AT&T CYBERSECURITY INSIGHTS™ REPORT

TENTH EDITION 2021

AT&T Business

AT&T Cybersecurity

5G AND THE JOURNEY TO THE EDGE

AT&T CYBERSECURITY INSIGHTS™ REPORT

TENTH EDITION

2021

Making it Safer to Innovate

The AT&T Cybersecurity Insights™ Report is an annual research report published by AT&T Cybersecurity. Currently in its tenth edition, the report provides rich insight into critical cybersecurity issues, trends, and emerging technologies to help executives, security professionals, and business leaders understand the current landscape of threats and develop strategies for building a resilient cybersecurity approach that protects the business today and tomorrow.

As the publisher of this report, we do our best to make sure the AT&T Cybersecurity Insights Report is vendor neutral and discusses the broader domain of cybersecurity. This report is based on primary research, including a global survey of security, IT, and line-of-business leaders, to understand first-hand what is most concerning to professionals within the cybersecurity industry and how broader technology and digital business trends impact security. Additionally, this report is informed by subject matter experts from leading cybersecurity vendors and AT&T Business to capture forward-thinking perspectives on topical technology and cybersecurity issues.

Our mission for the AT&T Cybersecurity Insights Report is to mesh the knowledge and experience of some of the best minds in the industry with empirical research to provide insight into what enterprises should consider to achieve a resilient cybersecurity approach that evolves with the business.

CONTENTS

EXECUTIVE SUMMARY

5G is a Journey and Demands Changes to Security 4

INTRODUCTION

5G Enables Innovation at the Speed of Business 6

SECURING 5G

Securing a 5G-Enabled Edge Computing World 12

NEXT STEPS

One Way to Bolster Courage is to Prepare 26

Key Takeaways 30

Conclusion 31

Appendices 32

5G IS A JOURNEY AND DEMANDS CHANGES TO SECURITY

5G will change where and how we harness compute power and promote unforeseen product and service innovation. Once 5G attains critical mass with a robust ecosystem, 5G will touch nearly every organization, promising new revenue potential across a myriad of industries. 5G will expand usage of edge computing, which locates network functions, applications, compute, and storage closer to end users, creating near real-time performance along with high bandwidth and low latency.

STANDALONE 5G IS MORE SECURE

Standalone 5G is more secure than any previous network generation. While the promise of 5G is universally recognized, the path to implementing 5G is unique to every organization. Enterprises should closely examine existing company networks and security models and rethink accordingly. Each organization will ultimately create a footprint in 5G and edge design that is unique and purpose built to that organization. 5G is not a one size fits all technology. How 5G is architected will determine how security is designed. Organizations can choose from an isolated on-premises private 5G network, independent of the public operator 5G network, or one that shares mobile operator 5G network resources. They can choose multi-tenant public options delivered as a service, with network slicing and virtualization to provide a single-tenant experience.

And then there's cloud. Cloud rapidly multiplies private and public 5G architectural options, and it is believed that 5G will create a wide range of brand-new applications and services in cloud computing. Which architecture an organization chooses will depend on the organization's industry, speed, and latency requirements and how each organization

How 5G is architected will determine how security is designed.

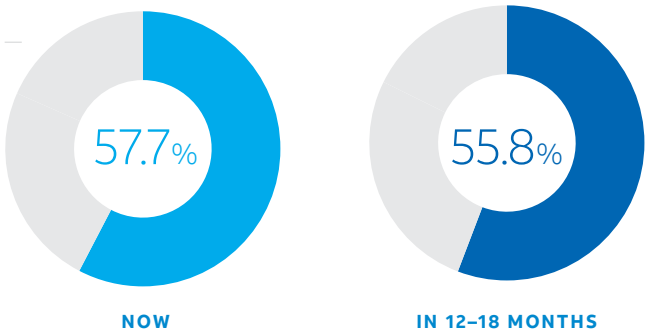
FIGURE 1

COMPANIES ARE ADOPTING 5G TO REMAIN COMPETITIVE.

Q. What is your primary concern for your organization's 5G implementation today and in 12–18 months?

% of respondents

A. Top use case now and in 12-18 months is to remain competitive:



N= 947 BASE Respondents who indicated their organization is researching/ implementing/completing 5G deployment

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey*, October 2020

desires to control access to data and applications. It has been said that data is the new oil, and it is an apt view to keep in mind as the market moves toward 5G universality. How data is consumed, input, accessed (and by whom), stored, and transported will influence an enterprise's unique footprint for protection.

In addition to technology considerations, the move to 5G is highly influenced by the business, which means that business and IT leaders need to collaborate on 5G strategies and implementation. Digital transformation is reshaping how organizations think about technology investments. The collaboration between IT and business leaders is key to a business' ability to grow and remain competitive in the next several years. In fact, according to a global survey conducted by AT&T Cybersecurity with IDC during September 2020, 80% of respondents are adopting 5G to remain competitive in their industry, to create new IT projects, and to establish new business models (see Figure 1). This is a drastic shift in how technology is being adopted, introduced, and used for competitive advantage.

Among some organizations, the implementation of 5G will be evolutionary as they navigate the transition from 4G to 5G and all the security issues that shift implies.

5G PROPELS A REVOLUTION IN COMPUTE HISTORY

Digital transformation, cloud adoption, and distributed assets already exist in today's modern hyperconnected enterprise, but this evolution in compute did not happen overnight. Similarly, the blending of 5G and edge compute won't happen immediately. And with this shift, enterprise businesses will want to focus on how these revolutionary new technologies are secured.

Some innovative organizations are already embracing 5G and edge computing. These leaders are designing security unique to their 5G model that will help them today and as 5G and edge computing gain ubiquity. Standalone 5G is part of the overall ecosystem that is emerging but not yet fully realized, which means that organizations today will need to start implementing 5G in conjunction with 4G. Implementation is evolving as organizations explore the various use cases and navigate the security issues inherent in a super-connected world.

To meet the business demand for innovation that can come with 5G, forward-looking organizations share that they are increasing adoption of software-driven service functions like software-defined networking (SDN), security virtualization, self-healing, and automated networks. And many have implemented a Zero Trust approach in their network for better enterprise visibility, reduced IT complexity, data protection, and support for cloud migration.

Security basics don't go away but rather get elevated in importance. Organizations cannot firewall their way around the distributed 5G edge — though firewalls and network segmentation are still relevant. Data security, identity and access management, threat intelligence, and visibility are more important than ever in finding threats and shutting them down commensurate with the near real-time promise of 5G.

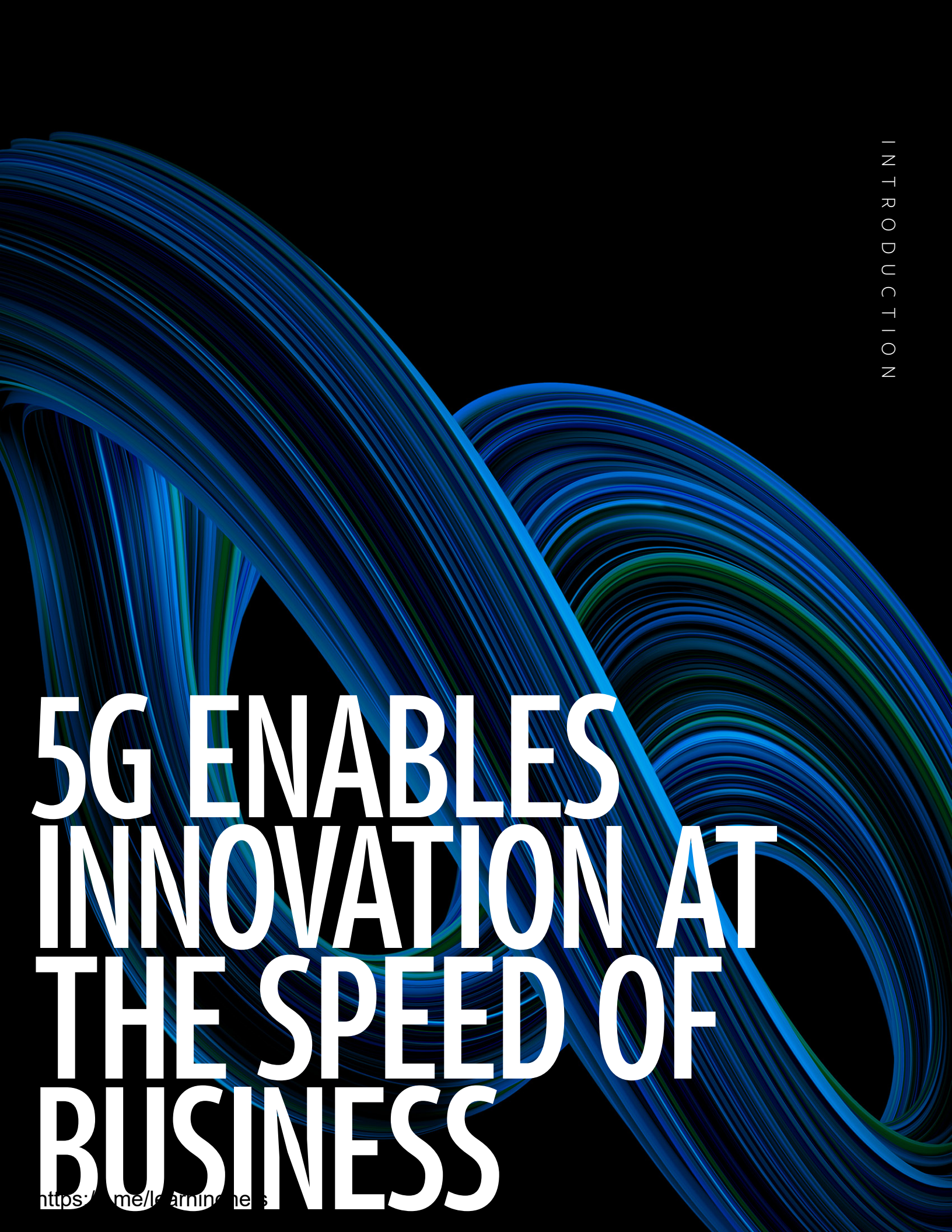
ENTERPRISE SECURITY APPROACHES DEPEND ON THE BUILDOUT OF 5G AND ENTERPRISE RISK APPETITE

The transition to 5G is unfolding with implementation requiring strategic planning and long-term investment. Organizations should be proactive today, act with purpose, and take action. Many trendsetters have begun their journey to the edge and 5G, setting the pace and cadence for the future of innovation. As additional enterprises join the journey to 5G, those organizations should seek to utilize existing security technologies in building a security road map.

This report highlights the need for a benefit-to-risk evaluation of data security and access management concerns juxtaposed against enhanced speed and reduced latency benefits. This evaluation requires a review of existing security programs, policies, and controls.

Other key areas useful for the enterprise to consider as it transitions to 5G are:

- Assess the organization's risk appetite.
- Consider asset and network topology.
- Determine the organization's innovation posture. Evaluate whether the organization is a leader or laggard in a software-defined world with the ability to enable a malleable 5G security architecture.
- Identify areas of security in need of immediate attention. Think about which currently deployed security assets can be utilized today that will make the journey to 5G with the business more efficient.
- Align 5G technology and digital transformation strategy with an enterprise-wide strategy. Coalesce a strategic, cross-functional tiger team to steer the initiative.
- Envision the end state. Consider segmentation as a first step to Zero Trust or choose an initial focus on creating platform visibility of threat intelligence, analytics, and response tools across existing assets.



5G ENABLES INNOVATION AT THE SPEED OF BUSINESS

5G

IS ENABLING innovations in smart cities, fleet management, supply chain, and IT automation by connecting billions of low-power internet of things (IoT) devices to the cellular network. By taking advantage of low latency, high speed, and ultra-high reliability, enterprises can one day actualize mission-critical and, in some cases, life-critical applications such as smart grids, remote surgery, and intelligent transportation systems. Unlike previous technology rollouts, 5G is finding an enthusiastic audience of line-of-business (LOB) executives that have seen the promise of IoT and edge-based applications in a 4G world and are pushing for the rapid adoption of 5G to realize all the speed and latency promises that 5G enables. When LOB executives are funding the technology and security improvements needed to realize the safe entry of these 5G use cases, 5G can be called a revolutionary, game-changing technology. Yet, among some organizations, the implementation of 5G will be evolutionary as they navigate the transition from 4G to 5G and all the security issues that shift implies.

The explosion of 5G-enabled hardware and the apps hosted on those devices bring about yet another elevated era of highly organized, commercialized, and potentially state-sponsored threat actors. These groups are ready and willing to destroy, steal, or hinder the data that these 5G-enabled devices utilize to further their criminal desires. Unlike prior improvements to the radio spectrum, the innovations that 5G brings mean that the vast amounts of data that is being created, hosted, and transmitted could potentially be probed by cybercriminals using the very same technology that allowed this data to move in the first place.

