2019
2020
NINTH EDITION

AT&T Cybersecurity Insights™ Report:

Security *at the* Speed *of* 5G

Preparing your business for 5G acceleration

AT&T Business

Welcome to the ninth edition of the AT&T Cybersecurity Insights Report!

For the past several years, we have been surveying cybersecurity professionals just like you to gain insight on the latest cybersecurity topics and trends. The newly formed AT&T Cybersecurity business unit is focused on helping you reduce complexity and the cost of fighting cybercrime.

This year, our Cybersecurity Insights Report is based on a survey of 704 cybersecurity professionals from around the globe and across a variety of market segments. All participants are from organizations with more than 500 employees. If you are one of the survey participants, I thank you for sharing your opinions with us.

The topic for this year's report is "Security at the Speed of 5G." The discussion is framed in context of the business opportunities and challenges that CISOs and CIOs need to consider in preparation for the adoption of 5G. In this report, we share:

- Your consolidated opinions on enterprise readiness for 5G
- The impacts of the new technology in terms of risk
- What that new risk means for your security policies

We also provide you with insight on the importance of security virtualization in the next decade, our point of view on a shared security model for 5G, and an overview of what 5G network security entails.

Traditionally, AT&T has served as a trusted advisor on cybersecurity for global businesses and organizations. Today, as AT&T Cybersecurity, we are using that knowledge and experience to renew our focus on understanding your needs and supporting your efforts toward cybersecurity resiliency. Please feel free to let us know how we can best serve you to help you achieve your cybersecurity goals.

Enjoy the report and the findings presented.

Barmak Meftah

President, AT&T Cybersecurity

Executive overview

5G technologies and networks will bring exciting new possibilities for the enterprise. Prudent organizations are taking a proactive stance by anticipating the security requirements that will come with the new technology. Given the multifaceted nature of 5G and security, it is critical to explore how well enterprises grasp the importance of this undertaking.

In a survey conducted by AT&T Cybersecurity with 451 Research in August and September of 2019, results show that many enterprises are getting a head start on 5G, yet many are challenged with understanding and appreciating all its dimensions. For example, edge deployments connected with 5G and the capacity for virtualization (both on the part of the 5G network service provider and the business) are critical to end-point protection.

Creating a 5G security posture means understanding the potential for new threats and putting up the right tools for a solid defense. There are resources for enterprises that want help anticipating and planning for security challenges arising with 5G. Specifically, service providers can supplement enterprise security with the features fully implemented in 5G. The optimal path is most likely to follow the example of the public cloud and develop a model of shared responsibility for 5G security.

Key findings

- Enterprises need to do more to prepare for 5G. Advancement in the 5G network will touch on many technology areas and eventually enable enterprises to use less expensive and more efficient solutions. Virtualization and software-defined networking (SDN) capabilities will be powerful elements that enterprises should be considering to help prepare for 5G security; likewise, enterprises should also take the opportunity to virtualize and automate security.

- Given the number of devices attaching to the network at more locations, including Multi-access Edge Computing (MEC) nodes, identity and authentication will be key to 5G security. In addition, enterprises should be considering how they can shore up their vulnerability management programs (both patching and mitigation) for devices at the edge which may carry vulnerabilities that go unnoticed and unpatched.

- For 5G, a shared security model, similar to that of the public cloud, is likely to emerge. This should enable enterprises to shift functions to carriers and ultimately heighten enterprise security.

Introduction

What 5G really means

The rollout of 5G stands apart from previous generations of mobile communications in that 5G will eventually bring about major changes in technology and network architecture, as well as how businesses protect both through their cybersecurity approach. The specifications that in large part define this next generation of mobile communications have been established by the 3rd Generation Partnership Project (3GPP). More than just another increase in speed, 5G is designed ultimately to imbue the network with new capabilities, such as network slicing. (Network slicing creates isolated domains for traffic; users can then be assigned slices with customizable bandwidth and quality of service.) 5G will also provide the capacity to eventually support millions of end devices, a density that will enable massive internet of things (IoT) deployments connected with ultra-low latency.

Unique from previous generations, 5G is being engineered with built-in security features*. Stronger over-the-air encryption is a part of the 3GPP 5G standard, and vendors will be able to use the latest encryption schemes to help enhance security. Subscriber identity privacy will help provide that 5G devices are connecting to the correct network, reducing the risk of eavesdropping devices that capture International Mobile Subscriber Identity (IMSI) numbers. Still, 5G alone is not enough to handle all business security needs. Enterprises must continue to be security-aware and act to protect their networks.

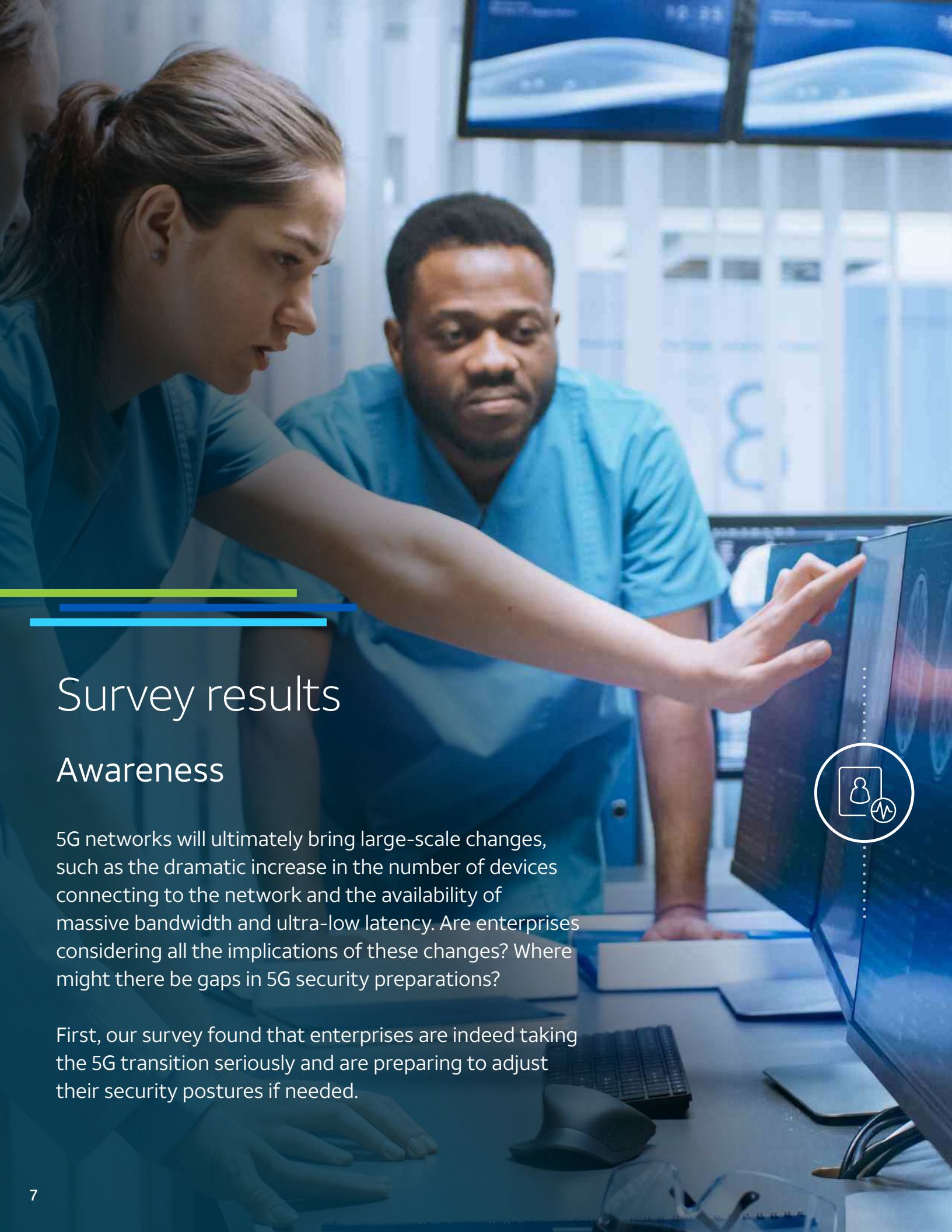
More than just another increase in speed, 5G is designed ultimately to imbue the network with new capabilities...

