

AT&T CYBERSECURITY INSIGHTS™ REPORT

ELEVENTH EDITION

2022



AT&T Cybersecurity

2022 SECURING THE EDGE

AT&T CYBERSECURITY INSIGHTS™ REPORT

ELEVENTH EDITION

2022

Making it Safer to Innovate

The 2022 AT&T Cybersecurity Insights Report: **Securing the Edge** is the third in a series. Previous reports are **5G and the Journey to the Edge** and **Security at the Speed of 5G**. View and download all reports [here](#).

The AT&T Cybersecurity Insights™ Report is an annual research report published by AT&T Cybersecurity. Currently in its eleventh 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	2
Introduction	3
The State of Edge	4
Edge Risk	13
Edge Networks and Components	18
Cybersecurity Controls	20
Investments in Edge Use Case Cybersecurity	30
Cybersecurity Controls Benefit-Cost Analysis	37
Conclusion	41
Appendices	42

EXECUTIVE SUMMARY

Edge means different things to different people, and vendors are defining edge according to their technology stacks. The ambiguity complicates security decisions. If this sounds familiar, it is. Consider what happened when cloud first emerged. Cloud was a momentous shift in IT and security, and so is edge, which moves computing from a centralized model to a decentralized model. The change is occurring in these motions:

- Away from datacenter consolidation
- Toward further distribution across cloud
- Toward placement of infrastructure, applications, and workloads closer to where data is generated or consumed

Decentralization moves operations away from “lights on” monolithic applications to “thing enabled” computing experiences that are fully democratized. In the near future, expect to see small, high-quality, ephemeral, data-focused applets that live at the edge.

A proactive stance on security best serves enterprises that are innovating at the edge. The stakes are too high for reactionary security decisions or security controls prescribed based primarily on past experiences or practices. Sensors and data are everywhere, and networks are always available.

Edge networks are being implemented for specific use cases to help drive business. A useful approach for decision makers is to think about this transition through the lens of security, risk appetite, innovation goals, and network strategy — considerations that carry forward from previous AT&T Cybersecurity Insights reports. In *5G and the Journey to the Edge*, for example, 56% of survey respondents said they understood that 5G will require a change to their security approach to accommodate network changes. In this report, respondents weigh

in on security controls and anticipated investments within the chosen edge network, the associated risk, and benefit-cost considerations.

KEY TAKEAWAYS

Business leaders who are evaluating alternatives and making edge security decisions will benefit from understanding the following context:

- Edge network definitions are in flux. It's more important to think about the essential characteristics of an edge network:
 - A distributed model of management, intelligence, and networks
 - Applications, workloads, and hosting closer to users and assets that are generating or consuming the data, which can be on premises and/or in the cloud
 - Software defined
- Edge is driving a distributed architecture in terms of applications, connectivity, and networking. Ideally, architecture is resilient – continuous, automated, and seamless. But this doesn't mean rip and replace. A hybrid approach that includes legacy cellular, 5G, wireless, and cloud makes sense for the foreseeable future.
- Edge use cases are plentiful and varied throughout industries and geographic regions. Survey findings indicate surprising momentum, despite considerable perceived risk of deploying and securing edge computing. Each industry will have multiple types of edge, and workloads will need to adjust to different types of data flow activity. The edges and workloads call for security strategies that cross locations, platforms, and partners.

- Assume that traditional security controls, such as firewalls are still relevant, but in a different, next-generation form. Secure access service edge (SASE) is in the spotlight, and SASE is on the radar of all industries surveyed.
- Edge can bring network and security closer together. Compared with legacy security controls, edge security controls need to provide broader, more centralized visibility across the entire attack surface. Threat intelligence and threat detection and response capabilities provide the necessary macro view.
- Edge cloud-delivered security will be increasingly led by automation and artificial intelligence (AI) analysis, which directs policy and response.
- Data location and security go hand in hand. Consider both in the context of an organization's systems, strategies, compliance requirements, and risk tolerance. Consider where data is stored, where data should be stored, and how data should be protected at rest and in transit.
- Expect to invest broadly and holistically in cybersecurity controls to secure the entire network and IT systems, of which edge is increasingly a part.

SASE is in the spotlight and on the radar of all industries.

INTRODUCTION

This AT&T Cybersecurity Insights report is the third in a series that highlights the need for security in a new compute paradigm underpinned by 5G and edge. This report paints a realistic portrait of the state of edge, risk, and security based on worldwide survey data and interviews. Previous reports are *5G and the Journey to the Edge* and *Security at the Speed of 5G*.

Many organizations have gone beyond the aspirational research, planning, and proof-of-concept (POC) stages to implement edge use cases. While there are laggards in adoption, most organizations surveyed express intention to lean into edge computing in the coming years. The reasons behind the intention may be linked to findings in the previously published *5G and the Journey to the Edge* report. Respondents identified the highest-rated definitions of cellular edge and/or multi-access edge computing (MEC):

- To enable near-real-time cloud services at the edge
- To enhance data management (data privacy continues to be top of mind)
- To support latency-sensitive applications

In addition, organizational leaders envisioning the future of their businesses are parsing factors such as:

- The creation and acceleration of 5G as a new edge network choice that's designed to increase network performance and data processing by reducing latency compared to previous generations of networks
- Cost-effective growth and expansion enabled by the scalability of edge datacenters, which are smaller datacenter facilities close to the populations and IoT devices they serve (Data can be processed and analyzed locally, which improves manageability of the volume of IoT device data and

helps leverage artificial intelligence and machine learning [ML] where it's beneficial.)