Combatting security vulnerabilities at the speed of 5G will require continuous and adaptive scanning and monitoring. But more than that, organizations will need to embrace new strategies like Zero Trust as well as advanced automation and analytics, artificial intelligence (AI), and machine learning (ML). Ingestion of new telemetry sources, some of which cannot fully be understood yet like industrial operational technology and IoT, will need to be correlated and contextualized to provide actionable intelligence to the security operations team. A platform approach is key here. Organizations will need to stop new threats and potential spread without sacrificing user experience to maintain the speed and continuity of business.

Speed creates new security concerns. The 5G-enabled edge applications that crave the low-latency possibilities of 5G also bring along some familiar headaches for the security and DevOps teams to tackle. The move of data to the edge has also seen the rise of supporting technologies and applications to process this data before it moves on to its final destination in the cloud.

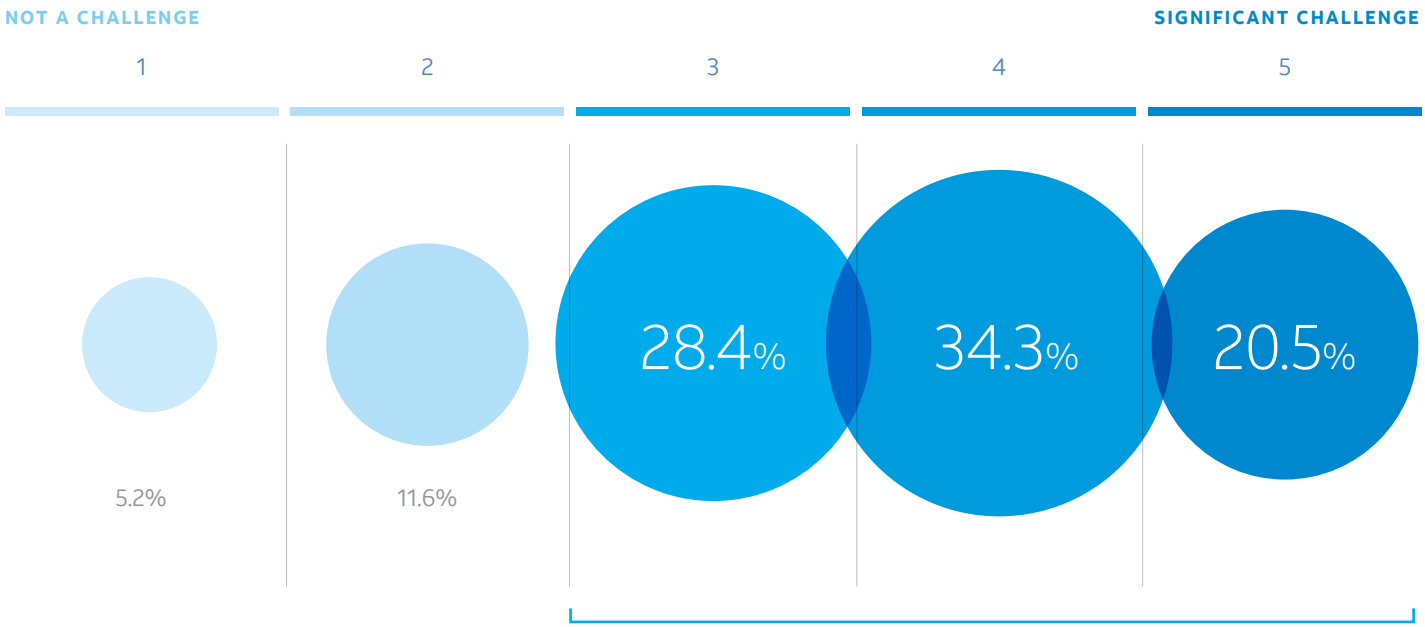
Consider for a moment the unique opportunities that having a containerized edge database can offer. While processing data closer to where it is collected allows for quicker decision making, it does not negate the need for protection of the data. To the contrary, processing data in this way requires extra oversight because data is being collected and processed to support critical functions. For example, cyber-resilience and software engineering principles that incorporate security first will be critical as software engineers develop modern cloud apps.

FIGURE 2

WEB-BASED APP ATTACKS PRESENT A CHALLENGE TO ADDRESS.

Q. In your opinion, when implementing 5G, how much of a challenge are web-based application attacks?

Note: Scores are based on a scale of 1–5, where 1 = not a challenge at all and 5 = significant challenge.



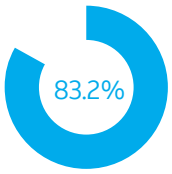
N= 947

BASE

Respondents who indicated their organization is researching/implementing/completing 5G deployment

SOURCE

IDC's Custom Survey, *5G Cybersecurity Impact Survey*, October 2020



83.2% of respondents believe attacks on web-based applications will be a challenge

Figure 2 shows that more than 54% of survey respondents recognize this, stating that web application attacks are a security challenge when implementing 5G.

Moving the data processing closer to the use case application certainly allows for near real-time, AI-enabled processing and decision making, but it's not without drawbacks. Along with it comes the possibility of older-style threats such as SQL injection attacks, unencrypted data travelling along private networks that may or may not have malware-sniffing apps looking at the data, and other yet-to-be identified security challenges.

In the near term, 4G will continue to exist. In fact, during the market's transition to 5G, traffic will move between 4G and 5G via roaming exchanges that have been established for 4G. Network operators provide that infrastructure and roaming interfaces at the signaling layer, and they are protected. The enterprise must be responsible for the data layer. A shared security model like that in public cloud is needed.

Yes, 5G is revolutionary, and businesses are banking on the capabilities that 5G promises. However, they concurrently recognize the need to team with the right service providers to help usher in the capabilities that 5G and edge computing have the potential to deliver in a safe, highly secure, and resilient way.

WHAT IS SECURE 5G AND WHY DOES IT MATTER?

With standalone 5G and mobile network rollouts accelerating globally, the impact to the enterprise is only just beginning. 5G is not simply a new radio upgrade or more advanced smartphone. 5G implies an adjacent investment in cloud and software-defined networks, both at the core layer and at the edge of the cellular network. Said differently, 5G will ultimately be defined as a new globally distributed mobile platform able to support a whole array of enterprise-grade and consumer devices. 5G will radically transform and empower operators to efficiently drive new market opportunities, all from a single 5G network platform.

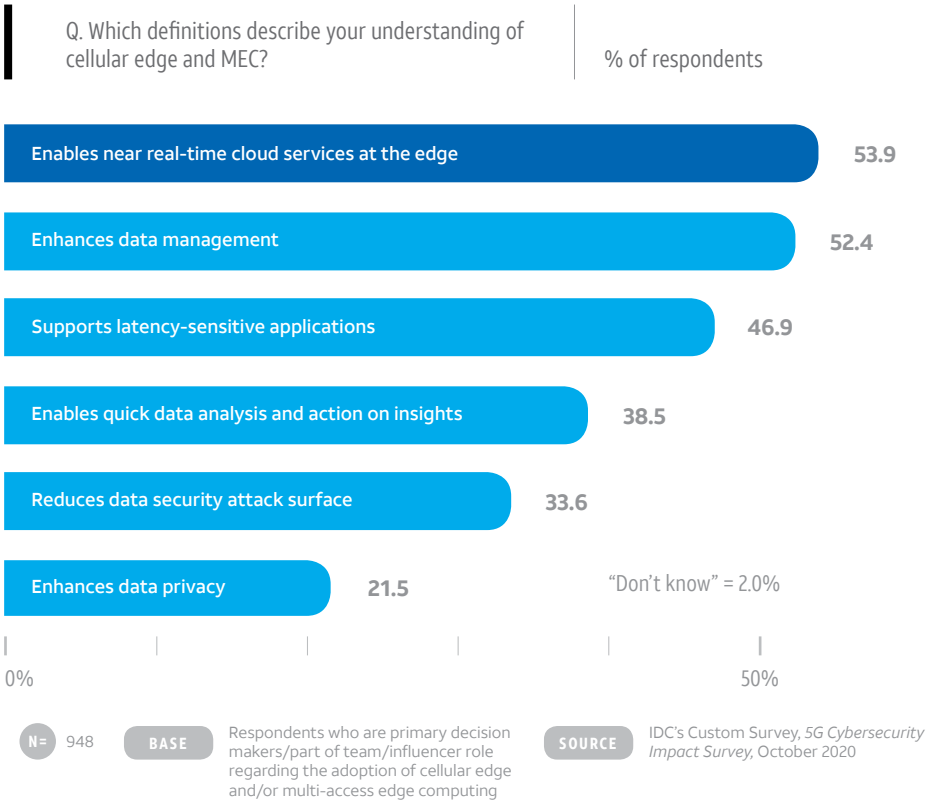
In fact, nearly 54% of our survey respondents who completed 5G implementations state that multi-access edge computing (MEC) enables near real-time cloud services at the edge and 52% believe MEC enhances data management (see Figure 3).

When it comes to securing the cellular edge or MEC, 31% of respondents think that 5G is secure out of the box from the network provider with no additional security required and another 26% have no strategic plan to address the security of 5G. This is in direct opposition to the 56% of respondents who understand that 5G will require a change to their security approach to accommodate network changes. In addition, nearly half of the survey respondents believe that 5G poses an elevated security threat, partly because there are more vectors through which adversaries can attack.

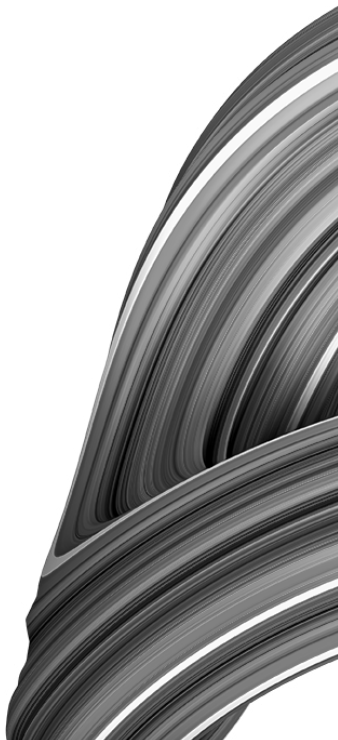
These diametrically opposing beliefs sum up the conundrum facing enterprises as they transition enterprise network architecture, including security infrastructure, to incorporate 5G. Nearly half of the survey respondents think 5G requires no change to their security infrastructure, while the other half understands that this shift demands a rework of the security posture to keep the business protected. And, as stated previously, how 5G and the edge are secured will ultimately come down to an organization's unique 5G and edge use case and site type, including the architectures and which data is consumed, input, accessed, stored, and transported (see Figure 4).

FIGURE 3

EDGE COMPUTING SPEEDS SERVICES AND ENHANCES DATA MANAGEMENT.



How 5G and the edge are secured will ultimately come down to an organization's unique 5G and edge use case.



Carriers plan to offer MEC architectures that can be used to create and distribute network software and services to enterprise customers. The standalone 5G core network is designed as a cloud-native solution, which means that specific network functions can be deployed in a cloud environment, whether those functions reside in a regional cloud datacenter or in the MEC appliance on premises. Deploying some of these functions, such as the User Plane Function (UPF), can provide significant gain in network latency and security — especially data security — as organizations can keep specific data cuts on premises. The dual use of 5G and MEC can be a force multiplier for any organization looking to get the most out of its 5G investments both in performance and security.

Whether deploying applications from a central cloud, an edge cloud, or an on-premises MEC — or a combination — enterprises need to take a proactive approach in defining their use cases and application performance needs from the outset. The 5G/MEC architecture should align to use cases, applications, and site type.

While broader 5G awareness will continue to gain traction, market understanding of how, why, and the best way to jointly deploy 5G and MEC also remains in question, with use cases specific to the enterprise largely influencing design decisions. However, it is widely recognized that the combination of 5G and MEC can help yield significant gains in latency, particularly when standalone 5G is abstracted and deployed alongside MEC.