*AT&T has long been engaged in thinking about 5G security issues. We published a white paper on 5G security, and participated in a collaboration at the Federal Communications Commission between the government and private sector to develop best practices.

Methodology

This report is based on a survey* of 704 security practitioners from North America, India, Australia, and the United Kingdom, conducted during August and September 2019. All respondents come from organizations with 500 or more 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 5G. Respondent titles included CISO, CIO, IT operations director, and IT director for information security. Respondents were spread across a variety of market segments, with manufacturing and construction (15%) and technology (14%) most heavily represented. On certain questions, participants could choose more than one response. In those cases, the responses will not round to exactly 100%.

*Further detail on respondent demographics is provided in the appendix section at the end of the report.



Survey results

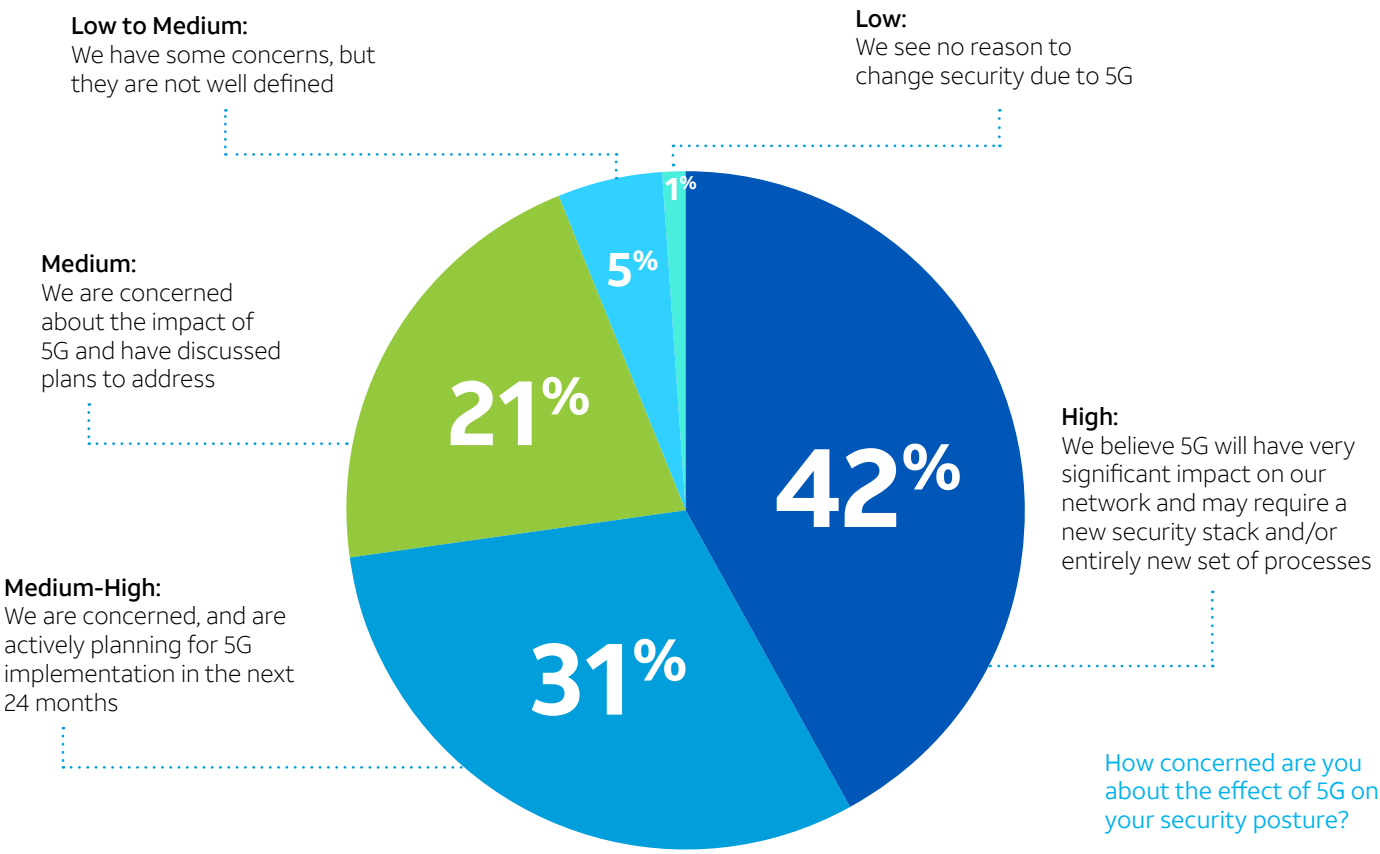
Awareness

5G networks will ultimately bring large-scale changes, such as the dramatic increase in the number of devices connecting to the network and the availability of massive bandwidth and ultra-low latency. Are enterprises considering all the implications of these changes? Where might there be gaps in 5G security preparations?

First, our survey found that enterprises are indeed taking the 5G transition seriously and are preparing to adjust their security postures if needed.

Security posture

FIGURE 1. Effect of 5G on security posture



72.5% of the respondents rated their level of concern as high or medium-high when it comes to the potential impact of 5G on security. (**See Figure 1.**) Not surprisingly, the communications market segment responded most strongly, with 54% of the 104 respondents in that vertical reporting a high level of concern.