- The ability to customize and pursue solutions and applications, such as energy grid monitoring and financial concierge services, that need to operate with real-time or near-real-time responsiveness
- Potential security enhancements resulting from distributed compute, storage, and applications (With fewer hops to make, data doesn't travel as far, lowering chances of interception and corruption. And security features are built into edge computing devices like MEC.)
- Cost and efficiency savings captured from lower bandwidth consumption and reduced data redundancy
- Support for local compliance requirements, privacy regulations, and data sovereignty requirements (New regulations are emerging worldwide that will influence the use of cloud or on premises for data residency. Some organizations already use edge and MEC to manage data privacy and data residency.)

The move to the cloud has been well documented for years, but the repatriation of applications to on premises isn't always examined rigorously. As edge evolves, the focus turns to where the data is being processed — this is closer to users and assets where processes exist. Edge adoption may indicate a transition of trust zones between and among datacenters and server farms. A proscribed edge to one environment is often met (in the middle of the processing environment) by an edge of the next environment. The potential consequences of moving to the edge, away from back-office IT operations to complex, hybrid network environments that involve multiple technologies and players, call for expertise and experience

with not only edge computing but also cloud and security controls.

Many more edge network projects are underway — and even completed — than one might anticipate. Many edge use cases are partially or fully implemented across industries and geographies using diverse network environments and security controls. The high number of partially implemented projects lends credence to the volume of use cases expected to be in production in three years.

This report presents:

- A perspective that recognizes the essential characteristics and key differences of edge networks and provides a realistic picture of the state of edge — guidance that is more useful than definitions
- An opportunity for decision makers to think differently about edge network and edge security strategies and plans (taking into account peer experiences and instances when perception and reality may not match)
- Insights into edge network architecture, perceived risk, security controls, and perceived benefit-cost analysis of security controls
- Recommendations to help secure assets at the edge

THE STATE OF EDGE

Edge networks continue to gain adoption. After all, edge networks are associated with the promise of 5G technologies, which drive the opportunity for low latency, high bandwidth, and massive machine environments. With edge network adoption comes a transition in data accessibility, agility, scale, and user/customer access — a change that can enable innovative use cases and business differentiation. But new and different risks also are part of the transition, and decision makers need to determine how to address them.

Organizations in all industries are forging ahead with use cases despite perceived risk for several reasons. The most important reason may be they don't have a choice. Critical thinking about edge security and edge networks takes into account:

- **Stiff competition in a global marketplace.** Enterprise survival depends on remaining competitive and meeting user and customer expectations.
- **Changing business models.** Board members and executives want change because they recognize that traditional infrastructure strategies won't carry their organizations into the future.
- **Rethinking operating and infrastructure strategies.** For many organizations, this story began in recent years and involves 5G and Zero Trust. In last year's *AT&T Cybersecurity Insights Report*, 94% of survey respondents said they were on a Zero Trust journey, including research, implementation, and completion. In addition, 57.7% of survey respondents were adopting 5G architecture at the time of the survey to remain competitive. Edge networks and security at the edge are the next chapter of the story.

- **Use case commonalities and variabilities by industry.** The findings in this report point to significant variability. The numerous approaches to edge networks and security controls combined with a lack of clear trends indicate an immature market. The lack of industry consensus confirms that edge is still emerging.
- **Managing stakeholder expectations.** Lines of business and IT appear to be working together on security spending and prioritizing ways to satisfy the needs of both groups. But given the number of players involved in edge implementations, anticipate the need to set realistic expectations.

The summary of security concerns and spending, the shared security responsibility model, edge network use case adoption, and the impact of 5G, presented in the sections that follow, gives enterprise leaders a realistic state-of-the-edge view.

SECURITY CONCERNS AND SPENDING ON USE CASES

Meaningful conversations about security at the edge encompass specific network environments, components, security controls, and risk. Decision makers are pondering this mix as they forecast security investments related to their use cases.