Among the top 5G use cases IDC sees are:

- The need to improve deployments in IoT, industrial IoT, and OT
- Enhancing data privacy
- The desire for broader network coverage
- Wanting to accelerate digital transformation projects

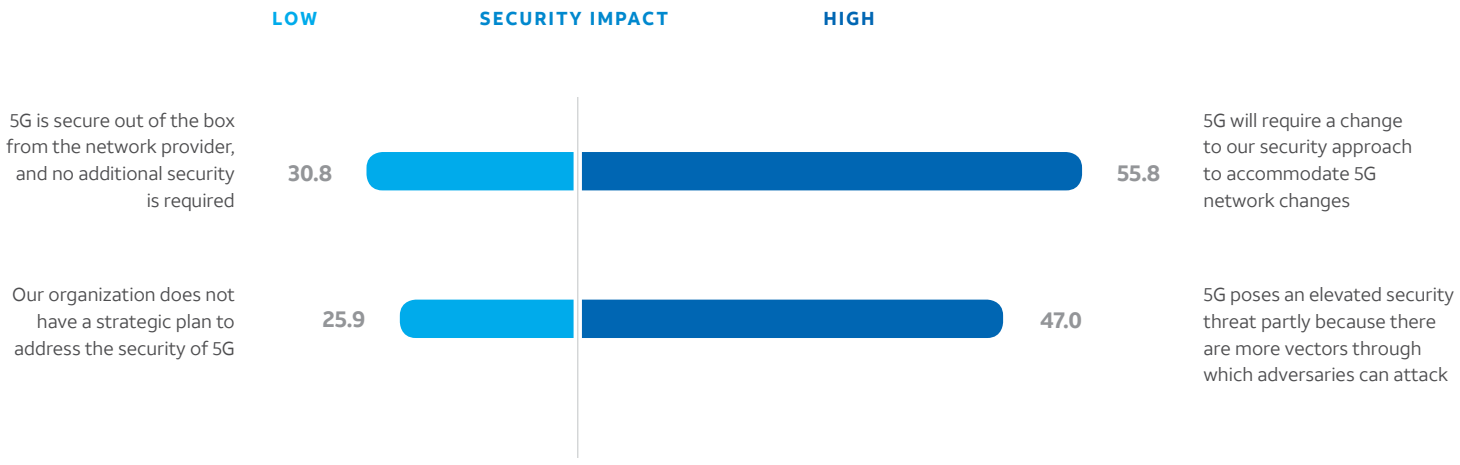
The 5G/MEC architecture should align to the use cases, applications, and site type.

FIGURE 4

5G AND THE EDGE WILL IMPACT HOW YOU APPROACH SECURITY.

Q. Please rank the top 3 according to your perception of their impact on your organization's security architecture due to the inclusion/adoption of 5G (overall rank).

% of respondents



N= 947 BASE Respondents who indicated their organization is researching/implementing/completing 5G deployment

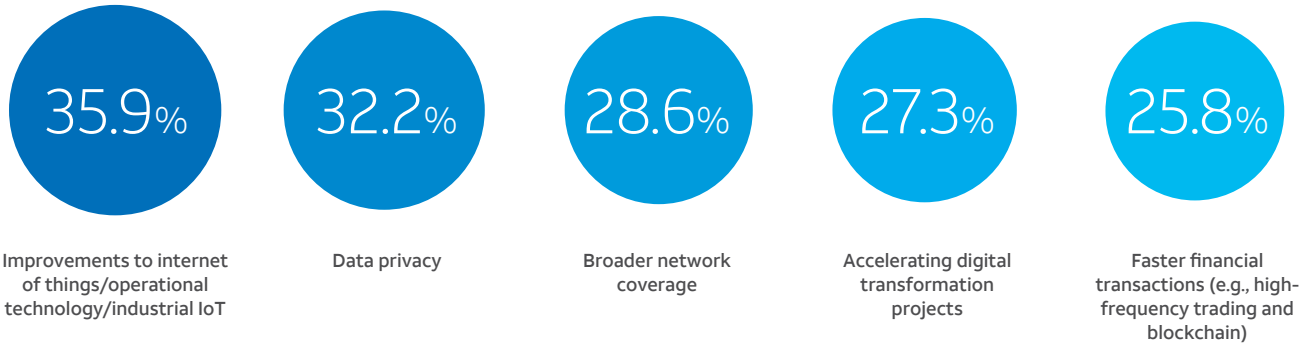
SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

FIGURE 5

5G USE CASES FOCUS ON NETWORK TRANSFORMATION FOR AGILITY, SPEED, AND PRIVACY.

Q. Please rank the top 3 5G use cases for your organization (overall rank).

% of respondents



N= 947 BASE Respondents who indicated their organization is researching/implementing/completing 5G deployment

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

Data privacy may be the second-ranked use case overall, but it is the highest ranked by both LOB and European respondents. It's no surprise that Europeans highly value data privacy, given the need to satisfy the General Data Protection Regulation (GDPR) law, but it's interesting to note that respondents worldwide, even beyond Europe, seek solutions for data privacy with 5G.

While there are clear risks associated with the proliferation of internet-facing devices accessing data at the speed of 5G, there are also opportunities to eventually make 5G an enabler of data privacy. For example, applications could be designed to deliver privacy alerts more rapidly and without impact to the user experience or turn around user consent in near real-time. Data governance could benefit from AI and ML technologies using the speed of 5G. For instance, AI and ML technologies can assist with the grueling tasks of keeping data records, knowing where data resides and how data is kept private, and keeping records of when users ask to confirm their data has been erased (per GDPR).

In fact, with the explosion of data that is expected to come with 5G, compliance administrators will no longer be able to manually update data repositories for GDPR and other regulatory bodies as they do today. Compliance will need to operate using advanced technologies to keep up (see Figure 5).

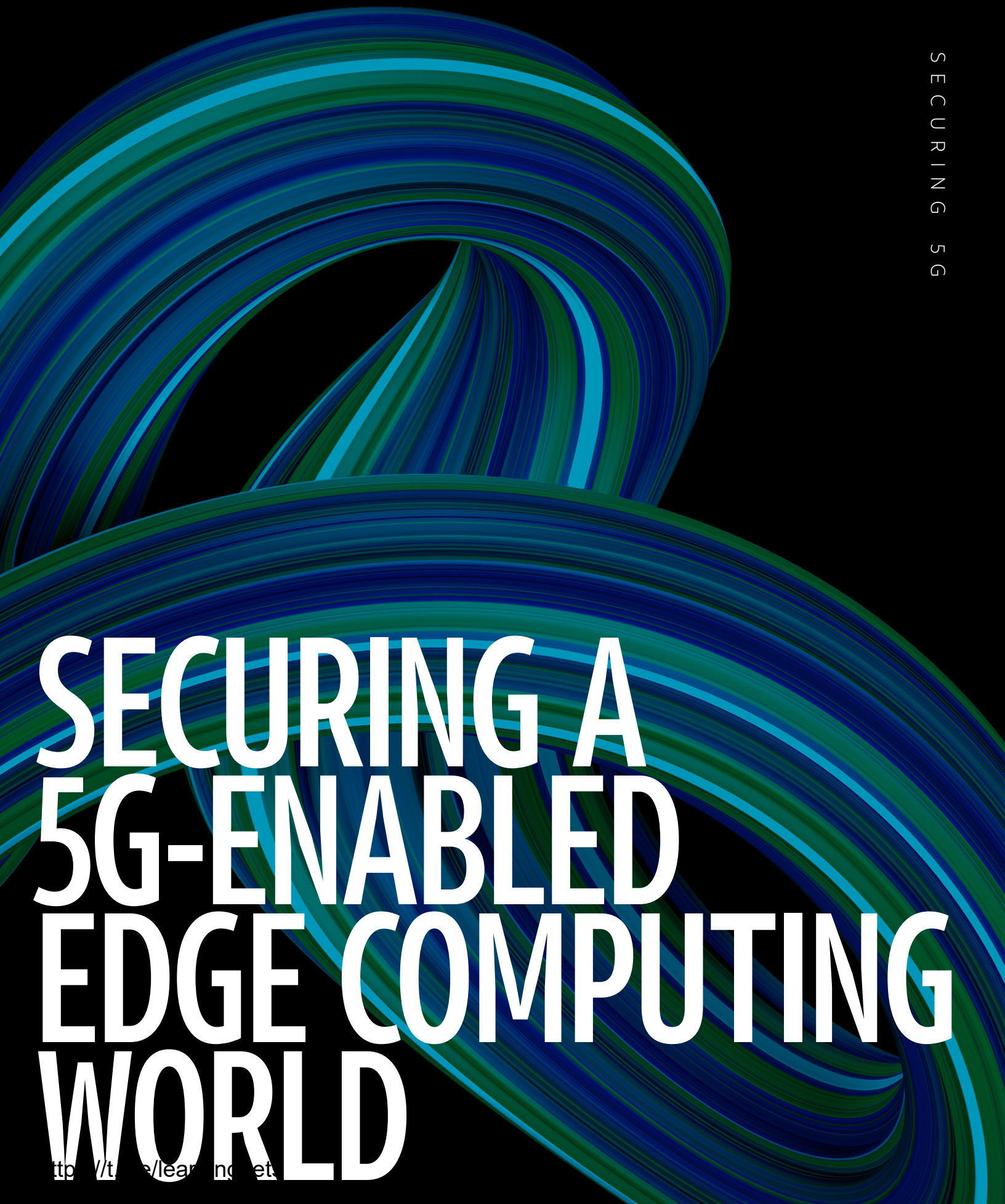
A key investment opportunity during the transition to 5G and MEC is to deploy highly secure architectures designed with the future in mind. Without a dedicated planning phase, enterprises risk either overspending or being ill-prepared to cope with the network needs of tomorrow. Enterprises should focus on one or two applications from the outset and scale to other applications as needed, with a thoughtful strategic direction. This provides for a formative understanding of how 5G and MEC intersect and how best to proceed regarding security.

RECOMMENDATIONS

Standalone 5G is more secure than any previous network generation. Yet, expanded attack surfaces mean opportunity for new threats as well as proliferation of unpatched existing threats. The right advisor for managed security solutions is critical.

Deploy network functions in public and private cloud environments or via multi-access edge computing on premises to provide improvements in network latency and security.

Most of all, organizations should take a thoughtful and strategic approach to design, since the 5G/MEC architecture should align to the use cases, applications, and site type.



SECURING A 5G-ENABLED EDGE COMPUTING WORLD

As an enterprise investigates the near future to see what a 5G-connected architecture looks like, it needs to take stock of its current cybersecurity posture.

AS

AN ENTERPRISE investigates the near future to see what a 5G-connected architecture looks like, it needs to take stock of its current cybersecurity posture. Adding 5G-enabled edge devices into an IT/OT converging infrastructure that has holes in its security posture is a risky proposition. Many 5G use cases will still make use of 4G and other methods of connectivity, so raising the enterprise's current level of cybersecurity maturity will help provide for the safe entry of 5G-connected infrastructure.

A single point of view on 5G security doesn't yet exist, as 5G is still nascent.

CONFUSION ABOUNDS IN 5G SECURITY

Fewer than 10% of respondents feel that their security posture is fully prepared for the rollout of 5G; this confidence increases slightly to 13% with the reality of implementation (see Figure 6). Findings from the 2019 AT&T Cybersecurity Insights™ Report showed a generally higher level of confidence in preparedness for the rollout of 5G. The fact that fewer than 10% of respondents feel their security posture is fully prepared today is an indicator that individuals are realizing the magnitude of change that will come with 5G and edge computing.

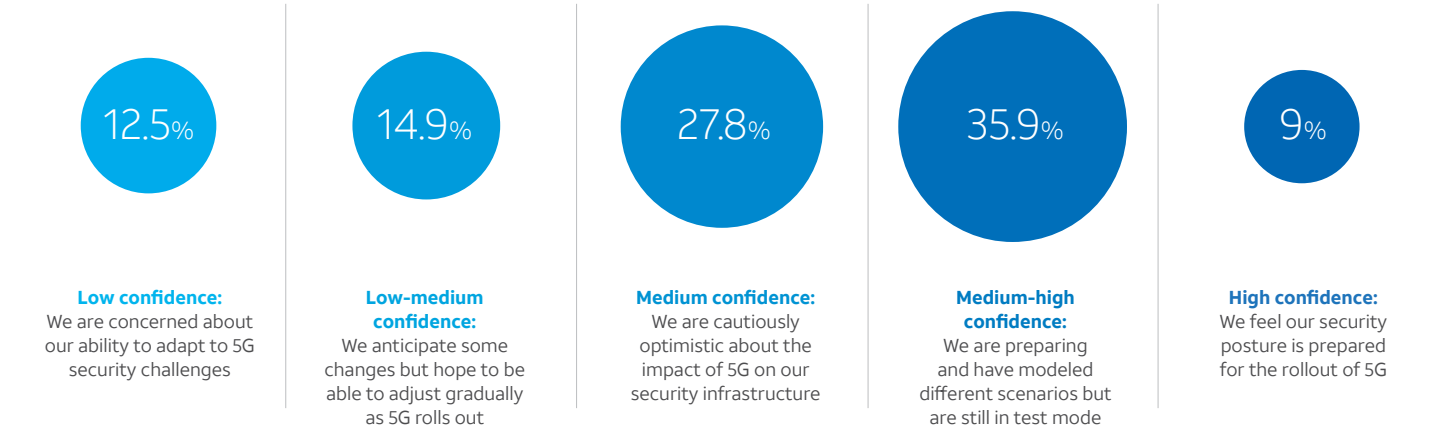
At the same time, there are opposing beliefs discussed previously that are facing enterprises as they transition to secure 5G — nearly half of the survey respondents believe that 5G poses an elevated security threat and the other half believe that 5G is secure out of the box and have no plan to address security changes. These contradictory perceptions will likely persist because a single point of view on 5G security hasn't yet formed. 5G is too nascent.

