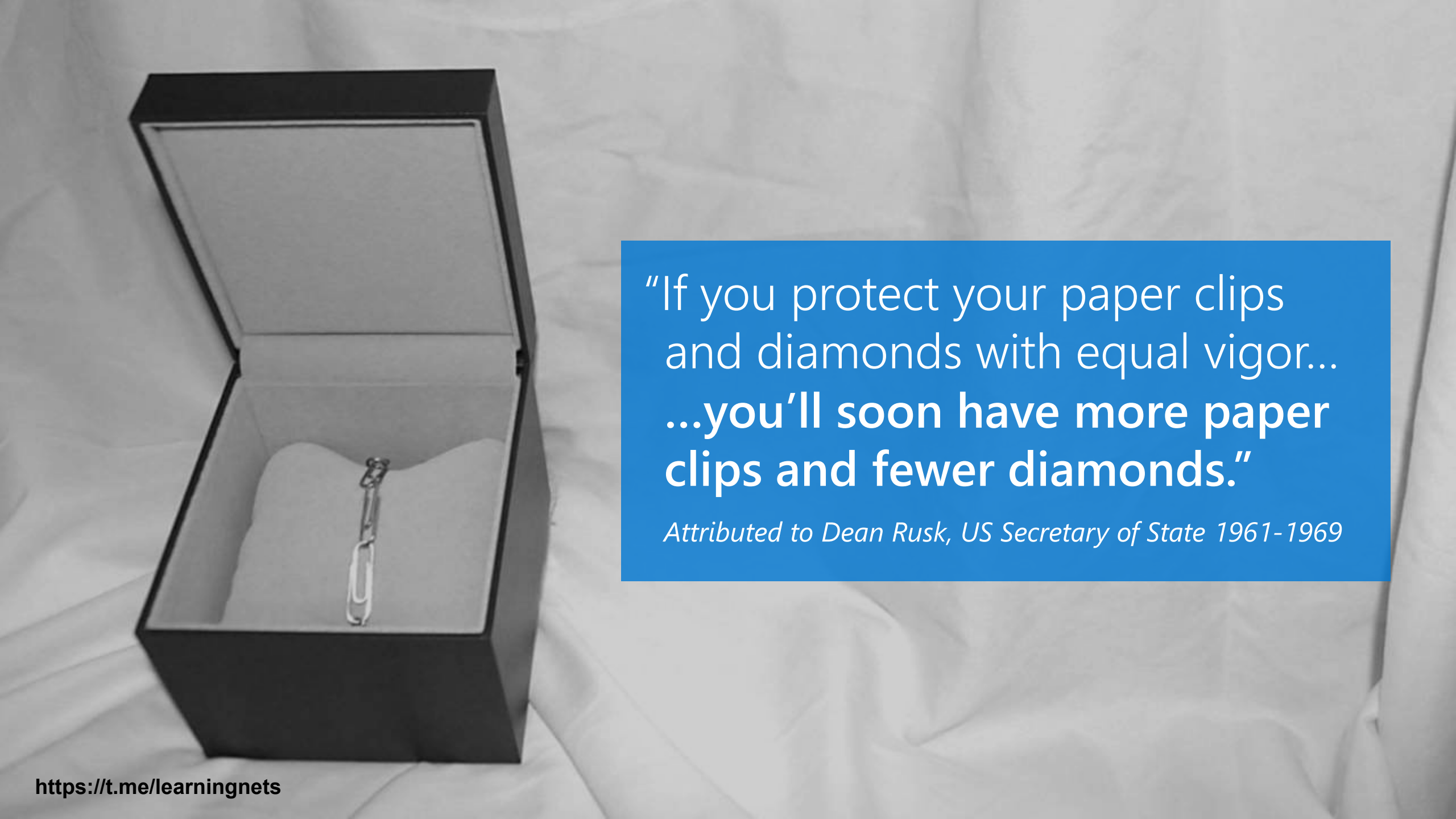
Microsoft

Microsoft CISO Workshop
5 - Information Protection Strategy

Microsoft Cybersecurity Solutions Group

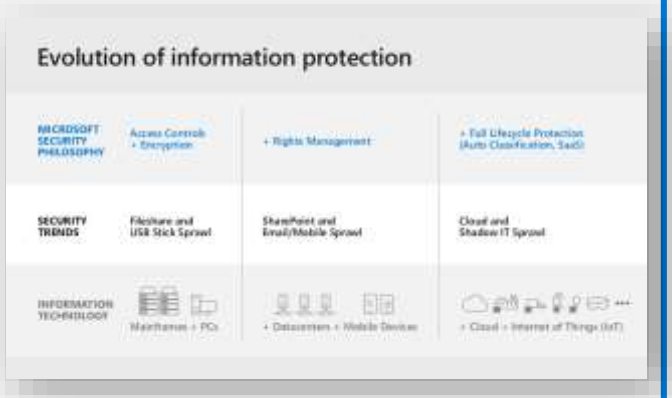


"If you protect your paper clips and diamonds with equal vigor…
…you'll soon have more paper clips and fewer diamonds."

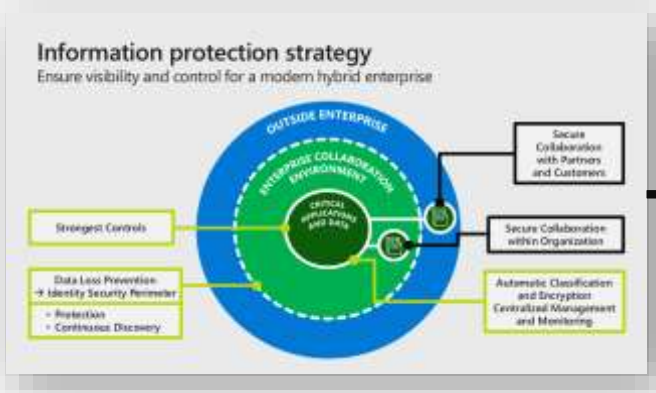
Attributed to Dean Rusk, US Secretary of State 1961-1969

Information Protection

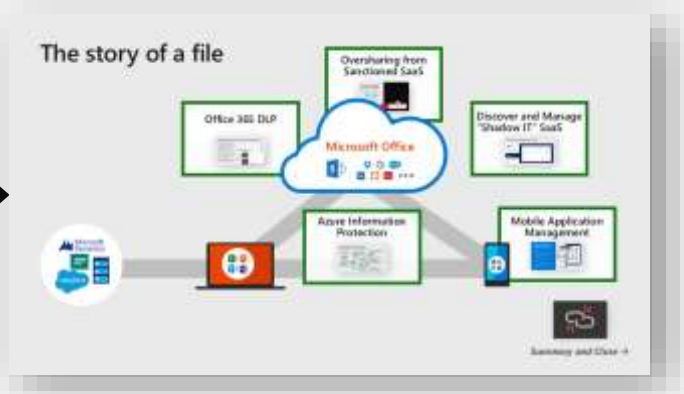
TRENDS AND STRATEGIES



STRATEGY AND CAPABILITIES



INFORMATION PROTECTION STRATEGY



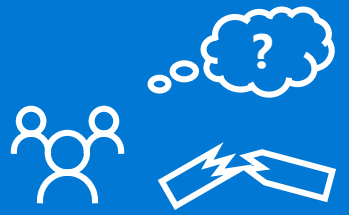
SENSITIVE DOCUMENTS

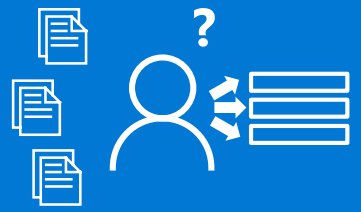
SQL AND STRUCTURED DATA

Evolution of information protection

MICROSOFT SECURITY PHILOSOPHY	Access Controls + Encryption	+ Rights Management	+ Full Lifecycle Protection (Auto Classification, SaaS)
SECURITY TRENDS	Fileshare and USB Stick Sprawl	SharePoint and Email/Mobile Sprawl	Cloud and Shadow IT Sprawl
INFORMATION TECHNOLOGY	 Mainframes + PCs	 + Datacenters + Mobile Devices	 + Cloud + Internet of Things (IoT)