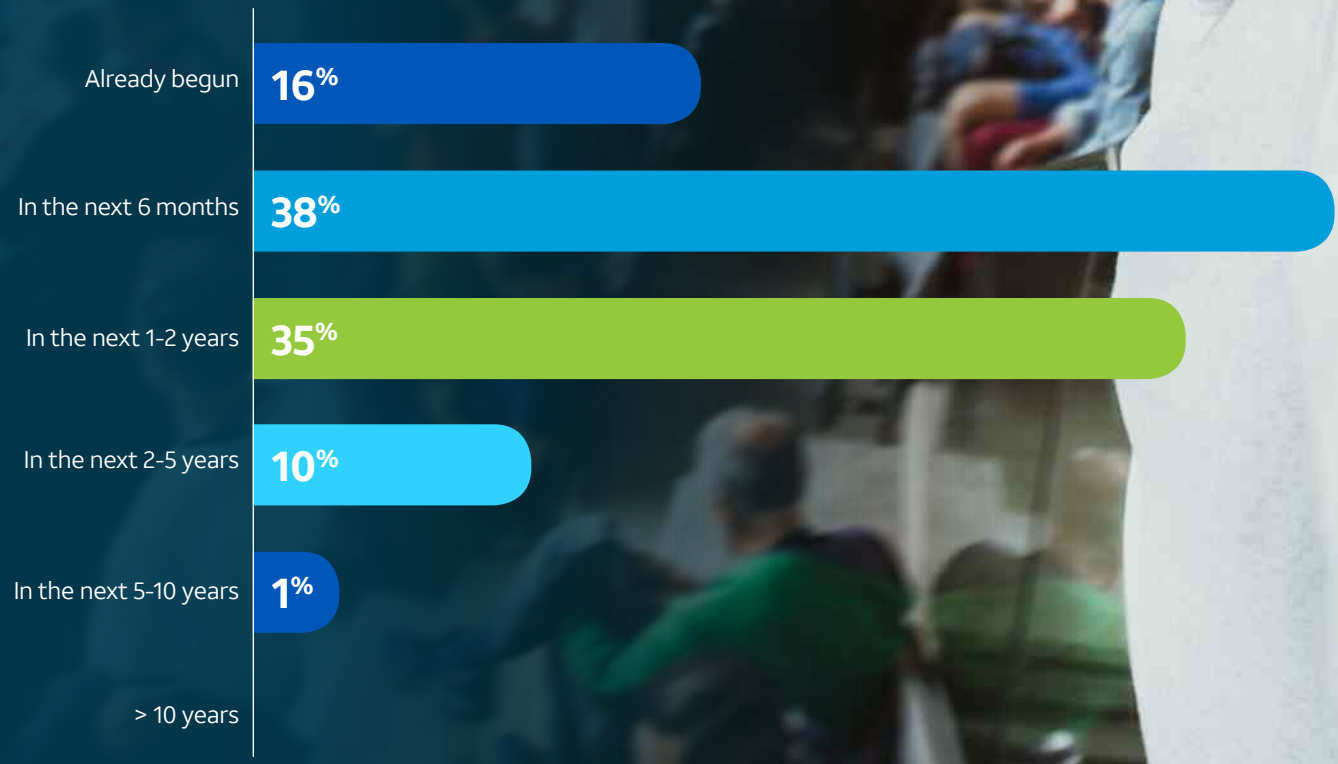
The survey also showed some understanding that 5G is a significant or extraordinary transition. Many of the likely attacks on 5G networks will be the same as those encountered today — perhaps in some cases taking advantage of faster bandwidth and a higher number of network-connected devices — yet still relying on familiar vulnerabilities and known attack methods. 76% of respondents, though, expect wholly new security threats to emerge out of a 5G world. (**See Figure 7.**)

Preparedness

Nearly all respondents in the survey expect to make 5G-related security changes within the next five years, and 16% say they have already started preparing before the mainstream wave of 5G deployments arrives. (**See Figure 2.**)

Time to implement security changes

FIGURE 2. Making security changes related to 5G

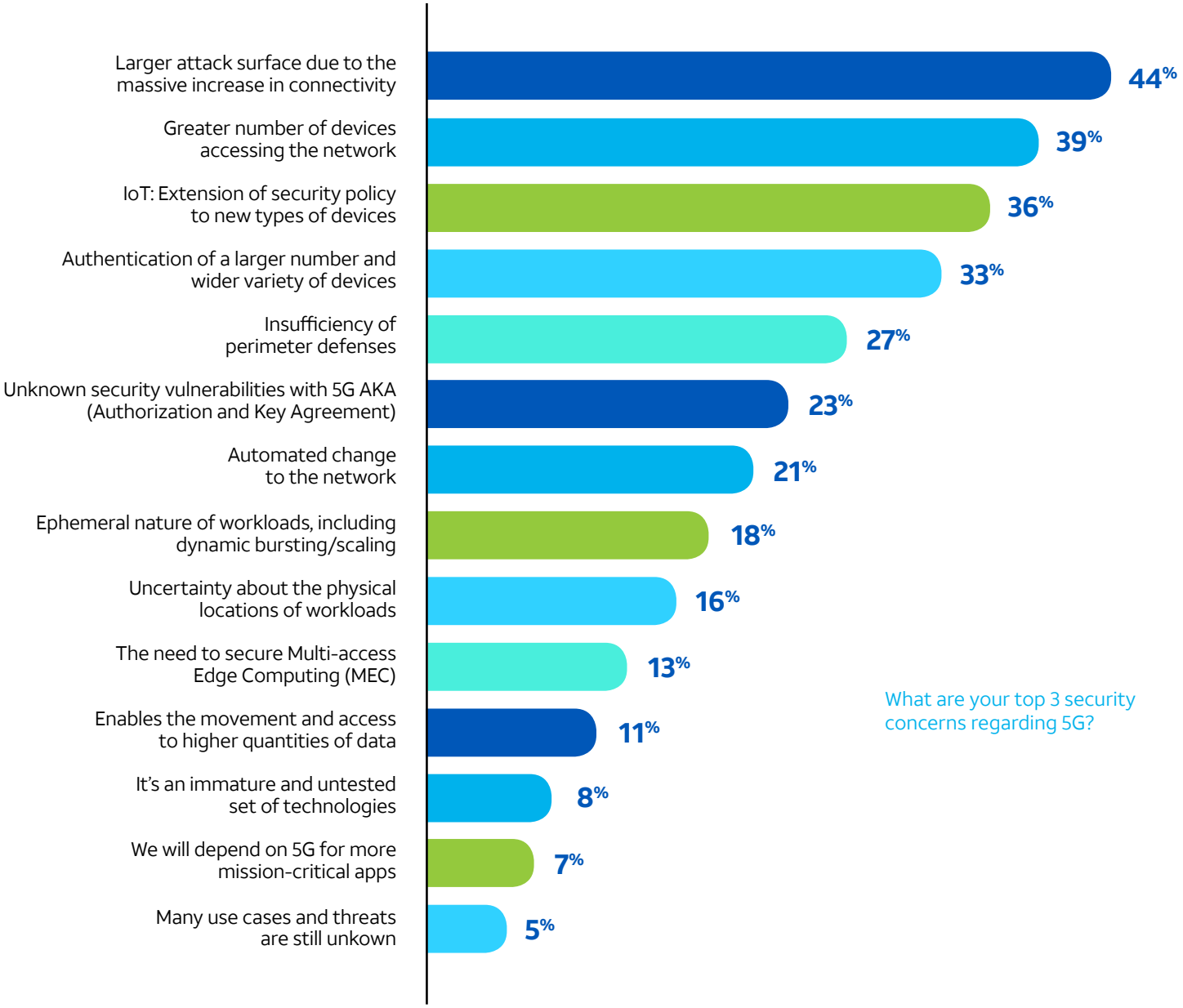


What is your timeframe to begin making security changes related to 5G?

But what are enterprises preparing for? The strongest concerns tend to focus on the proliferation of devices in a 5G network. Broad concerns — the larger attack surface and the number of devices — topped the list, followed by the need to extend security policy to IoT devices and the need to authenticate a larger number of devices. (**See Figure 3.**)

Top 3 security concerns regarding 5G

FIGURE 3. Frequency of Top-3 ranking



These are legitimate concerns, but there is a wider view to consider. Most of the transitions in networking have been about faster speeds or increased capacity. 5G introduces more complex networking and is being delivered with virtualization in mind. The latter appears to be a crucial gap in the way enterprises are preparing for 5G, as enterprises will need to take advantage of virtualization to make the network nimbler and more responsive, with the ability to provide just-in-time services. Many enterprises are not considering this as a possibility, according to our data.

> **...enterprises will need to take advantage of virtualization to make the network nimbler and more responsive, with the ability to provide just-in-time services.**

Technologies and gaps

In this section we zoom in on the survey results related to specific technologies. We examine how enterprises perceive the challenges associated with these technologies and discuss the factors that seem to be overlooked.