FIGURE 6

ENTERPRISES ARE CAUTIOUSLY OPTIMISTIC AND PREPARING FOR THE IMPACT OF 5G.

Q. How confident are you of your organization's preparedness for the challenges 5G may bring to security?

% of respondents



N= 947 BASE Respondents who indicated their organization is researching/implementing/completing 5G deployment

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

A CALL FOR SHARED SECURITY RESPONSIBILITY

It's well known that 5G solution providers embed security into the network architecture. 5G network operators are also building security into their networks. For example, the standards organization focused on 5G (3rd Generation Partnership Project or 3GPP), is building security into 5G standards from the ground up. In addition, 5G ushers in a new era of network security with encryption of the International Mobile Subscriber Identity (IMSI) to protect network traffic data sent over 5G radio networks. In the future, operators will provide correlation of location by IMSI and International Mobile Equipment Identity (IMEI), essentially providing geofencing in a mobile world.

These are important improvements upon previous generations of wireless from 3G to 4G LTE, where security was more of an overlay onto established specifications. However, there is still work to be done within the enterprise to provide that the data is protected both at rest and in motion. Hence, it is becoming clear that, much like the early days of public cloud adoption, a shared security responsibility model is needed with 5G (see Figure 7). This model should help enterprises shift many network functions to carriers and ultimately heighten enterprise-grade security. In this model, carriers and cloud service providers are responsible for the network and cloud infrastructure. Their job is to comply with applicable regulatory standards and frameworks and provide continuous monitoring of the network and the data traversing across it.

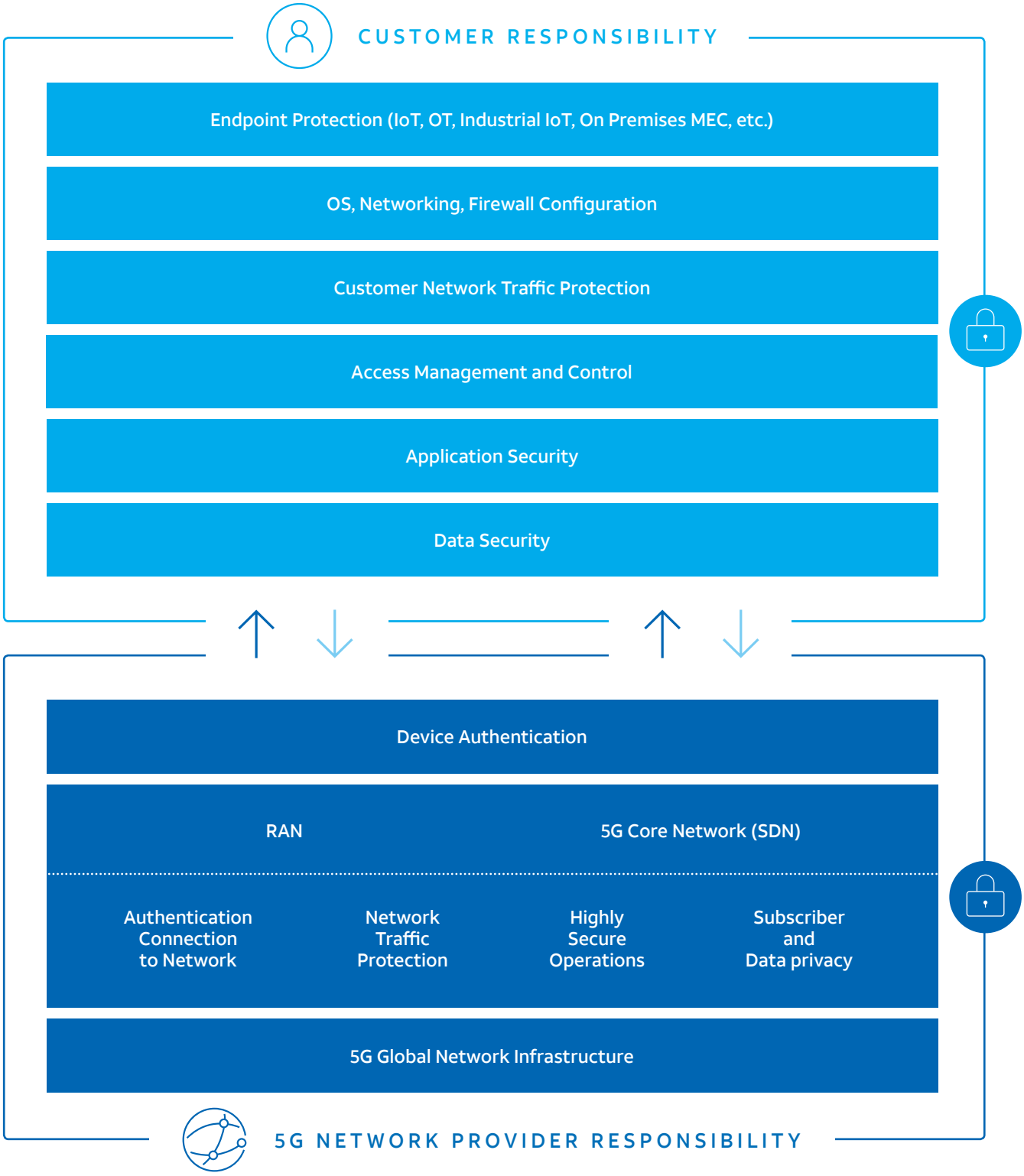
As in public cloud, the enterprise must provide for the security of its own devices and endpoints as well as the data within. Enhanced identity access management and data protection suites are needed in addition to the physical security of any on-premises customer equipment used for multi-access edge computing.

Much like the early days of public cloud adoption, a shared security responsibility model is needed with 5G.

FIGURE 7

5G SHARED RESPONSIBILITY MODEL

Security is a shared responsibility – enterprise customers are responsible for what they connect to the network.



IT REALLY IS ALL ABOUT THE DATA

During the transition to 5G, there are many security challenges left for the enterprise to sort out. It is becoming very clear that the theme of protecting data, regardless of where it is stored or the communication channel that it traverses, is one of the biggest concerns that needs to be tackled by the business. Note the commonality of "data" that is listed as the top two security challenges of implementing 5G shown in figure 8. Data privacy and managing the security of the data accessed by mobile endpoints are both of significant concern to survey respondents. Efforts will need to focus on securing data at rest and in motion, as well as showcasing responsiveness to data privacy requirements.

The security of data in transit at the speed of 5G is only as strong as the weakest link in the security chain. Carriers can do a sufficient job of securing data as it travels within the confines of the carrier network, but the carrier's highly secure

FIGURE 8

PERCEIVED SECURITY CHALLENGES WHEN IMPLEMENTING 5G SPAN MULTIPLE SECURITY CONTROLS.

Q. In your opinion, when implementing 5G, how much of a security challenge are the following?

(Scale of 1-Not a challenge at all and 5-Significant challenge) (Mean)

N= 947 BASE Respondents who indicated their organization is researching/implementing/completing 5G deployment

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey*, October 2020

network engineering is useless if the IoT device that sends or receives that data is not encrypting the data when it is at rest.

In addition, an insider could use a larger and faster network pipe that 5G enables to quickly forward intellectual property in bulk. To monitor for this, enterprises will need to make better use of advanced analytics to help detect anomalous behavior in network traffic so they can quickly detect possible data exfiltration.

An individual's access to confidential data, regardless of the person's stature, should be continuously monitored for unusual patterns of use. It will be just as critical to track and assess anomalous patterns of use by applications and devices. Firms should be clearly establishing, maintaining, and continuously monitoring and enforcing policy based on the who, when, and, where principles of who should be granted access to data, when they should have it, and (in a nod to international concerns surrounding privacy) where data can be consumed.

Many of these challenges noted here simply extend the current tasks that the chief information security officer (CISO) already faces in the run up to 5G. In addition to the CISO, locking down accessibility of data is also a key consideration for the chief risk officer (CRO) and chief compliance officer (CCO). Executives, the board, and anyone who produces or consumes data — which is just about everyone — need to be reminded that security in this new 5G-enabled world is all about protecting one of the most valuable assets in business — data, data, and more data (see Figure 9).

5G EDGE COMPUTING AND ZERO TRUST ARCHITECTURES

Adoption of a Zero Trust security approach is rapidly gaining traction as organizations grapple with hybrid and multi-cloud architectures. This model is well suited to 5G-enabled architecture and enables granular and identity-aware data management. The rapid shift of the workforce to work from anywhere at any time, along with the rise of insider

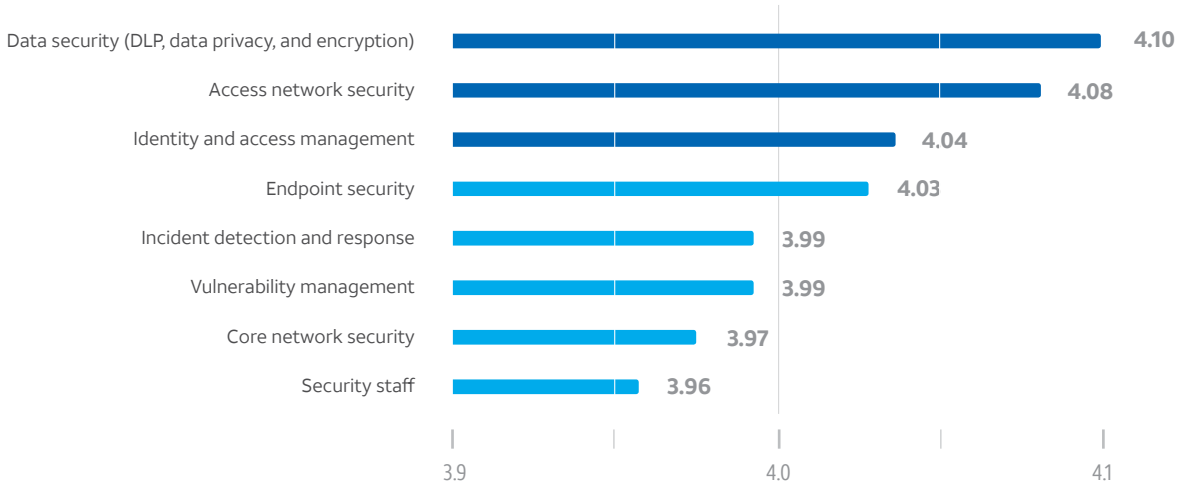
Locking down accessibility of data is a key consideration for the chief risk officer, chief compliance officer, and chief information security officer.

FIGURE 9

SECURING DATA AND ACCESS TO IT ARE THE TOP CONCERNS.

Q. Please rate the importance of each security capability in your organization's transition to 5G.

Scores are based on a scale of 1–5, where 1 = not important at al and 5 = very important. (Mean)



N= 947 BASE Respondents who indicated their organization is researching/implementing/completing 5G deployment

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

threat attacks, has given firms even more reason to deploy Zero Trust in their environments.

The analogy of treating enterprise infrastructure as though it were operating in a neighborhood café is exactly how a Zero Trust model works. The "never trust, always verify" overarching Zero Trust principle stands in sharp contrast to how many firms have traditionally approached access management and control. Prior to Zero Trust, users and applications had largely free reign to access anything once authenticated and inside the perimeter of the network. This model of securing access is no longer viable.

Zero Trust requires creating a hierarchy of workload and data sensitivity and categorizing access by this sensitivity. Data access is at the center of the Zero Trust security model, and purpose-driven security policies are designed to provide least-privilege access only when multiple contextual variables are satisfied. Zero Trust goes beyond the legacy "who" and "what" access model to consider the context of the request and the risk of the environment being accessed. And, keep in mind that access requests may come not just from users but also from autonomous IoT devices or other workloads.

Metaphorically speaking, least privilege is another living, breathing process that requires continual tuning. Interdepartmental cooperation is needed to tune on a regular basis what actual privileges are needed for each user. Continuous change is inevitable at any enterprise today. As the procedures for how jobs are performed change, so too should a review of what specific permissions are still needed.

Another principle of Zero Trust worth considering is providing that a device requesting access to a resource is in a highly secure posture and is being accessed by an authorized user. In addition, providing that multifactor authentication is part of the authentication process helps validate that the right user is present to access the resource.

Microsegmentation, where groups of devices are isolated from other parts of the network, is another foundational principle aimed at possibly limiting any lateral movement of a cybercriminal. For example, it makes sense that members of the accounting department probably don't need to be on the same network that the manufacturing team is on.