Data security challenges





Reduce and Manage Risk of User Errors

Collaboration to create new business value requires data sharing and data mobility

Critically important to prevent unauthorized disclosure, modification, or destruction

Classification is Challenging

Manual user classification is impractical at scale

Large set of existing documents and more being created all the time

Data Must Be Protected Outside of the Network

Data must be protected as it traverses mobile devices and cloud services

Data created outside the network must be classified and protected

Compliance and Security Require a Complete Strategy

Compliance penalties are increasing and measuring outcomes vs. methods

Need full lifecycle protection for information assets (appropriate to valuation)

Top Information Protection Use Cases

DISCOVER – CLASSIFY – PROTECT – MONITOR

Information Protection and Data Governance Strategy

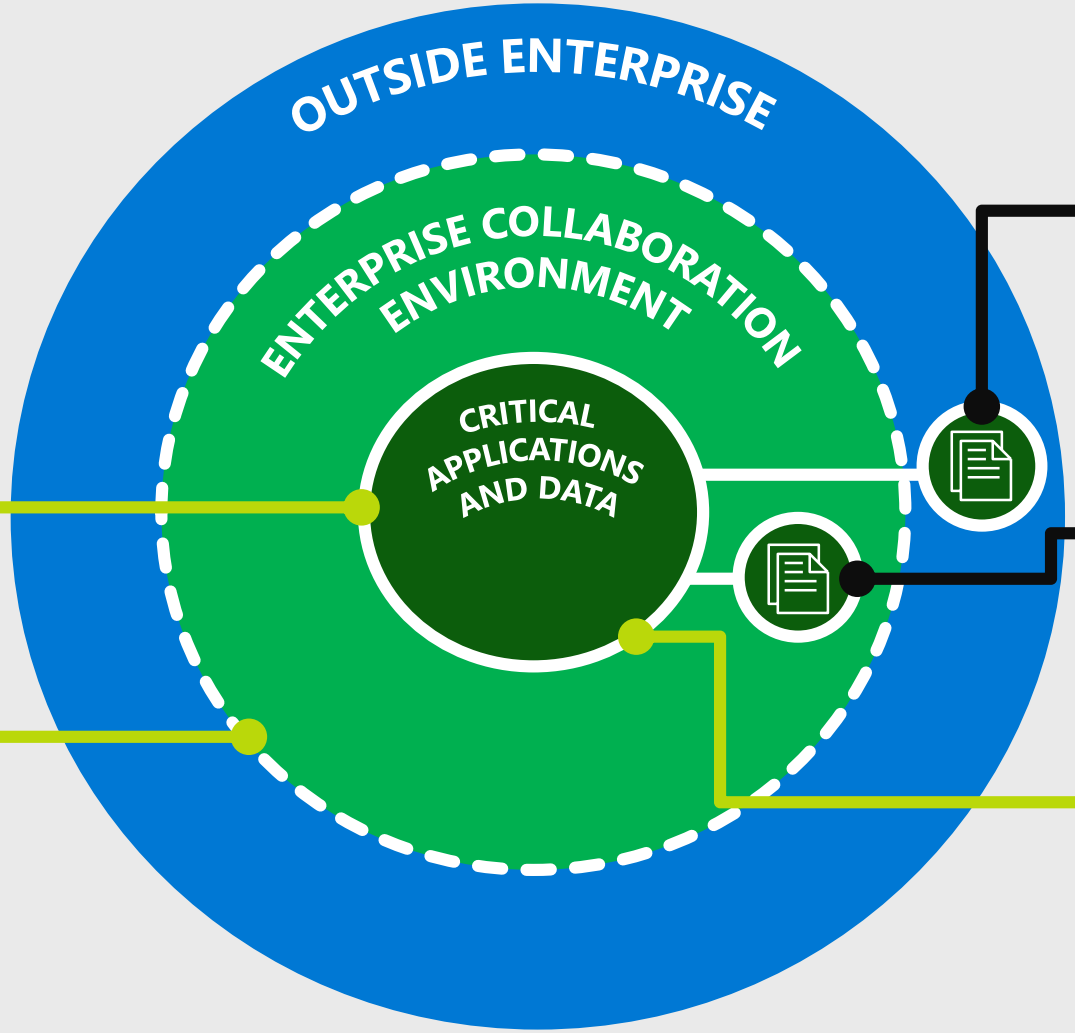
- Label, track, and show data loss or manipulation of a file.
- Implement corporate policies to protect different levels of sensitive data

Protecting sensitive information

- Challenging to discover and classify data across mobile devices, SaaS, cloud infrastructure, and on-premises
- Need full lifecycle data protection for identified data including encryption, permissions, visual markings, access revocation, retention and deletion

Information protection strategy

Ensure visibility and control for a modern hybrid enterprise



Strongest Controls

Data Loss Prevention
→ Identity Security Perimeter

- Protection
- Continuous Discovery

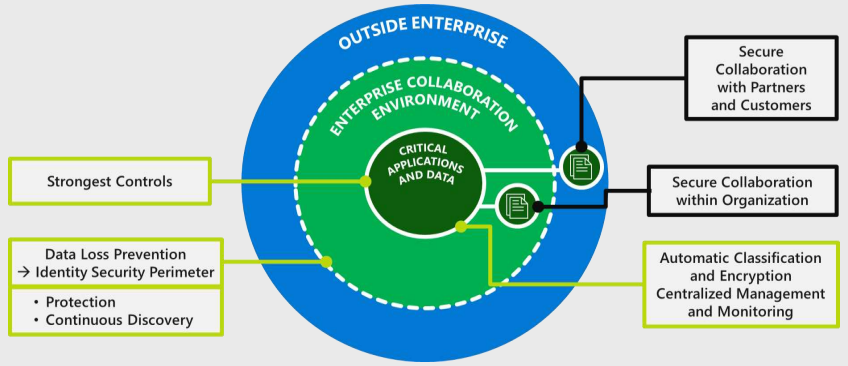
Secure Collaboration with Partners and Customers

Secure Collaboration within Organization

Automatic Classification and Encryption
Centralized Management and Monitoring

Strategy core goal

Protect at the appropriate level



3 **HIGHEST VALUE ASSETS**

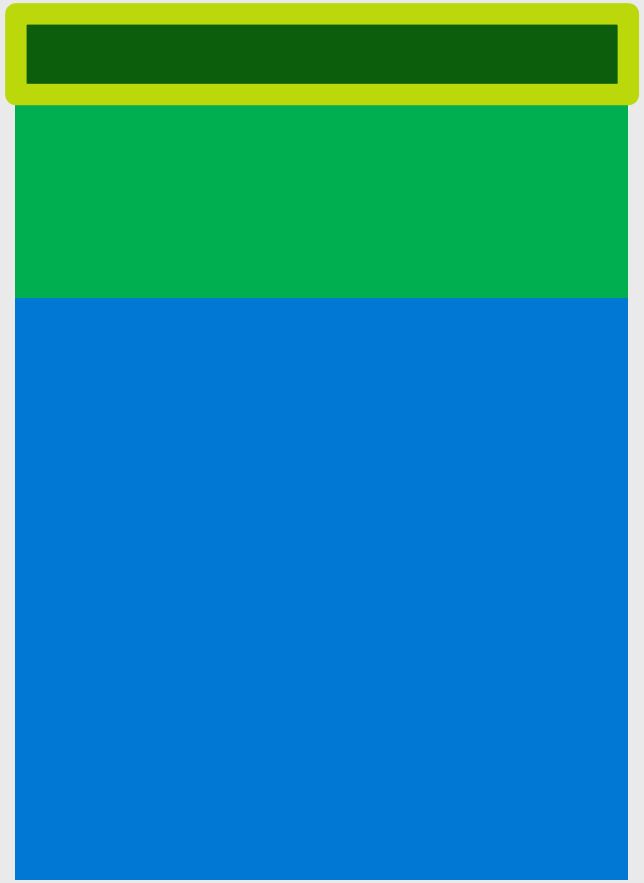
Level 2 + Specialized Protection and processes

2 **SENSITIVE INFORMATION**

Reduce risk of theft, modification, and destruction

1 **BASELINE PROTECTION**

Building an Identity Security Perimeter



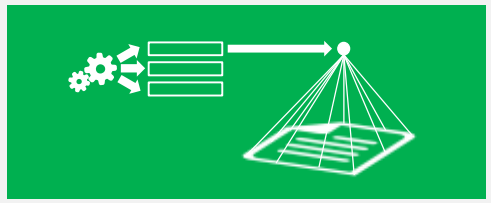
Success criteria—information protection

Information Protection and Data Governance Strategy

COVERAGE – Structured and unstructured, backups, SaaS, etc.

