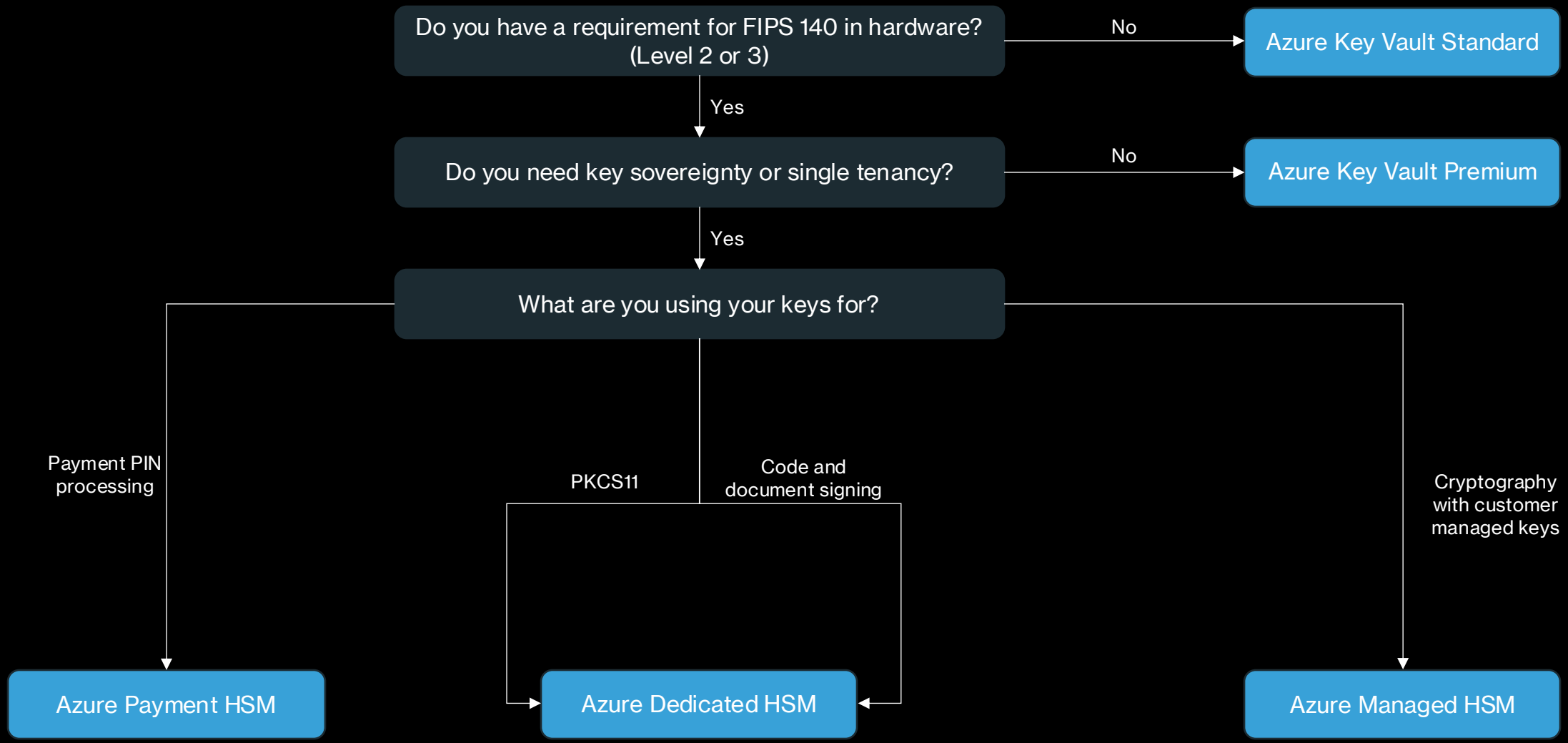



- An identity in Entra ID is required to access Azure Key Vault
- Access keys or SAS do not exist for Azure Key Vault
- Managed identities are highly recommended for apps
- Data should be protected with soft delete and purge protection



Source: https://learn.microsoft.com/en-us/azure/key-vault/general/overview

# Azure Key Vault Tiers




Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management-choose

# Dedicated HSM

- FIPS 140-2 Level-3 compliance
- Azure Key Vault only supports FIPS 140-2 Level-2 validated HSMs
- You are fully responsible for the entire key management process



Source: What is Dedicated HSM? - Azure Dedicated HSM | Microsoft Learn

# Defender for Cloud




Source: [What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud | Microsoft Learn]

# Defender for Cloud – CSPM and CWP Plans

## CSPM

- Foundational CSPM
- Defender CSPM

## CWP

- Defender for Servers
- Defender for App Service
- Defender for Databases
- Defender for Storage
- Defender for Containers
- Defender for Key Vault
- Defender for Resource Manager
- Defender for APIs

# Defender for Cloud Built-in Roles

| Role | Add/assign initiatives (including) regulatory compliance standards) | Edit security policy | Enable / disable Microsoft Defender plans | Suppress alerts | Apply security recommendations for a resource | View alerts and recommendations |
|---|---|---|---|---|---|---|
| Security Reader | - | - | - | - | - | ✓ |
| Security Admin | ✓ | ✓ | ✓ | ✓ | - | ✓ |
| Contributor / Owner RG Level | - | - | - | - | ✓ | ✓ |
| Contributor Subscription Level | - | - | ✓ | ✓ | ✓ | ✓ |
| Owner Subscription Level | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |



Source: User roles and permissions - Microsoft Defender for Cloud | Microsoft Learn

# What is Cloud Security Posture Management (CSPM)?

- Proactive and preventive security instead of waiting for threats
- Detailed visibility into the security state of your assets and workloads
- Hardening guidance to help you efficiently and effectively improve your security posture



Source: Protect your resources with Defender CSPM plan on your subscription - Microsoft Defender for Cloud | Microsoft Learn

# CSPM - Plans

| Feature | Foundational CSPM | Defender CSPM |
|---|---|---|
| Security recommendations | √ | √ |
| Asset inventory | √ | √ |
| Secure score | √ | √ |
| Data visualization and reporting with Azure Workbooks | √ | √ |
| Data exporting | √ | √ |
| Workflow automation | √ | √ |
| Tools for remediation | √ | √ |
| Microsoft Cloud Security Benchmark | √ | √ |
| Security governance | | √ |
| Regulatory compliance standards | | √ |
| Cloud security explorer | | √ |
| Attack path analysis | | √ |
| Agentless scanning for machines | | √ |
| Agentless discovery for Kubernetes | | √ |
| Container registries vulnerability assessment | | √ |
| Data aware security posture | | √ |
| EASM insights in network exposure | | √ |



Source: Select a Defender for Servers plan - Microsoft Defender for Cloud | Microsoft Learn

# Asset Inventory

- Inventory of all Azure resources connected to Defender for Cloud
- Can be leveraged to answer questions such as:
  - Which of my subscriptions have outstanding recommendations?
  - Which of my machines with the tag ‘Critical’ are missing the Azure Monitor agent?
  - Which machines in a specific resource group have a known vulnerability (using a CVE number)?



Source: Using the asset inventory to view your security posture - Microsoft Defender for Cloud | Microsoft Learn

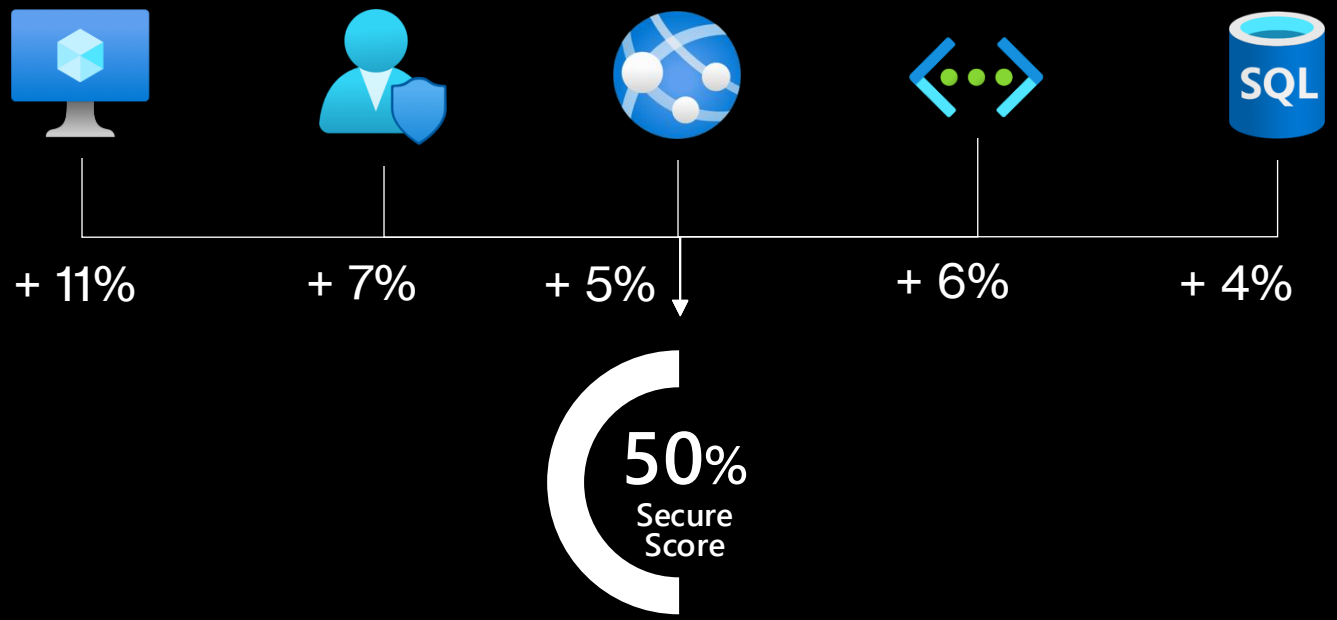
# Security Recommendations

- Defender for Cloud assesses your resources against security controls in Azure, AWS and GCP
- Based on that assessment, security recommendations are provided
- Recommendations are implemented via Azure Policy



Source: Review security recommendations in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

# Secure Score






Source: Secure score in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

# Data Visualization with Azure Workbooks

- Workbooks allow for data visualization and dashboarding
- Workbooks can be built from scratch or customized
- Defender for Cloud includes prebuilt workbooks, such as:
  - Secure Score over Time
  - Vulnerability Assessment Findings
  - DevOps Security
  - System Updates



Source: Workbooks gallery - Microsoft Defender for Cloud | Microsoft Learn

# Data Exporting

- There are built-in Azure tools for ensuring you can view your alert data in all of the most popular solutions in use today, including:
  - Microsoft Sentinel
  - Splunk Enterprise and Splunk Cloud
  - IBM's QRadar
  - ServiceNow
  - ArcSight
  - Power BI
  - Palo Alto Networks

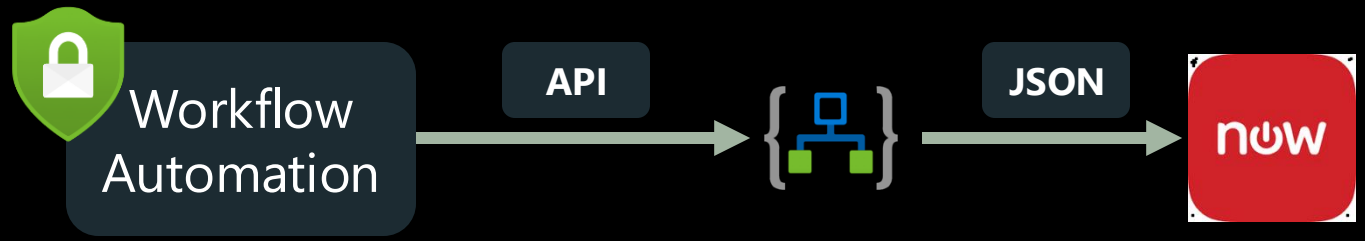


Source: Stream your alerts from Microsoft Defender for Cloud to Security Information and Event Management (SIEM) systems and other monitoring solutions - Microsoft Defender for Cloud | Microsoft Learn

# Workflow Automation

- Workflow Automation allows you to leverage Azure Logic Apps for complex automations and SOAR

**Example 1:** A new security recommendation leads to ticket creation in ServiceNow.






Source: Workflow automation - Microsoft Defender for Cloud | Microsoft Learn

# Remediation

- Security recommendations should be remediated frequently
- Defender for Cloud always explains how to do this in general
- There is also a quick fix option available. Be careful if:
  - You manage resources with IaC
  - You don’t know the workload as you can heavily impact it by applying a fix automatically



Source: Remediate security recommendations in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

# Microsoft Cloud Security Benchmark

- Benchmark provides best practices and recommendations for your resources
- Control Domains
  - Network Security
  - Identity Management
  - Privileged Access
  - Data Protection
  - Asset Management
  - Logging and Threat Detection
  - Incident Response
  - Posture and Vulnerability Management
  - Endpoint Security
  - Backup and recovery
  - DevOps Security
  - Governance and Strategy



Source: Overview of the Microsoft cloud security benchmark | Microsoft Learn

# Governance Rules

- You can define rules that assign an owner and a due date for remediating a recommendation
- Governance rules drive accountability and establish an SLA for the remediation process of recommendations



Source: Drive remediation of security recommendations with governance rules in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

# Regulatory Compliance Standards

- Defender for Cloud assesses your resources against popular frameworks and regulatory standards, e.g.:
  - ISO 27001
  - NIST 800-53R4
  - PCI DSS v4
  - SOC 2 Type 2
  - CIS Microsoft Azure Foundations Benchmark



Source: Improve regulatory compliance in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

# Cloud Security Explorer

- Cloud security explorer allows you to query resources and logs without the need for writing KQL queries
- You can query all resources connected to Defender for Cloud
- KQL still has more capabilities but the barrier to use cloud security explorer is way lower



Source: Build queries with cloud security explorer in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

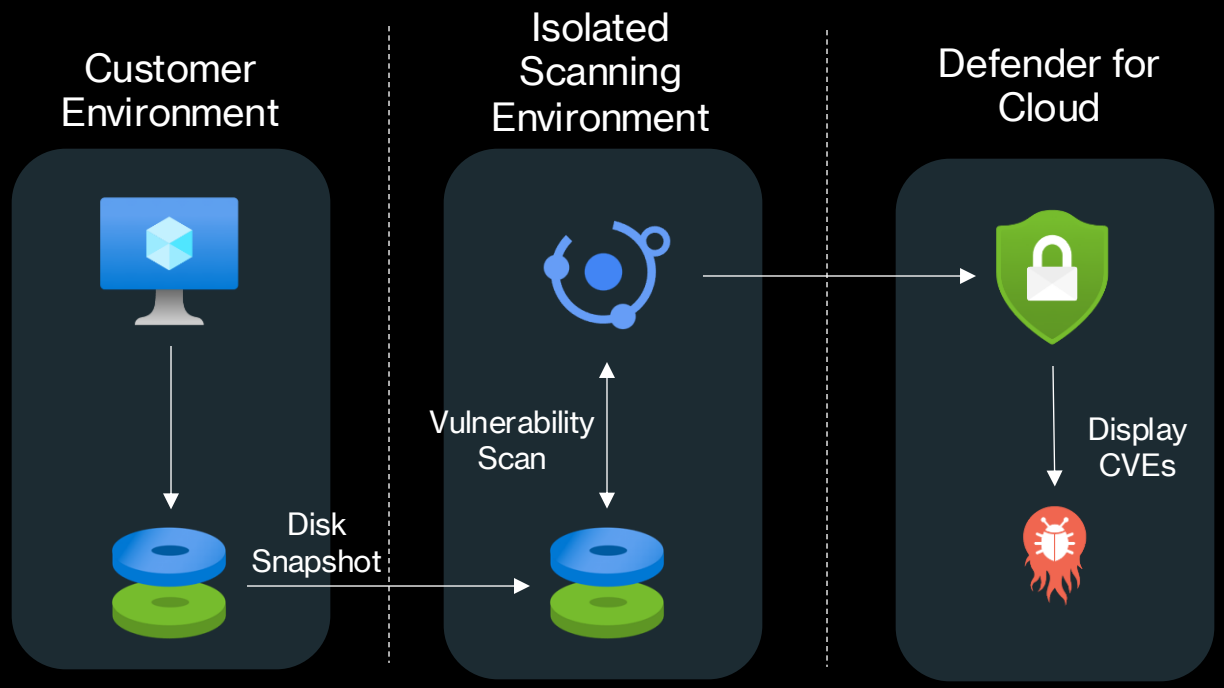
# Attack Path Analysis

- Visualizes exploitable attack paths in your environment, e.g.:
  - VM containing critical vulnerabilities is exposed to the internet
  - VM containing critical vulnerabilities is exposed to the internet with read permissions to a key vault
  - Azure Blob storage with sensitive data is publicly accessible



Source: Identify and remediate attack paths in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

# Agentless Scanning for VMs






Source: Learn about agentless scanning for VMs - Microsoft Defender for Cloud | Microsoft Learn

# Agentless Discovery for Kubernetes

- API-based discovery of your Kubernetes clusters, their configurations, and deployments
- Allows you to get an idea of your Kubernetes cluster configuration and its security posture



Source: Agentless container posture in Defender CSPM - Microsoft Defender for Cloud | Microsoft Learn

# Container Registry Vulnerability Assessment

- Container Vulnerability Assessment is powered by MDVM (Microsoft Defender Vulnerability Management)
- Scans the Azure Container Registry (ACR) and identifies vulnerabilities
- Also included in Defender for Containers



Source: Agentless container posture in Defender CSPM - Microsoft Defender for Cloud | Microsoft Learn

# Data Aware Security Posture

- Data-aware security posture automatically and continuously discovers managed and shadow data resources across clouds, including different types of objects stores and databases
- Defender for Cloud uses the built-in sensitive information types in Microsoft Purview, e.g.
  - International banking account number (IBAN)
  - Credit card number
  - U.S. social security number (SSN)
  - Client secret / API key
- Full list of sensitive information types: Sensitive information types supported by Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn



Source: Data-aware security posture - Microsoft Defender for Cloud | Microsoft Learn

# Defender External Attack Surface Management (EASM)

- Defender EASM continuously discovers and maps your digital attack surface to provide an external view of your online infrastructure.
- This visibility enables security and IT teams to identify unknowns, prioritize risk, eliminate threats, and extend vulnerability and exposure control beyond the firewall.
- Attack Surface Insights are generated by leveraging vulnerability and infrastructure data to showcase the key areas of concern for your organization.



Source: https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview

# Defender External Attack Surface Management (EASM)

- Microsoft's proprietary discovery technology recursively searches for infrastructure with observed connections to known legitimate assets to make inferences about that infrastructure's relationship to the organization and uncover previously unknown and unmonitored properties.
- These known legitimate assets are called discovery 'seeds'
- Defender EASM first discovers strong connections to these selected entities, recursing to unveil more connections and ultimately compile your Attack Surface.