Protecting data and applications using a Zero Trust strategy will help make it easier for a security team to handle the anticipated growth of 5G-connected devices. Figure 10 shows the acknowledgment among security leaders that traditional security approaches are no longer effective for today's dynamic and highly distributed IT/OT environments, leading to an overwhelming desire to embrace Zero Trust. Nearly two-thirds of the respondents said their Zero Trust implementations are either underway or complete and roughly one-third are in the process of researching.

The adoption of Zero Trust, likely accelerated by the move to remote working, is a giant step forward, helping establish the resiliency needed to effectively protect the business today while also being adaptable to adjust to new digital initiatives for 5G and the edge. In reality, however, that journey is never 100% complete.

5G SECURITY INVOLVES ENTERPRISE, OPERATOR, MANUFACTURER, AND SERVICE PROVIDER

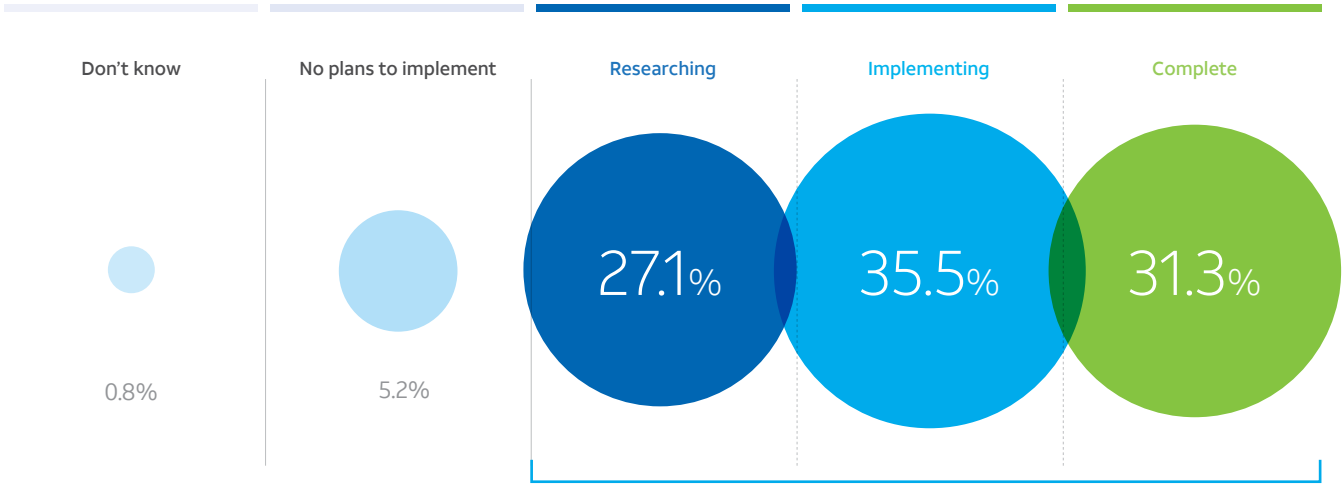
There are many team members called to the 5G security effort. Those with the biggest part to play are the enterprise internal IT and network teams, but they need to play in harmony with the 5G equipment and solutions manufacturers. In some cases, consultants and managed security service providers will also be asked to participate in the effort. Some organizations may hire a coordinator to help reduce discord between business and technology counterparts (see Figure 11).

FIGURE 10

THE ZERO TRUST JOURNEY IS WELL UNDERWAY.

Q. How far along is your organization in implementing Zero Trust?

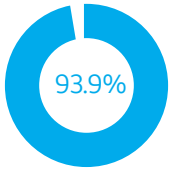
% of respondents



N= 980

BASE Respondents that are primary decision maker/ part of team/influencer role regarding Zero Trust

SOURCE DC Custom Survey, *5G Cybersecurity Impact Survey,* October 2020



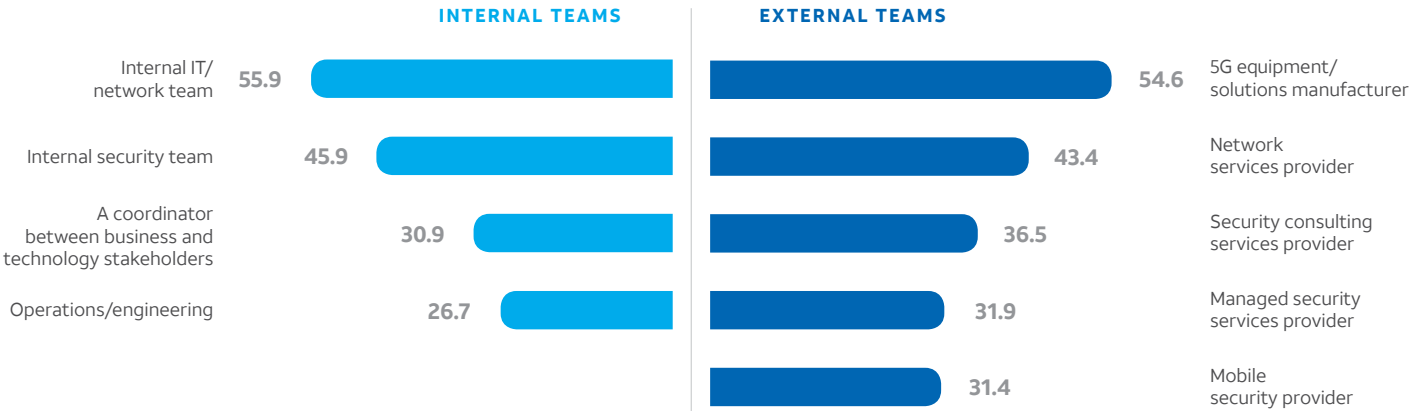
93.9% of respondents indicate they are researching, implementing, or have completed a Zero Trust initiative.

FIGURE 11

SECURITY IN A 5G WORLD REQUIRES A TEAM APPROACH.

Q. Securing 5G will require increased engagement with which type of internal and external teams?

% of respondents



N= 947

BASE Respondents who indicated their organization is researching/implementing/completing 5G deployment

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

Firms that have completed 5G implementation expect approximately 57% growth in IoT-connected devices over the next 18-36 months

EXPLOSION OF DIVERSE CONNECTED "THINGS"

To absorb attacks, organizations need to know what assets they have and where sensitive data resides. It is no surprise that initial use cases for IoT are in IT applications and asset management (see Figure 12). Through wearables and sensors, IoT can help doctors track a patient's physical well-being, but these devices can also help track the health and well-being of other "things." When an IoT device can provide relevant information about its own operation, performance, and environmental conditions, the device enables humans to more efficiently monitor and control it remotely.

According to IDC, the number of connected IoT devices is forecast to be 31.6 billion in 2020 and grow to 41.5 billion by 2025 (see *Worldwide Global DataSphere IoT Device and Data Forecast, 2020–2024*, July 2020). Non-IoT devices, such as PCs and mobile phones, round the total in 2025 to nearly 56 billion. Today, most companies have fewer than 10,000 IoT-connected devices that autonomously connect bidirectionally using IP connectivity within the organization, but this number is expected to increase by an average factor of nearly 50% in the coming 18–36 months. Those firms that have completed 5G implementation expect approximately 57% growth.

BOTNETS AND ZOMBIES, OH MY!

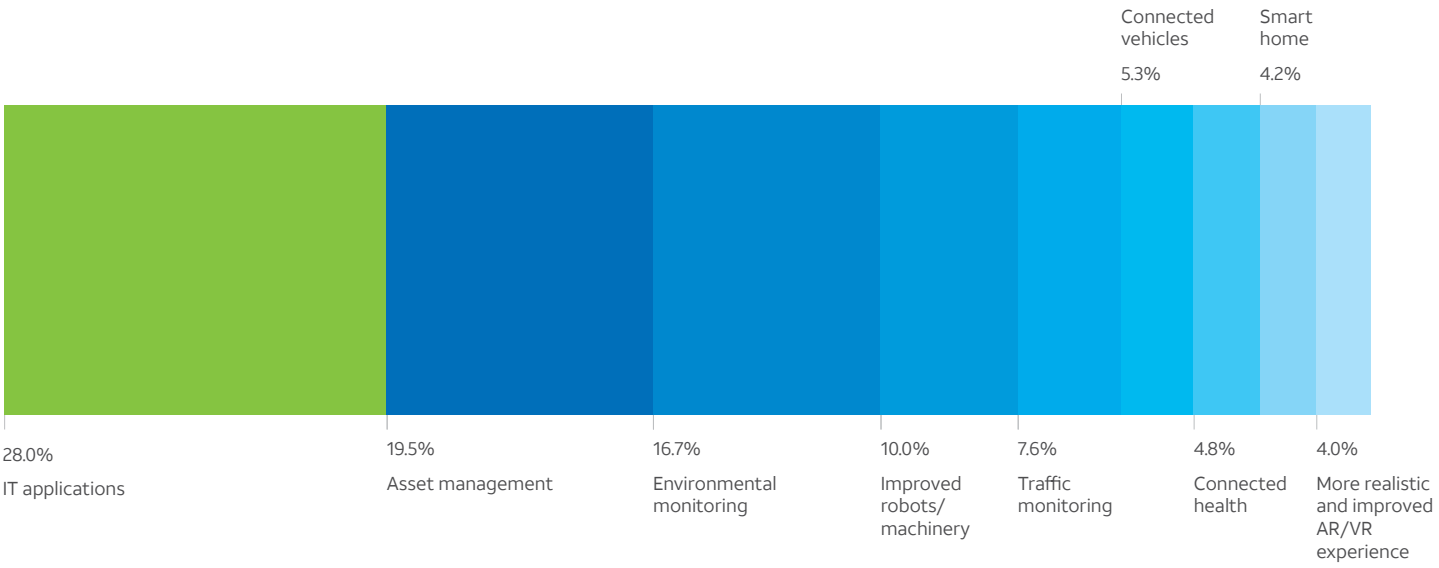
While IoT devices can help organizations manage and monitor the health and well-being of their environment, these devices also introduce new vulnerabilities.

FIGURE 12

IoT BRINGS NEW APPLICATIONS AND IMPROVED MANAGEMENT AND MONITORING.

Q. Which of the following is the primary use case for your organization's IoT/OT/ Industrial IoT?

% of respondents



N= 647 BASE Respondents who indicated their organization is currently in pilot/proof of concept and in production in single/multiple locations for IoT

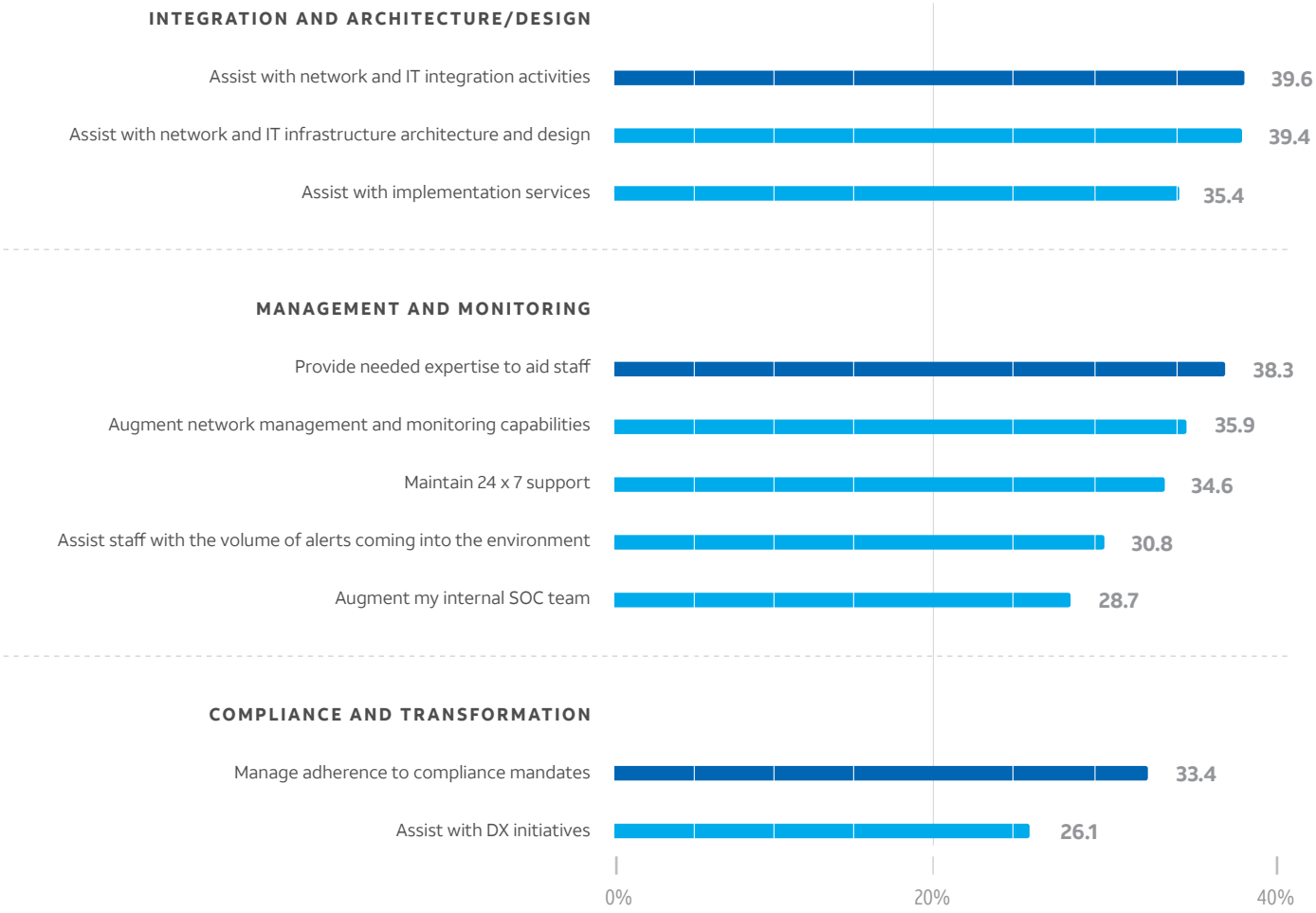
SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey*, October 2020

FIGURE 13

ENTERPRISES WILL SEEK EXPERTISE TO AUGMENT STAFF SHORTAGES.