INTEGRATION – New capabilities with existing DLP processes (and tools)

Sensitive Information Success Criteria



Centralized control – Monitor and revoke access to documents

Automatic classification – Of new, existing, and exported documents

Embedded protection – Protect the data, not just storage/networks

Persistent protection – For your sensitive data anywhere it goes

FULL STACK FOR HIGHEST VALUE ASSETS – Host/device/identity/etc. security + user education

The story of a file

Oversharing from Sanctioned SaaS

Office 365 DLP

Microsoft Office

Discover and Manage "Shadow IT" SaaS

Azure Information Protection

Mobile Application Management

Microsoft Dynamics

SAP

salesforce

Summary and Close →

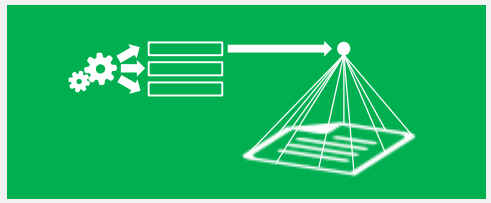
Success criteria—information protection

Information Protection and Data Governance Strategy

COVERAGE – Structured and unstructured, backups, SaaS, etc.

INTEGRATION – New capabilities with existing DLP processes (and tools)

Sensitive Information Success Criteria



Centralized control – Monitor and revoke access to documents

Automatic classification – Of new, existing, and exported documents

Embedded protection – Protect the data, not just storage/networks

Persistent protection – For your sensitive data anywhere it goes

FULL STACK FOR HIGHEST VALUE ASSETS – Host/device/identity/etc. security + user education

Microsoft

Questions?

References

Additional Resources – Information Protection

Microsoft Cloud App Security integration with 3rd party DLP engines

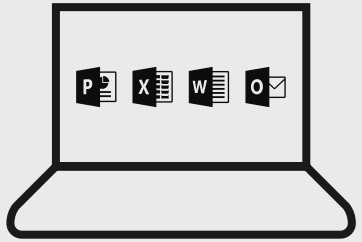
https://cloudblogs.microsoft.com/enterprisemobility/2018/01/30/microsoft-cloud-app-security-integrates-with-third-party-data-loss-prevention-solutions/

Protecting sensitive information

Persistent classification and protection of your documents

Set policies appropriate to organization

User creates a sensitive file at work



Classify and Label Data Automatically

Collaborate through SharePoint Online

Collaborate with existing tools

Upload to other cloud service for external sharing

Centralized control of keys and data

Monitor and

Revoke Access

Edge DLP

Endpoint DLP

Policy and encryption persists on data

User opens file from home PC or mobile device

Configure DLP to read labels

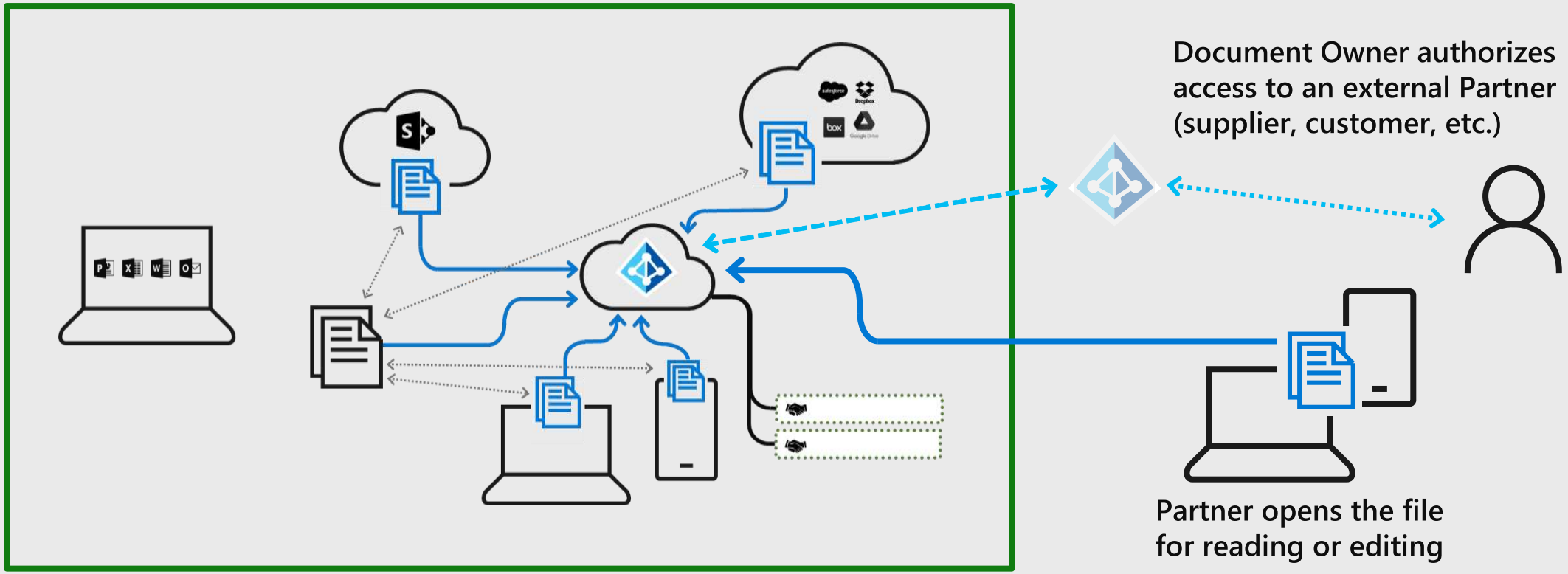
Leverage Existing Tools and Processes

Modern information protection

Collaborate securely with partners

Documents restricted to only authorized users

Enable simple external collaboration



Document Owner authorizes access to an external Partner (supplier, customer, etc.)

Partner opens the file for reading or editing

Key classification scenarios

Automatic

Set policies to automatically applying classification and protection to data

Recommended

Prompt with suggested classification based on the content you're working on

Reclassification

Enable users to override a classification (and optionally require providing a justification)

User Set

Manually apply a sensitivity label to the email or file they are working on

Support required formats for sensitive data

Coverage for popular formats + extensibility

Microsoft Office Formats

Built into

Microsoft Office

PDF

Partner(s)

Foxit

nitro

...and more

AutoCAD

Partner(s)