Source: https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview

# Defender External Attack Surface Management (EASM)

Defender EASM includes the discovery of the following kinds of assets:

- Domains
- IP Blocks
- Hosts
- Email Contacts
- ASNs
- WHOIS Organizations



Source: https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview

# Defender External Attack Surface Management (EASM)




Source: https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview

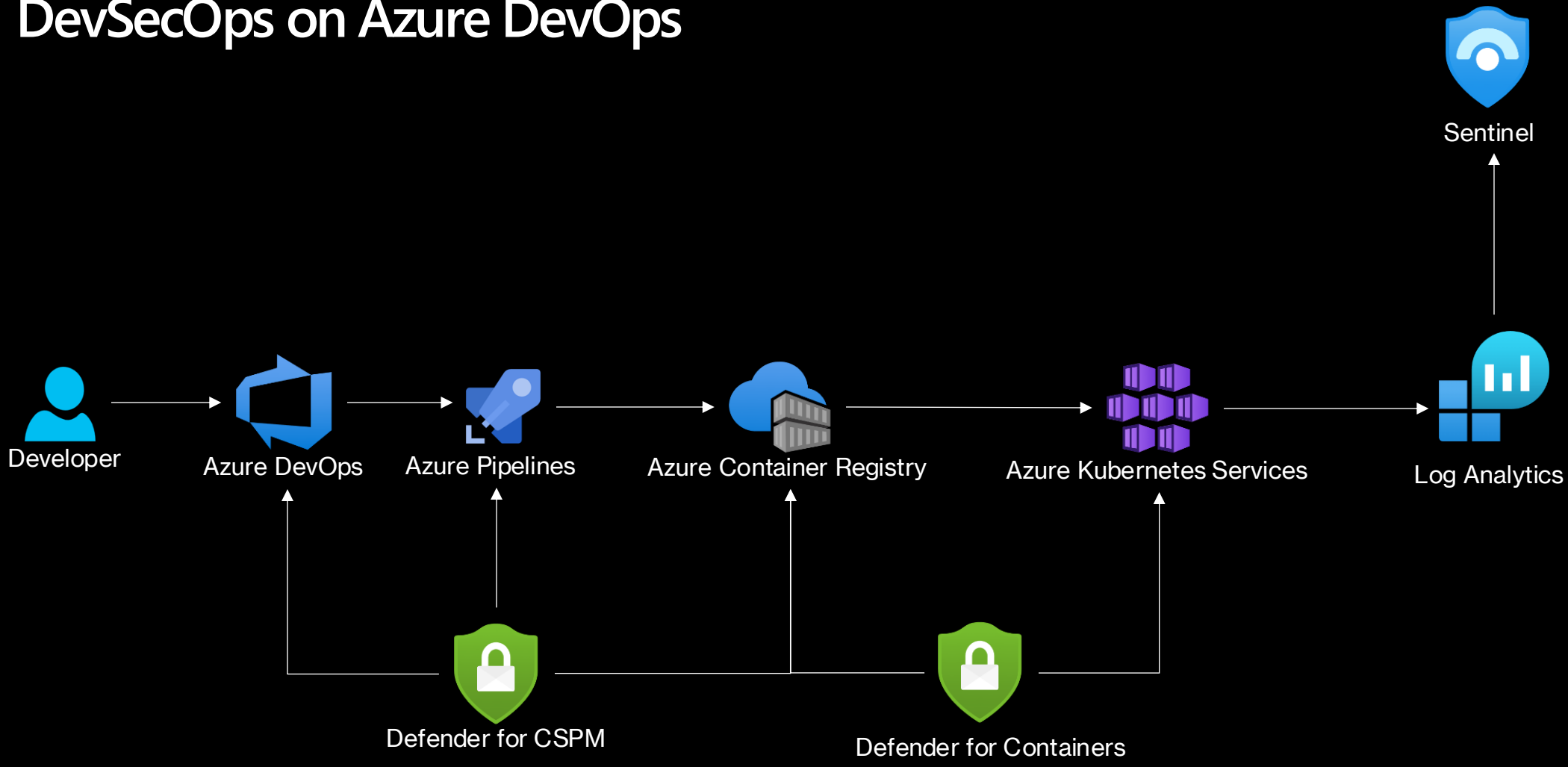
# EASM Insights in Network Exposure

- Defender External Attack Surface Management (EASM)
- EASM collects data for publicly exposed assets (“outside-in”)
- Defender for Cloud CSPM (“inside-out”) can use that data to assist with internet-exposure validation and discovery capabilities, to provide better visibility to customers



Source: Microsoft Defender for Cloud integration with Defender External attack surface management (EASM) - Microsoft Defender for Cloud | Microsoft Learn

# DevSecOps on Azure DevOps

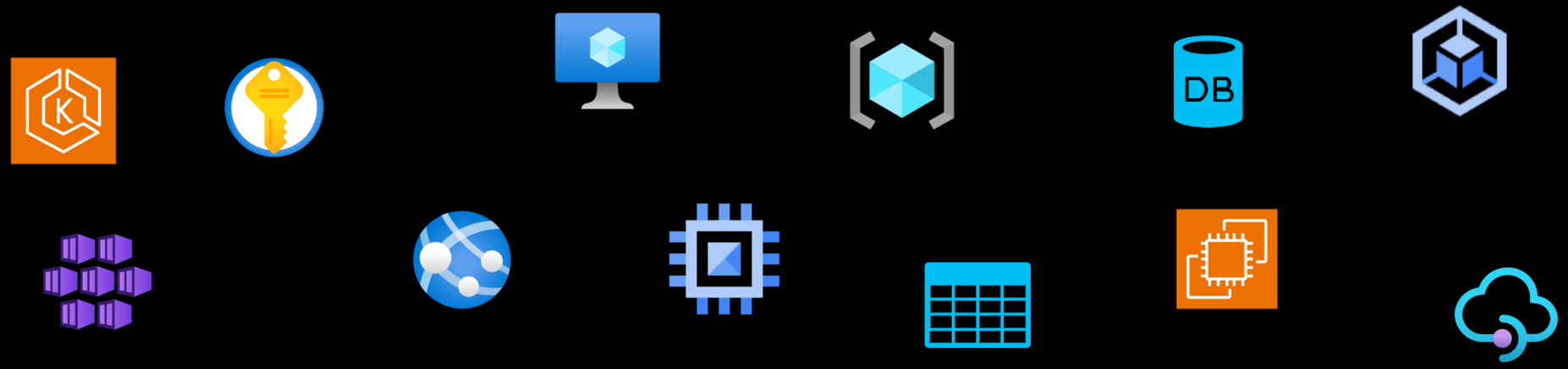



Christopher Nett

Source: Microsoft Defender for Cloud DevOps security - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

# What is Cloud Workload Protection (CWP)?

- Realtime threat protection for your workloads in Azure, multicloud and on-premises scenarios
- Integration with SIEM and XDR
- Available for most resource types

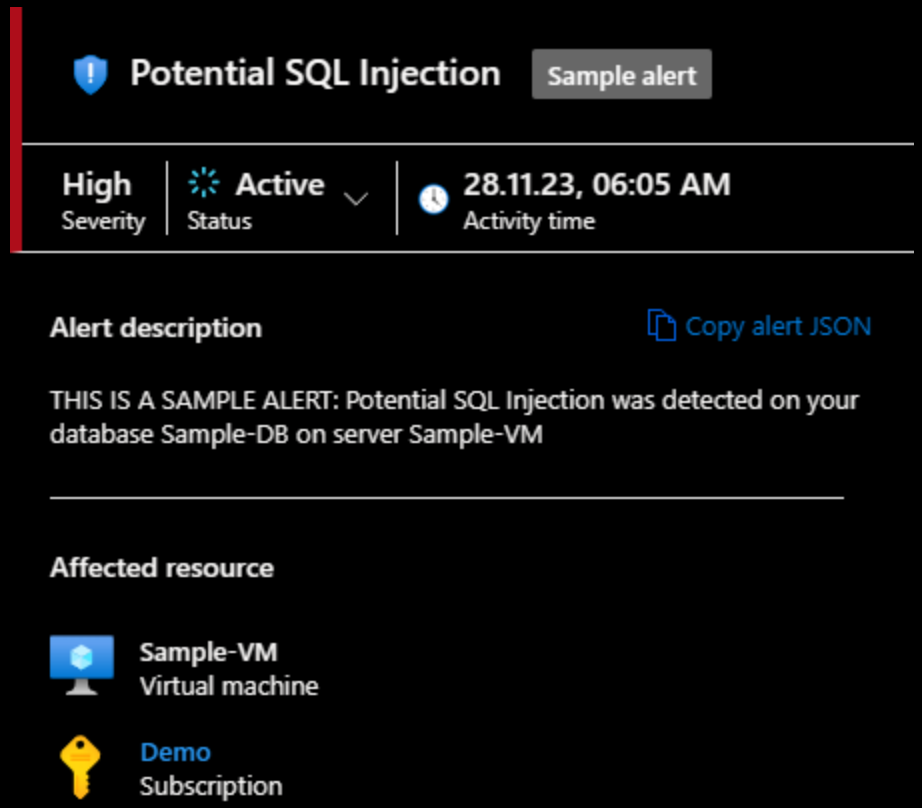





Source: Review workload protection in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

# Alert Queue & Alert Correlation

- CWP generates Alerts for your resources






Source: Review workload protection in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

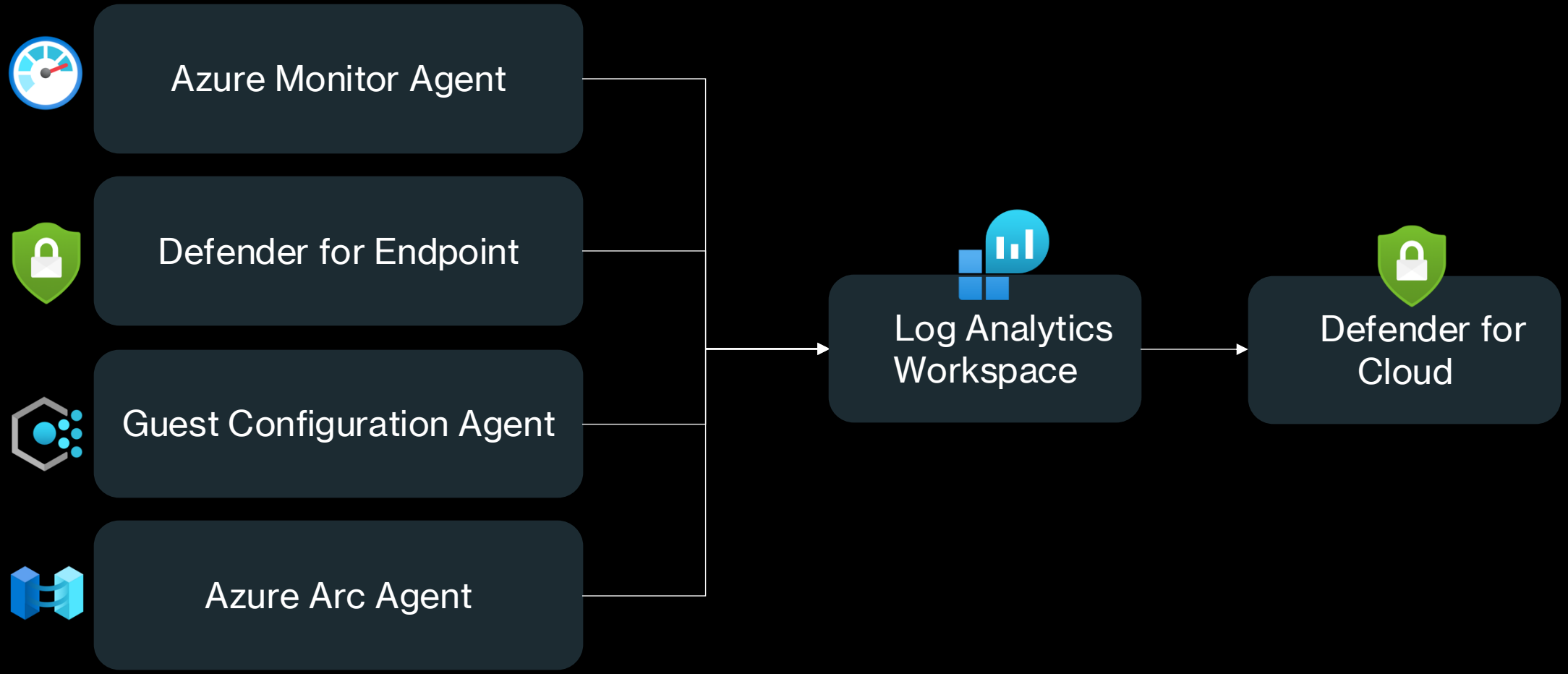
# What is Defender for Servers? 

- Server Protection for Windows and Linux
- Provides EDR, Antivirus, Threat & Vulnerability Management, and more
- Two Plans:
  - Defender for Servers Plan 1: Defender for Endpoint
  - Defender for Servers Plan 2: Defender for Endpoint + Advanced Capabilities



Source: Plan a Defender for Servers deployment to protect on-premises and multicloud servers - Microsoft Defender for Cloud | Microsoft Learn

# Agents






Source: Plan Defender for Servers agents and extensions deployment - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Server - Plans

| Feature | Plan 1 | Plan 2 |
|---|---|---|
| Defender for Endpoint integration | √ | √ |
| Licensing | √ | √ |
| Defender for Endpoint provisioning | √ | √ |
| Unified view | √ | √ |
| Threat detection for OS-level (agent-based) | √ | √ |
| Threat detection for network-level (agentless security alerts) | | √ |
| Microsoft Defender Vulnerability Management (MDVM) Add-on | | √ |
| Security Policy and Regulatory Compliance | | √ |
| Qualys vulnerability assessment | | √ |
| Adaptive application controls | | √ |
| Free data ingestion (500 MB) to Log Analytics workspaces | | √ |
| Free Azure Update Manager Remediation for Arc machines | | √ |
| Just-in-time virtual machine access | | √ |
| File integrity monitoring | | √ |
| Adaptive network hardening | | √ |
| Docker host hardening | | √ |
| Network map | | √ |
| Agentless scanning | | √ |



Source: Select a Defender for Servers plan - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Endpoint integration

- Defender for Servers integrates with Defender for Endpoint which includes the following features:
  - Attack Surface Reduction
  - Next-generation protection with Defender Antivirus
  - EDR
  - Threat and Vulnerability Management



Source: Using Microsoft Defender for Endpoint to protect native, on-premises, and AWS machines. - Microsoft Defender for Cloud | Microsoft Learn

# Licensing

- Defender for Servers covers licensing for Defender for Endpoint.
- Licensing is charged per hour instead of per seat, lowering costs by protecting virtual machines only when they're in use



Source: Select a Defender for Servers plan - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Endpoint provisioning

- Defender for Servers automatically provisions the Defender for Endpoint sensor on every supported machine
- Prerequisite: Machine must be connected enrolled in a Defender for Servers Plan



Source: Select a Defender for Servers plan - Microsoft Defender for Cloud | Microsoft Learn

# Threat detection for OS-level

- Defender for Servers and Defender for Endpoint detect threats at the OS level
- This includes VM behavior instead of only signature based detections
- Fileless attack detection



Source: Select a Defender for Servers plan - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Windows Machines 

- Antimalware Action Taken
- Fileless attack technique detected
- Suspicious process executed
- Suspicious PowerShell cmdlets executed
- Suspicious double extension file executed



Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Linux Machines 

- Behavior similar to ransomware detected
- Disabling of auditd logging
- Digital currency mining related behavior detected
- Fileless Attack Behavior Detected
- Antimalware real-time protection was disabled temporarily while code was executed in your virtual machine



Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Threat Detection for Network Level (formerly Defender for DNS)

- Detects threats that are directed at the control plane on the network, including network-based security alerts for Azure VMs, e.g.:
  - Data exfiltration from your Azure resources using DNS tunneling
  - Malware communicating with command-and-control servers (C2)
  - DNS attacks - communication with malicious DNS resolvers
  - Communication with domains used for malicious activities such as phishing and crypto mining
- Previously this feature was an individual Defender plan named “Defender for DNS”



Source: Microsoft Defender for DNS - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

# Security Policy and Regulatory Compliance

- Customization of security policies based on Azure Policy
- Assessment of resources against popular frameworks and regulatory standards, e.g.:
  - ISO 27001
  - NIST 800-53 R4
  - Azure CIS Benchmark

# Qualys Vulnerability Assessment

- Requires Defender for Servers Plan 2
- Available for Azure VMs and Arc-enabled machines




Source: Enable vulnerability scanning with the integrated Qualys scanner - Microsoft Defender for Cloud | Microsoft Learn

# Adaptive Application Controls

- Define an allowlist of safe applications for VMs, which allows you to:
  - Identify potential malware in early stages of an attack or missed by Antivirus/EDR
  - Improve compliance with policies that dictate the use of only licensed software
  - Identify outdated or unsupported versions of applications
  - Identify software that's banned by your organization but is running on your machines
- No enforcement/blocking available



Source: Adaptive application controls - Microsoft Defender for Cloud | Microsoft Learn

# Free Data Ingestion to Log Analytics Workspaces

- Defender for Servers provides an allocation of 500 MB per node per day for machines against the following subset of security data types in Log Analytics:
  - SecurityAlert
  - SecurityBaseline
  - SecurityBaselineSummary
  - SecurityDetection
  - SecurityEvent
  - WindowsFirewall
  - SysmonEvent
  - ProtectionStatus

# Free Azure Update Manager Remediation for Arc machines

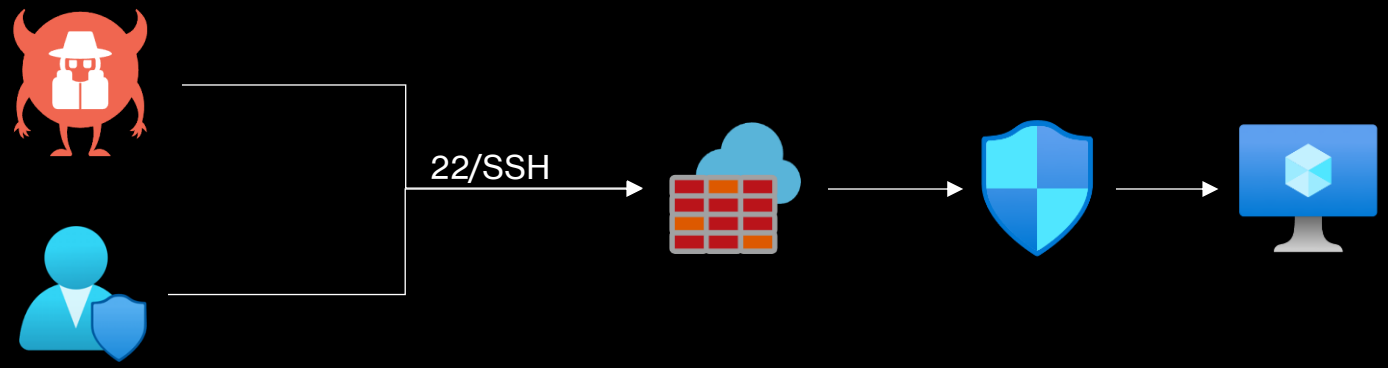
- Azure Update Manager remediation of unhealthy resources and recommendations is available at no additional cost for Arc enabled machines
- This allows you to trigger patching of vulnerable resources

# Just-in-time (JiT) virtual machine access

Scenario 1:

Azure Firewall and NSG allow TCP/IP 22 SSH from anywhere.

No JiT.