Virtualization

Virtualization continues to surface as a must-have technology that enterprises should use to their advantage for 5G. This includes such things as software-defined networking (SDN) and network functions virtualization (NFV).

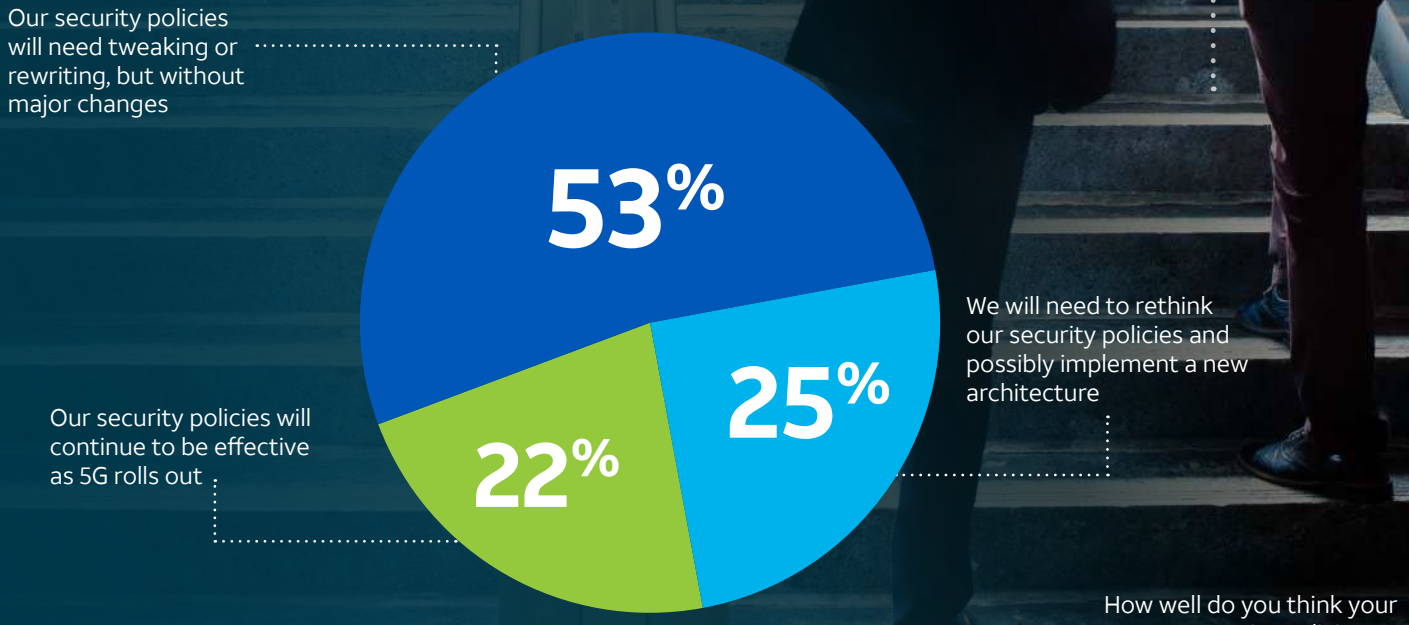
Only 29% of respondents, however, say they plan to implement security virtualization and orchestration during the next five years. With the majority of survey participants expecting to make their 5G security changes within the next two years, it is clear that security virtualization is not included in their 5G roadmap.

This is important because of the power of virtualization. Virtualized security can be deployed quickly to arbitrary network locations, and when a new type of attack is discovered, the network's "immune system" can respond immediately by spinning up a security element such as a firewall. The key is that this response can be automated.

Along similar lines, only 25% of the survey participants believe their current security policies will continue to be effective under 5G. A majority, 53%, believe at least some adjustments will be needed, while 22% expect to rethink their security policies altogether. (**See Figure 4.**) A virtualized and automated set of security responses would apply policy changes globally, doing so more reliably and quickly than manual updates could.

Adaptability of current security policies

FIGURE 4. Security policies: Effects of 5G



Recommendations

5G has the potential to bring significantly more devices onto the network which increases the possibility of new threats. Security organizations relying on manual changes will face challenges in keeping up. At a large scale, security needs to be dynamic and automated in order to accommodate the scope and potential speeds of 5G networks. In addition, virtualization can help to complement and enable a flexible response against unknowable future threats, and that flexibility can be used to update security policies to counter newly evolved attack strategies.

Virtualization also enables an organization to universally apply security policy changes across its footprint. This is a good practice to begin with to avoid having islands of the network that operate under outdated policies and/or have not been steeled against new threats and vulnerabilities.

> At a large scale, security needs to be dynamic and automated in order to accommodate the scope and potential speeds of 5G networks.

Security virtualization could be the most crucial advancement related to 5G security, for both the provider and their enterprise customers. Enterprise IT is becoming more distributed, and through virtualization networking is following suit. Security needs to follow that trend.

Organizations concerned with their ability to maneuver the complexity and rapid innovation that 5G will foster might look to a managed security service provider. This route could also remove issues for an organization stemming from rapid obsolescence of technology procured too early in the innovation cycle.

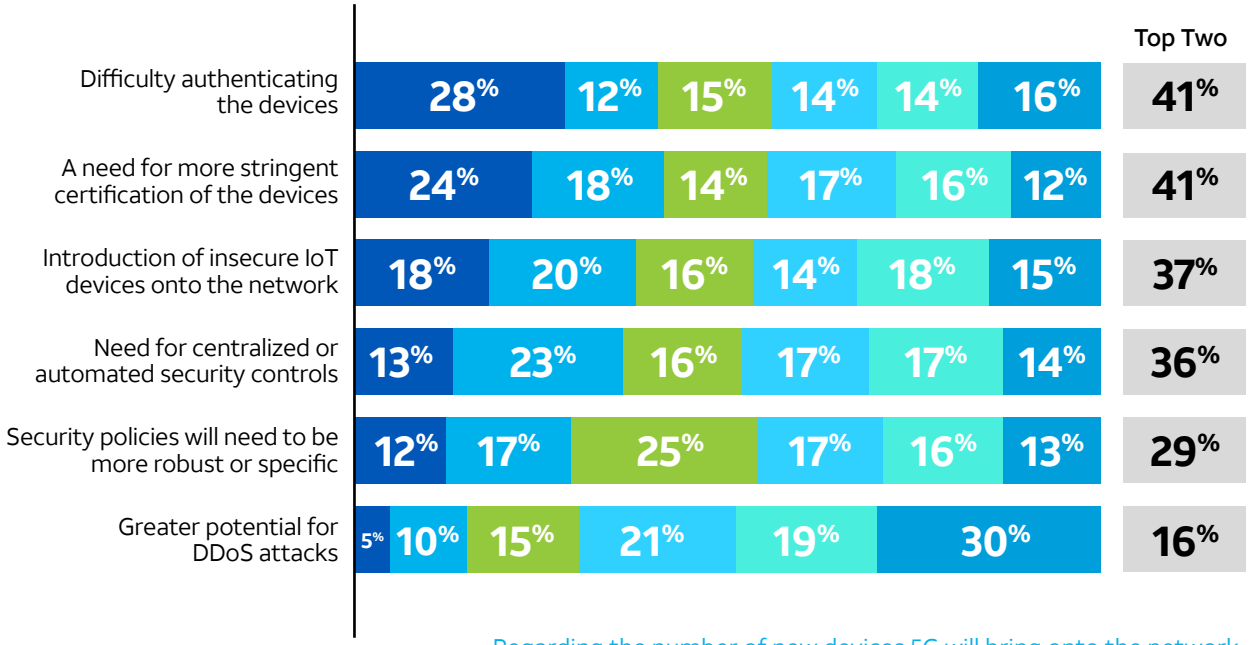
Endpoint security

5G will likely connect more devices to the network, and it will certainly be used for connecting new devices. Not surprisingly, this is a concern for 80% of the enterprises surveyed. Authentication and certification topped the list in our survey as challenges incurred by these new devices, but only by a narrow margin. The presence of non-secure IoT devices and the need for centralized or automated security controls were also at the top of the list. (**See Figure 5.**)

Despite these concerns, only 33% of the respondents are planning to implement tighter network access controls in the next five years, and only 37% are planning new systems for device authentication*.