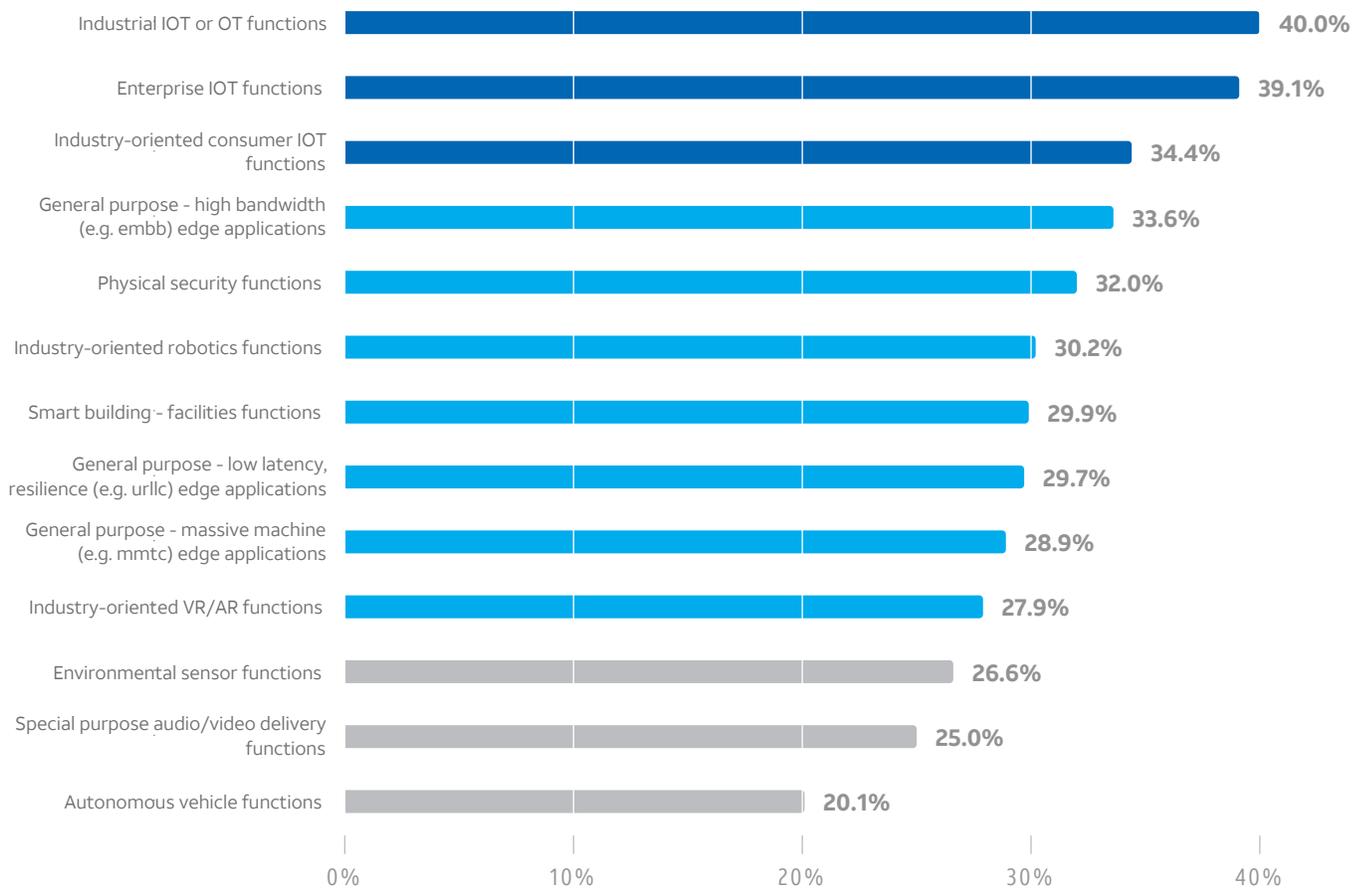
Survey respondents express concern about all attack vectors listed in the survey. More than two-thirds of respondents rate the likelihood of compromise and the impact of compromise a four on a scale of one to five (highest). Ransomware and sniffing attacks are top attack concerns across all segments.

FIGURE 1
IOT AND OT LEAD FUNCTIONS LEAD

Q. Which of the following EDGE NETWORK use cases does your organization expect to be using in PRODUCTION within the next 3 YEARS?

% of respondents

General Use Cases Expected to be in Production Within Three Years



N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

Edge computing brings cloud into the equation, which means that shared security responsibility becomes more important. Cloud providers will need to solve more security requirements.



WHAT IS MEC?

Edge computing devices come in many shapes and sizes because edge computing devices are purpose built. Edge computing devices have in common their support for data processing above and beyond current cloud capabilities. Multi-access edge computing (MEC) is essentially a computer and cellular network architecture that brings real-time, high-bandwidth, low-latency access to latency-dependent mobile applications. MEC works with LTE or 5G and connects with cloud service providers. MEC also can be deployed in the cloud.

Survey findings reveal a lack of agreement associated with traditional total cost of ownership (TCO) versus effectiveness of security controls. Respondents were asked what percentage of their organization's total combined investment will be in security for all use cases to be in production within three years. Overall regional and industry responses indicate that:

- 7% or less of respondents expect to invest 1–5%
- 29–42% of respondents expect to invest 6–10%
- 40–55% of respondents expect to invest 11–20%
- 8–17% of respondents expect to invest 21% or more

IT and line-of-business respondents are similar in their spending plans, which supports the notion that these groups are in sync or at least communicating and aligning their edge deployment spending.

THE SHARED SECURITY RESPONSIBILITY MODEL

Similar to the shared security responsibility model used in cloud computing, 5G and edge computing also demand shared security responsibility, as discussed in the *5G and the Journey to the Edge* report. In fact, the shared responsibility model is more relevant than ever because edge brings in a third component. Responsibilities for cybersecurity are spread across public cloud service providers (SPs), carriers, and enterprises.

Enterprises are responsible for securing their devices and endpoints and the data within them. Ideally, enterprise security includes the latest identity access management and data protection technologies, as well as methods of securing on-premises equipment used for MEC. 5G network operators are building security into their networks to protect data sent over 5G radio access networks (RANs).