SealPath

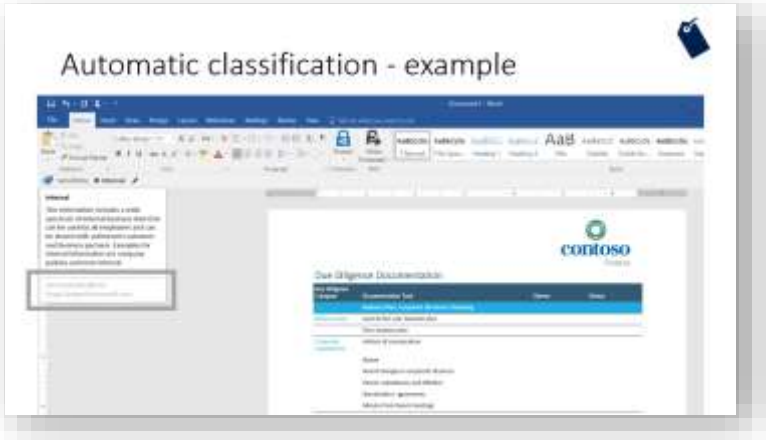
Others

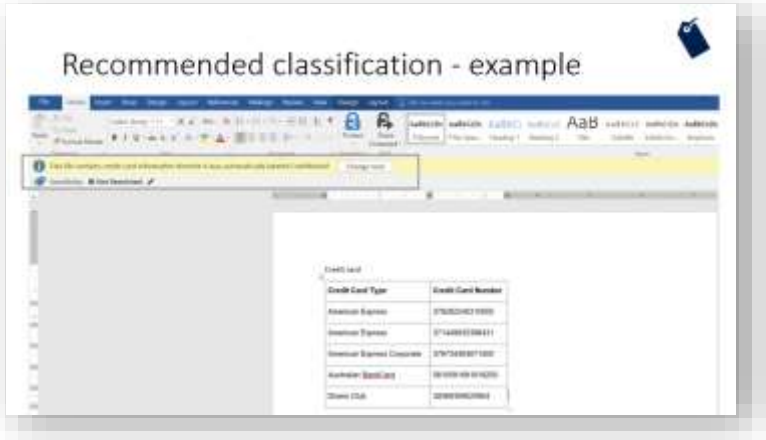
SECUDE — SAP Data Export

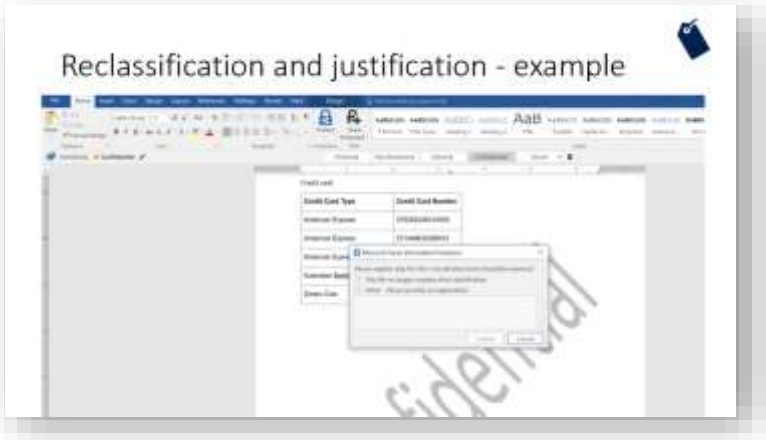
...and more

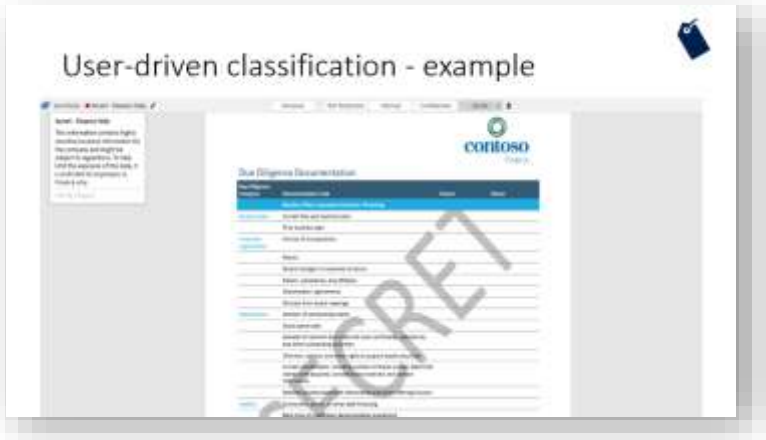
SDK — Software Development Kit

Azure Information Protection Experience









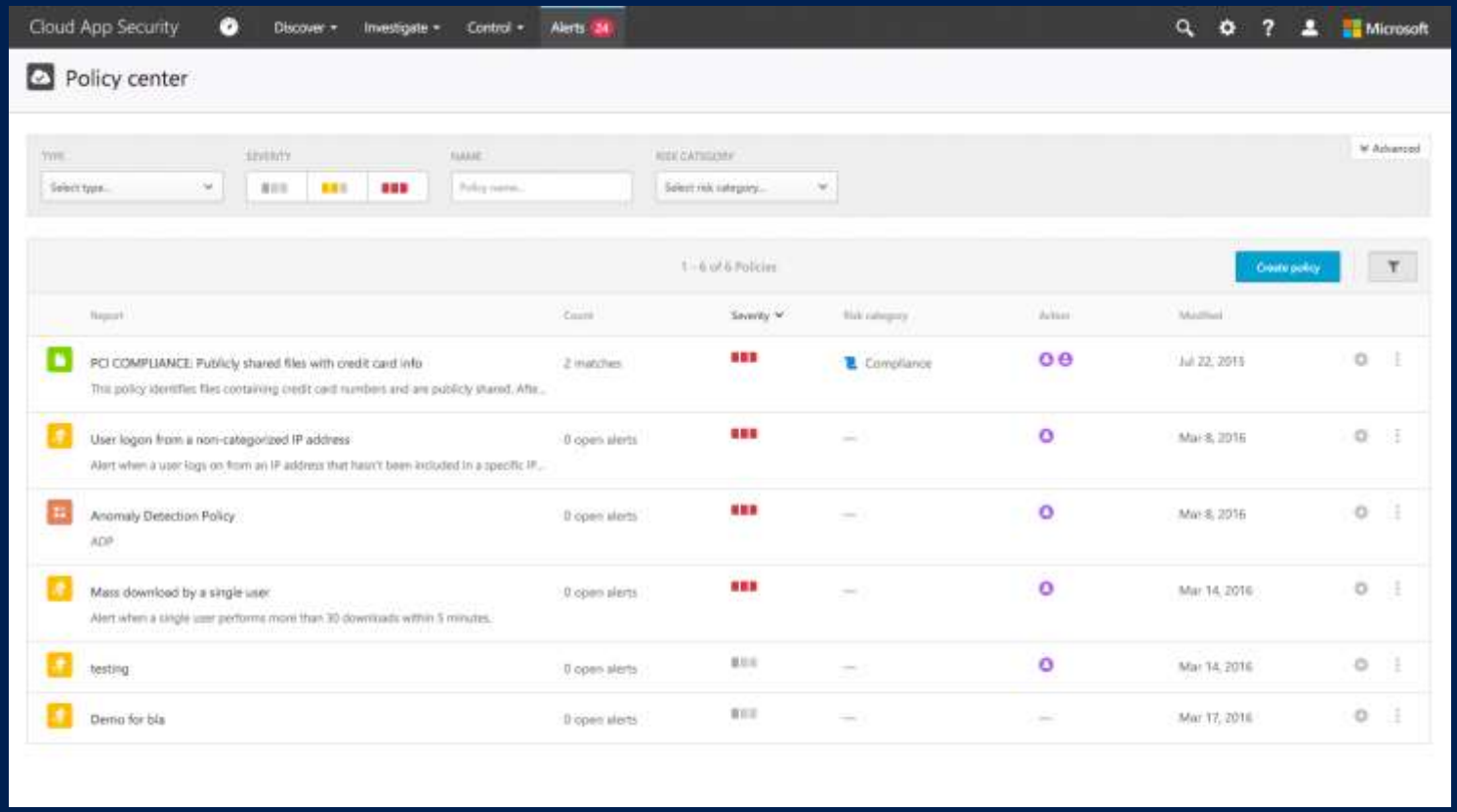
Finding and protecting data on SaaS

Discover

Investigate

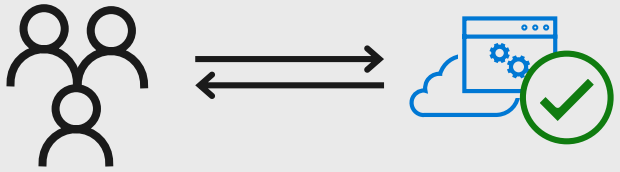
Control

Alerts

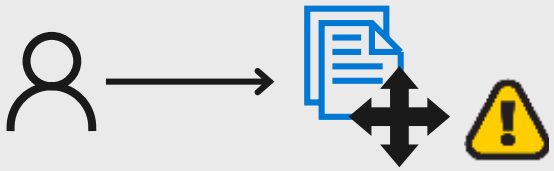


Scenario: oversharing from sanctioned SaaS

1 IT department sanctions SaaS application and provisions user access



2 User uploads sensitive file to SaaS and shares openly with everyone



3a Cloud app security detects oversharing of sensitive document, quarantines it, and issues alert