Most important challenges of new devices under 5G

FIGURE 5. Rank the most important challenges



Regarding the number of new devices 5G will bring onto the network, which do you consider to be the most important challenges?

*Reference to data from survey not shown graphically within report.

Recommendations

There is more happening here than an increase in the volume of new devices connecting to the network. The topology of the network is changing. We can no longer assume that traffic is entering the network through a pinch-point such as an internet gateway. This has strong implications in the areas of authentication and identity, which is discussed in more detail in the next section.

When it comes to device certification, even if standards become stronger, it seems a given that most manufacturers, eager to keep costs low, will satisfy only the bare minimum requirements. We can expect IoT devices to continue to have vulnerabilities such as factory-default passwords, so enterprises will want to take some responsibility for safeguarding against rogue devices. This plays into a shared security model that's described in more detail later in this report*.

It is worth noting that stronger distributed denial-of-service (DDoS) attacks, enabled by the number of devices on the network, was clearly a lesser concern for survey respondents.

This could be because of the sensational publicity around DDoS attacks; respondents might have already "maxed out" their DDoS protections. Even so, volumetric attacks could hit new peaks given a greater number of devices for malicious actors to corral and the amount of bandwidth at their disposal. If they have not already, enterprises should make sure that their DDoS defenses can plausibly handle an attack of unforeseen size. A network service provider, aided by a network with the scale to absorb large attacks, can also provide complementary services for DDoS protection.

...volumetric attacks could hit new peaks given a greater number of devices for malicious actors to corral and the amount of bandwidth at their disposal. If they have not already, enterprises should make sure that their DDoS defenses can plausibly handle an attack of unforeseen size.

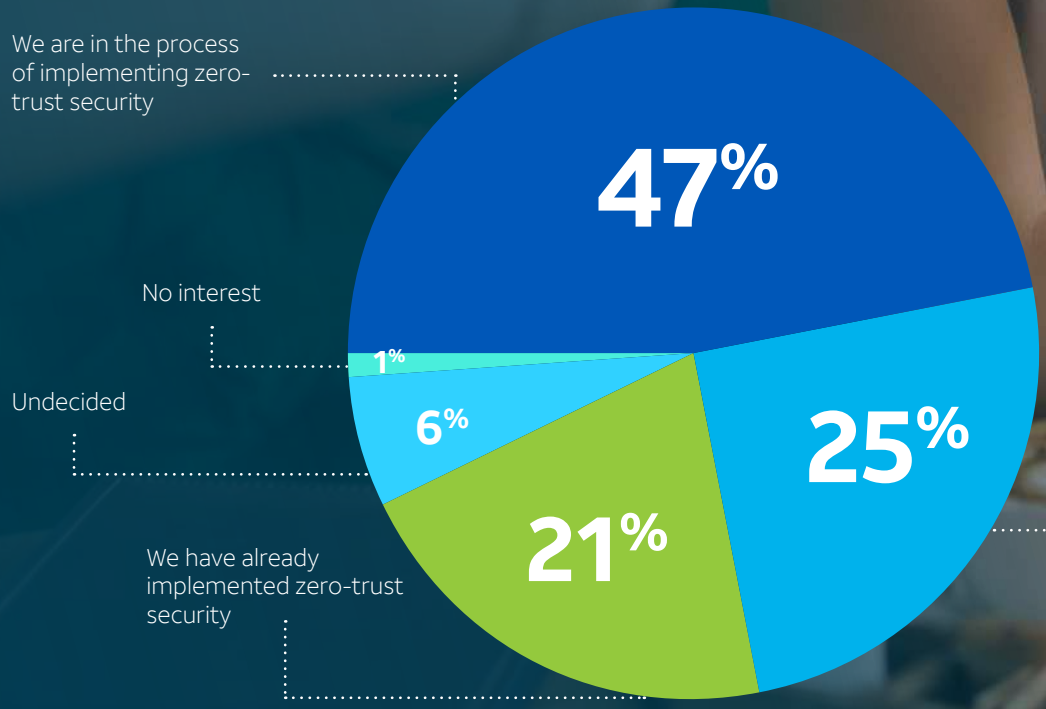
*AT&T led work at the White House National Security Telecommunications Advisory Committee (NSTAC) recommending that all elements of the Internet ecosystem must be involved in such efforts, including network service providers, device manufacturers, software developers, and cloud, application, and hosting providers. See the report.

Authentication and identity

Enterprises are growing increasingly worried about authentication due to the increased number of connected devices that 5G will potentially bring to the network. This raises questions about identity and authorization. With more devices accessing the network from more locations, including Multi-access Edge Computing (MEC) nodes, it is natural to worry about who might be on the network and what permissions they have been granted. A zero-trust security model can address some of those concerns by continually checking a user's presence and behavior, whether that user is a human or a machine.

Zero-trust security

FIGURE 6. Interest in a zero-trust security model



What is your level of interest in a zero-trust security model?

Enterprises are embracing zero-trust, as 68% have either implemented it or are in the process of doing so. (**See Figure 6.**) Elsewhere in the survey, however, only 35% of enterprises say they have implemented identity governance and privileged access management*.

A primary goal of MEC is to reduce latency by removing geographic distance. MEC places compute nodes at the edge of a network near the client instead of a distant cloud. That edge could be on a service provider network, inside a datacenter, or on the enterprise premises. Regardless, it presents new potential locations for data exfiltration or malware introduction that could originate from a trusted user's access. Moreover, IoT devices at the edge could carry vulnerabilities that go unnoticed and unpatched.

On a related note, multi-factor authentication (MFA) is a useful tool for identity management, but enterprises have been slow to adopt it — only 33% of enterprises have implemented MFA and 7% say they plan to implement it during the next five years.

Recommendations

Multi-edge computing in 5G creates a situation calling for distributed security controls. This again emphasizes the importance of security virtualization, which security practitioners can use to help avert attacks that suddenly materialize at the edge. Think of spinning up firewalls on demand or detecting and mitigating a DDoS attack in its early stages.

The 5G service provider can help confirm device identity as well, because the network will know a device's physical location. This points to the benefits of a managed security service or at least a shared security model, where the service provider uses the network itself as a security tool.

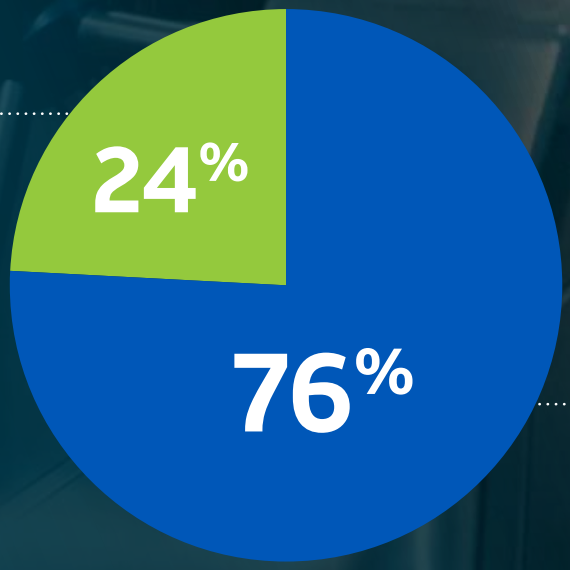
*Reference to data from survey not shown graphically within report.