EDGE NETWORK USE CASE ADOPTION

This report explores both general cross-industry use cases and industry-specific use cases. Figure 1 lists the general use cases that organizations expect to be in production within three years. In the survey, industrial IoT (IIoT) or OT leads, followed by enterprise IoT and industry-oriented consumer IoT. This finding makes sense because IoT in a broad sense is the application or use case that generates the data that's moving around the edge.

The study also examines six stages of edge compute adoption (ideation, research, planning, POC, partial implementation, and full implementation) in six industries and industry-specific use cases. For simplicity, the six stages are conflated to three:

- **Low stage:** Ideation and research
- **Mid-stage:** Planning and proof of concept
- **Mature stage:** Partially implemented and fully implemented

For ease of readership, this report focuses on the top two stages. Implementation stages are fluid, however, given the ongoing evolution of edge and the introduction of new standards, regulations, and ancillary use cases. Given this reality, “full implementation” may be transitory.

Figure 2 shows the distribution of edge use cases across implementation stages by industry that are expected to be in production within the next three years.

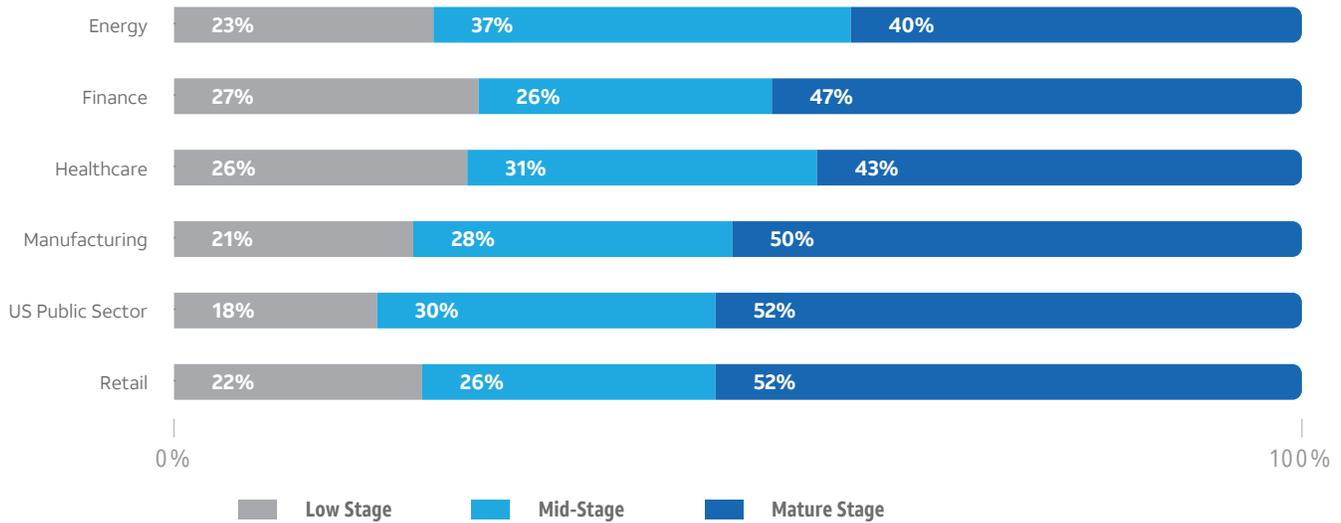
Partially implemented use cases are the most prevalent, a finding that reinforces the observation that edge is making its way across industries. When partially and fully implemented use cases are combined, public sector and retail lead, followed by manufacturing and finance. The energy and utilities industry is notable for leading with projects in the planning stage.

Some industries are farther along than others. Over two-fifths of the surveyed population are in the mature stage of adoption. The remaining three-fifths are split disproportionately, with more in the mid-stage. The highest adoption rate occurs in both retail and public sector, with just over half of the respondents stating they are in the mature stage.

FIGURE 2
RETAIL AND PUBLIC SECTOR LEAD EDGE NETWORK ADOPTION

Q. You indicated your organization expects to be using the following EDGE NETWORK use case(s) in PRODUCTION within the next 3 YEARS. What stage is your organization currently at in the deployment process for each of these use cases?

% of respondents



N= 1520

BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

Note: Due to rounding, data will not always equal 100%.

TABLE 1
HIGHEST USE CASES IN MID AND MATURE STAGES

Q. You indicated your organization expects to be using the following edge network use case(s) in production within the next three years. What stage is your organization currently at in the deployment process for each of these use cases?

*Highest use cases overall in the mature stage

	Mid-Stage of Adoption: Planning and POC	Mature Stage of Adoption: Partially Implemented and Fully Implemented
Energy/Utilities	Video-based site surveillance/inspection	Remote control operations
Finance	Real-time fraud prevention	Concierge services
Healthcare	Hospital at home	Consumer virtual care
Manufacturing	Augmented maintenance	Video-based quality inspection*
US Public Sector	Research and Development within Higher Education	Public Safety and Enforcement*
Retail	Real time inventory mgmt.	Loss prevention*

EDGE SECURITY X HEALTHCARE

In healthcare, 74% of respondents globally are planning, have partially, or have fully implemented an edge use case.

TOP USE CASE

The consumer virtual care use case, also known as “care anywhere,” ranks highest within the healthcare industry for full or partial implementation. Though the use case has an average perceived risk, it also has the highest perceived impact from an attack.