3 Unknown parties find and access the document, creating business risk

Secure the data, not just the SQL database

Automated **discovery** of sensitive data

Labeling (tagging) sensitive data on column level with persistency

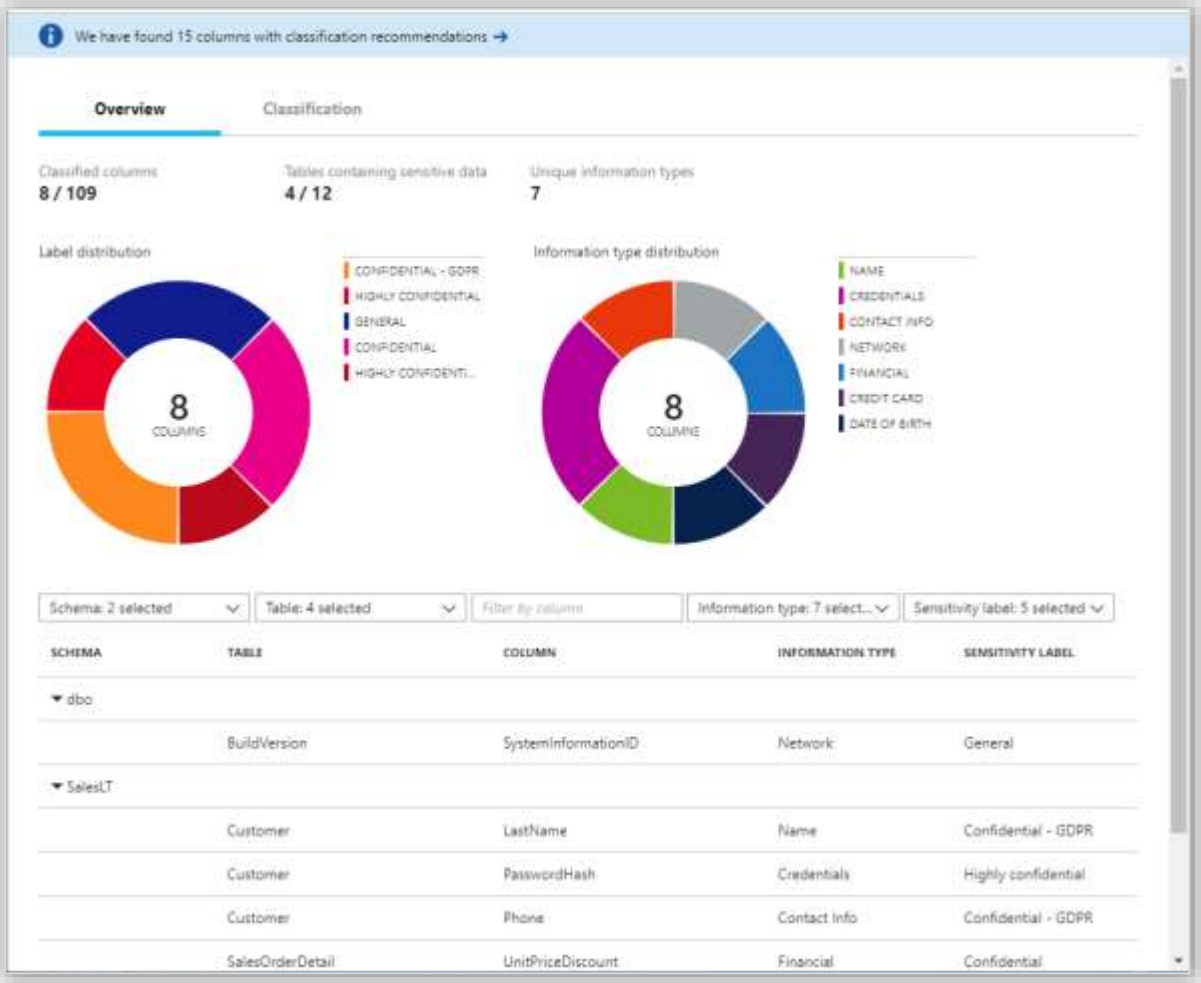
Classification as **infrastructure** for **protection & compliance**

Audit access to sensitive data

Sensitivity metadata flows with data for **protection outside database boundaries**

Hybrid – cloud + on-premises

Centralized IP policy management



Mobile Application Management (MAM)

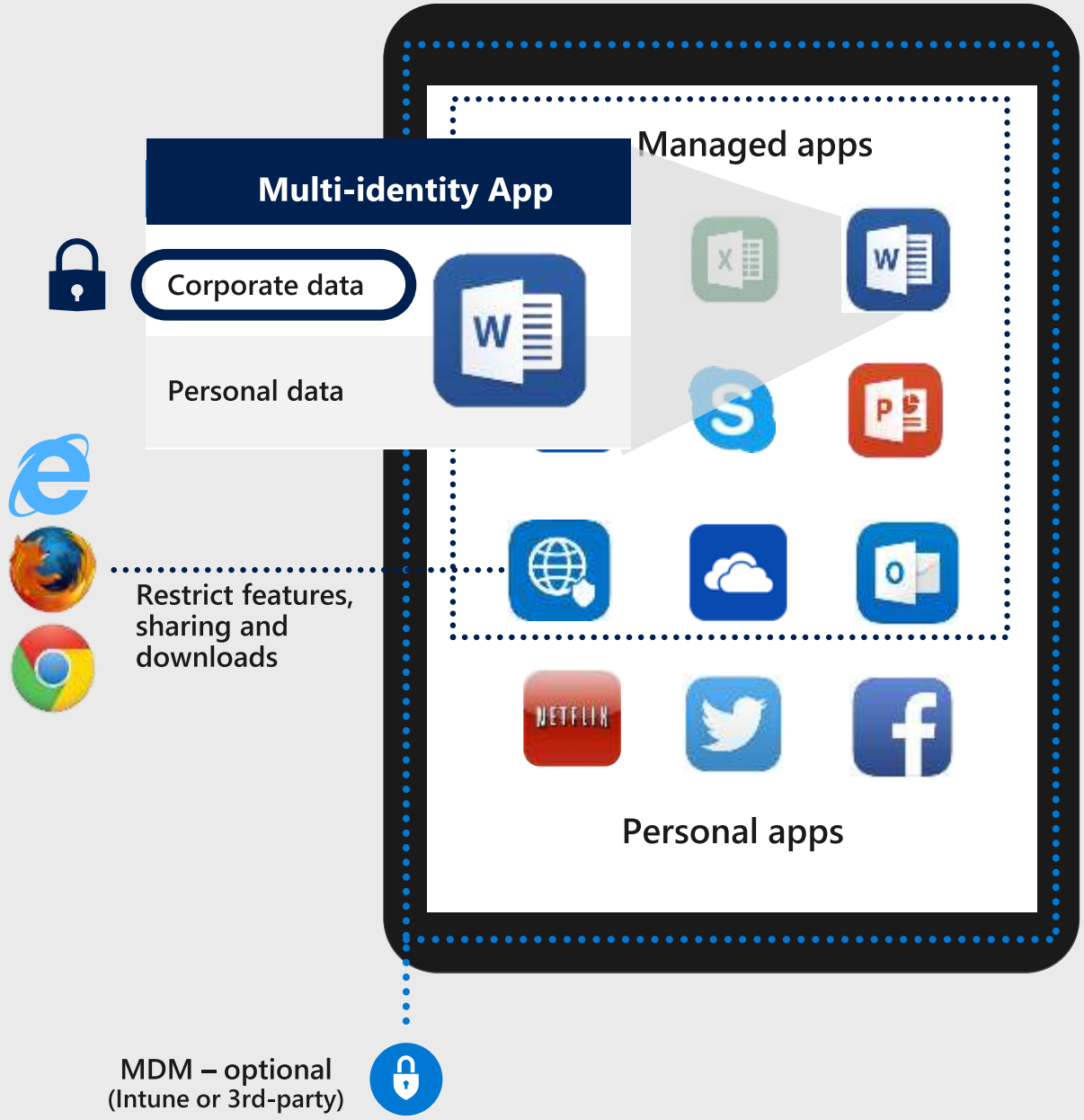
Works with or without MDM

Strong protections for corporate data

- Restrict “Save as” and cut/copy/paste
- Secure viewing of PDFs, images, videos
- App encryption at rest
- App access control – PIN or credentials
- Managed web browsing