Vulnerability management and mitigation

Recall that 76% of enterprises believe 5G will enable entirely new types of threats, those that are not simply extensions of today's threats. (**See Figure 7.**) However, vulnerability management appears to be a weak spot among enterprises. According to survey respondents, only 33% of organizations have implemented asset discovery and management and 30% have implemented vulnerability assessment and remediation — results that seem surprisingly low considering enterprises are already swimming in vulnerabilities*.

Perception of 5G security threats

FIGURE 7. 5G security perception



I expect the fundamentals of attacks to remain the same as 4G (albeit faster and potentially more voluminous)

I expect entirely new security threats to emerge as 5G becomes established

As it relates to 5G which of the following statements do you agree with more?

*Reference to data from survey not shown graphically within report.

Recommendations

While 5G technology will potentially generate new threats, it also brings new networking capabilities that can be used to source threat data for analysis. In other words, the things that may be a concern for a 5G network also make it more powerful for sourcing threat intelligence to help protect the enterprise. The most accurate threat intelligence (whether from a third-party, an enterprise, or a network provider) draws from many sources of information in terms of the scale and diversity of data. This may include a vendor or service provider's customers, which could increase the odds that newly emerged threats arising from 5G and its related technologies are added to the security system's vocabulary.

New vulnerabilities and the potential expanded attack surface of 5G creates more avenues for attackers. Enterprises need to be able to launch a rapid and effective response once an attack is spotted. As noted above, virtualization and SDN can help. For example, connectivity can be reconfigured to isolate a problem spot. Automating this capability, a step made possible by having virtualized security controls, gives the network a fighting chance to respond quickly to previously unknown threats.

Threat detection and response

Only 33% of the survey respondents say they have implemented network security threat analytics, which typically includes some form of threat intelligence, and only 30% are using external threat intelligence*. The complexity of a 5G network arguably calls for more robust practices into threat detection and response, including the use of adequate threat intelligence and supporting response capabilities, such as automation of response playbooks.

Threat detection will become particularly important given that 5G will likely spur a surge in the volume of connected devices, such as IoT devices. Threat detection practices that monitor the environment for anomalous behavior will have more activity to track and data to sift through. This includes both internal data within the enterprise and external data on emerging and evolving threats, which is likely to be more complex as well. The contextual information around devices will also become important for making security assessment decisions. This is a scenario where machine learning becomes imperative, making it practical to interpret this data at scale and within the accelerated timelines needed for response. Enterprises should give their security teams the means to support complex and large-scale datasets to prepare their threat detection and response capabilities for the 5G world.

The nature of threats likely to affect 5G deployments may include not only new attacks against 5G components but also attacks against the higher-level processes that 5G will enable, such as a network of sensors that collects production data on a manufacturing floor and then uses cloud software to turn the data into insights about the efficiency of operations. With that in mind, it is critical that security practitioners have access to new threat intelligence research and understand how 5G will likely change the tactics, techniques, and procedures (TTPs) of known and emerging threat groups. That threat intelligence should come from the analysis of a globally diverse pool of threat data, including updates that are based on observations of many enterprise environments and attacks against other organizations worldwide.

*Reference to data from survey not shown graphically within report.

As is common in other security scenarios, the organization's security architecture should be resilient to the occurrence of individual component failures. After all, a brand-new attack might bypass initial defenses. Therefore, it is critical for an organization's threat defense capabilities — aided by analytics and threat intelligence — to have the ability to initiate automated response and remediation at multiple stages of an attack along the Kill Chain®, i.e. installation, delivery, command and control, etc. This circles again back to virtualization: the network should be able to quickly spin up defense resources in such a manner that they contain the threat, while also supporting further investigation and remediation. This can take the form of network access control, increased telemetry/observability, and automatic reconfiguration of network components as needed.

Recommendations

As organizations prepare for 5G rollouts and applications, now is the time to validate that security programs have the necessary scale, agility, and analytics capabilities to address potential 5G security scenarios. This will likely include machine learning-enabled analytics, support for integrated threat intelligence, and automated responses. Manual intervention, including humans responding to alerts, will not be enough if 5G gives rise to new varieties of threats, as many enterprises, 5G security architects, and threat intelligence experts expect.

The look of a more secure 5G network

Putting together these pieces, what would 5G network security potentially look like?

- **Virtualized, automated security controls.** By now it is clear that the expanded surface area of a 5G network — including MEC and potentially compounded by the faster speeds of 5G — creates territory where automation can more efficiently be used to manage an environment. Automated remediation and virtualized security controls will help to equip enterprises to mitigate risks of the future.

- **Machine learning and threat detection.** 5G devices and MEC will generate a lot more activity on the network, which may dramatically increase the amount of data that security tools must analyze. Threat detection and threat intelligence will need to be informed by machine learning and other forms of artificial intelligence in order to keep pace.

- **A zero-trust environment.** If they are not implementing a zero trust approach to their environment, at the very least security practitioners should be considering a more sophisticated approach to identity and authorization. This is required for the number of devices involved and for the possibility that authorized users can inadvertently introduce malware to the network.

- **A shared security model.** Even though 5G offers some inherent security features, the enterprise must take responsibility for covering many aspects of security. (More on this below.)

Most of these recommendations represent a properly rigorous and modernized security posture, even without the context of 5G. That is why it is justifiable to act now while 5G is still in its early stages of deployment and before some of these technologies become more urgently necessary.

The shared security model

In the public cloud, security is a shared responsibility. For example, cloud providers protect the cloud infrastructure, such as the physical servers and storage devices, but customers are responsible for the security of the guest operating system (OS) and the applications they install.

The same approach should apply to 5G. The network operator would be primarily responsible for elements of security spelled out in 3GPP frameworks and standards, such as data encryption. The operator would likewise handle security of the network infrastructure itself, one example being the radio access network (RAN). The enterprise would assume responsibility for devices on the network. This would include mobile device management, certification of applications that the enterprise runs on the network, and identity and access management (IAM).

The dividing lines can be subtle. For example, when it comes to device authentication, the operator would be primarily responsible for authentication from the network side. That is, the operator would verify that the device should be permitted to connect to the network. On the other hand, the customer would be responsible for security of the device's hardware, software, and OS.

One way an enterprise can cover its security responsibilities is by enlisting a managed service provider. This is a good option for organizations that are short-staffed in terms of security personnel.

Conclusions

Under 5G, the number of devices connecting to the network will likely swell, along with the number of points of connectivity for those devices. The speed at which those devices are connecting is predicted to increase, which in turn could potentially accelerate the pace at which an attack or breach takes place. This means the enterprise will need to address security on multiple fronts:

- New attacks may take advantage of 5G speeds. Security must take advantage of virtualization and automation to deploy countermeasures immediately at the point of attack.
- 5G creates a widely distributed network topology that will eventually be accessed by an unprecedented number of devices, some of them robotic rather than human-driven. Enterprises cannot rely on manufacturer-driven device certification to keep bad actors off the network. The enterprise will need to take a more active role in device authentication and authorization.