EDGE ADVANTAGE

Initiatives span care provided in non-traditional settings such as remote clinics to remote health monitoring of patients. Virtual care services surged during the pandemic, as they are convenient for consumers and help reduce healthcare costs by providing care in settings such as patients’ homes. Technology and human risk intersect due to increased perceived risk of discontinuity of care, data fragmentation, data silos, and inaccurate quality reporting.

SECURITY CONTROLS

Healthcare respondents rank intrusion and threat detection, multi-factor authentication, data encryption at rest, and endpoint and device monitoring as the most efficient and effective security controls at their disposal.

SURVEY INSIGHT

63%

of respondents in healthcare perceive attacks against associated cloud workloads as the most likely objective of an attack



EDGE SECURITY X FINANCE

In finance, 73% of respondents are planning, have partially, or have fully implemented an edge use case.

TOP USE CASE

The concierge services use case ranks highest for full or partial implementation in the finance sector. Respondents indicate a higher concern of cyberattack impact for concierge services compared with other finance use cases but it is not the highest perceived risk overall.

EDGE ADVANTAGE

The importance of concierge services is being driven by demand, with financial services companies increasingly nurturing high-touch, personalized relationships that can increase wallet share by improving customer experience and potentially increasing trust, engagement, and loyalty. The use of advanced technologies alongside edge network environments can enable the delivery of real-time advice to customers.

SECURITY CONTROLS

Finance respondents rank external traffic encryption at a gateway or proxy, data encryption at rest, firewall at the network edge, and application proxy (e.g., secure web gateway, CASB, etc.) among the most efficient and effective security controls at their disposal.

SURVEY INSIGHT

69%

of respondents in finance perceive sniffing attacks against user endpoint devices and components (user to the radio access network, RAN) as the most likely attack vector.



Manufacturing follows retail in the survey, with a surprising 50% of respondents in the mature stage of adoption. Energy and utilities has the lowest representation, 40% of respondents, in the mature stage. And 60% of energy and utilities respondents are in the low mid-stage of adoption.

Globally and across industry use cases, loss prevention in retail and video-based quality inspection in manufacturing have the highest rate of mature stage adoption (59%), which is higher than retail and public sector overall. Within the US public sector, public safety and enforcement (gunshot detection and surveillance) garnered the highest representation, 70% of respondents, in the mature stage. Table 1 summarizes the highest percentage of use case adoption in each of the three stages.

IMPACT OF 5G

5G is nascent but having an impact.

Organizations aren't focusing exclusively on 5G at the edge. Instead, 5G is viewed as a driver, but in the context of a hybrid model. No enterprise will be 100% 5G. 4G/LTE will be part of the edge mix, especially in rural areas, for the foreseeable future.

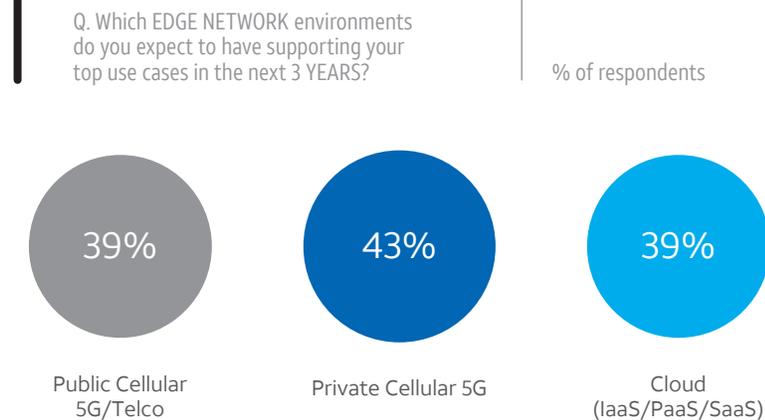
Of the 5G environments considered in the survey, private 5G is the largest network environment, followed by public cellular 5G (see Figure 3).

The top 5G use cases are being built on general-purpose computers, individual devices, and MEC. There is a likelihood that respondents believe they are using 5G today, when in actuality they're toggling between 4G and 5G for the edge use case they're implementing. A manufacturing plant, hospital, or stadium may be using 5G locally, but 5G standalone may not yet be possible when data is sent beyond the four walls of a building or when an edge use case involves moving data in smart cities or transportation scenarios. As 5G evolves, use cases will be more fully supported by 5G where 5G is relevant and advantageous (e.g., enabling data not to "hairpin" back to the datacenter or point of origin).

One of the greatest 5G security concerns relates to the vast number of connected IoT devices that will process enormous amounts of data. 5G speeds and low latency mean communications

FIGURE 3

PRIVATE 5G IS THE LARGEST PLANNED EDGE NETWORK ENVIRONMENT



N= 1520

BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

happen in near real time. Lagging security and a historical lack of or insufficient level of built-in device security and simple authorization controls increase vulnerability.

As 5G evolves, the firewall will connect to the network control plane with an additional interface that enables the firewall to recognize devices and provide the identities of those devices. In LTE, the identity is unencrypted and therefore vulnerable to attack. In 5G, device identifiers will be encrypted and therefore can provide greater trust.