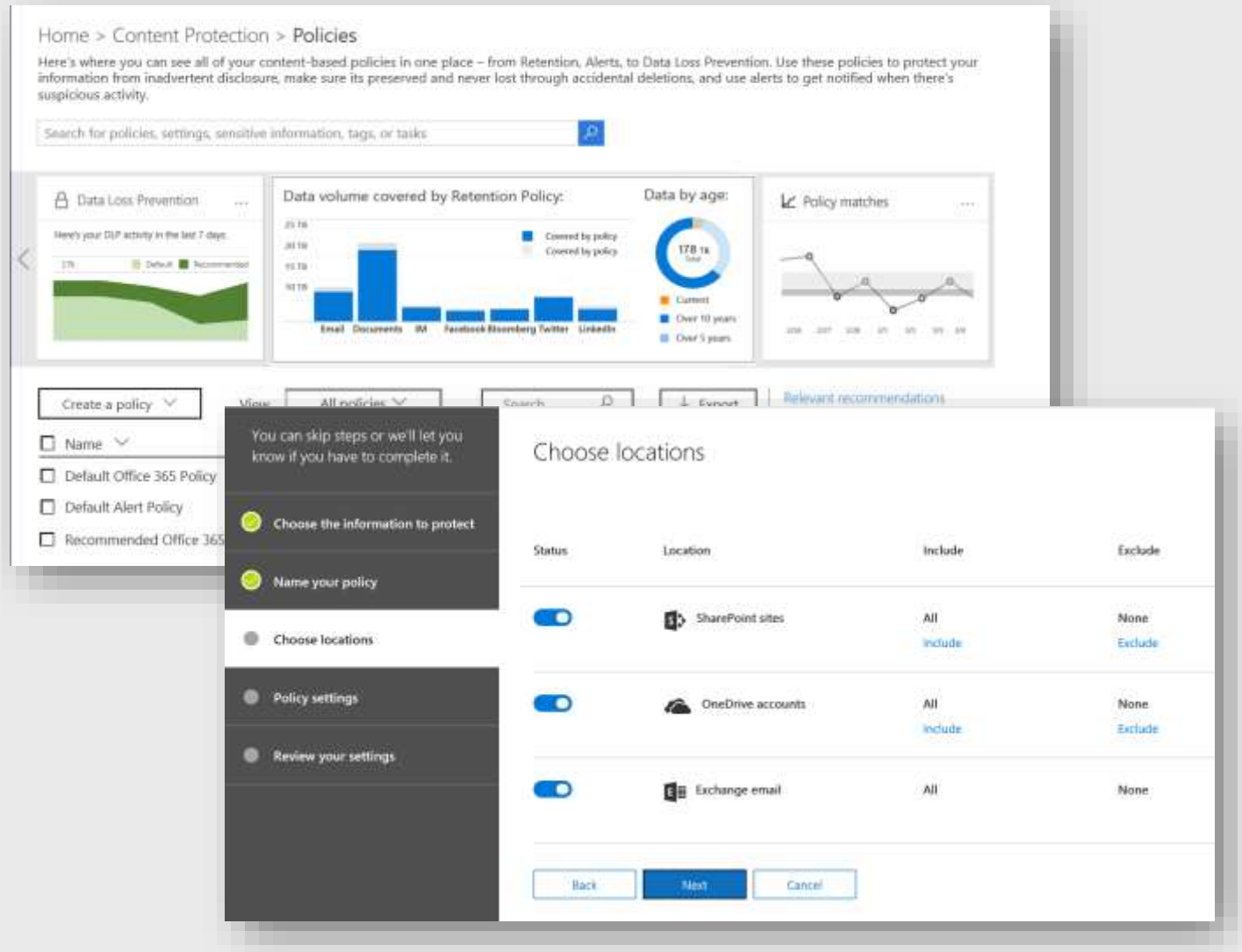
Support multi-identity applications

Selective wipe of corporate data without affecting personal data



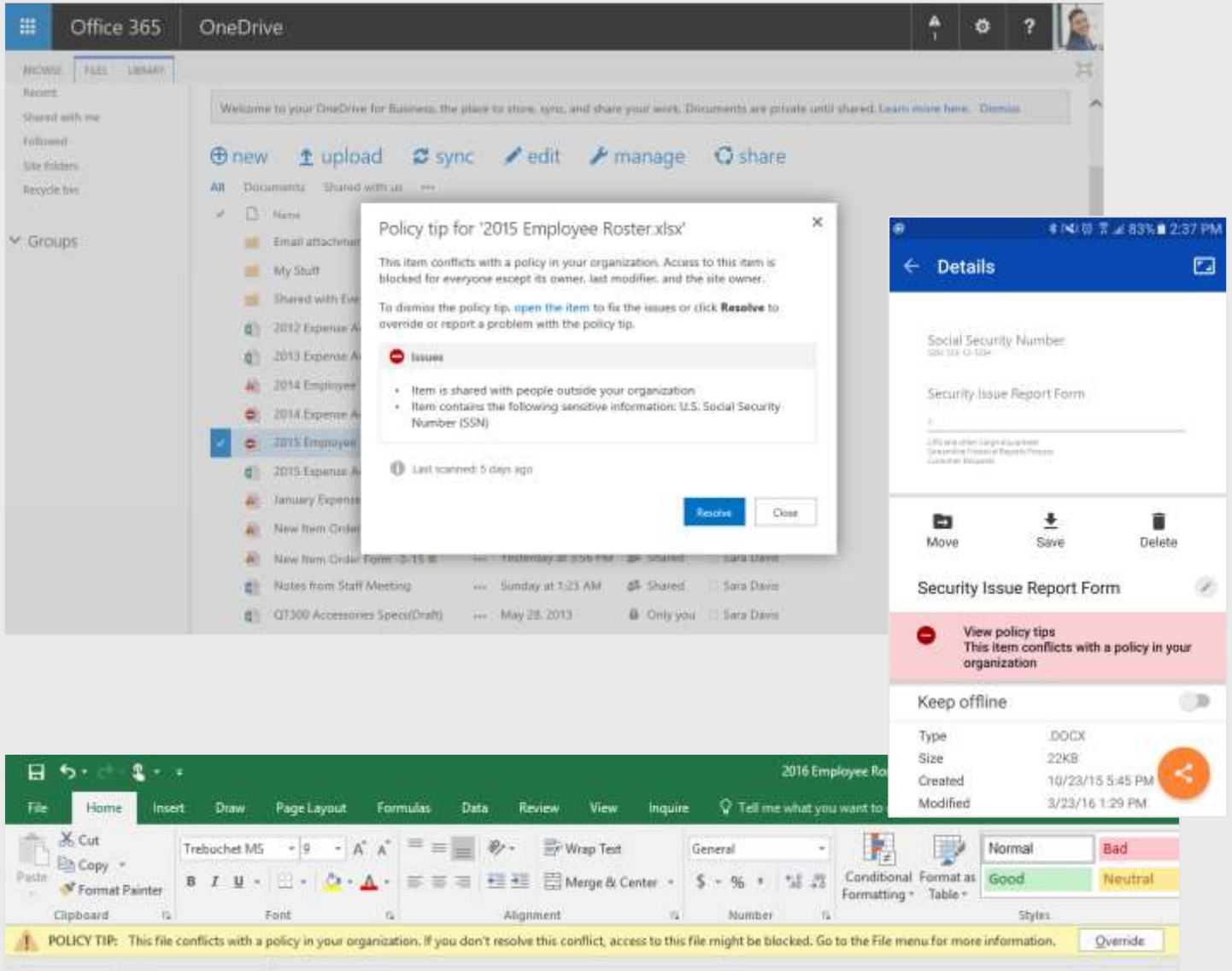
Sophisticated Built-in Protection Across Office 365