Q. In what areas will your organization need additional staffing to support IoT requirements?

% of respondents



N= 647

BASE Respondents who indicated their organization is currently in pilot/proof of concept and in production in single/multiple locations for IoT

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

2.9% Don't know

Cybercriminals will benefit from the connected device explosion, the increased speed, and lower latency as well, potentially compromising machines (zombies) to proliferate botnets at the speed of 5G. Botnet attacks in recent years have been well documented, but keep in mind that the COVID-19 pandemic has introduced different, often new, and additional vulnerabilities with remote workers leaving home networks exposed.

Home-based devices connecting through unprotected routers may offer further criminal opportunity to assume control and build out large-scale botnet attacks. To prepare for this, distributed denial-of-service (DDoS) protection providers are already expanding capacity by adding scrubbing centers to handle redundancy and enhance performance. With an influx of IoT botnets expected, identity and access management (IAM) and endpoint

With an influx of IoT botnets expected, identity access management (IAM) and endpoint security technologies are increasingly important.

security technologies are increasingly important to determine which IP addresses can connect to which network and when they should be blocked. This is especially important when those connecting to IP addresses are not users but massive machine-to-machine "things."

RESOURCES NEEDED FOR 5G IoT SECURITY

With new vulnerabilities, security alerts will also propagate at scale. Hence a chief concern is to add the appropriate technology and staff with the expertise to handle the increased volume of alerts. Security will have to be virtually effortless to help reduce the risk of security analysts becoming overwhelmed. The use of automation, advanced analytics, and machine learning will no longer be a "nice to have." It will be required for sifting through massive volumes of data that are to come with 5G and edge computing, helping to predict anomalous behaviors and find unknown threats faster than humans can. These capabilities will need to scale to match today's threats and those in the future as manual alert inspection will become impossible.

Enterprises will seek additional expertise to support their IoT requirements amid a global security resource shortage, which will add pressure. Top of mind is finding security personnel with knowledge of designing and architecting IoT systems that integrate across the highly-complex and hybrid environments that come from the new distributed 5G/edge, multi-cloud, and on-premises architecture (see Figure 13).

Today, as security staff monitor and investigate potential anomalous behavior in the network, they are increasingly adopting advanced capabilities such as threat detection and response, threat hunting, threat intelligence, and (as mentioned previously) advanced analytics and automation to help mitigate, contain, remediate, and investigate attacks with as much expediency as possible.

The number of existing vulnerabilities within enterprise networks will not slow down as 5G gets implemented. New vulnerabilities can be created due to spinning up a new virtualized instance or cloning a virtual instance with an unaddressed vulnerability. Security teams will need to be prepared to prevent these threats from spreading rapidly within their environment by addressing those that are most exposed and ripe for attack. This includes comprehensive discovery and identification, prioritization based on internal security controls and external factors such as known exploits in the wild, and ongoing patch management and mitigation.

Organizations will need to expand threat detection and response and network security technologies, as well as deploy multifactor authentication to handle the software-defined, cloud-based environment of the 5G-enabled IoT framework. Threat detection and response offerings are evolving to include better algorithmic detection, thereby reducing mean-time-to-detect metrics today, but they will need to include complementary controls such as application security in the future. These offerings will also need to monitor and detect threats in diverse and complex environments.

5G will also speed up software development cycles, potentially worsening today's already extant Achilles' heel of security vulnerabilities. Moving to a software-defined world pushes the importance of application development up front, which changes how security is viewed and who is responsible for making sure security is embedded in the design phase. Respondents currently implementing 5G rank application security as their number one concern with regard to cyberattacks in IoT infrastructure (see Figure 14).

When engaging security service providers, vulnerability testing, security training, and breach and attack simulation (BAS) are top of mind. With the growing cybersecurity skills shortage, enterprises need to consider reskilling and utilizing creative (non-STEM) associates to fill the IoT security gap.

Enterprise security teams cannot take the same approach with operational environments as they do with legacy IT environments because the environments are fundamentally different and have legacy technology. In addition, once the technology is deployed, it is often more difficult to patch. As a result, when engaging in new IoT use cases, enterprises should consider the security implications from the start and IT and line-of-business groups should discuss security implications collaboratively.

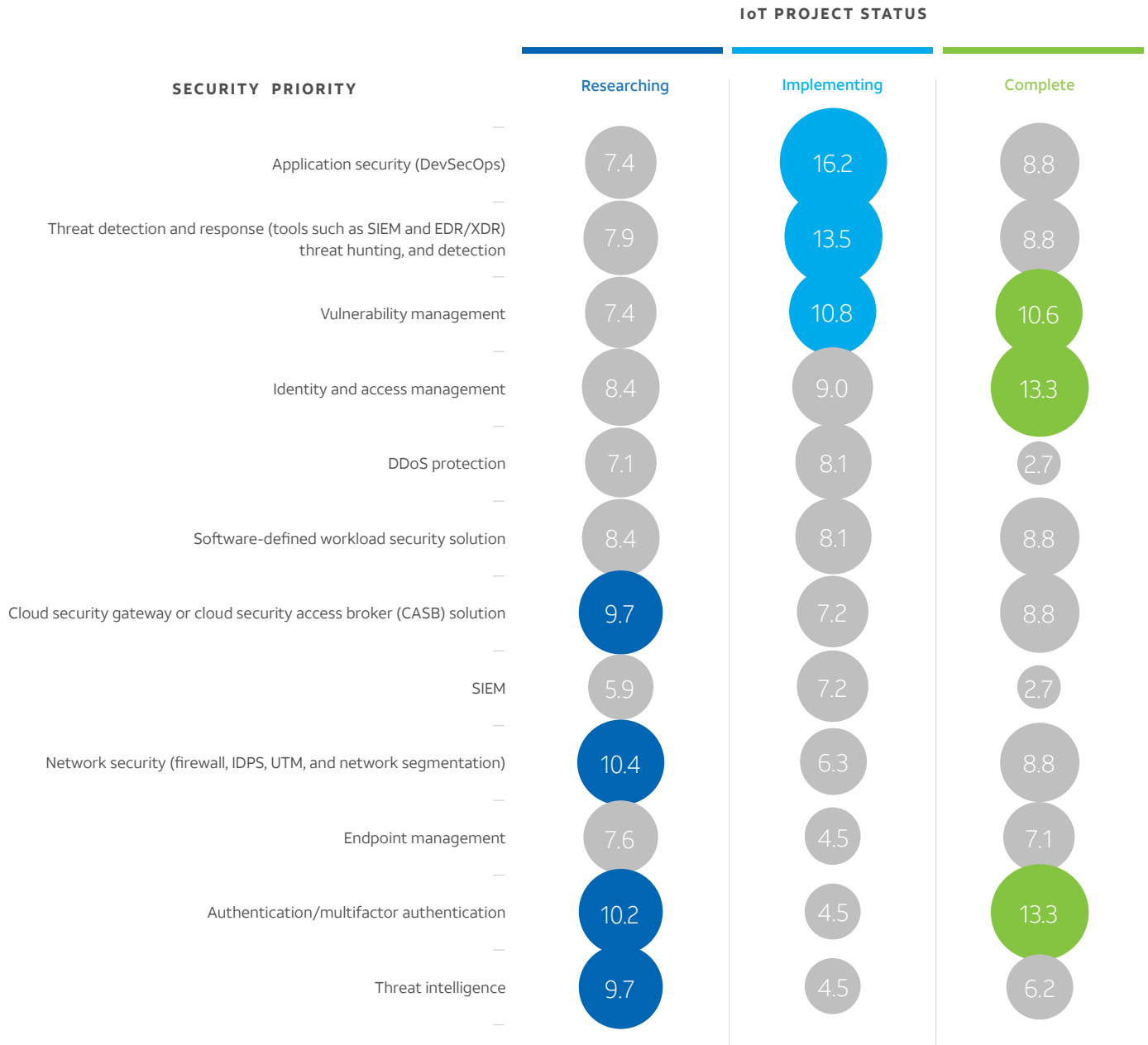
When engaging security service providers, vulnerability testing (62%), security training (51%), and breach and attack simulation (46%) are top of mind.

FIGURE 14

SECURITY PRIORITIES SHIFT AS IoT PROJECTS MOVE TO COMPLETION.

Q. Which security functions/ controls are the most important within your own network to control possible cyberattacks to your IoT/ OT infrastructure (rank 1)?

% of respondents



N= 647 BASE Respondents who indicated their organization is currently in pilot/proof of concept and in production in single/multiple locations for IoT

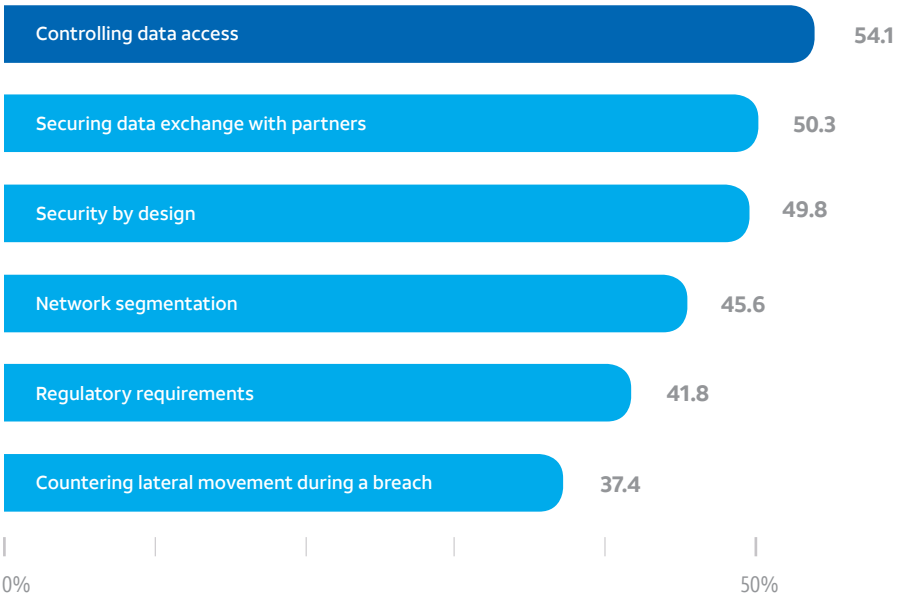
SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

FIGURE 15

ZERO TRUST IS NOT JUST ABOUT ACCESS CONTROL.

Q. In which areas do you believe Zero Trust will help your organization?

% of respondents



N= 921

BASE Respondents indicated organization researching/implementing/complete Zero Trust

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

Team collaboration drives a holistic approach to security and creates "security by design." Approximately half of the respondents see Zero Trust not only as a way to better control data access but also as a strategic approach that helps drive security by design (see Figure 15). In addition, 45.6% respondents believe Zero Trust will help the organization through network segmentation, which is a tactic that can potentially minimize east-west lateral movement should an incident or breach occur in an IoT/OT environment.

Highly securing 5G IoT usage is seen as an area of strong concern. Nearly 40% of respondents have a medium-to-high degree of concern about highly securing 5G IoT usage and another 33% have medium concern (see Figure 16).

Enterprises will need advice on the right security tools to implement for the protection of IoT/OT environments and to help evaluate return on investment. Applying unified security controls and functions can assist in the consolidation of soft costs, such as time spent on upgrades and education. Working with a managed security services provider can help alleviate hard costs associated with the investment of products and licensing, hiring, and reskilling people.

Security design should incorporate automation and the ability to apply security policies dynamically.