Imminent 5G innovation — standalone core — will help accelerate edge adoption. But standalone core depends on a parallel effort: manufacturers producing and enterprises adopting devices that can access 5G. The timing of this effort will influence the pace of adoption.

Today, edge use cases are being built based on enterprise experience and familiarity, such as using legacy technology components. Autonomous mobile vehicles and robots are coming, but they are further out than use cases built on individual devices and general-purpose computers. The combination

of 5G standalone and the buildout of 5G infrastructure globally will enable enterprises to realize the predicted hyperconnectivity. Many use cases that today are considered too expensive, too risky, or technologically impossible will be within reach. As standalone core and infrastructure buildout are realized and security requirements are understood, use case diversity will flourish.

EDGE RISK

EDGE RISK: BY INDUSTRY

Each industry has multiple types of edges (see Figure 4). The enterprise, device, cloud, telco, and industrial edges may be more familiar than tactical edge, which refers to short-term, often emergency or critical services such as Red Cross disaster relief. These use cases need edge resources capable of operating in harsh environments with resilience and reliable security.

Edge IT is diverse, distributed, and largely unattended:

- Locations include cloud service providers, colocation providers, and settings such as operations, field, and remote offices.
- Partner coordination is required with telcos, communications service providers, cloud SPs, systems integrators, hardware and software providers, and others.
- Edge IT runs on various compute architectures such as hyperconverged infrastructure (HCI), standard x86, cloud IaaS and PaaS, and bare metal.

Security strategies will vary depending on edge type and because workloads will need to adjust to different types of data flow activity. For example, physical protection, monitoring, and intrusion control will differ for industrial edge and device edge workloads. As edge use cases mature and industries place more dependence upon these edge resources and workloads, business risk increases with any gaps in service or downtime.

Edge risk is clearly on the minds of survey respondents. Figure 5 shows all use cases studied by industry and their perceived risk as determined by expected frequency and impact of cybersecurity attacks.

FIGURE 4
EDGE TYPES

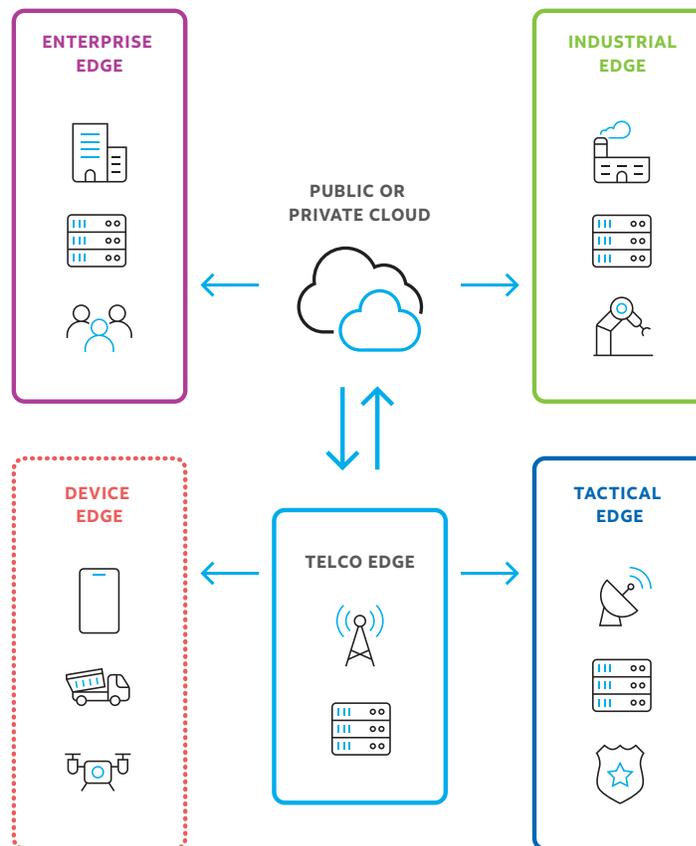
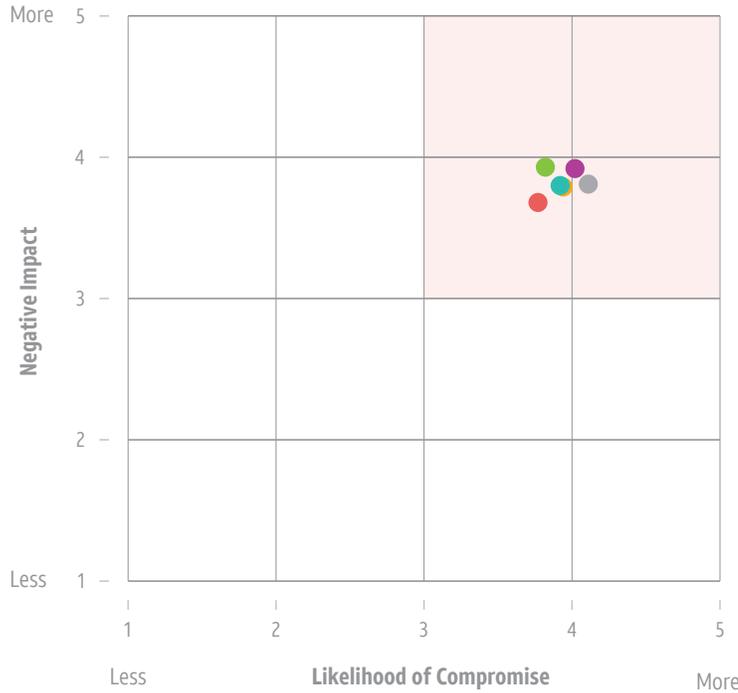


FIGURE 5
EDGE RISK IS FELT BY EVERYONE

Perceived Edge Risk by Industry

Scale of 1-5



Q. For each of the use cases your organization expects to be using in PRODUCTION within the next 3 YEARS, please assess your LIKELIHOOD OF COMPROMISE, taking into consideration the technical architecture, volume of activity, number of devices and network locations, and any other pertinent information. (Scale: 1=Very Low Likelihood; 5=Very High Likelihood.)