Conclusions cont'd.

- Enterprises will need to become more rigorous in identity and access management, given the eventual flood of mobile devices connecting to the network from unpredictable locations.
- DDoS attacks remain a threat and could potentially intensify under 5G. A network service provider can be a helpful partner in absorbing volumetric attacks.
- 5G has the potential to expose new types of vulnerabilities in the network. Enterprises will need to augment threat intelligence with machine learning and automated remediation in order to combat new forms of attack.
- The complexity of 5G security will encourage a shared responsibility model between the network service provider and the enterprise.
- MSSPs can serve a critical key role in helping companies in their transition to 5G. Whenever businesses face rapid innovation, change, and complexity, the MSSP can help minimize the obsolescence of technology that an organization procured too early in the innovation cycle.

Final thoughts

5G promises exciting new possibilities for the enterprise. It will also bring new security risks. Prudent organizations are taking a proactive stance by anticipating the security requirements that will come with the new technology. Creating a security posture that is ready for the speed and threat surface of 5G means understanding the potential for new threats and putting up the right tools for a solid defense.

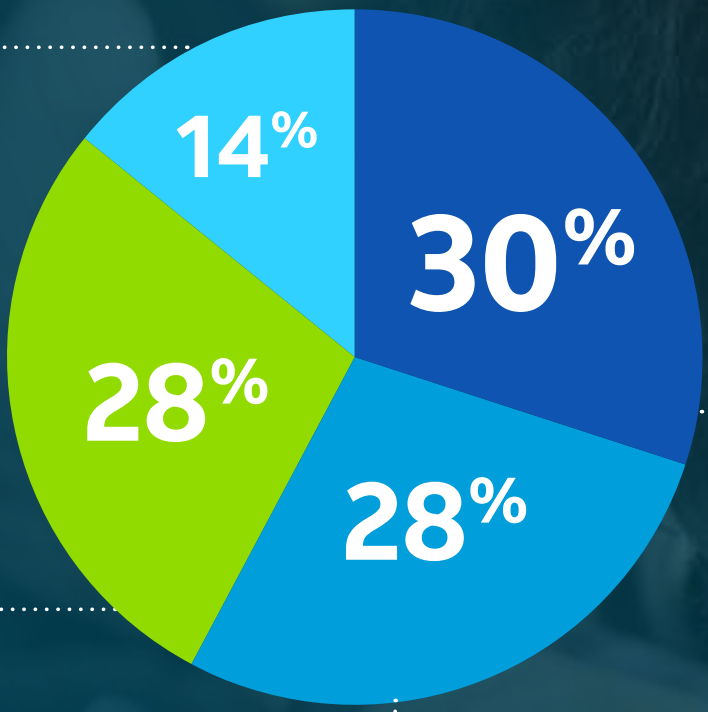
The survey results in this report reveal that organizations need to do more to prepare their cybersecurity for 5G. Key among these preparations are virtualization, automation, and software-defined networking; enhanced measures for identity and authentication; continuously updated and globally-informed threat intelligence; shifting functions to managed security services; and preparing your security posture now while 5G is still in its early stages of deployment.

Ultimately, the future of 5G can be even more promising with the right, edge-to-edge cybersecurity approach.

Appendix

Respondent Demographics

Demographics - Country



Australia

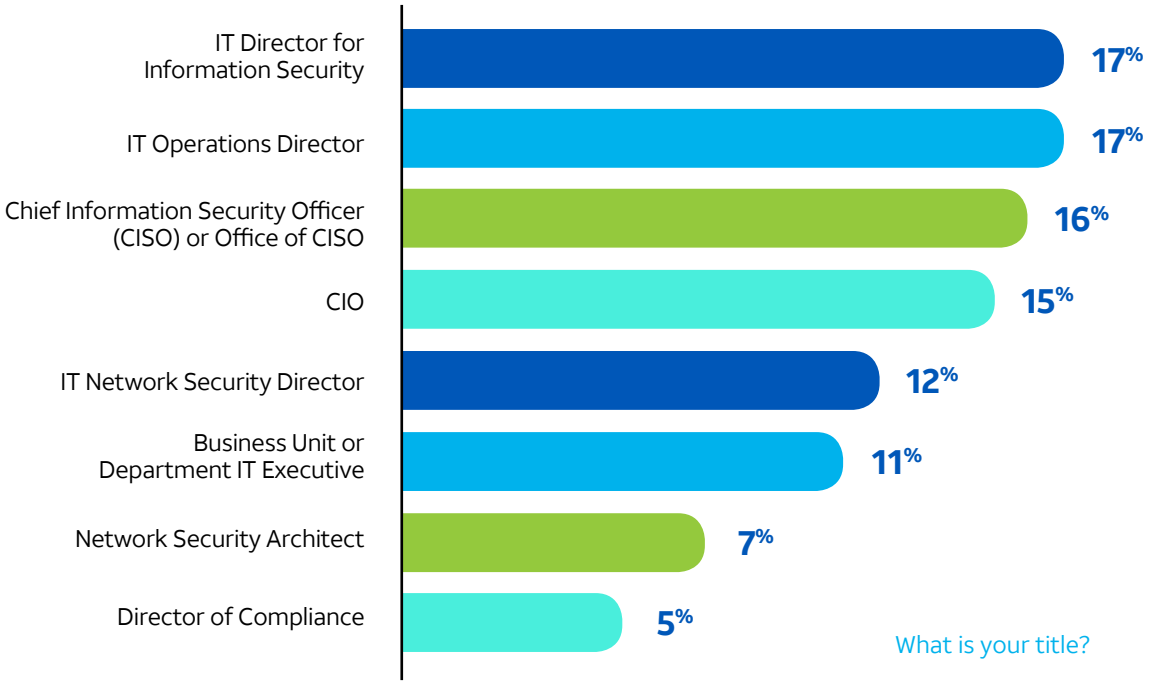
North America (US & Canada)