RECOMMENDATIONS

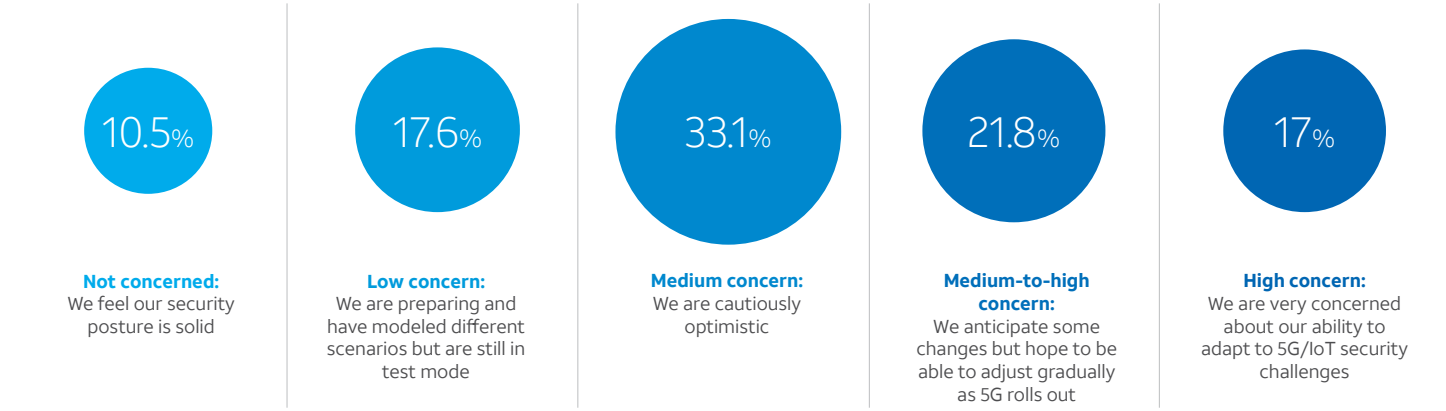
Look to machine learning, artificial intelligence, and other advanced analytics. The explosion of 5G-enabled IoT devices will likely increase advanced threats and attacks. While most respondents noted that detection and response capabilities are a top security control needed for their IoT use cases, many have not considered the scale of changes that have to occur due to the plethora of devices connecting to the network. Security design should incorporate automation and the ability to apply security policies dynamically to keep up with the speed and scale of 5G networks. Utilizing advanced technologies such as AI/ML, continuously updated threat intelligence, and other analytic capabilities can help improve rapid detection and response of new threats as networks become increasingly complex and the number of devices connecting to those networks explodes.

FIGURE 16

5G IoT SECURITY POSTURE: UNCERTAINTY AND APPREHENSION EXISTS.

Q. How concerned are you about the impact on your security posture due to the introduction of 5G across IoT use cases?

% of respondents

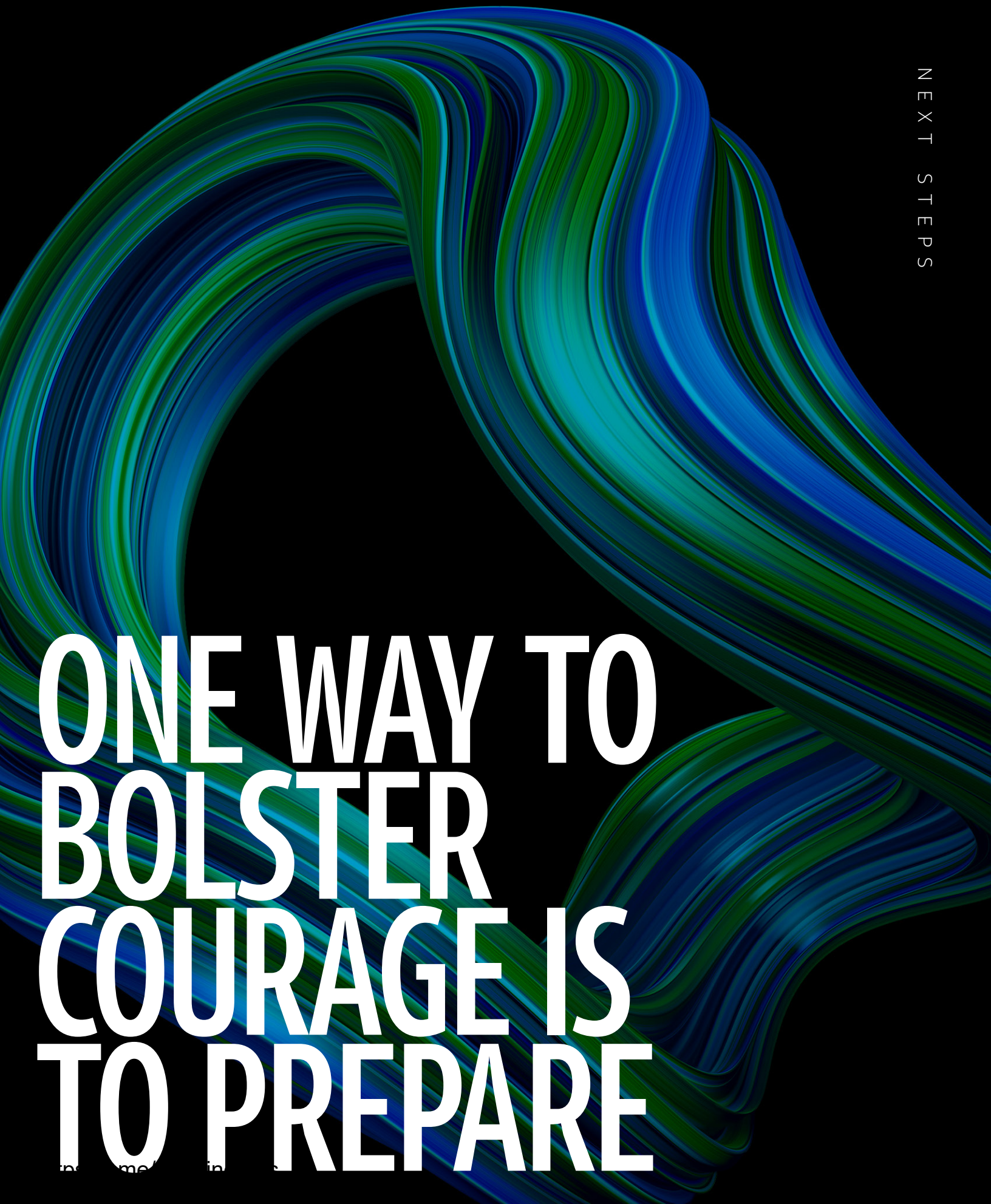


N= 647 BASE Respondents who indicated their organization is currently in pilot/proof of concept and in production in single/multiple locations for IoT

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey*, October 2020

Evaluate software-defined networks and security. With 5G and IoT implications, attackers will potentially have greater opportunities to exploit vulnerabilities to gain valuable data from enterprises. Software-defined networking (SDN) should be considered as a security enabler for the future set of technologies being implemented. With the increase of applications being developed, SDN enables embedding security into the design and architecture of the network. Security that is enabled with SDN presents the capabilities to help improve policy enforcement and anomaly detection and mitigation. SDN will allow applications to block malicious activity occurring on a network and enforce policies across security services, such as firewalls and intrusion detection and prevention systems, as well as help enterprises rapidly implement new security services.

Consider virtual network functions (VNF). Virtualization is a technology that can be implemented across distributed networks quickly. Because of this, enterprises can spin up security components, such as firewalls, while also pushing security policies to many devices efficiently. Because these controls ramp up quickly, virtual security controls can deploy technologies that will help prevent attackers' lateral movements, apply micro-perimeters to protect applications, embed security in the network, and utilize SDNs to detect and mitigate threats.



ONE WAY TO BOLSTER COURAGE IS TO PREPARE

The

GAP BETWEEN the current cybersecurity posture and what organizations will need in the hyperconnected 5G-enabled world can be vast. Organizations should be deliberate and strategic as they move to 5G in designing both the network and the relevant security posture. Security must be part of an organization's comprehensive digital transformation road map as a competitive differentiator. IDC predicts that, by 2023, 75% of organizations will have comprehensive digital transformation implementation road maps, up from 27% today, resulting in true transformation across all facets of business and society.

Organizations must, likewise, recognize that investments are needed to obtain the business opportunities that 5G brings. 5G innovations are likely to be driven first by the business reaching out to the CISO, sometimes concurrently, and other times as an afterthought. Security leaders should seek to be the department of, "Yes, how can we enable that idea?"

The C-suite and the board need to recognize that 5G is not just a faster 4G. Strategic investments will need to be made to protect this new, rapidly approaching frontier. In fact, when asked what percentage of the overall security budget will be spent today and in 12–18 months on 5G security, survey respondents that are either implementing 5G or have completed 5G implementation indicated that they spend 18–23% of their budget on 5G security today and that they will increase this spend to nearly a quarter of their overall budget in 12–18 months. Figure 17 shows organizations' security spend by area.

Forward-thinking enterprises that have already invested in cloud-based firewalls, software-defined networks, and virtual desktop infrastructures (VDI) had a smoother journey to the work-from-home new normal. Enterprises that failed to make these investments had to scramble to protect the expanded risk surface that the new working environment exposes.

Organizations should take stock of where they are on the path to a safer and more secure 5G future and then make the necessary key investments in people, processes, and security technologies.

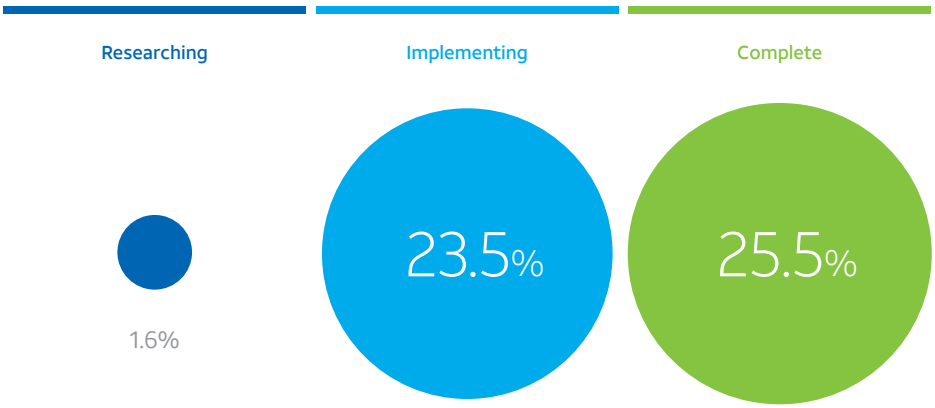
FIGURE 17

5G SECURITY IS EXPECTED TO BITE INTO BUDGETS.

Q. To the best of your ability, please estimate the percentage of your security budget spent on the following areas in 12–18 months.

% of respondents

Percentage of budget spent on "Security for 5G implementation"



N= 1,014 BASE All respondents SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

WHAT ARE THE NEXT STEPS?

Engage experts. Calculating all the steps that need to occur to provide a functional, resilient, and protected 5G infrastructure can best be accomplished when a team of professionals with a "been there, done that" background is engaged. Nowhere is this more important than utilizing the proper outside resources that can help install and even possibly manage the enhanced security solutions put in place.

When considering security service providers for a 5G implementation, there are interesting regional differences to consider. Asian countries show less than 2% planning to use in-house resources, while 8% of North Americans feel more confident with their in-house teams implementing 5G. Considering the literal number of moving parts to a 5G implementation, along with all the touch points in and out of the classic perimeter, the do-it-yourself approach is arguably a risk-filled, as opposed to a risk-averse, path to take.

Survey respondents chose engaging with a MSSP or a communication service provider as the top two choices when deploying 5G and edge computing, at 23% and 21% respectively. This is not a big surprise, given the cybersecurity skills gap and nature of 5G technology as a communication enabler (see Figure 18).

Look for service providers that can combine the various tools and services that are needed into a platform-based deliverable. For example, the use of correlated threat intelligence to provide contextualized information about the tactics, techniques, and procedures (TTPs) of potential adversaries is a recognized baseline element of a mature security posture.