Q. For each of the use cases your organization expects to be using in PRODUCTION within the next 3 YEARS, please assess the IMPACT that a successful compromise would have, considering the lost value, incident costs, downtime, damaged reputation, and any other pertinent information. (Scale: 1=Very Low Impact; 5=Very High Impact.)

- Energy and Utilities
- Manufacturing
- Finance
- US Public Sector
- Healthcare
- Retail

N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

A look at perceived risk on a 1–5 (1 is lowest / 5 is highest) scale by industry confirms that respondents are concerned about security as they move to the edge. Respondents from all industries perceive greater than average risk, but the value of the scores lies in interpreting them relative to each industry. Retail and energy and utilities have the highest perceived risk across the six industries studied.

Retail is more concerned with the impact of cyberattacks than the frequency of attacks, perhaps because this industry has seen very large public attacks, such as the largest retail breach of 2014, that negatively impacted brand. Retail also is highly regulated by the Payment Card Industry Data Security Standard (PCI DSS). Retail and finance were early adopters of digital technology even before COVID-19.

The pandemic accelerated the need to engage customers virtually and provide enhanced digital customer experience (CX).

Healthcare has the lowest perceived risk across the six industries but still is above the midline. Healthcare has experienced both frequency and impact of cyberattacks through ransomware in recent years. The US public sector sees

higher potential frequency and impact of attacks than healthcare. The US executive order of May 2021 has elevated an understanding of cybersecurity requirements, and this may explain the risk expectation.

Finance and manufacturing cluster in the center of both impact and frequency of cyberattacks. Finance is no stranger to cybersecurity risk, and the middle placement of risk perception may be influenced by the industry's relatively high cybersecurity maturity. Banking and insurance understand fraud as well as material and logical risk. They've had cybersecurity controls in place longer than any other industry. Manufacturing is newer to digital environments and the coming together of IT and OT (operational technology) is a well-known challenge. At best, manufacturing is immature in cybersecurity, yet perceived risk is relatively lower than it is for retail and energy and utilities.

The descriptions of industry use cases in the sections that follow reveal expected risk nuances within each industry.

ENERGY AND UTILITIES

Energy and utilities and other critical infrastructure environments have been slow to adopt digital technologies until recently. The *remote control operations* use case is not the highest perceived risk, but the use case is higher than average and is the most mature in adoption in energy and utilities. Software for remote operations can enable industrial organizations to adopt remote staffing, centralized and flexible resourcing, and autonomous operations. Edge will accelerate autonomous operations.

FINANCE

Concierge services, provided by a financial advisor or concierge, is the most mature use case in adoption within finance. Concierge services isn't perceived as the lowest risk use case, but its importance is driven by customer demand. Concierge services indicate higher concern of cyberattack impact compared with other finance use cases but not the highest perceived risk overall. Respondents report higher-than-average potential risk, but

the rewards likely outweigh the perceived risk. Concierge services promote high-touch, personalized relationships that can increase wallet share by improving customer experience and potentially increasing trust, engagement, and loyalty. The use of advanced technologies alongside edge network environments can enable the delivery of real-time advice to customers.

MANUFACTURING

Video-based quality inspection is one of the lowest in perceived risk and also the highest in adoption. Human quality control (QC) operators are skilled at finding many kinds of visible and audible defects from inspection during video playback. But human QC doesn't scale well considering the large number of files and formats typically found in a modern workflow. Scale is especially challenging when adaptive streaming video packages are involved. Human inspection also is inherently subjective. What allows for scale across multiple, global facilities is the deployment of specialized AI models. These are possible as a result of the reduced bandwidth, lower latency, and proximity of data in edge computing that uses AI and IoT-driven automation. Perceived risk may be lower because machine-enabled quality inspection reduces cognitive hacking (unintended or malicious cognitive influence during visual inspection).

RETAIL

The *loss prevention* use case is adopted at a higher rate than other retail use cases, and it is perceived as a lower-than-average risk. This makes sense because loss prevention has been used in retail for a long time. As retailers build loss prevention at the edge using advanced cognitive tools, the use case will benefit from big data analytics and real-time video analytics to move it from reactive, where it identifies a loss, to proactive and preventative. Loss prevention also enhances key performance indicators (KPIs) by preventing inventory loss, discount abuse, pilferage, shoplifting, theft, and return fraud.

Manufacturing is newer to digital environments and the coming together of IT and OT is a well-known challenge.

Ransomware is perceived as the top objective of attack in all industry segments. Asia and South Korea are the most concerned region and country.