UK

India

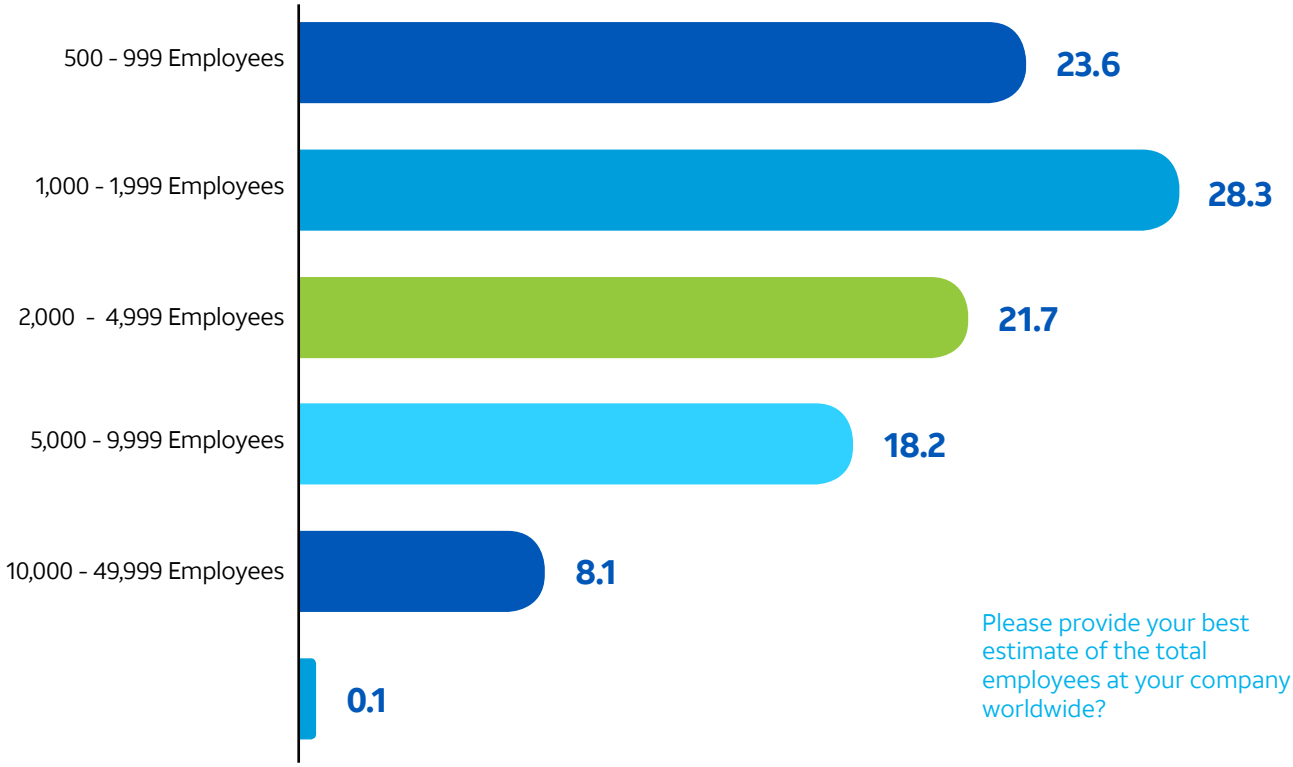
What country are you located in?

Demographics - Job Title



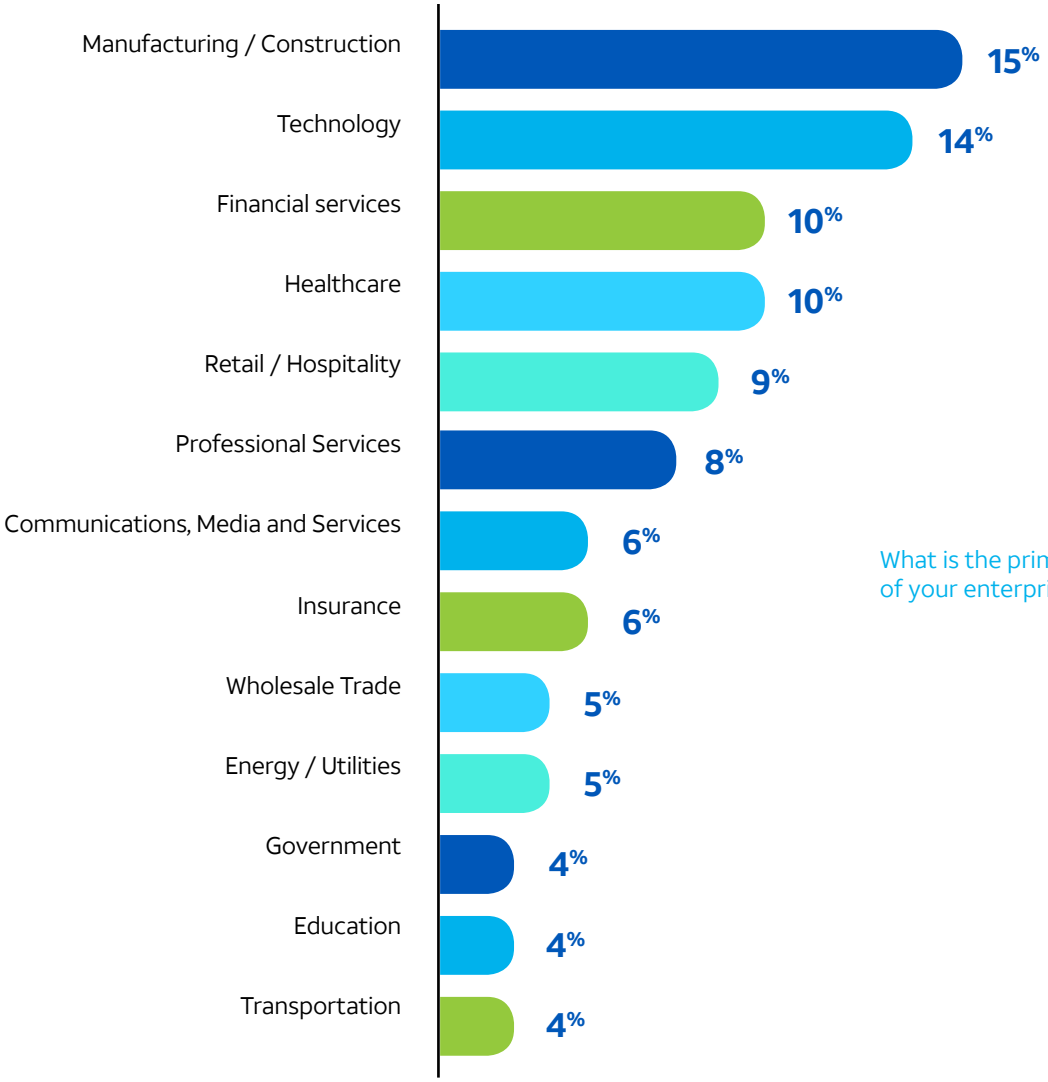
What is your title?

Demographics - Company Size



Please provide your best estimate of the total employees at your company worldwide?

Demographics - Vertical



What is the primary business of your enterprise?

Acknowledgements

To publish a report of this magnitude, we rely on a team of contributors from AT&T and within the global cybersecurity industry. We would like to thank everyone who gave their time, energy, and industry knowledge to the success of this publication. This includes the 704 security practitioners who participated in the report research, subject matter experts who provided insight into the future of 5G, and the writers, editors, designers, and project managers who shepherded the report from initial research through completion.

Authors and contributors

AT&T Cybersecurity's edge-to-edge technologies provide outstanding threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs™ researchers, security operations center (SOC) analysts, and machine learning – helping to enable our customers around the globe to anticipate and act on threats to protect their business.

Alien Labs delivers continuously updated threat intelligence to the cybersecurity products and services our customers trust to help protect their business. Alien Labs includes a global team of threat researchers and data scientists who analyze one of the largest collections of threat data in the world to provide powerful insight into adversary tactics, techniques, and procedures (TTPs). By identifying and understanding the behaviors of adversaries (and not just their tools), Alien Labs helps power resilient detection of and protection against threats, even as attackers change their approach or an organization's IT systems evolve.

AT&T Chief Security Office™

The Chief Security Office (CSO) and its comprehensive programs are dedicated to the protection of both our network backbone and our enterprise. The CSO maintains a global security organization comprised of more than 700 security professionals, and more than 1,400 additional security specialists across AT&T. These additional specialists work closely with the CSO to address department-specific issues and help secure their respective areas. The CSO supports a broad range of functions from security policy management to security solutions. Additionally, the group reviews and assesses our security control posture to keep pace with industry developments and to satisfy regulatory and business requirements. The CSO's technical personnel work in partnership with other AT&T business units to evaluate threats, determine protective measures, create response capabilities, and assess compliance with security best practices. Additionally, the audit committee of the AT&T Board of Directors oversees the company's risk management strategy, which includes cybersecurity and defense of our network. The Board and the Audit Committee receive regular updates on network and data security and the associated risks.

Visit us at AT&T Cybersecurity

AT&T Business