- Centralized console - define policy once, apply across Office 365 services and client end-points
- Built in to Exchange Online, SharePoint Online, and OneDrive for Business
- Focused on secure productivity
- Admins - Default policy for most common sensitive content (which can be customized)
- Users - Policy Tips integrate security education into user workflow



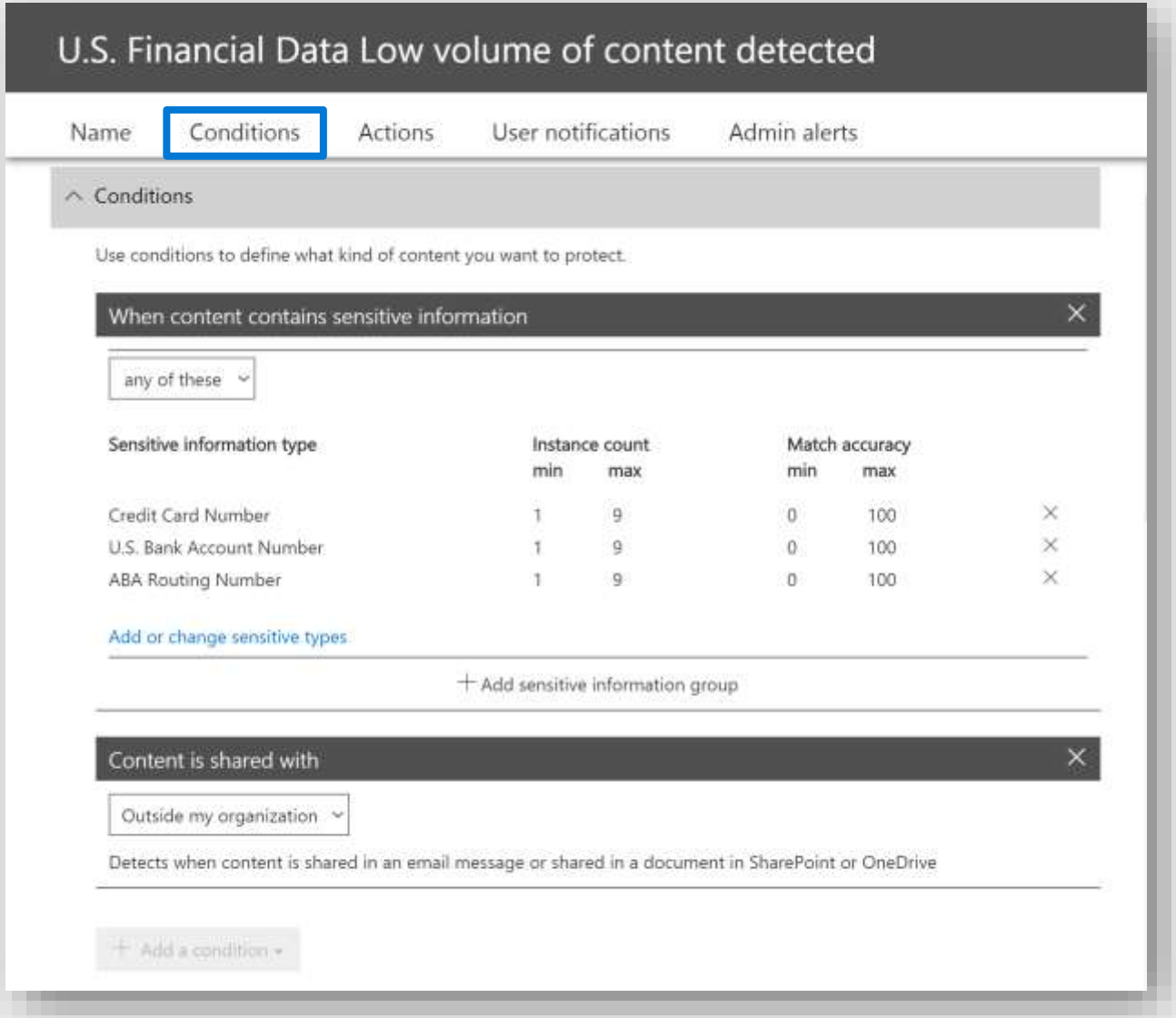
Balancing User Productivity and Risk

- Policy Tips help educate users when they are about to violate a policy
- Available in desktop, web, and mobile apps



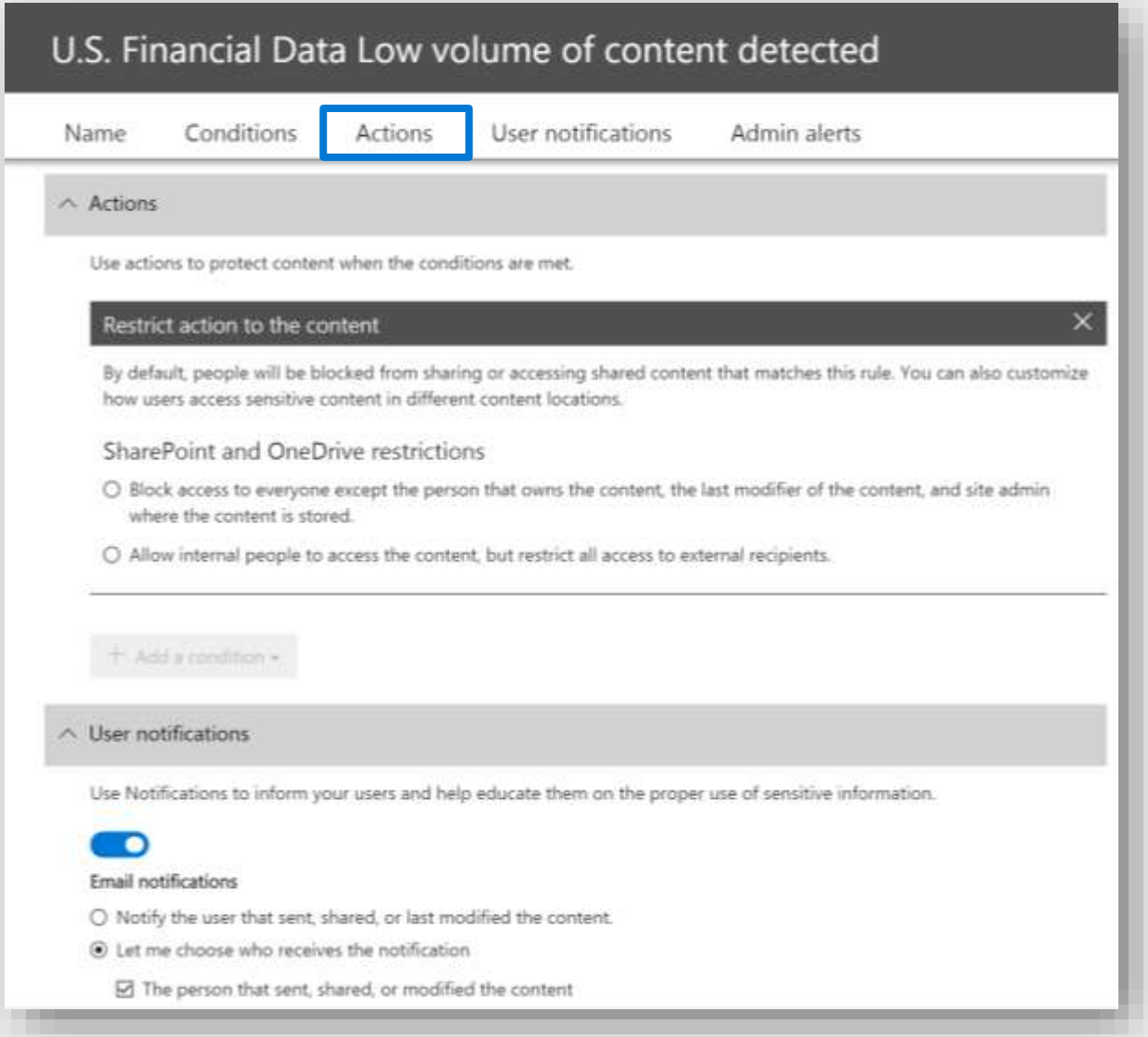
DLP Policy Rules - Conditions

- Describe the policy objective – model business risk and mitigation actions
- Set of conditions describing when rule applies
- Set of actions applied when conditions match
- Range of actions covering insights and automatic remediation
- Generic action behavior integrated for natural experience across each workload