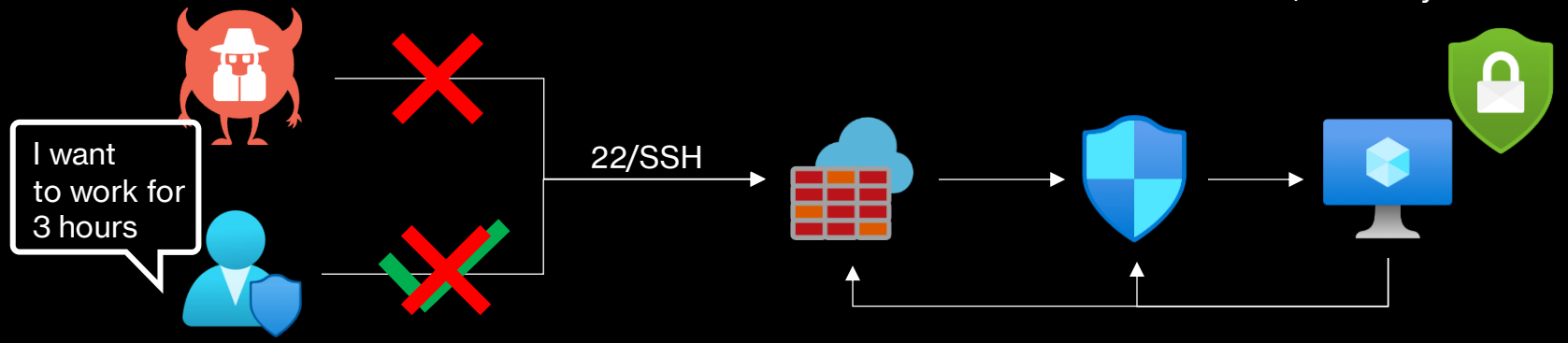



Scenario 2:

Azure Firewall and NSG deny TCP/IP 22 SSH from anywhere.

JiT is leveraged.

1) Check User RBAC for VM
2) Modify Azure Firewall
3) Modify NSG






Source: Enable just-in-time access on VMs - Microsoft Defender for Cloud | Microsoft Learn

# Adaptive Network Hardening

- Adaptive network hardening provides recommendations to further harden the NSG rules based on the actual traffic
- Supported Ports for both UDP and TCP:
  - 13, 17, 19, 22, 23, 53, 69, 81, 111, 119, 123, 135, 137, 138, 139, 161, 162, 389, 445, 512, 514, 593, 636, 873, 1433, 1434, 1900, 2049, 2301, 2323, 2381, 3268, 3306, 3389, 4333, 5353, 5432, 5555, 5800, 5900, 5900, 5985, 5986, 6379, 6379, 7000, 7001, 7199, 8081, 8089, 8545, 9042, 9160, 9300, 11211, 16379, 26379, 27017, 37215



Source: Adaptive network hardening - Microsoft Defender for Cloud | Microsoft Learn

# File Integrity Monitoring (FIM)

- FIM monitors files and registry for changes that might indicate an attack
- Available for:
  - Windows files
  - Windows registry
  - Linux system files



Source: Track changes to system files and registry keys - Microsoft Defender for Cloud | Microsoft Learn

# File Integrity Monitoring (FIM)

- Recommended Windows files and registry keys to monitor:
  - C:\Windows\regedit.exe
  - C:\config.sys
  - HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
- Recommended Linux files and to monitor:
  - /bin/passwd
  - /bin/login
  - /etc/init.d



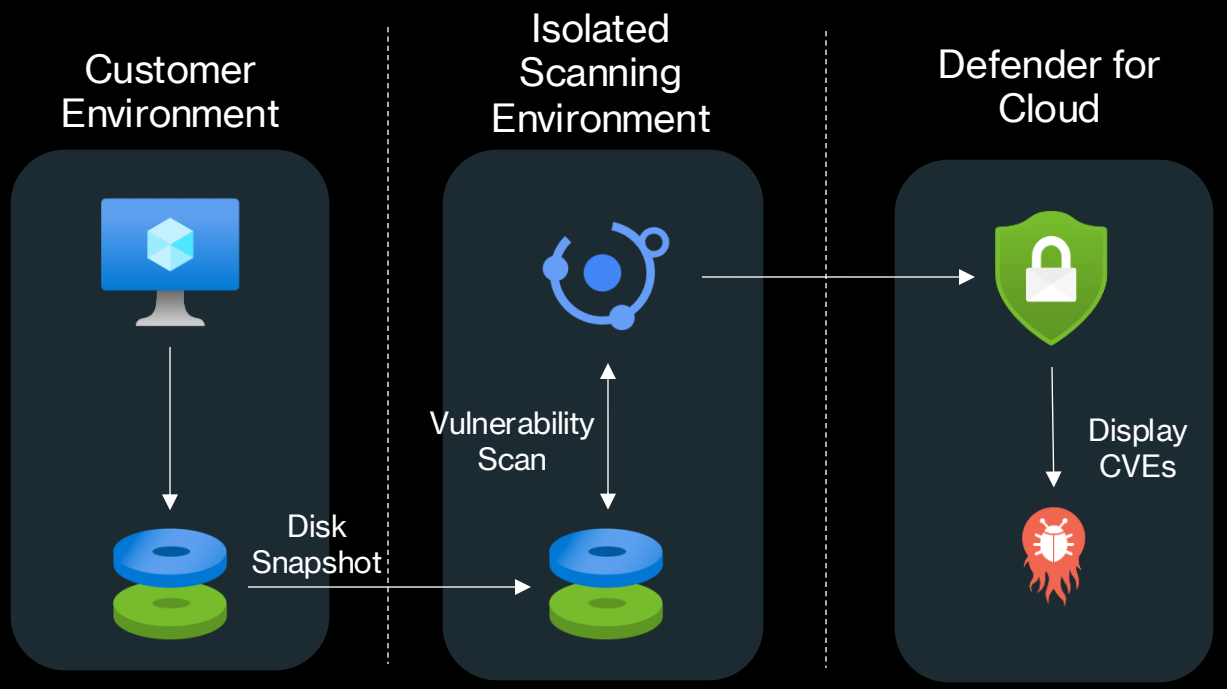
Source: Track changes to system files and registry keys - Microsoft Defender for Cloud | Microsoft Learn

# Network Map

- The network map provides a graphical view with security overlays giving you recommendations and insights for hardening your network resources.
- View network topology of your Azure workloads
- Connections between your virtual machines and subnets
- Can be leveraged to verify your network Microsegmentation implementation

# Agentless Scanning for VMs

- Requires Defender for Servers Plan 2 or Defender CSPM
- Available for Azure, AWS and GCP






Source: Learn about agentless scanning for VMs - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Databases

- Defender for Databases has for sub-plans for various database offerings in Azure:
  - Azure SQL Databases
  - SQL servers on machines
  - Open-source relational databases
  - Azure Cosmos DB
- Advanced Threat Protection
  - Detects e.g.: SQL Injection, Brute-Force, Privilege Escalation...
- SQL Vulnerability Assessment
  - Identifies Database vulnerabilities



Source: Protect your databases with Defender for Databases - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Azure SQL Databases 


- ⚠ Log on from an unusual location
- ⚠ Login from a suspicious IP
- ⚠ Suspected brute force attack using a valid user
- ⚠ Potential SQL injection
- ⚠ SQL Server potentially spawned a Windows command shell and accessed an abnormal external source



Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Open-Source Relational Databases 

- Suspected brute force attack using a valid user
- Suspected successful brute force attack
- Log on from an unusual location
- Attempted logon by a potentially harmful application
- Login from a suspicious IP



Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Azure Cosmos DB 

- Access from a Tor exit node
- Access from a suspicious IP
- Access from an unusual location
- Suspicious extraction of Azure Cosmos DB account key
- Unusual volume of data extracted

Christopher Nett

Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Storage 

- Defender for Storage provides Security for:
  - Azure Blob Storage
  - Azure Files
  - Azure Data Lake Storage

- By leveraging:
  - Microsoft Threat Intelligence
  - Microsoft Defender Antivirus
  - Sensitive Data Discovery



Source: Microsoft Defender for Storage - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Storage




Source: Microsoft Defender for Storage - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Storage 

- Access from a suspicious IP address
- Potential malware upload to a storage account
- Storage account identified as source for distribution of malware
- Unusual amount of data extracted from a storage account
- The access level of a sensitive storage blob container was changed to allow unauthenticated public access



Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Containers 

Defender for Containers can be utilized in:

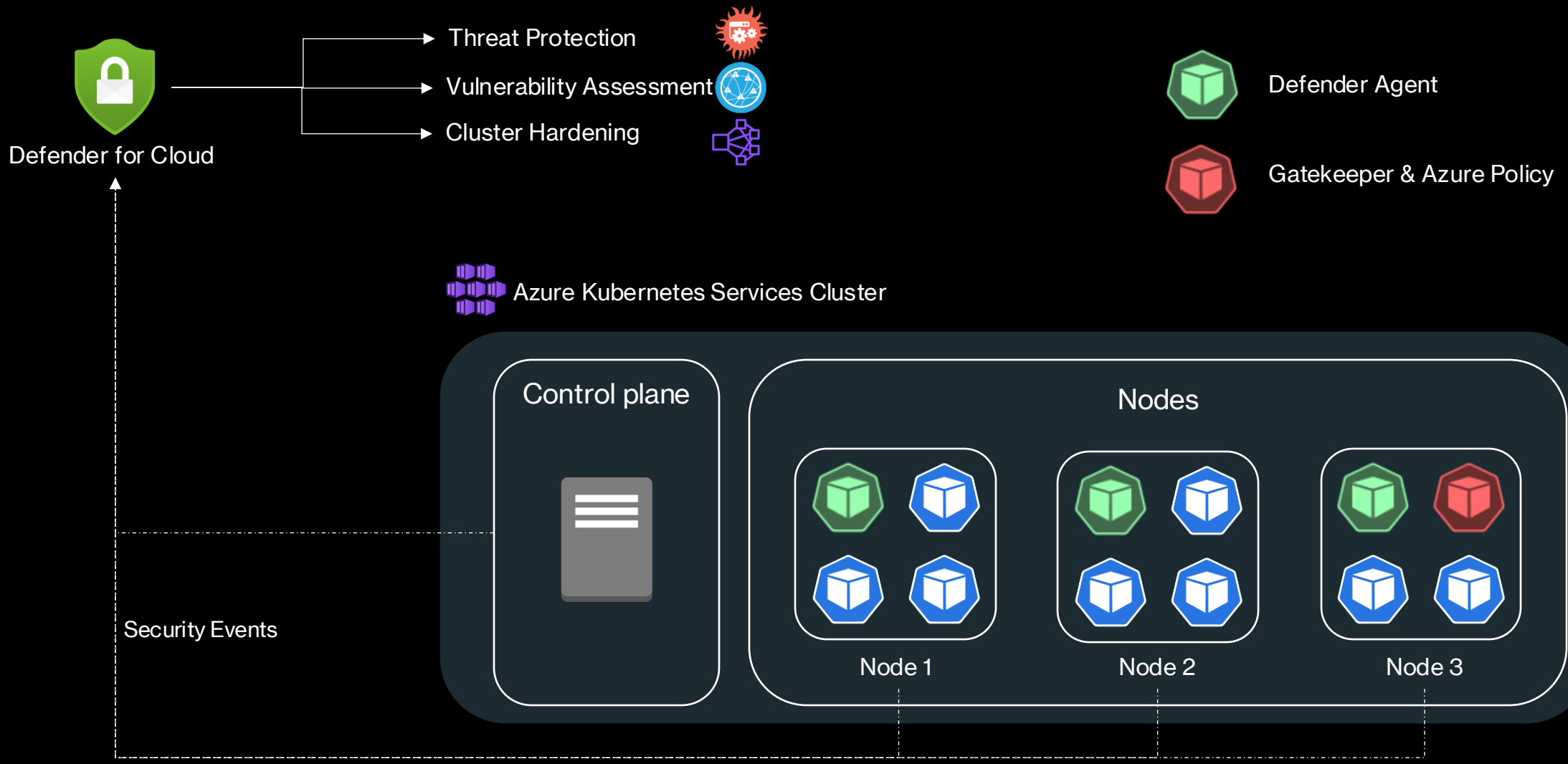
- Azure Kubernetes Service (AKS)
- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Another Kubernetes distribution (using Azure Arc-enabled Kubernetes)

# Defender for Containers 

Defender for Containers provides 3 core benefits:

1. Environment hardening
2. Vulnerability assessment
3. Runtime threat protection

# Defender for Containers - Architecture






Source: Container security architecture - Microsoft Defender for Cloud | Microsoft Learn

# Defender Agent Component Details

| Pod Name | Namespace | Kind | Short Description | Capabilities | Resource Limits | Egress Required |
|---|---|---|---|---|---|---|
| microsoft-defender-collector-ds-* | kube-system | Daemon Set | A set of containers that focus on collecting inventory and security events from the Kubernetes environment. | SYS_ADMIN, SYS_RESOURCE, SYS_PTRACE | memory: 296Mi<br>cpu: 360m | No |
| microsoft-defender-collector-misc-* | kube-system | Deplyo ment | A set of containers that focus on collecting inventory and security events from the Kubernetes environment that aren't bounded to a specific node. | N/A | memory: 64Mi<br>cpu: 60m | No |
| microsoft-defender-publisher-ds-* | kube-system | Daemon Set | Publish the collected data to Microsoft Defender for Containers backend service where the data will be processed for and analyzed. | N/A | memory: 200Mi<br>cpu: 60m | Https 443 |



Source: Container security architecture - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Containers - Hardening

- Defender for Containers constantly evaluates your clusters' configurations against the initiatives in your subscriptions
- It identifies misconfigurations and generates security recommendations
- Install Azure Policy for Kubernetes to safeguard your container workloads. This add-on for your AKS cluster monitors every Kubernetes API request, ensuring compliance with best practices before saving to the cluster

# Defender for Containers – Hardening Recommendations

| Recommendation Name | Security control |
|---|---|
| Container CPU and memory limits should be enforced | Protect applications against DDoS attack |
| Container images should be deployed only from trusted registries | Remediate vulnerabilities |
| Least privileged Linux capabilities should be enforced for containers | Manage access and permissions |
| Containers should only use allowed AppArmor profiles | Remediate security configurations |
| Services should listen on allowed ports only | Restrict unauthorized network access |
| Usage of host networking and ports should be restricted | Restrict unauthorized network access |
| Usage of pod HostPath volume mounts should be restricted to a known list | Manage access and permissions |
| Container with privilege escalation should be avoided | Manage access and permissions |
| Containers sharing sensitive host namespaces should be avoided | Manage access and permissions |
| Immutable (read-only) root filesystem should be enforced for containers | Manage access and permissions |
| Kubernetes clusters should be accessible only over HTTPS | Encrypt data in transit |
| Kubernetes clusters should disable automounting API credentials | Manage access and permissions |
| Kubernetes clusters should not use the default namespace | Implement security best practices |
| Kubernetes clusters should not grant CAPSYSADMIN security capabilities | Manage access and permissions |
| Privileged containers should be avoided | Manage access and permissions |
| Running containers as root user should be avoided | Manage access and permissions |



Source: Kubernetes data plane hardening - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Containers – Vulnerability Assessment

- Container Vulnerability Assessment is powered by MDVM (Microsoft Defender Vulnerability Management)
- It comes with the following capabilities:
  - Scanning OS packages
  - Language specific packages
  - Image scanning in Azure Private Link
  - Exploitability information



Source: Vulnerability assessments for Azure with Microsoft Defender Vulnerability Management - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Containers – Vulnerability Assessment

For Azure Container Registry (ACR), there are several scan triggers:

- One-time triggers
  - On Push
  - On Import
  - Imaged pulled within the last 30 days are scanned on a weekly basis
- Continuous rescan triggers. Rescans are performed daily for:
  - Images pushed in the last 90 days.
  - Images pulled in the last 30 days.
  - Images currently running on the Kubernetes clusters monitored by Defender for Cloud



Source: Vulnerability assessments for Azure with Microsoft Defender Vulnerability Management - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Containers – Alerts

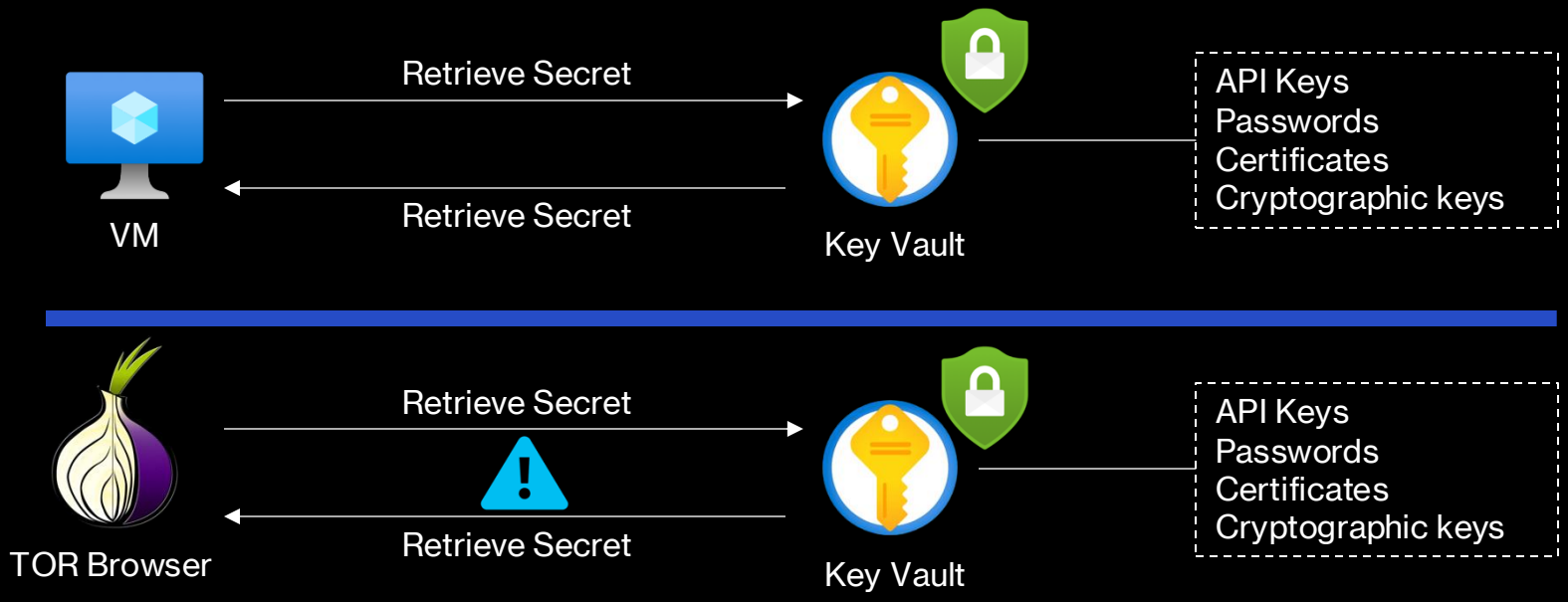
- Digital currency mining container detected
- Exposed Kubernetes dashboard detected
- Kubernetes penetration testing tool detected
- Potential reverse shell detected
- Possible malicious web shell detected



Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Key Vault

- Defender for Key Vault provides threat protection for Azure Key Vault
- These alerts include the details of the suspicious activity
- It also shows Recommendations on how to investigate and remediate threats






Source: Microsoft Defender for Key Vault - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Key Vault 