Consider network segmentation and Zero Trust. There are several key technologies that organizations can start to put into place in their own unique run up to a 5G-powered future. Implementing a Zero Trust architecture is a key enabler of securing most 5G use case. For the

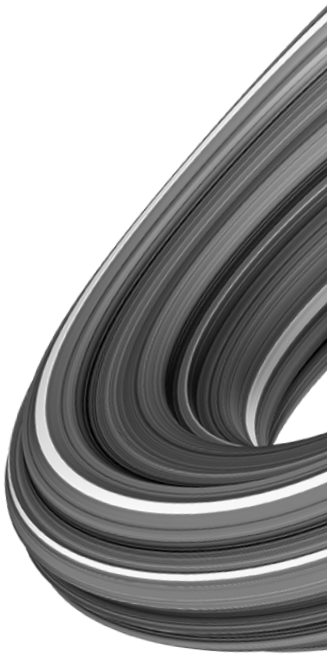
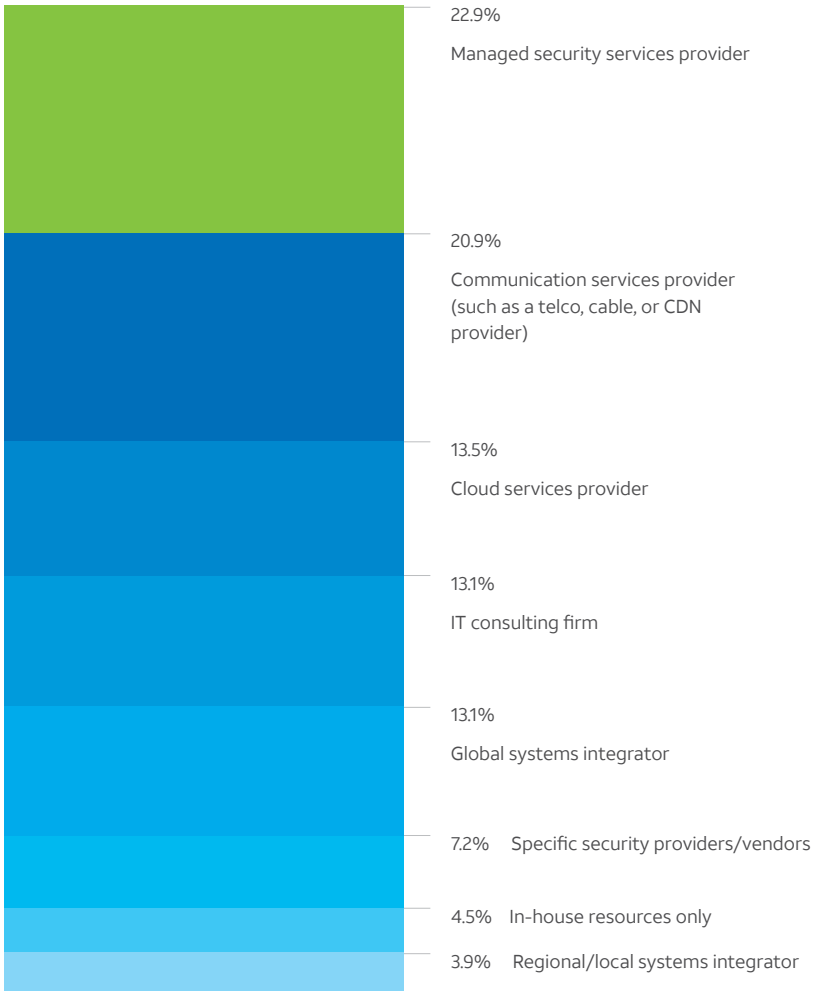


FIGURE 18

ENTERPRISES LARGELY LOOK TO MSSPS AND COMMUNICATION SERVICE PROVIDERS FOR SUPPORT.

Q. Who is/was/will be the primary security service provider for security in your organization's 5G implementation?

% of respondents



N= 947

BASE Base = respondents who indicated their organization is researching/implementing/completing 5G deployment

SOURCE IDC's Custom Survey, *5G Cybersecurity Impact Survey,* October 2020

45% of survey respondents who are researching or still implementing a Zero Trust architecture, the steps taken in the lead-up to deploying Zero Trust can be beneficial on their own.

Concepts like microsegmentation of the network can slow down possible lateral movement of an attack. The core principle of microsegmentation is that having departments such as accounting and manufacturing on the same network segment unnecessarily widens the risk surface.

Identify assets. Other steps such as mapping out data flows can identify where high-value assets reside. This heightened visibility gives the security team the extra awareness of which assets require higher visibility and monitoring.

Build virtualized security into the network. Because virtualization is a technology that can be implemented across distributed networks quickly, enterprises can use this technology to spin up security components such as a firewall while also pushing security policies to large numbers of devices. Virtualized networks can quickly scale up and down and change user policies rapidly within software-defined networks. Because these controls are spun up quickly, virtual security controls can rapidly deploy technologies that will prevent attackers' lateral movement, such as applying micro-perimeters to help protect applications or using software-defined networks to help detect and mitigate threats.

DDoS prevention is essential. Another key capability needed now and even more so in a 5G IoT-connected device future is strong distributed denial-of-service prevention. Criminal groups often enlist the IoT devices that are fueling so many of the 5G use cases as their "virtual soldiers." DDoS protections can absorb cyberattacks and provide the resilience needed to keep fulfilling IoT core functions. In addition, service providers need to provide ongoing vulnerability assessments and continuously updated threat intelligence to protect these IoT devices from being incorporated into a cyber attacker's virtual army.

KEY TAKEAWAYS: HOW TO CREATE A MORE SECURE 5G NETWORK

Recognize that 5G is not an evolution but more of a revolutionary new technology, however transition will not occur overnight. The sheer quantity of devices that will be connected from different places at faster speeds will stress security teams. Organizations will not be able to assume that every connected device is safe. Zero Trust principles are a natural fit for a 5G world.

Implement 5G and edge in a manner unique to the organization. Design the 5G and edge footprint in alignment with the specific business goals, desired innovations, and industry parameters of the company. And, because this design will be unique to business needs, security must also be tailored to protect the company's individual architecture.

Observe and be aware of what needs protection. Learn about the tactics, techniques, and procedures (TTPs) of the cybercriminals that like to attack organizations in the same region and industry and prepare the security team to better respond to those attacks that do end up landing in the environment. Deploy a unified platform that incorporates integrated and continuously updated threat intelligence from a broad set of telemetry, threat hunting, and other threat detect-and-response capabilities.

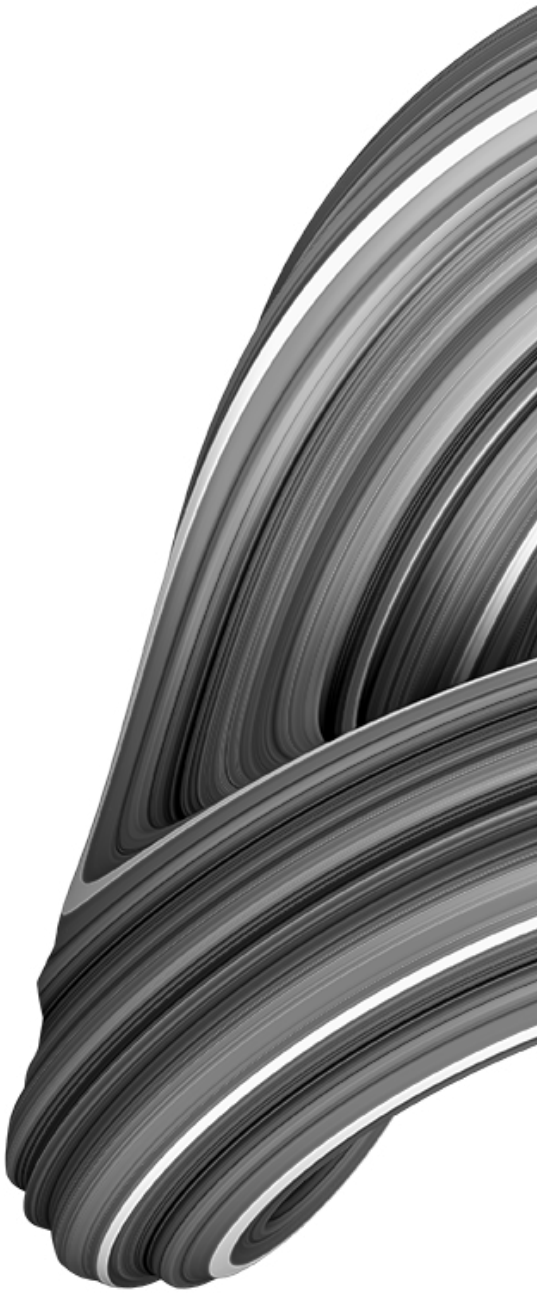
Evaluate every user and verify every device. Validating the security condition of every device that connects can proactively prevent introducing intentionally or accidentally compromised devices into the network.

Establish baselines of normal behavior and activity for the network and users. Be prepared to contain and respond to anomalies.

Bear in mind that secure by design is the operating principle. Incorporate secure design principles into the development of 5G use cases. Recognize that security gets shifted left.

Reduce complexity and risk to enhance security. Utilizing more redundant tools in the security operations center (SOC) can lead to increased cost and complexity. When utilizing service providers for security, look to work with with providers that have a broad platform of capabilities.

CONCLUSION



COVID-19 has altered human reality but has also changed the technical landscape by accelerating adoption to digital business and cloud. Businesses are increasingly concerned about insider threats. By all accounts, 5G is here today and will become ubiquitous. Organizations must be bold, as 5G will ultimately enter the organization in one form or another.

This report highlights many scenarios that will broaden connections among humans and machines more quickly and efficiently but also bring advanced attacks that can take down businesses, utilities, and even cities. This study outlines many opportunities to change the network, offload capabilities to operators and service providers, and engage assistance with security service providers to provide for business resiliency.

One way to bolster courage is to prepare for and start planning the necessary changes for network security as transition moves relentlessly toward true 5G. The current security firefighting method has been necessary, but over time, in a newly minted, software-defined, and virtualized 5G plus edge network, organizations have options to protect their businesses in a better way.

Network operators have designed 5G with better encryption and network slicing capabilities. But 5G requires a shared security responsibility, much like that in the public cloud. Every organization must keep that in mind.

By all accounts, 5G is here today and will become ubiquitous. Organizations must be bold. 5G will ultimately enter the organization in one form or another.

APPENDICES

APPENDIX A

METHODOLOGY

This report is based on a survey of 1,000 security practitioners from the United States, Canada, India, Australia, Singapore, South Korea, France, Germany, Ireland, and the United Kingdom conducted during September 2020. All respondents come from organizations with 1,000+ employees to reflect larger organizations' knowledge of, and readiness for, the security implications of 5G. Respondents were limited to those with direct knowledge of their organizations' 5G plans or with decision-making responsibilities related to securing 5G as well as direct knowledge of IoT, cloud, edge and MEC, and Zero Trust. Respondent titles included CISO, CIO, vice president of security, IT operations director/manager, IT director/manager for information security, and telecom director. Respondents were spread across a variety of market segments, with financial services (19.5%) and manufacturing (19%) being most heavily represented. On certain questions, participants could choose more than one response. In those cases, the responses will not round to exactly 100%.

APPENDIX B

ACKNOWLEDGEMENTS

To publish a report of this magnitude, we rely on a team of contributors from AT&T and within the global cybersecurity community. We want to thank everyone who gave their time, energy, and industry knowledge to the success of this publication. This includes the 1,000 security, IT, and business professionals who participated in the report research, subject matter experts who provided their technology insights, along with the writers, editors, designers, and project managers who shepherded the report from initial research through completion. A big thank you to all!

Contributing Authors

IDC
Patrick Filkins
Christina Richmond
Craig Robinson
Martha Vazquez

AT&T
Elisha Girken
Tawnya Lancaster
Theresa Lanowitz

Contributors

AT&T
Will Amores
Adam Berman
Jaime Blasco Bermejo
Christopher Boyer
Rupesh Chokshi
Alicia Dietsch
Suzanne Galvanek
Amy Johnson
Leslie Johnson
Skyler King
Tawnya Lancaster
Theresa Lanowitz
Deon Ogle
Jeffrey Shafer
Bindu Sundaresan
Todd Waskelis
Alex Waterman

Altitude Management Inc.
Paul Cavanaugh
Bryan Reid

Akamai Technologies, Inc.
Anthony Lauro

Check Point Software Technologies Ltd.
Aviv Abramovich

Digital Defense, Inc.
Mike Cotton

Fortinet
Richard Orgias

Lookout
Brian Buck
Jeff Radebaugh

McAfee
Christie Karrels

Ivanti
Russell Mohr

Palo Alto Networks
Sree Koratala

SentinelOne
Brian Hussey

APPENDIX C

CONTRIBUTING ORGANIZATIONS

AT&T Business

IDC ANALYZE THE FUTURE

Akamai Experience the Edge

DIGITAL DEFENSE INCORPORATED

ivanti

paloalto NETWORKS

SentinelOne

Check Point SOFTWARE TECHNOLOGIES LTD

FORTINET

Lookout

McAfee

AT&T Cybersecurity

About AT&T Cybersecurity

AT&T Cybersecurity helps make your network more resilient. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

5G AND EDGE COMPUTING MARK A REVOLUTION THAT WILL TAKE TIME TO ADAPT AND MATURE. EVERY COMPANY'S 5G IMPLEMENTATION WILL BE SHAPED BY UNIQUE BUSINESS NEEDS AND REQUIRE A TAILORED SECURITY SOLUTION TO PROTECT IT.