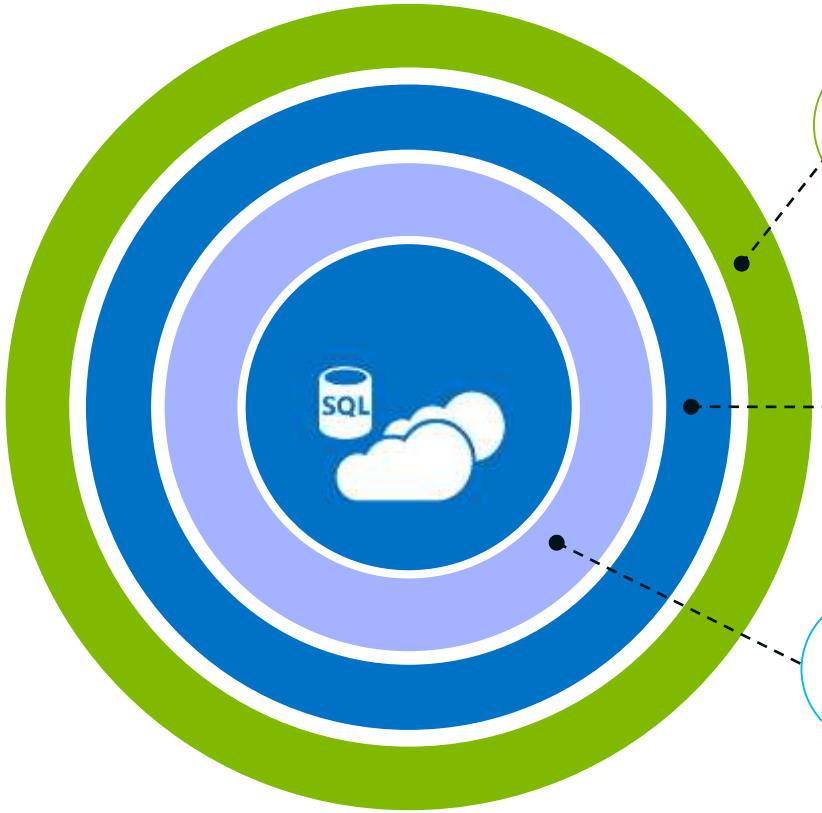


DLP Policy Rules - Actions

- Describe the policy objective – model business risk and mitigation actions
- Set of conditions describing when rule applies
- Set of actions applied when conditions match
- Range of actions covering insights and automatic remediation
- Generic action behavior integrated for natural experience across each workload



Securing Structured Data in Azure SQL



Activity Monitoring

Tracking activities : ***Auditing***
Detecting threats : ***Advanced Threat Detection***
Centralized dashboard : ***ASC Integration & OMS Integration***

Access Control

Server access : ***SQL Firewall***
Database access: : ***SQL*** *and* ***Active Directory Authentication***
Application access : ***Row-Level Security*** *and* ***Dynamic Data Masking***

Data Protection

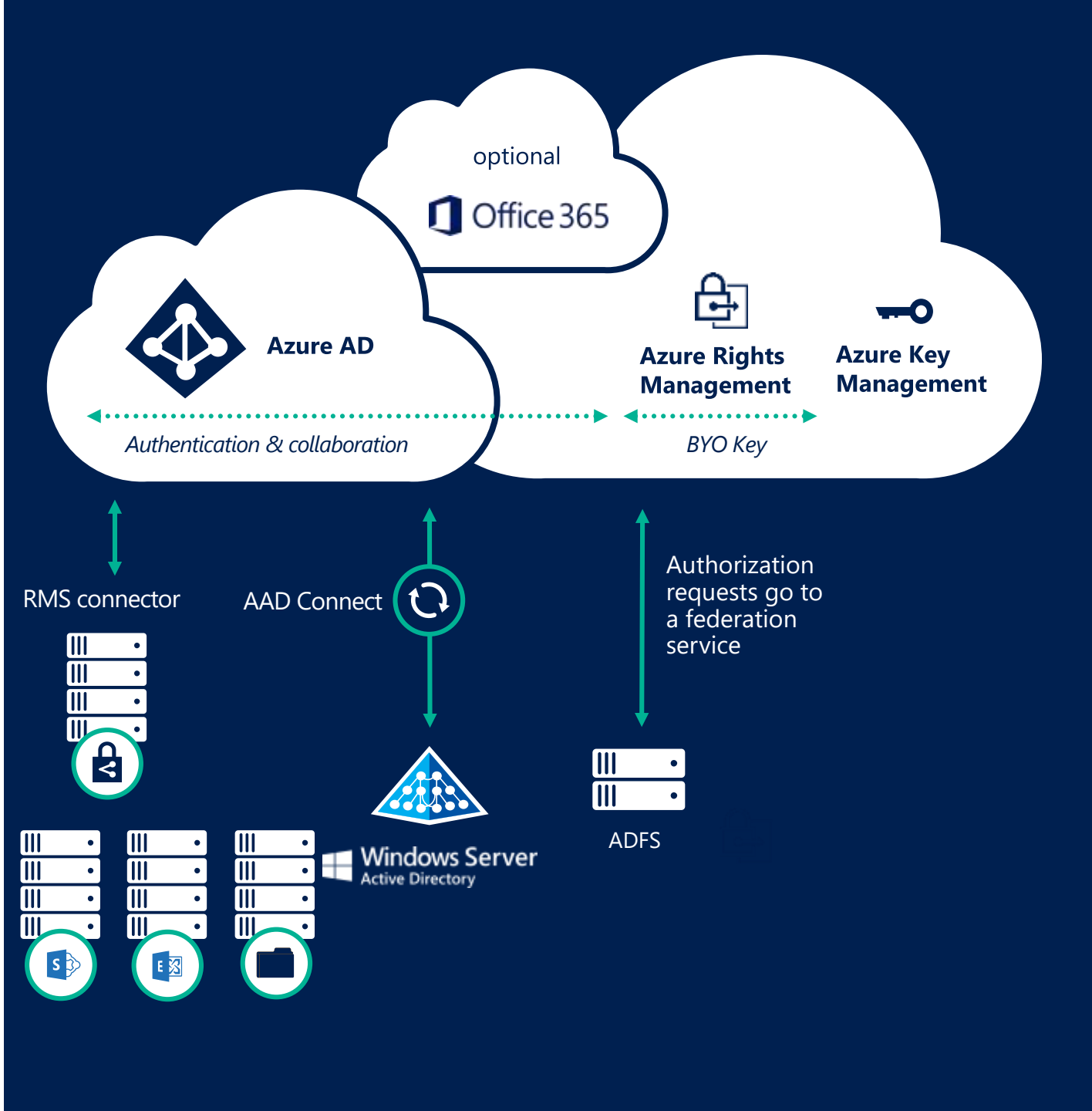
Encryption in transit : ***Transport Layer Security***
Encryption at rest : ***Transparent Data Encryption***
Encryption in use : ***Always Encrypted***

Compliance: FedRAMP, (government), HIPAA, (medical), PCI, (payment), EU Model Clauses , (personal), UK G-Cloud, (public sector) ISO,

Recommended Topology

Azure Information Protection

- Data protection for organizations at different stages of cloud adoption
- Ensures security because sensitive data is not sent to the RMS server
- Integration with on-premises assets with minimal effort



Regulated Topology
Azure Information Protection

- Data protection for organizations at different stages of cloud adoption
- Ensures security because sensitive data is not sent to the RMS server
- Integration with on-premises assets with minimal effort
- Hold Your Own Key with on-premises key retention