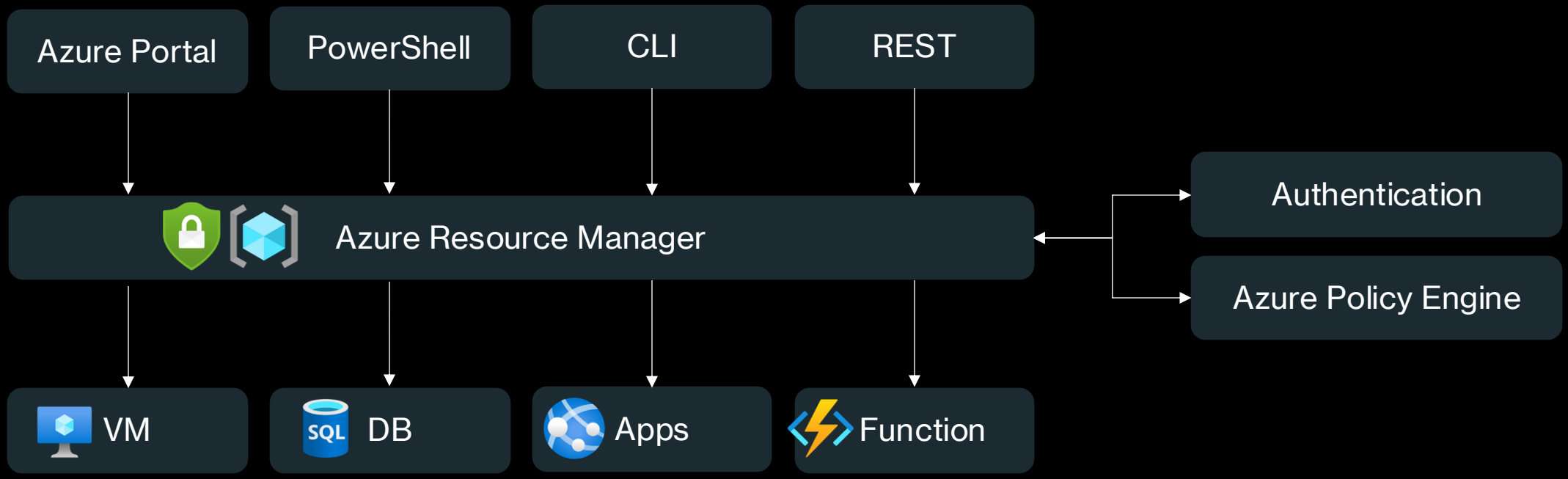
- Access from a suspicious IP address to a key vault
- Access from a TOR exit node to a key vault
- User accessed high volume of key vaults
- Unusual operation pattern in a key vault
- Suspicious policy change and secret query in a key vault



Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Defender for Resource Manager

- Detection of suspicious resource management operations
- Use of exploitation toolkits like PowerZure
- Lateral movement from the Azure management layer to the Azure resources data plane






Source: Microsoft Defender for Resource Manager - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

# Alerts for Resource Manager 

- Azure Resource Manager operation from suspicious IP address
- Azurite toolkit run detected
- Suspicious management session using an inactive account detected
- Suspicious elevate access operation
- Suspicious Azure role assignment detected



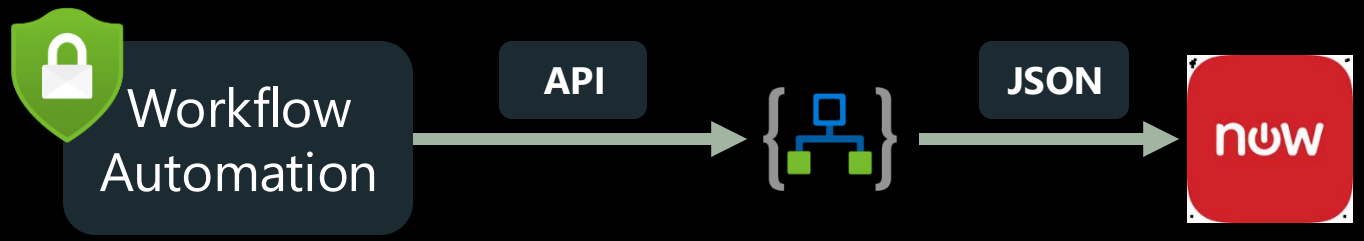
Source: Reference table for all security alerts - Microsoft Defender for Cloud | Microsoft Learn

# Why automate?

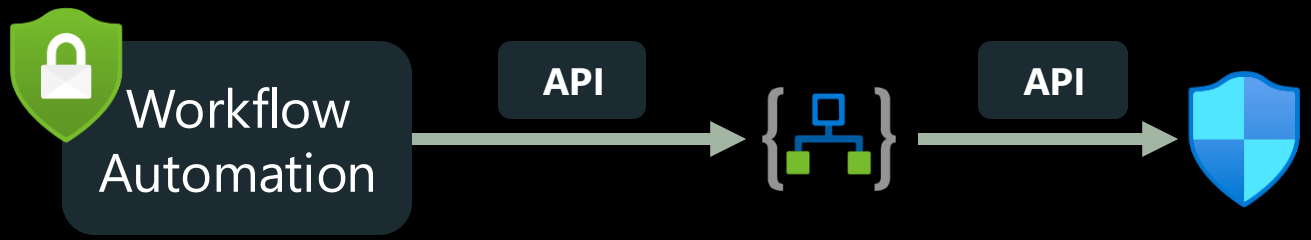
- Security Automation is not: Isolating machines
- Security Automation is: Mimicking the steps an Analyst would take when responding to incidents
- Automation has a positive impact on:
  - Mean time to react
  - SOC efficiency
  - Cost
  - Standardized responses to incidents

# Azure Logic Apps

**Example 1:** A new security recommendation leads to ticket creation in ServiceNow.



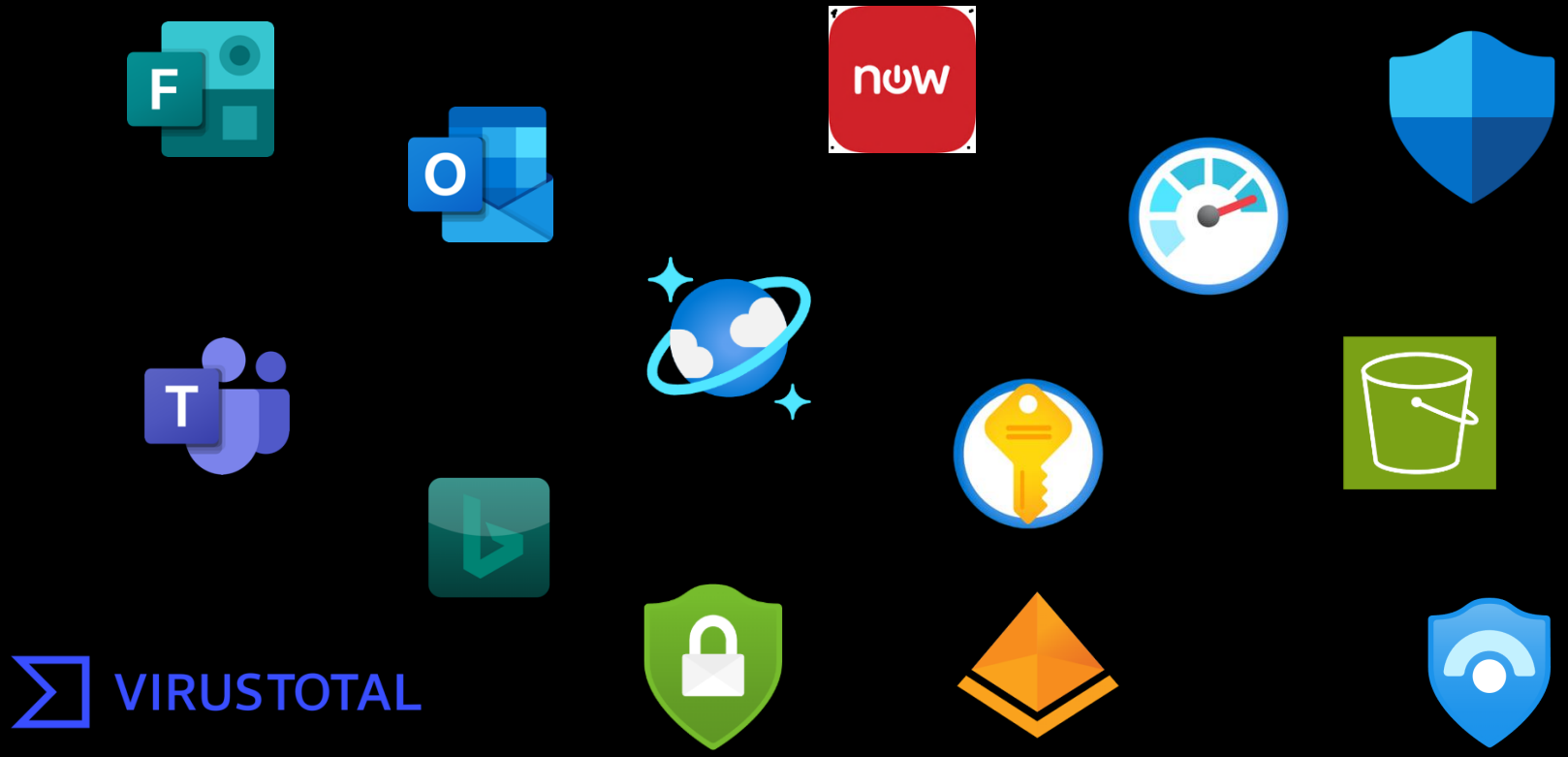

**Example 2:** Create a new deny rule in a NSG to stop an active brute-force attack.






Examples for Workflow Automations: Microsoft-Defender-for-Cloud/Workflow automation at main · Azure/Microsoft-Defender-for-Cloud · GitHub

# Logic App Connectors






List of all Logic App Connectors: List of all Logic Apps connectors | Microsoft Learn

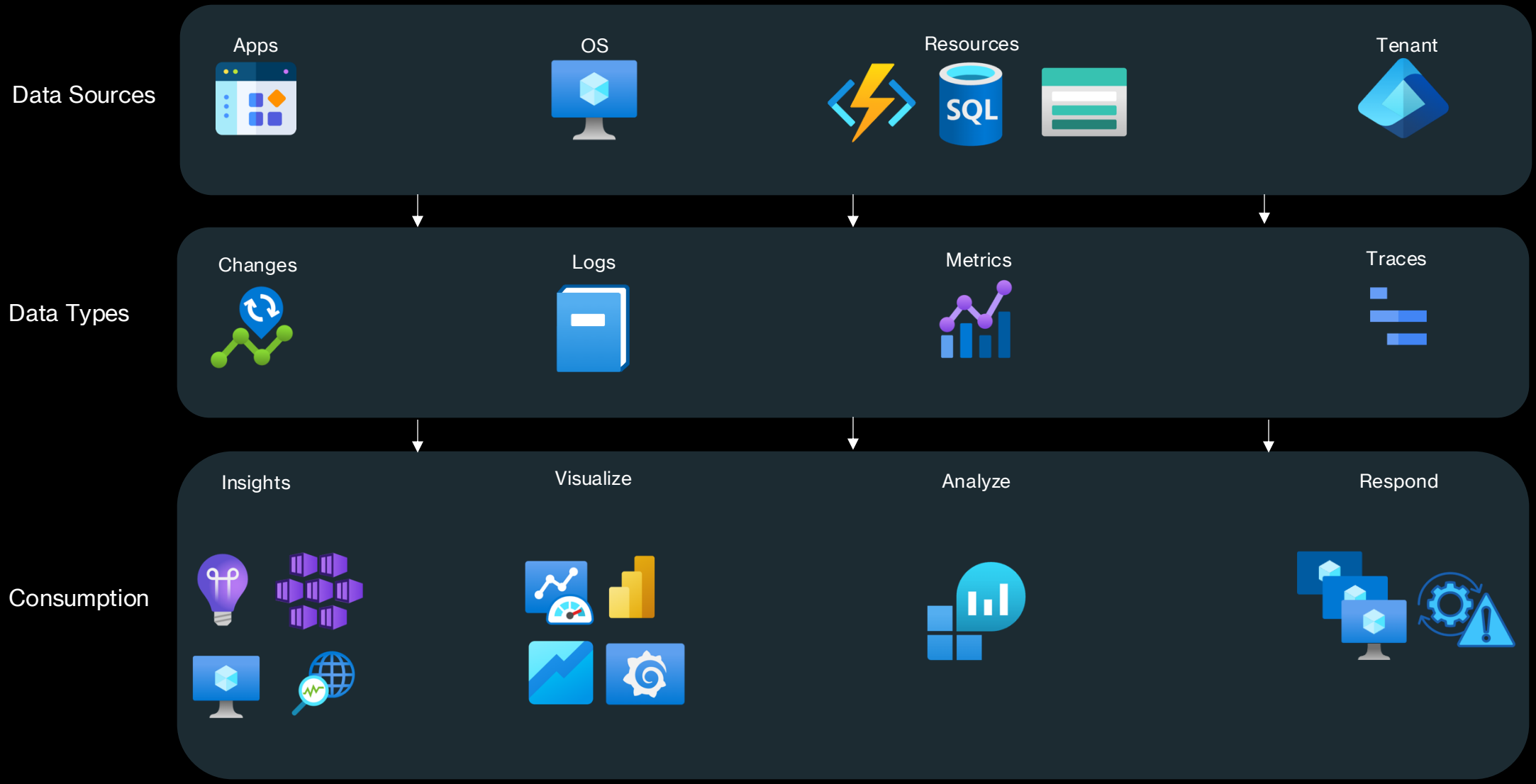
# Azure Monitor 

- Azure Monitor is a comprehensive monitoring solution for collecting, analyzing, and responding to monitoring data from your cloud and on-premises environments.
- Azure Monitor can monitor these types of resources in Azure, other clouds, or on-premises:
  - Applications
  - Virtual machines
  - Guest operating systems
  - Containers including Prometheus metrics
  - Databases
  - Security events in combination with Azure Sentinel
  - Networking events and health in combination with Network Watcher
  - Custom sources that use the APIs to get data into Azure Monitor



Source: https://learn.microsoft.com/en-us/azure/azure-monitor/overview

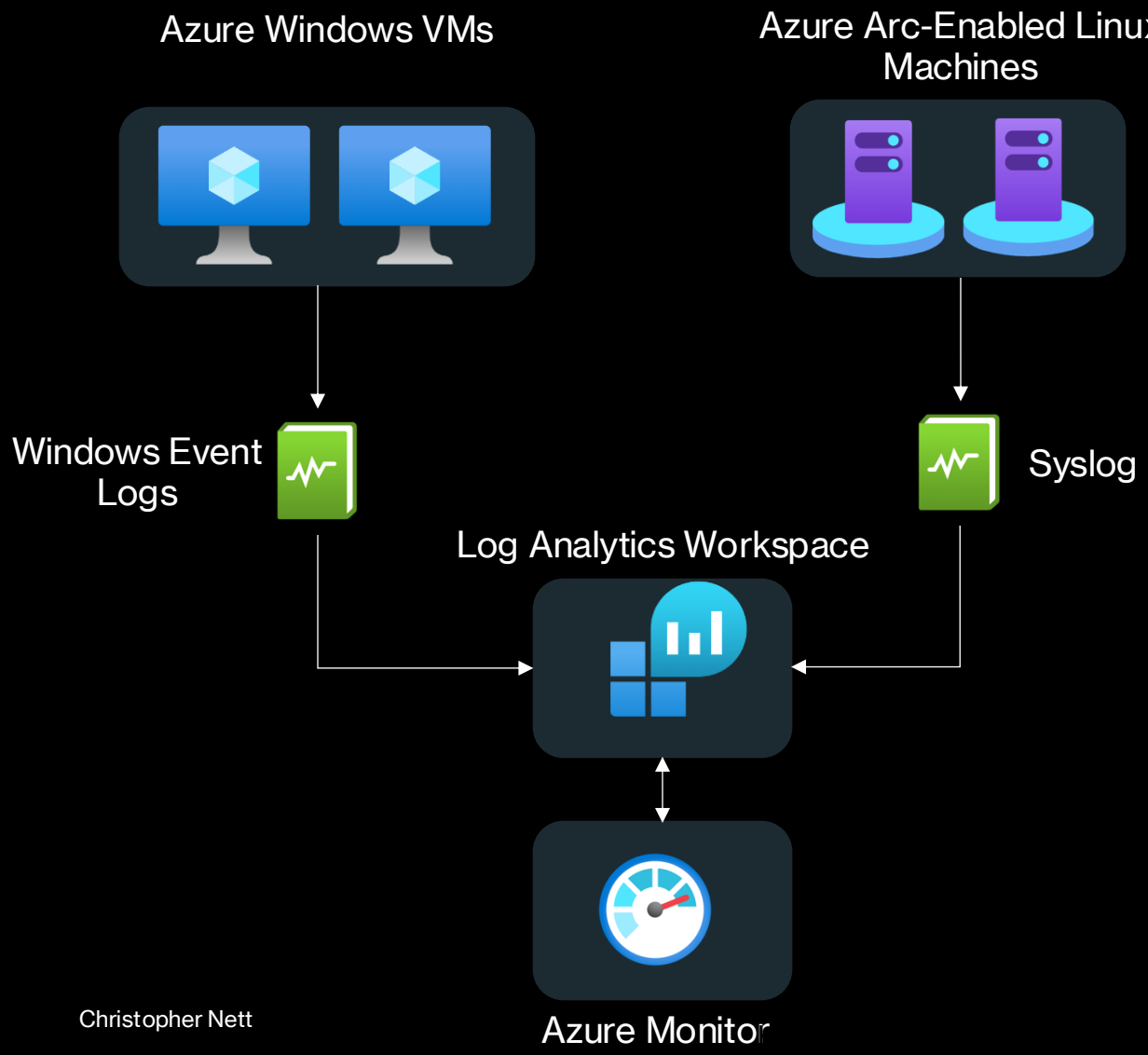
# Azure Monitor



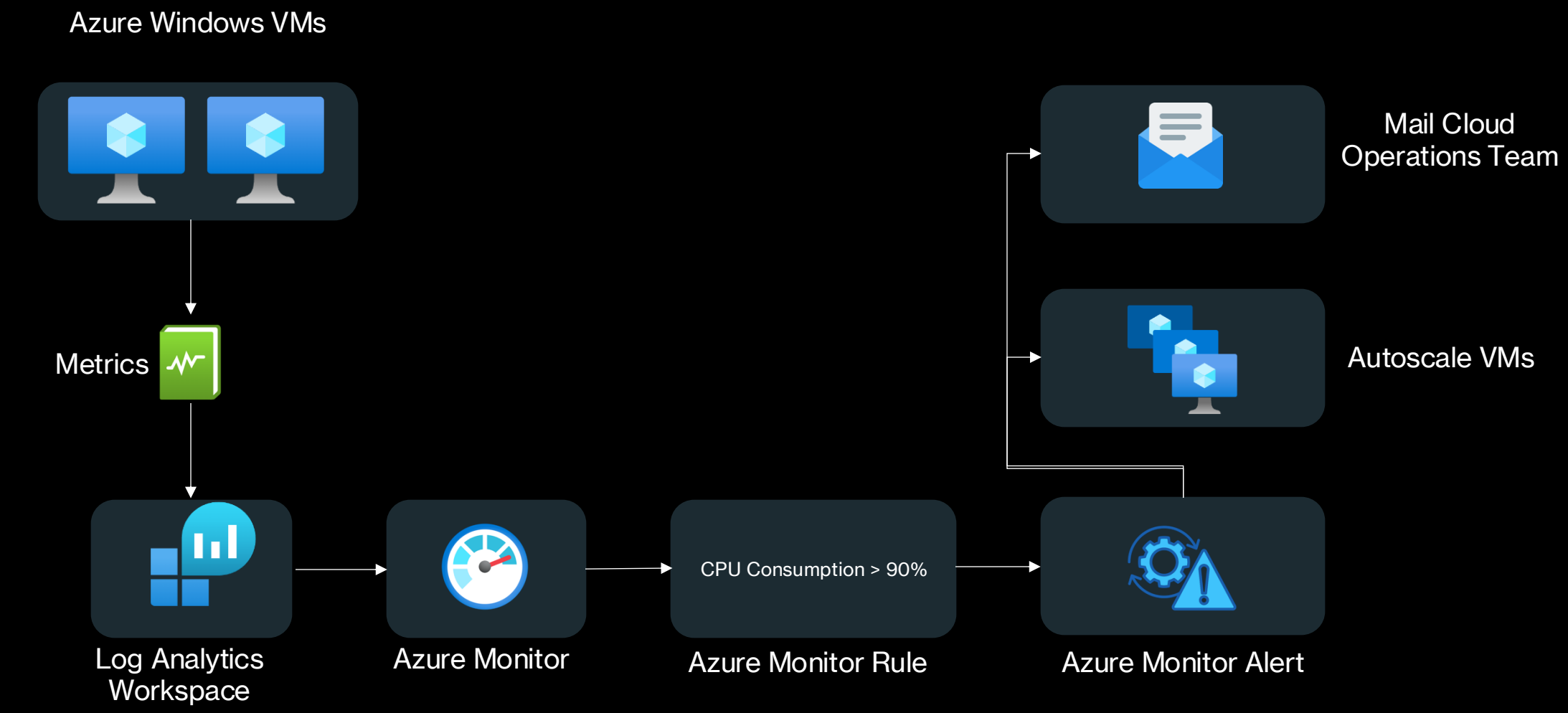

Christopher Nett

Source: https://learn.microsoft.com/en-us/azure/azure-monitor/overview

# Azure Monitor



# Azure Monitor



# Azure Monitor 

Important Considerations:

- Do not confuse Azure Monitor with security monitoring services such as Microsoft Sentinel
- Azure Monitor alerts are throttled (1SMS/call every 5 minutes and 100 emails per hour)



Source: https://learn.microsoft.com/en-us/azure/azure-monitor/overview

# What is Microsoft Sentinel?

- Cloud-native SIEM & SOAR
- Pay-as-you-go
- Collect data at scale
- Detect and investigate threats
- Respond to threats rapidly



Source: What is Microsoft Sentinel? | Microsoft Learn

+

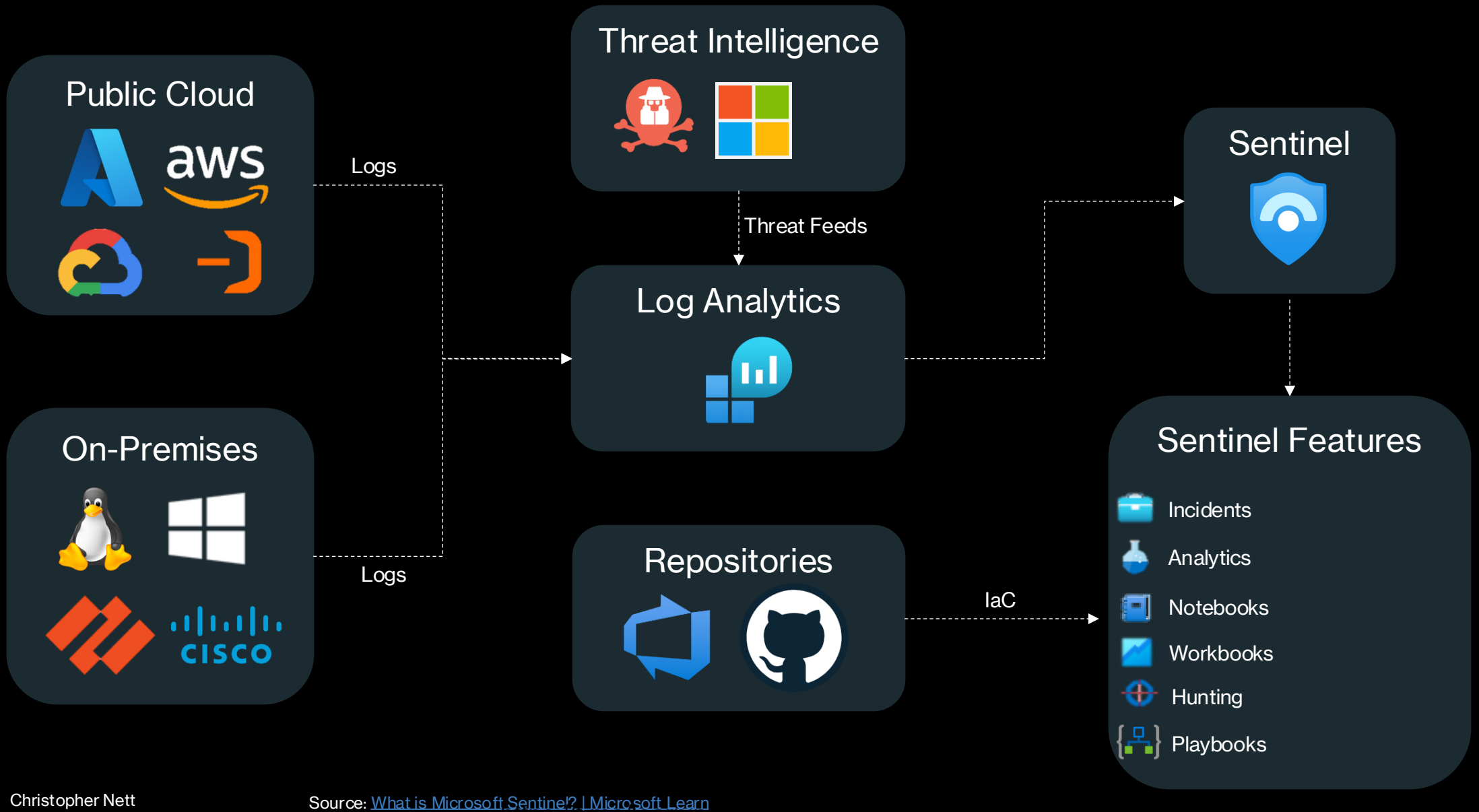
# Software as a service (SaaS)

- Azure provides everything but the configuration of the applications
- You cannot control anything but the configuration of the applications
- Example for a SaaS service: Microsoft Sentinel

| Responsibility | SaaS |
|---|---|
| Information and Data |  |
| Devices (Mobile and PCs) |  |
| Accounts and Identities |  |
| Identity and Directory Infrastructure |  |
| Applications |  |
| Network Controls |  |
| Operating System |  |
| Physical Hosts |  |
| Physical Network |  |
| Physical Datacenter |  |



Source: Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn




Christopher Nett

Source: What is Microsoft Sentinel? | Microsoft Learn

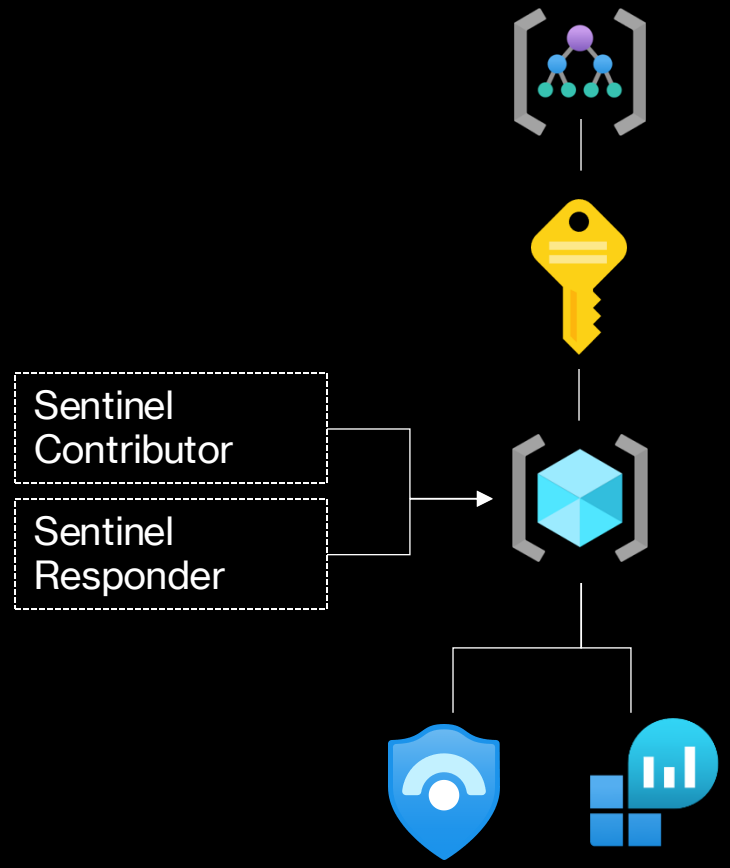
# Deploying Sentinel

- There are a few prerequisites to deploy Sentinel:
  - Azure Tenant
  - Active Azure Subscription
  - Azure Resource Group
  - Azure Log Analytics Workspace



Source: What is Microsoft Sentinel? | Microsoft Learn

# Azure RBAC






Source: What is Microsoft Sentinel? | Microsoft Learn

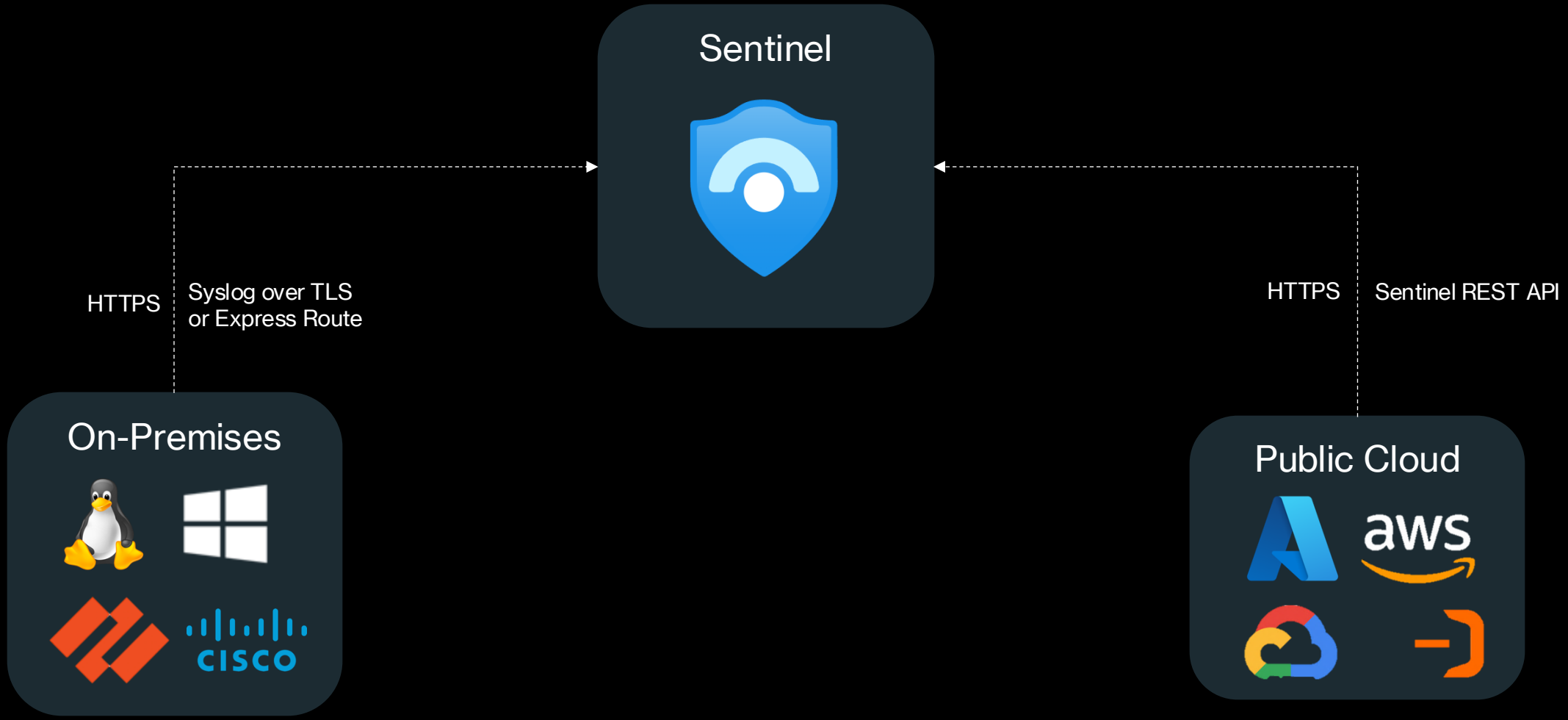
# Sentinel Built-in Roles

| Role | Create and edit Analytics rules, Workbooks, and other Microsoft Sentinel resources | Manage incidents (dismiss, assign, etc.) | View data, Incidents, Workbooks, and other Microsoft Sentinel resources | Configure data connectors | View and run playbooks | Create and edit playbooks |
|---|---|---|---|---|---|---|
| Microsoft Sentinel Reader | -- | -- | ✓ | -- | -- | -- |
| Microsoft Sentinel Responder | -- | ✓ | ✓ | -- | -- | -- |
| Microsoft Sentinel Contributor | ✓ | ✓ | ✓ | ✓ | -- | -- |
| Microsoft Sentinel Playbook Operator | -- | -- | -- | -- | ✓ | -- |
| Logic App Contributor | -- | -- | -- | ✓ | ✓ | ✓ |

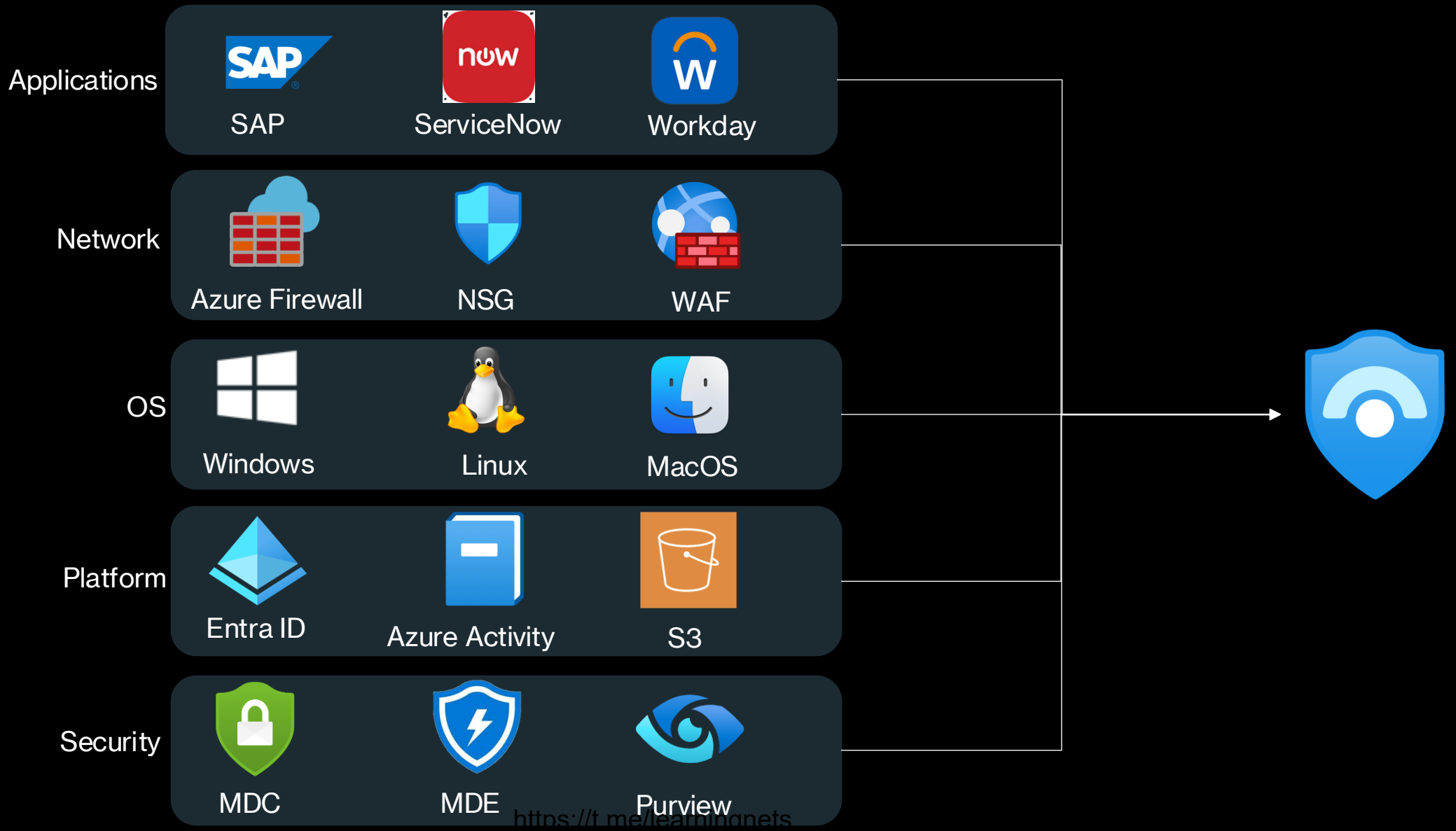


Source: Roles and permissions in Microsoft Sentinel | Microsoft Learn

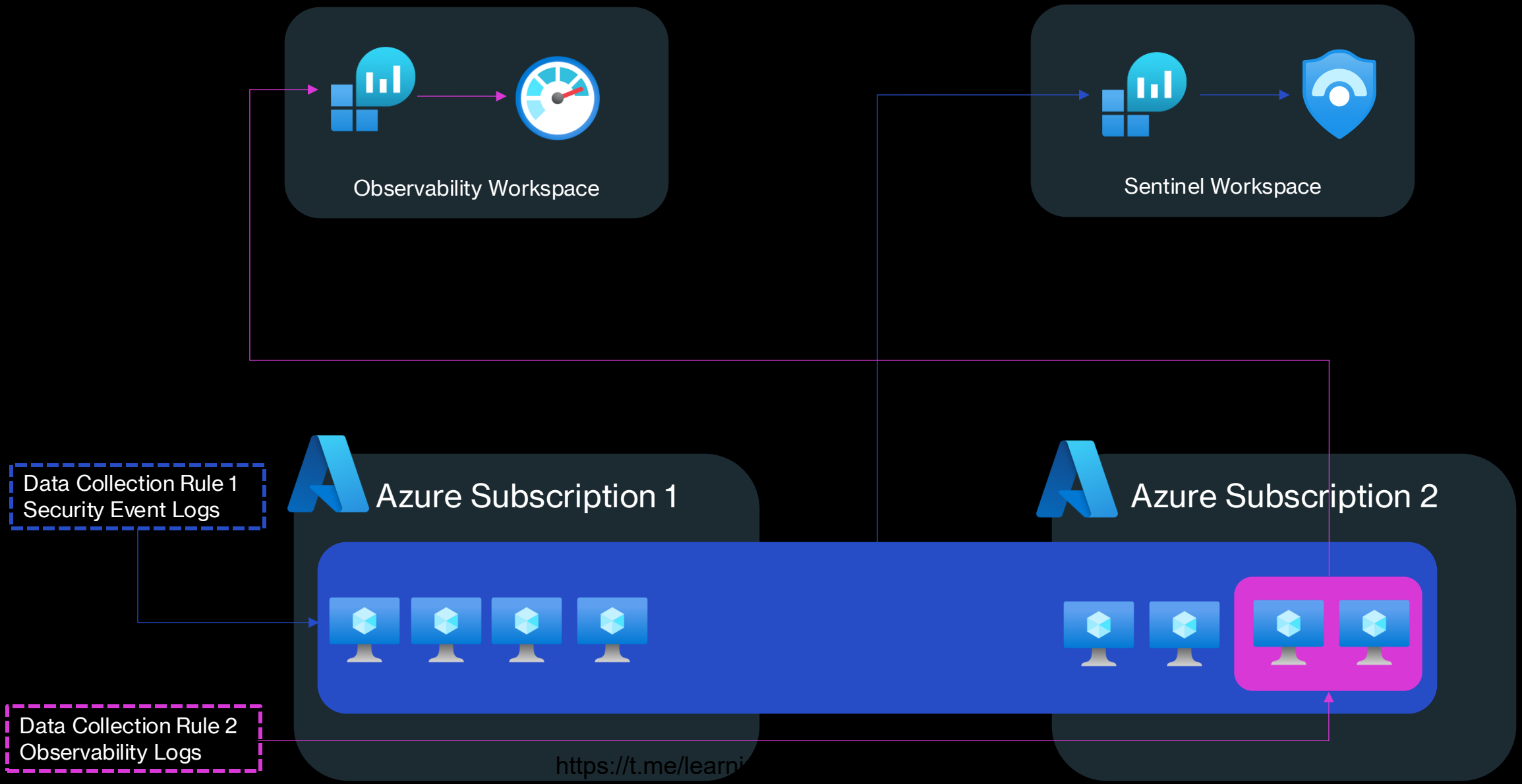
# Collect security logs from anywhere



# Typical data sources for a SIEM



# Azure Monitor Agent (AMA) and Data Collections Rules (DCR)

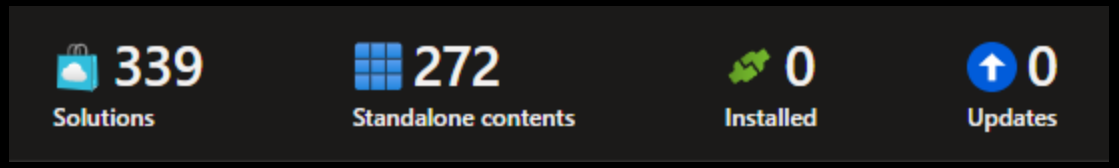


# Data Connectors

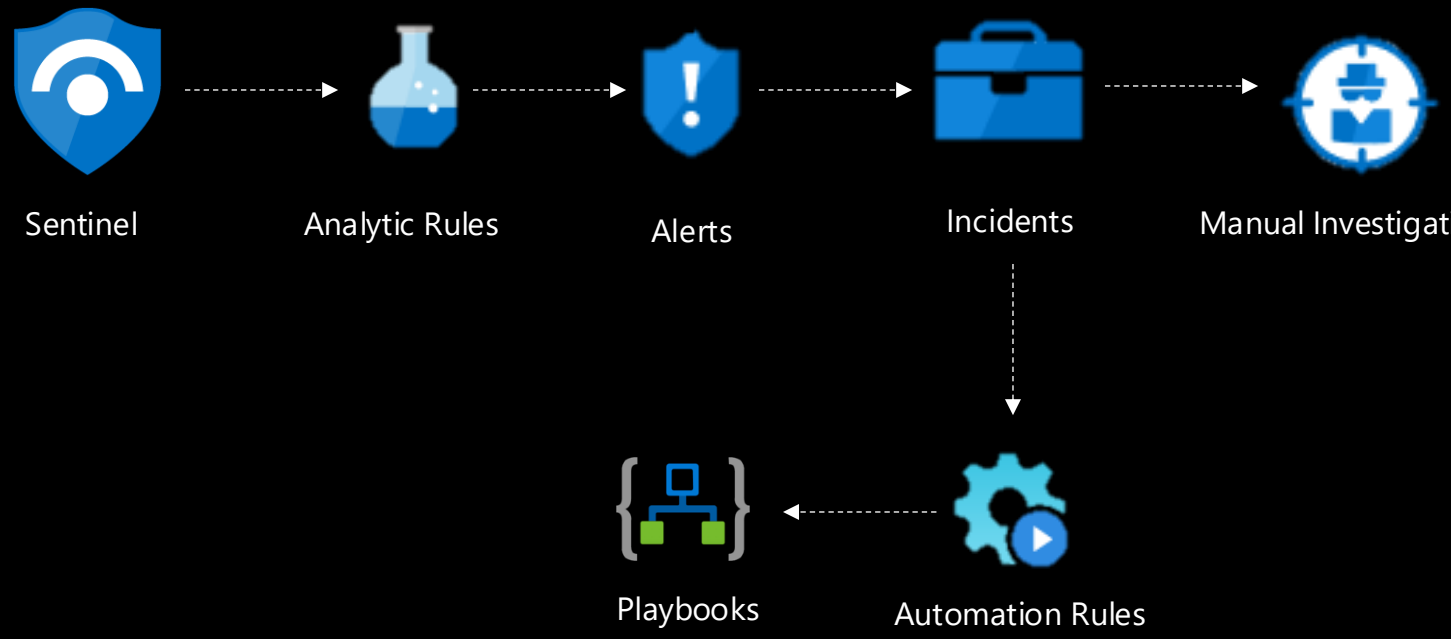
- Over 200 prebuild connectors are available in the content hub, e.g.
  - Entra ID
  - Entra ID Protection
  - M365 Defender
  - Defender for Cloud
  - Azure Activity
  - AWS
  - Threat Intelligence – TAXII
- You can also build custom connectors if your data source is not in the content hub yet

# Sentinel Content Hub

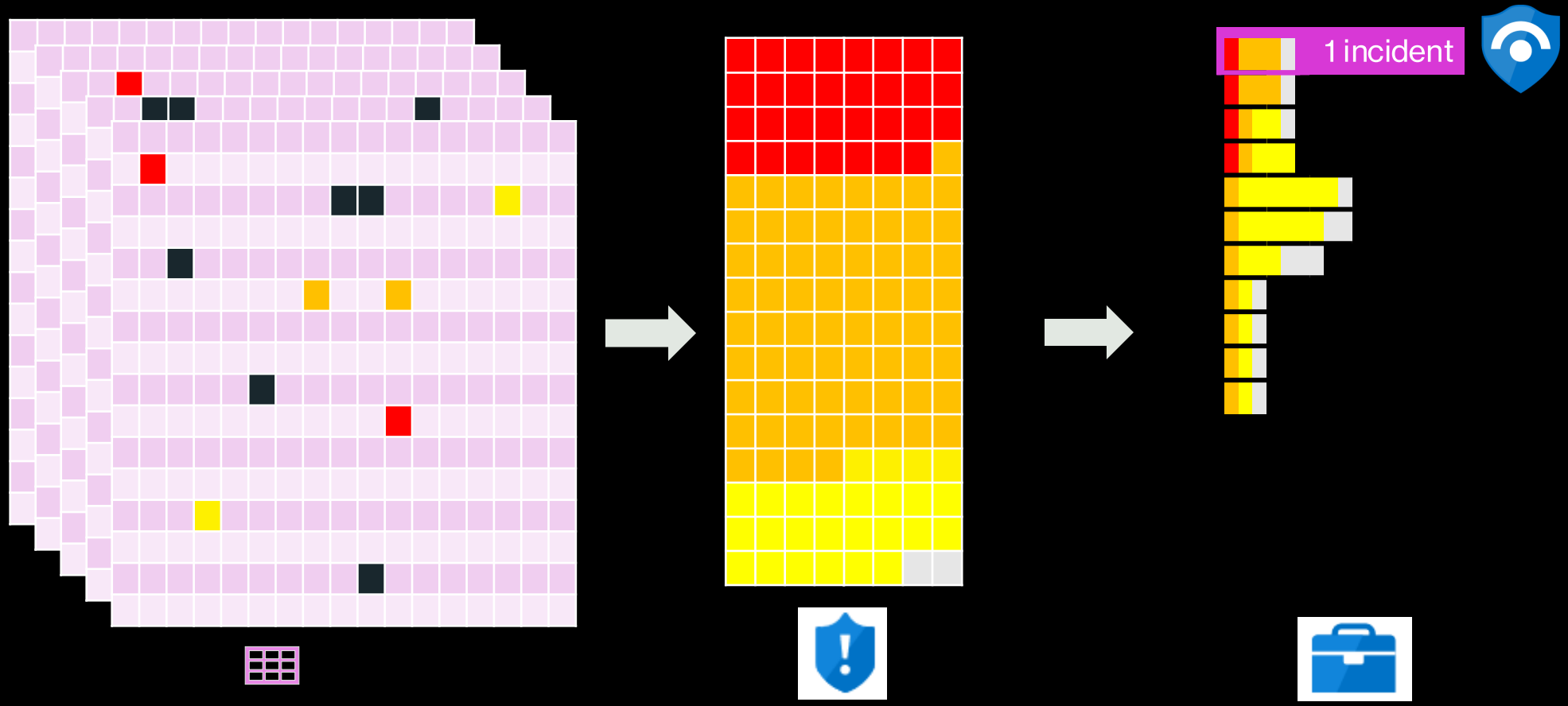
- Marketplace for ARM-based sentinel solutions such as connectors, analytic rules, hunting queries & more
- Includes Microsoft data sources but also 3rd party solutions, from e.g. :
  - Zscaler
  - Palo Alto
  - CrowdStrike
  - CheckPoint



# Sentinel Workflow



# Sentinel Incident Correlation




**Events**

millions to billions

**Alerts**

group/promote interesting Events

**Incidents**

group related Alerts

# Analytic Rules

- Analytic Rules are your SIEM use-cases defined via KQL
- Sentinel comes with over 500 rule templates
- Limit of 512 rules per workspace
- 7 Types of analytic rules:
  - Scheduled
  - Near-Real-Time (NRT)
  - Fusion
  - ML Behavior Analytics
  - Threat Intelligence
  - Microsoft Security
  - Anomaly

# Scheduled Rules

- Analytic Rules that continuously run in a defined timeframe
- An alert is fired if a condition is met
- Scheduled rules are the default rule type and most analytic rules will have this rule type

# Near-Real-Time Rules (NRT)

- Analytic Rules that run continuously and shall provide “up-to-the-minute” threat detections
- NRTs run once every minute in reality
- Limit of 50 NRT rules per workspace

# Fusion

- Analytic Rule that is an advanced multistage attack detection feature including over 120 detections across multiple Microsoft data sources:
  - Entra ID Protection
  - Defender for Cloud
  - Defender for IoT
  - Defender XDR
  - Sentinel scheduled rules
  - Sentinel NRT rules
- There can only be one Fusion rule per Sentinel workspace

# ML Behavior Analytic Rules

- Analytic Rule that monitors for unusual Windows RDP and Linux SSH logons based on pre-defined scenarios
- Scenarios include:
  - Unusual IP - This IP address has not or has rarely been seen in last 30 days.
  - Unusual Geo - The IP address, city, country and ASN have not (or rarely) been seen in last 30 days.
  - New user - A new user logs in from an IP address and geo location, both or either of which are not expected to be seen in the last 30 days.

# Threat Intelligence Rules

- Generates an alert when a Microsoft Defender Threat Intelligence Indicator gets matched with your event logs
- The alerts are very high fidelity

# Microsoft Security Rules

- Analytic rules that are alert forwarders from other Microsoft security services, such as:
  - Defender for Endpoint
  - Defender for Identity
  - Defender for Cloud

# Anomaly Rules

- Non-alerting informational rules from UEBA
- Detect deviations from a baseline
- Designed to provide more context on entities and to enrich threat hunting

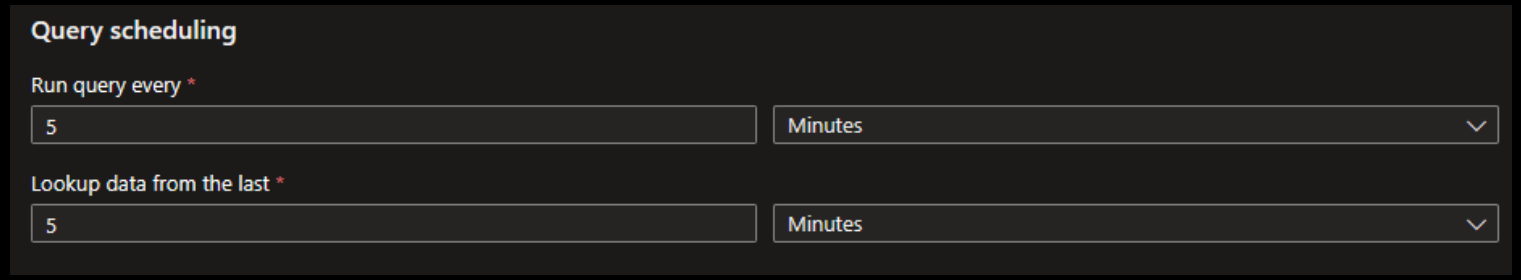
# What is Ingestion Delay?

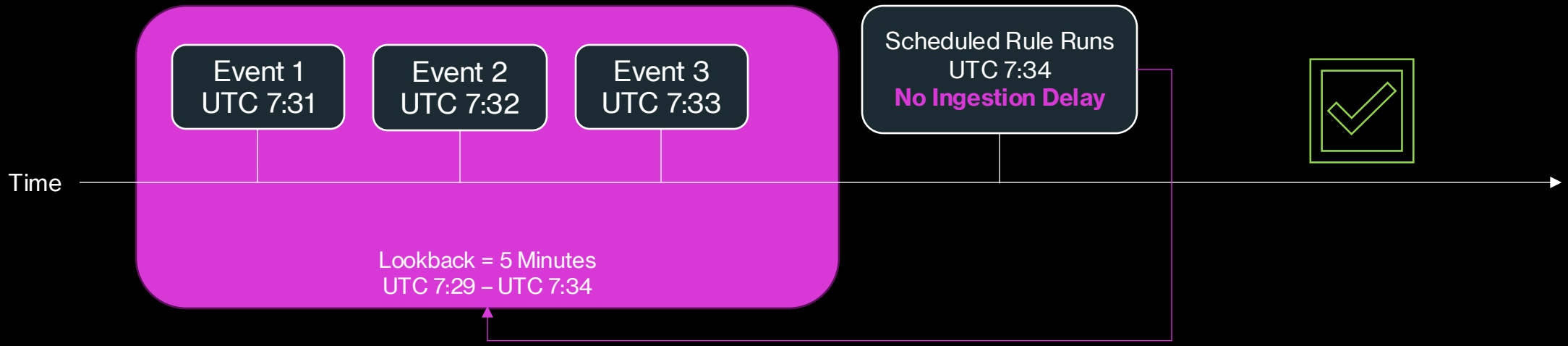
- Ingestion Delay is the time between log creation at the source and ingestion into Sentinel
- Ingestion Delay can significantly mess with your scheduled analytic rules
- Important: Scheduled Rules consider the timestamp of the data source not the timestamp of ingest



Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

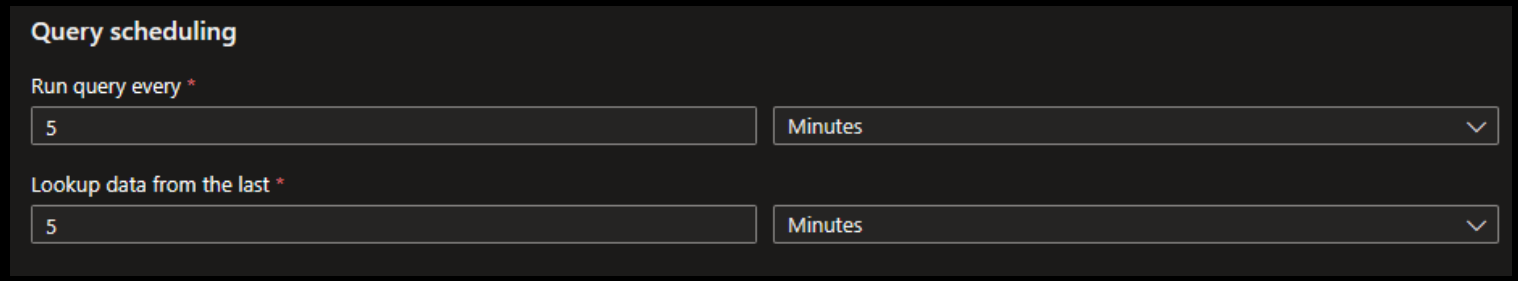
# Countering Ingestion Delay 1/3

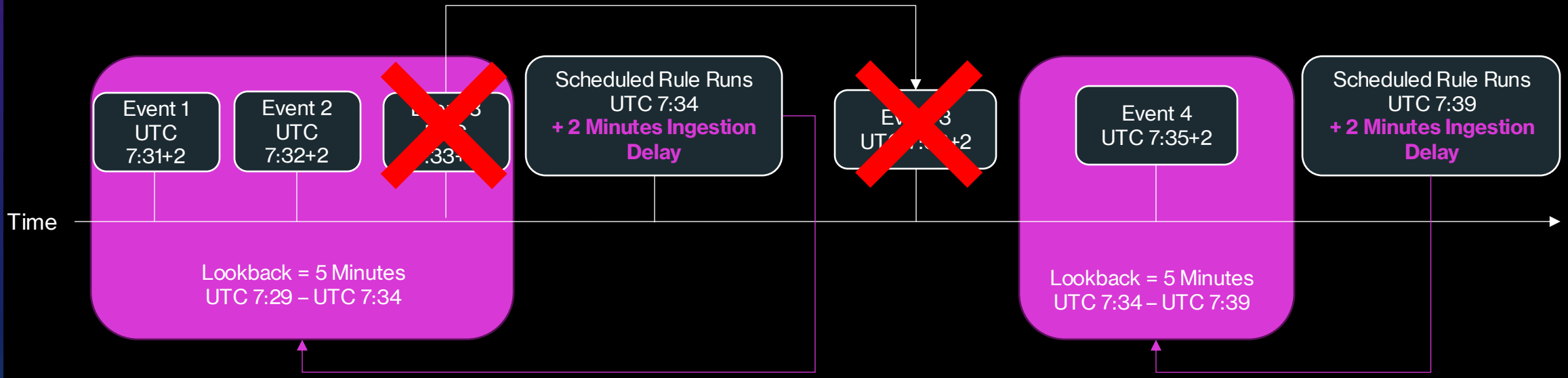



Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

# Countering Ingestion Delay 2/3




Christopher Nett

Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

# Countering Ingestion Delay 3/3

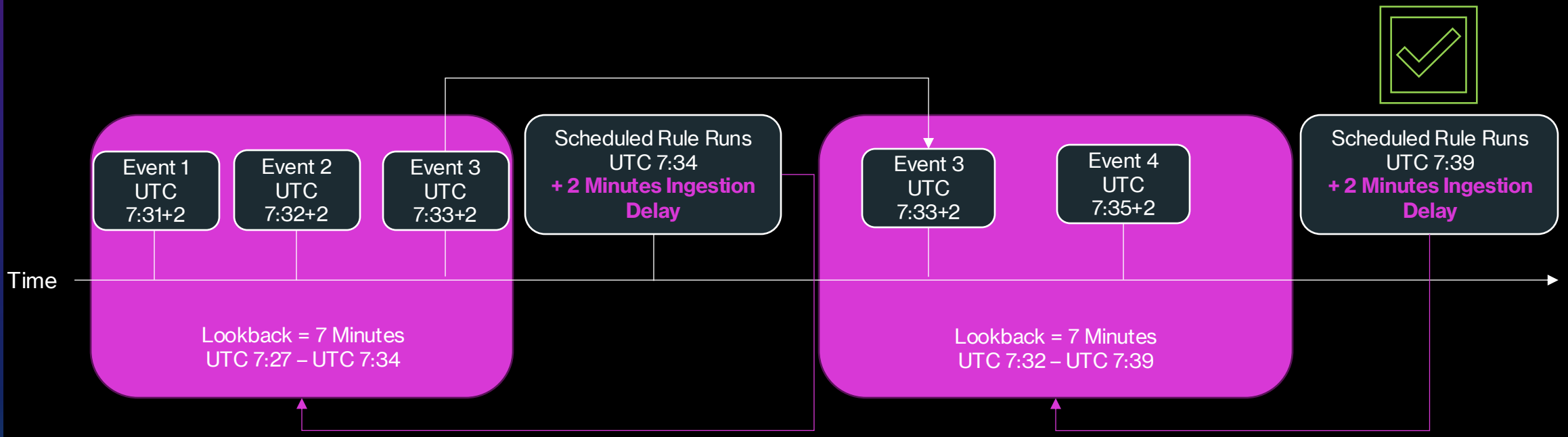
**Query scheduling**

Run query every *

5 | Minutes

Lookup data from the last *

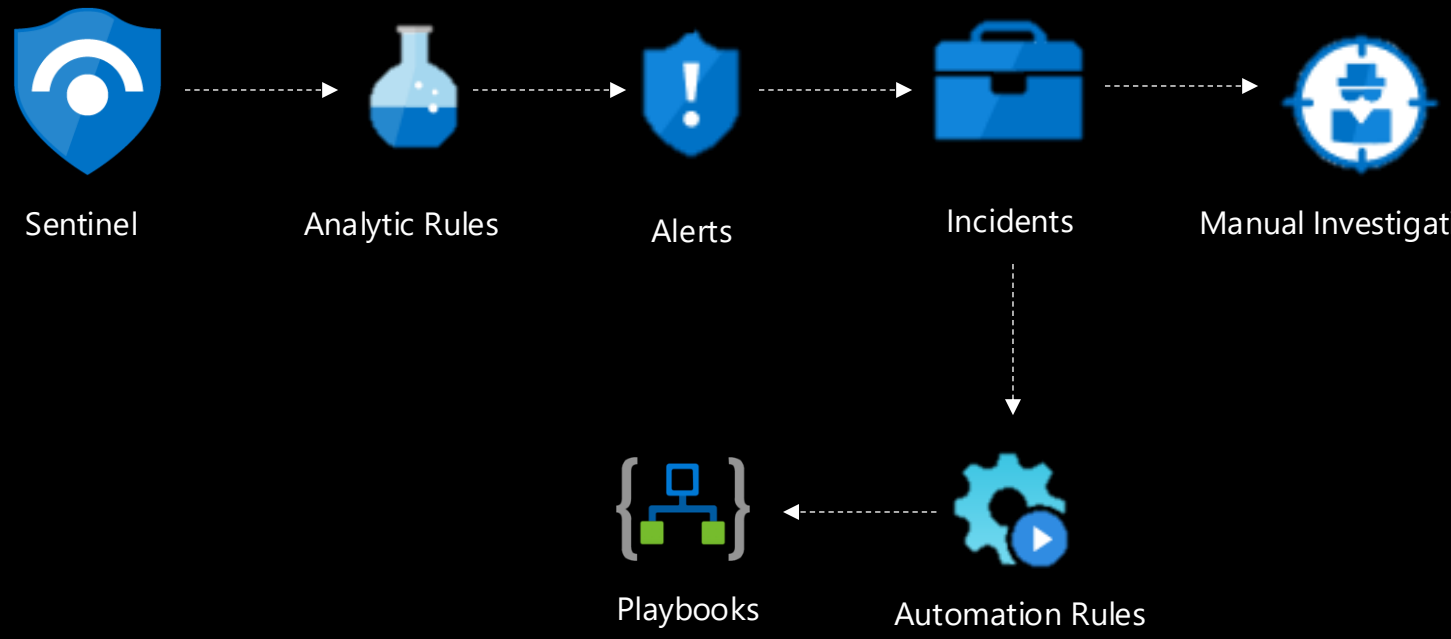
7 | Minutes



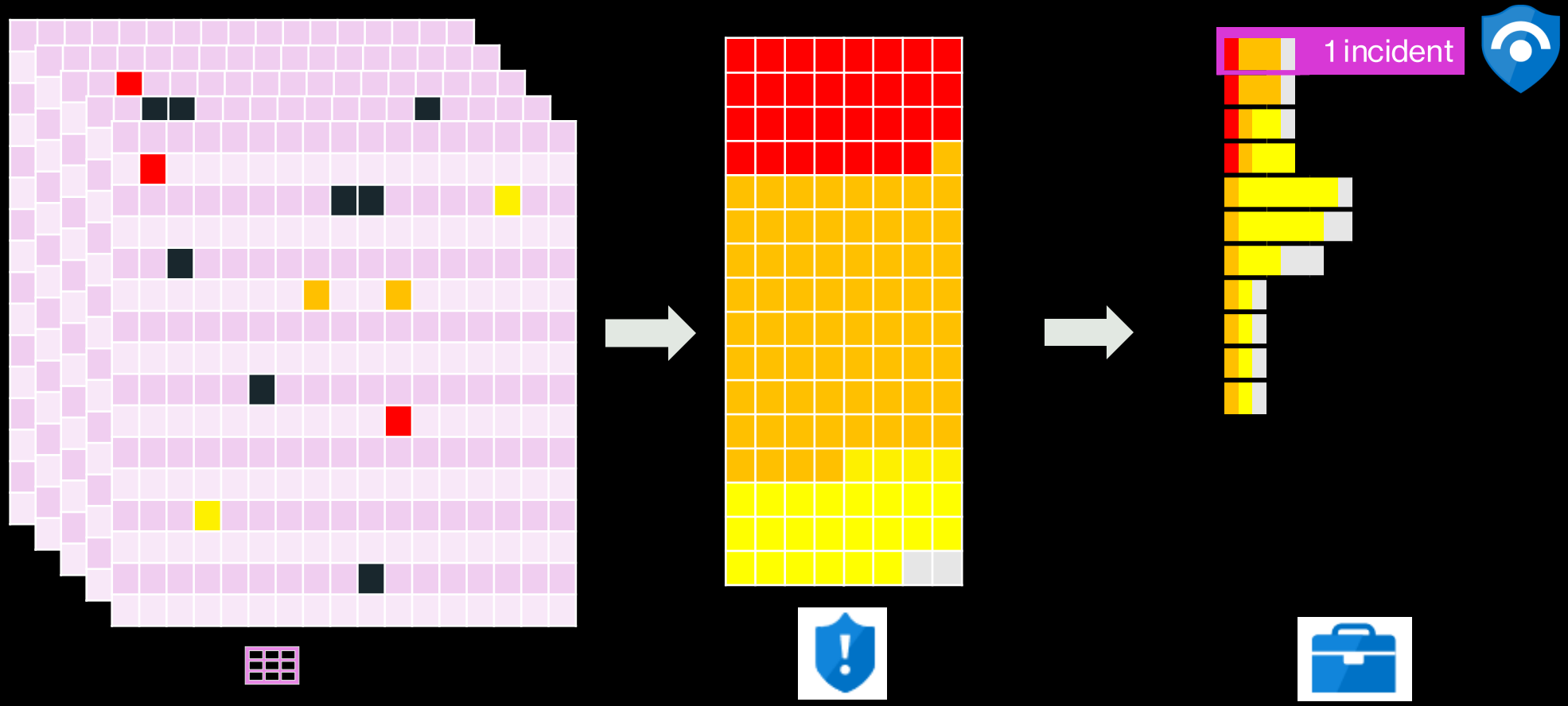



Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

# Sentinel Workflow



# Sentinel Incident Correlation




**Events**

millions to billions

**Alerts**

group/promote interesting Events

**Incidents**

group related Alerts

# Analytic Rules

- Analytic Rules are your SIEM use-cases defined via KQL
- Sentinel comes with over 500 rule templates
- Limit of 512 rules per workspace
- 7 Types of analytic rules:
  - Scheduled
  - Near-Real-Time (NRT)
  - Fusion
  - ML Behavior Analytics
  - Threat Intelligence
  - Microsoft Security
  - Anomaly

# Scheduled Rules

- Analytic Rules that continuously run in a defined timeframe
- An alert is fired if a condition is met
- Scheduled rules are the default rule type and most analytic rules will have this rule type

# Near-Real-Time Rules (NRT)

- Analytic Rules that run continuously and shall provide “up-to-the-minute” threat detections
- NRTs run once every minute in reality
- Limit of 50 NRT rules per workspace

# Fusion

- Analytic Rule that is an advanced multistage attack detection feature including over 120 detections across multiple Microsoft data sources:
  - Entra ID Protection
  - Defender for Cloud
  - Defender for IoT
  - Defender XDR
  - Sentinel scheduled rules
  - Sentinel NRT rules
- There can only be one Fusion rule per Sentinel workspace

# ML Behavior Analytic Rules

- Analytic Rule that monitors for unusual Windows RDP and Linux SSH logons based on pre-defined scenarios
- Scenarios include:
  - Unusual IP - This IP address has not or has rarely been seen in last 30 days.
  - Unusual Geo - The IP address, city, country and ASN have not (or rarely) been seen in last 30 days.
  - New user - A new user logs in from an IP address and geo location, both or either of which are not expected to be seen in the last 30 days.

# Threat Intelligence Rules

- Generates an alert when a Microsoft Defender Threat Intelligence Indicator gets matched with your event logs
- The alerts are very high fidelity

# Microsoft Security Rules

- Analytic rules that are alert forwarders from other Microsoft security services, such as:
  - Defender for Endpoint
  - Defender for Identity
  - Defender for Cloud

# Anomaly Rules

- Non-alerting informational rules from UEBA
- Detect deviations from a baseline
- Designed to provide more context on entities and to enrich threat hunting

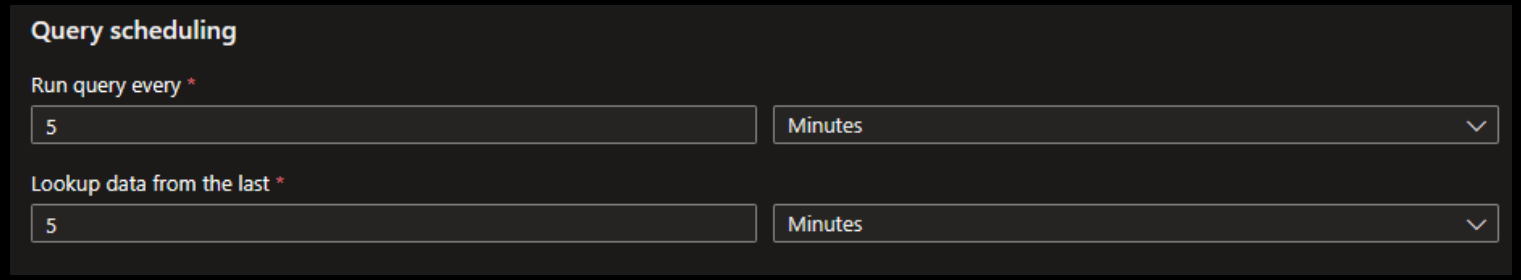
# What is Ingestion Delay?

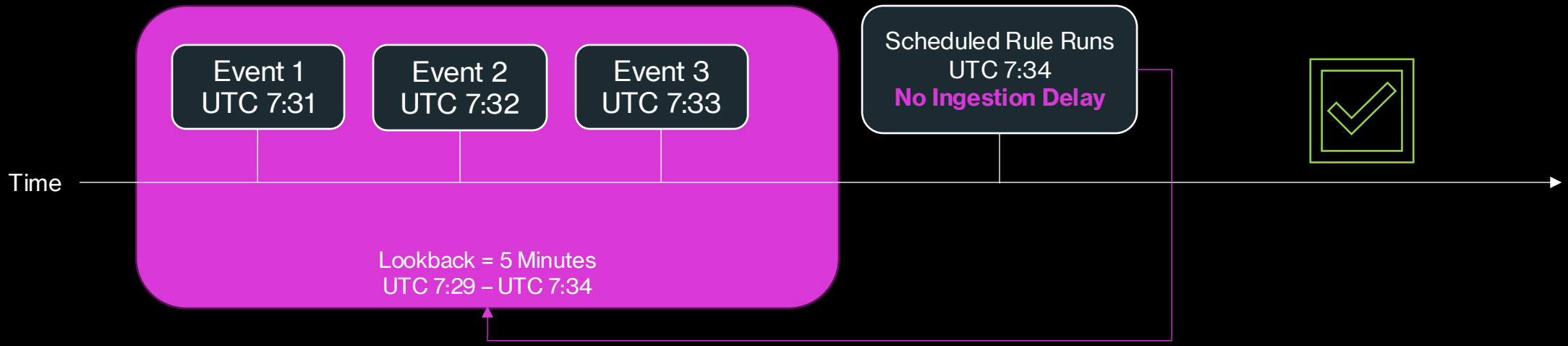
- Ingestion Delay is the time between log creation at the source and ingestion into Sentinel
- Ingestion Delay can significantly mess with your scheduled analytic rules
- Important: Scheduled Rules consider the timestamp of the data source not the timestamp of ingest



Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

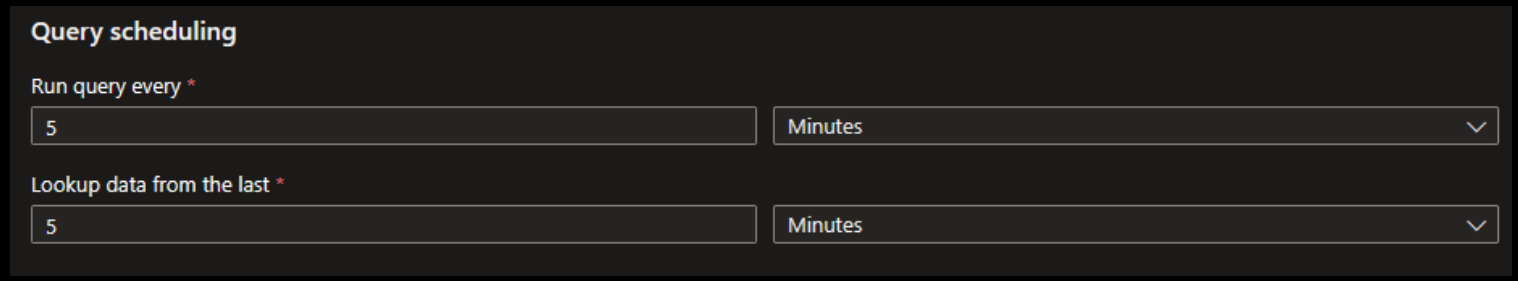
# Countering Ingestion Delay 1/3

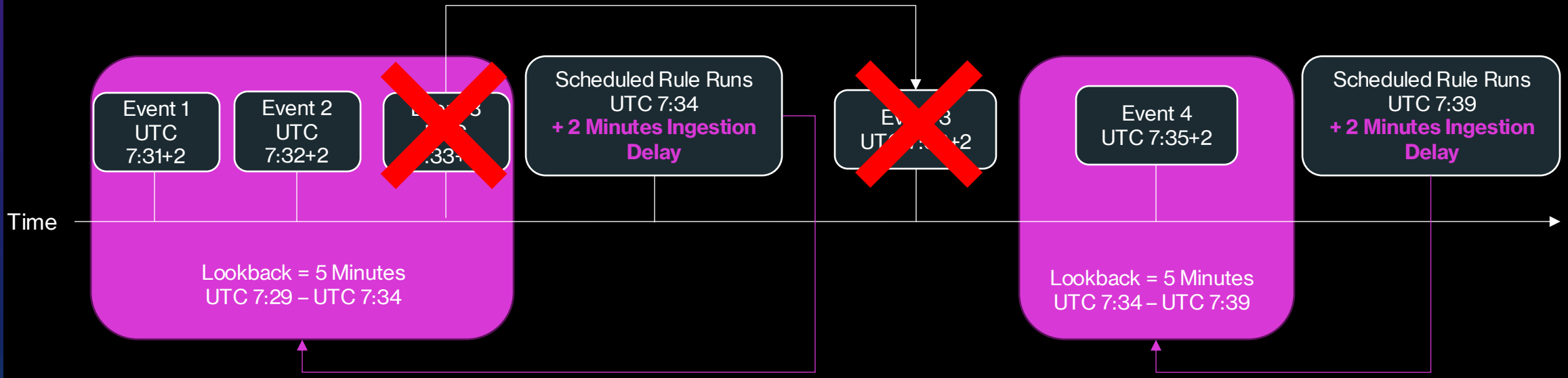



Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

# Countering Ingestion Delay 2/3




Christopher Nett

Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

# Countering Ingestion Delay 3/3

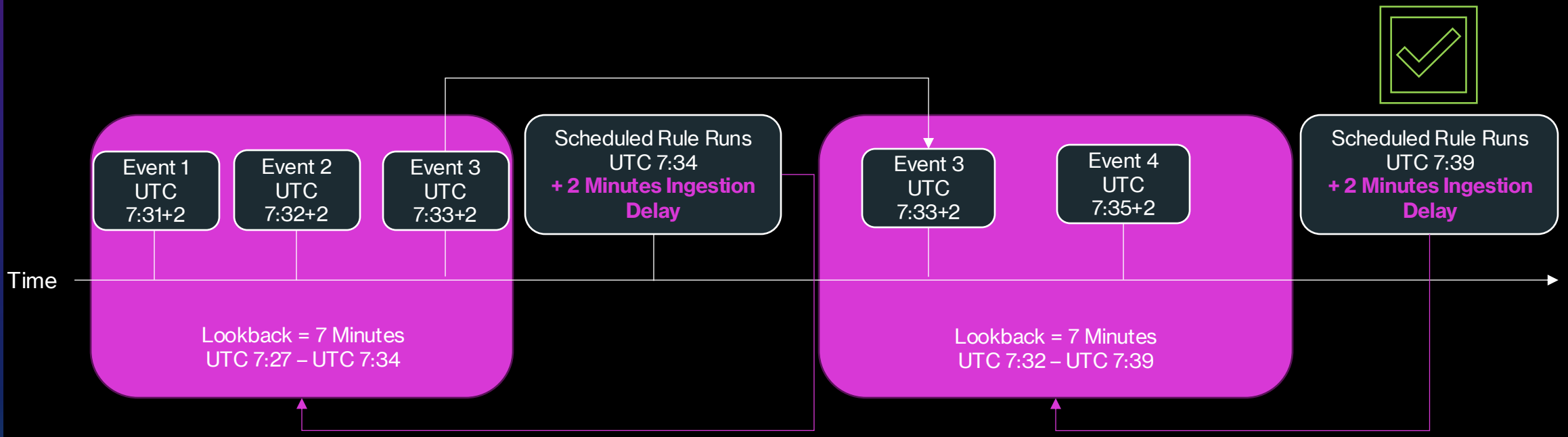
**Query scheduling**

Run query every *

5 | Minutes

Lookup data from the last *

7 | Minutes






Source: Handle ingestion delay in Microsoft Sentinel | Microsoft Learn

# Threat Hunting

What is Threat Hunting?

- Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in your environment
- Instead of only relying on your analytic rules in Sentinel you additionally hunt for threats via KQL



Source: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

# Threat Hunting

There are two Threat Hunting Models:

1) Intelligence-based Hunting → Utilizes IoCs, hash values, IP addresses, domain names or host artifacts
2) Hypothesis-based Hunting: Hunts are done based on IOAs and TTPs of adversaries



Source: https://www.ibm.com/topics/threat-hunting

# KQL Query Development Process

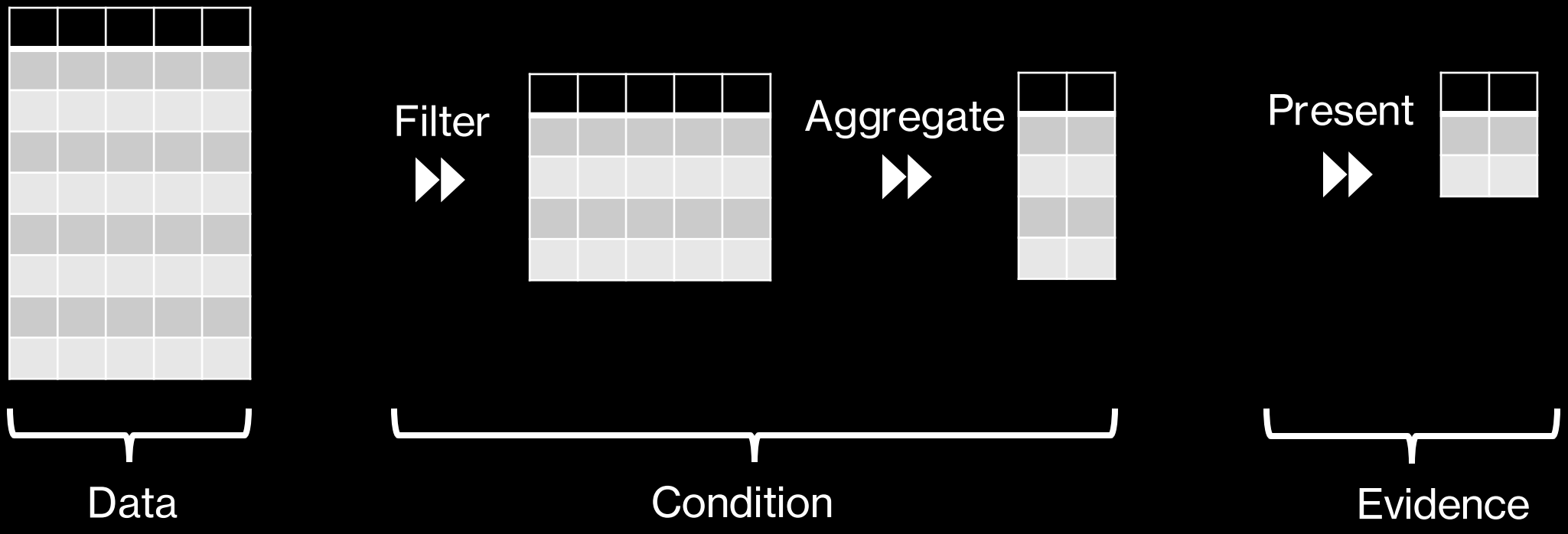
1. Hypothesis
   - A query always begins with a hypothesis that you want to prove or disprove, such as: Is this IoC part of my logs?
2. Determine required tables
   - Determine the required tables for your query
3. Explore table schema
   - Consider the schema
4. Filter away
5. Visualize



Source: Kusto Query Language (KQL) overview - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

# Kusto Query Language (KQL)

```
SecurityEvent
| where EventID == “4264”
| summarize count () by Account
| top 10 by count
```

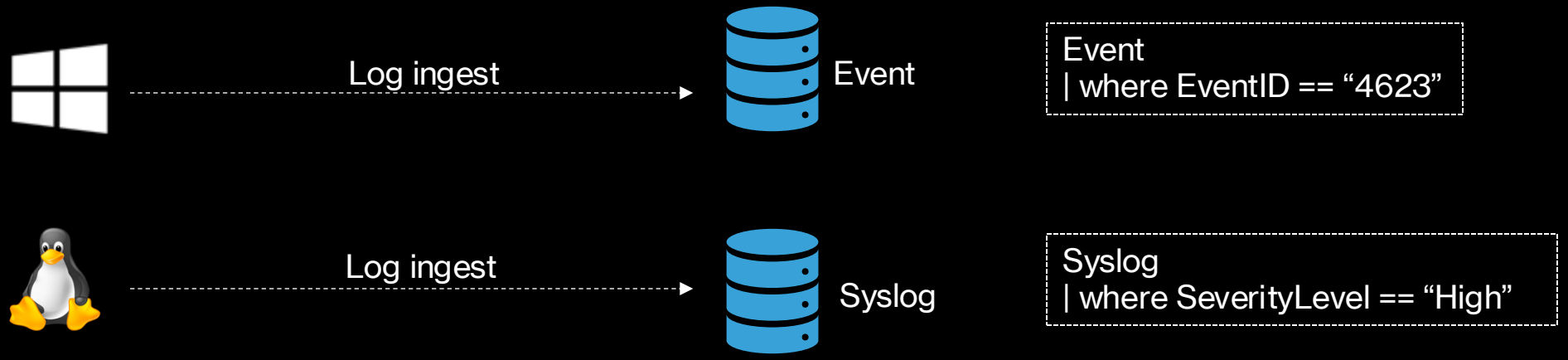



Christopher Nett

Source: Kusto Query Language (KQL) overview - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

# Log Analytics - Tables

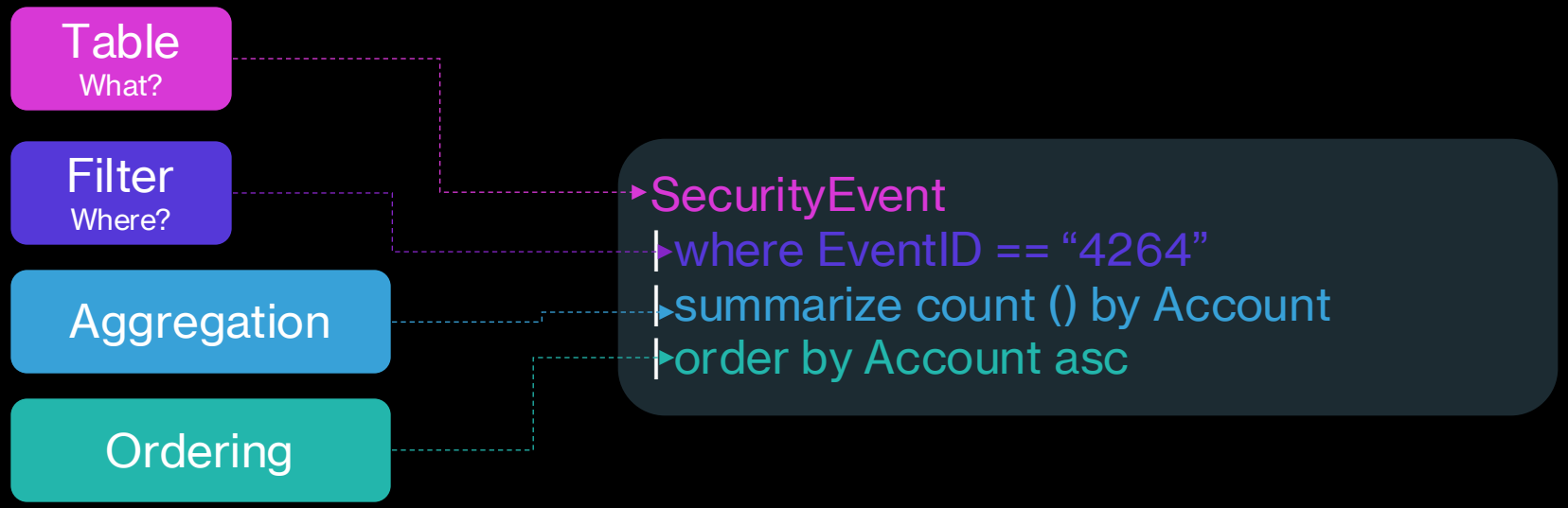
- All connected data sources are ingested in specific tables






Source: Kusto Query Language (KQL) overview - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

# KQL 101






Source: Kusto Query Language (KQL) overview - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

# KQL – Important Operators

| Operator | Action |
|---|---|
| where | Filters on a specific predicate |
| search | Searches all columns in the table for the value |
| limit /take | Returns the specified number of records |
| count | Counts records in the input table |
| summarize | Groups the rows according to the by group columns, and calculates aggregations over each group |
| render | Renders results as a graphical output, e.g. a piechart |
| extend | Creates a calculated column and adds it to the result set |
| project | Selects the columns to include in the order specified |
| distinct | Produces a table with the distinct combination of the provided columns of the input table |
| sort | Sort the rows of the input table by one or more columns in ascending or descending order |
| let | Creates a temporary variable that can be referenced |
| union | Takes two or more tables and returns all their rows |
| join | Merges the rows of two tables to form a new table by matching values of the specified columns from each table |



Source: KQL quick reference - Azure Data Explorer & Real-Time Analytics | Microsoft Learn

# Cyber Threat Intelligence

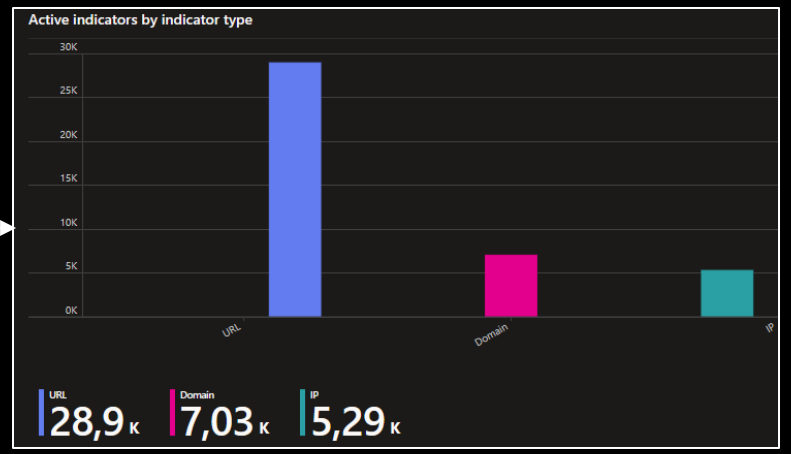
Log Analytics

```
1  ThreatIntelligenceIndicator
2  | where TimeGenerated > ago(1d)
3  | limit 5
```

Results | Chart | Add bookmark

| TimeGenerated [UTC] | Action | Type |
|---|---|---|
| 5.12.2023, 06:06:13.719 | alert | ThreatIntelligenceIndicator |
| 5.12.2023, 06:06:13.713 | alert | ThreatIntelligenceIndicator |
| 5.12.2023, 06:06:13.703 | alert | ThreatIntelligenceIndicator |
| 5.12.2023, 06:06:13.697 | alert | ThreatIntelligenceIndicator |
| 5.12.2023, 06:06:13.689 | alert | ThreatIntelligenceIndicator |

Workbooks




CTI Sources

Threat Hunting

Analytic Rules

TI Map IP Entity to AzureActivity

| Medium | Content hub | Scheduled |
|---|---|---|
| Severity | Content Source | Rule Type |

Rule query

```
let dt_lookBack = 1h; // Look back 1 hour for AzureA
let ioc_lookBack = 14d; // Look back 14 days for thr
// Fetch threat intelligence indicators related to I
let IP_Indicators = ThreatIntelligenceIndicator
  | where TimeGenerated >= ago(ioc_lookBack)
  | summarize LatestIndicatorTime = arg_max(TimeGener
```

Incidents

Playbooks

Christopher Nett

Source: Cyber threat intelligence in Microsoft Sentinel - Azure Example Scenarios | Microsoft Learn

# STIX & TAXII

- STIX (Structured Threat Information eXpression)
- TAXII (Trusted Automated eXchange of Indicator Information)
- Purpose: Share Threat Intelligence

# STIX & TAXII

- STIX
  - Standardized language build on JSON
  - Enables the exchange of CTI between systems
- TAXII
  - The protocol that transmits STIX insights via HTTPS

# Threat Intelligence in Sentinel

In Sentinel, Threat Intelligence can be used in:

- Analytic Rules
- Threat Hunting
- Incidents
- Workbooks
- Notebooks
- Playbooks

# Why automate?

- Security Automation is not: Isolating machines
- Security Automation is: Mimicking the steps an Analyst would take when responding to incidents
- Automation has a positive impact on:
  - Mean time to react
  - SOC efficiency
  - Cost
  - Standardized responses to incidents

# Automation Capabilities

- Automation Rules 
  - Basic Automations
- Playbooks
  - Complex Automations →Think SOAR 

# Automation Rules 

- Allow for centralized automation of incident handling
- Used to automate simple actions in your triage, such as:
  - Assigning users to incidents
  - Tagging incidents
  - Changing status of incidents
  - Triggering playbooks

# Playbooks 

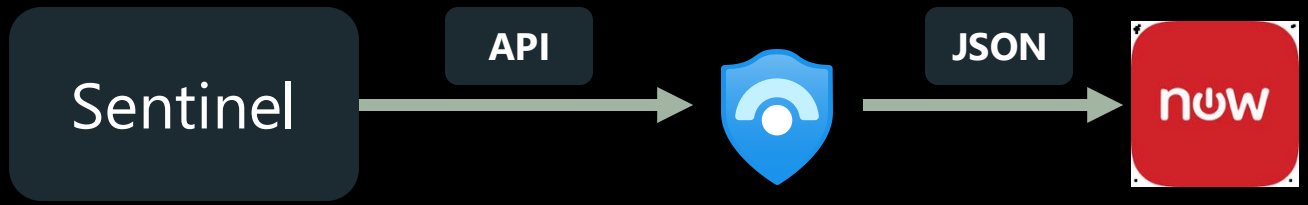
- Used to automate complex tasks → this is your SOAR!
- Used to trigger Azure Logic Apps
- Playbooks can also be triggered from Automation Rules

# Automation Rules vs. Playbooks

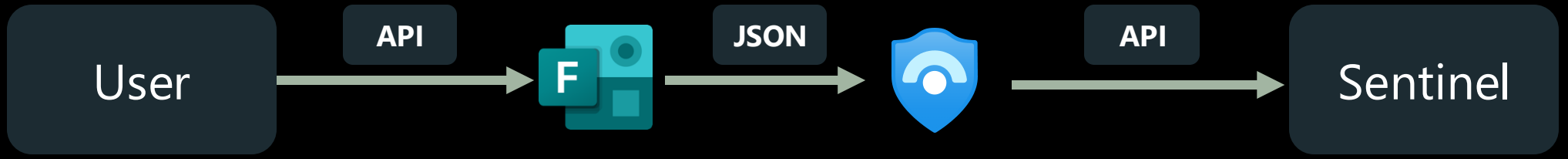
| | **Playbooks** | **Automation Rules** |
|---|---|---|
| Price | Logic Apps | Free |
| Purpose | SOAR | Automation as part of Triage |
| Scope | Close to limitless | Limited to Sentinel |
| Rule Types | Scheduled rules only | All rule types |
| Trigger | Sentinel & external triggers | Sentinel incidents |

# Azure Logic App Workflows

**Example 1:** Sentinel playbook triggers ticket creation in ServiceNow ITSM




**Example 2:** User completes security incident form that creates an incident in Sentinel






Source: Introduction to automation in Microsoft Sentinel | Microsoft Learn

# Azure Logic App Workflows

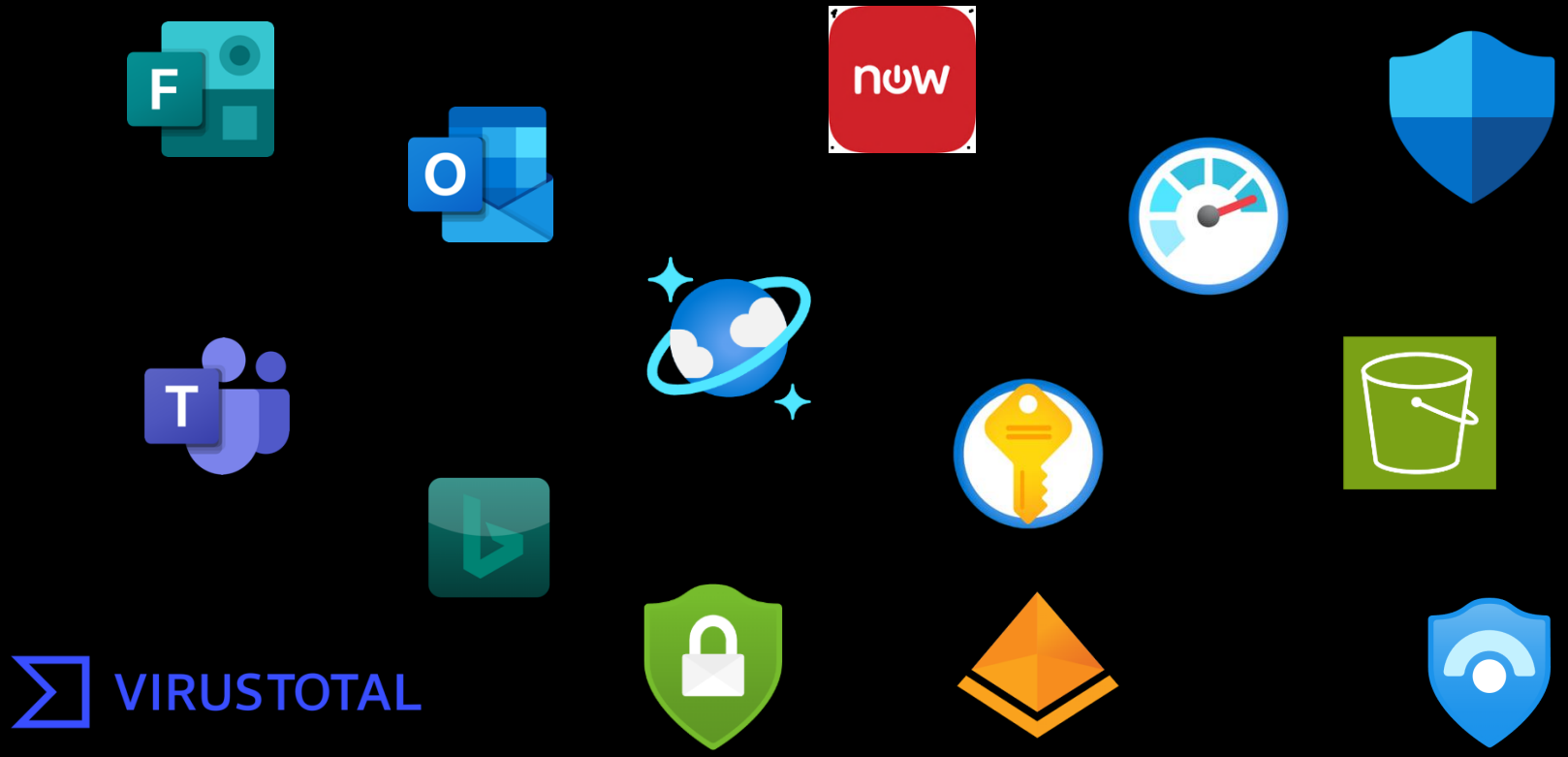
**Example 3:** ChatGPT enriches Incident with explanation for a MITRE ATT&CK Tactic


**Example 4:** VirusTotal enriches Incident with analysis of IoCs




Source: Introduction to automation in Microsoft Sentinel | Microsoft Learn

# Logic App Connectors






List of all Logic App Connectors: List of all Logic Apps connectors | Microsoft Learn

# Sentinel REST API

- Sentinel has several APIs that you can interact with:
  - Sentinel Management API
  - Microsoft Graph Security API
  - Azure Log Analytics API
  - HTTP data Collector API

# Sentinel REST API

Sentinel Management API

CREATE / GET / UPDATE Incidents
CREATE / GET / UPDATE Analytic Rules

Sentinel

Microsoft Graph Security API

GET / POST Alert Information

HTTP Data Collector API

Store logs in LAW

Log Analytics

Log Analytics API

Query stored logs