HEALTHCARE

Consumer virtual care, also known as “care anywhere,” has the highest perceived impact from an attack of all healthcare use cases. Cybercriminals have discovered that healthcare is a viable target for ransomware, protected health information (PHI), and payment information from health records. This use case is very close to the average perceived risk within the industry, and it is also the most mature in adoption. Initiatives span care provided in nontraditional settings like retail clinics to remote health monitoring of patients. Virtual care services surged during the pandemic. Virtual care services are convenient for consumers and help reduce healthcare costs by providing care in settings such as patients’ homes, which is a less expensive option than hospitals. Technology and human risk intersect due to increased perceived risk of discontinuity of care, data fragmentation, data silos, and inaccurate quality reporting.

US PUBLIC SECTOR

The use case farthest in implementation, *public safety and enforcement* (gunshot detection and surveillance), is about average in perceived risk. Perhaps this is because gunshot detection technologies have been used for many years and still include human verification, which can raise concerns about data validity. *Automation of public services* is second in adoption maturity and has a much higher perceived risk. These services use robotic process automation (RPA), chatbots, ML, AI and, in some cases, blockchain. Blockchain technology, and blockchain technologies’ inherent need for higher quality, offers many potential applications used to manage personally identifiable information (PII). Applets at the edge also require higher quality. Blockchain will serve the public sector well; however, blockchain is still in its infancy, especially with regard to security and privacy.

Latin America is concerned about attacks on servers, sniffing against the endpoint, and attacks against the endpoint or user. North America is most concerned about attacks against server/data at the network edge.

Threats emerging from a particular component aren’t one dimensional. A component opens up the threat vector to the rest of the network.

EDGE RISK: MOST LIKELY ATTACK VECTORS

Respondents are concerned about all attack vectors offered as options in the survey. Across all use cases, 74% of respondents say the likelihood of compromise is 4 or 5 (5 is very likely). EMEA and Latin America are less concerned across all attack types than North America and Asia.

Ransomware was rated highest in concern. Ransomware is perceived as the most likely objective of attack overall across verticals and regions. Ransomware is rated highest by energy and utilities (75%) and the lowest by healthcare (62%).

Sniffing attacks against the RAN landed in fourth position overall (65%), with energy and utilities most concerned (80.5%). The lowest rated perceived attack vectors (tied at 61%) are distributed denial of service (DDoS) against the RAN and attacks against the MEC.

Table 2 shows which attack types are of highest concern to each industry.

Within industries, the least worrisome are supply chain attacks, attacks against 5G core (telco), physical attacks, DDoS attacks against the RAN, and attacks against MEC, although these are highly represented overall. Since supply chain attacks enable other attacks, supply chain isn’t always thought of as a standalone attack vector. If the goal is exfiltration of data at the edge, supply chain attacks often are a conduit to ease that exfiltration.

Whether perceived risk is viewed by likelihood of frequency and impact or attack vector, respondents across regions and industries express concern to varying degrees. This reality validates the need for discussion and decisions about cybersecurity controls as a core part of edge adoption.

TABLE 2

RANSOMWARE CONTINUES TO BE A TOP CONCERN

Q. In your opinion, how likely are the following attack vectors? (Scale: 1=Very Unlikely; 5=Very Likely.)

% of respondents

Attacks of Highest Concern by Industry

	Total	Energy and Utilities	Finance	Healthcare	Manufacturing	Retail	US Public Sector
Ransomware	66.1	74.5	63.3	61.8	69.4	61.6	65.7
Attacks against user / endpoint devices	65.5	68.9	64.8	59.8	71.3	65.2	62.9
Sniffing attacks against the radio access network (RAN -> Core)	65.5	80.5	67.2	56.3	65.9	58.4	64.5
Attacks against server / data at the network edge	65.5	68.9	62.5	63.8	65.9	62.8	68.9
Sniffing attacks against the endpoint (user) devices and components (User ->RAN)	64.5	70.5	68.8	57.9	65.1	59.6	64.9
Attacks against associated cloud workloads	63.7	68.9	60.5	63.4	64.7	59.2	65.3
Attacks against applications at the network edge	63.3	69.3	57.8	59.4	65.9	58.8	68.5
Supply chain attacks	63	69.7	58.6	60.2	64.7	57.6	66.9
Attacks against the 5G core network (telco)	62.2	71.7	62.9	56.3	62.4	60	60.2
Physical attacks against technical components such as IoT devices, abandoned assets, etc.	61.8	70.5	62.9	57.5	63.2	54	62.9
DDoS against RAN	60.9	63.7	60.9	55.9	60.9	56.4	67.3
Attacks against MEC	60.9	66.9	62.1	53.5	62.8	54.4	65.3

N= 1520

BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

EDGE NETWORKS AND COMPONENTS

Energy and utilities' top network pick is private cellular. But energy and utilities also select public, branch office, and cloud. The public and cloud options most likely apply when: private isn't practical or affordable, spectrum for private isn't an option, or when multitenant is relevant to a use case (no highly sensitive data that requires private).

In energy and utilities, branch is a useful strategy for distributed locations such as branch offices and remote sites spread widely across distant geographies and connected by multiple networks leased from different network service providers.

Survey respondents were asked to comment on edge network environments and components expected to be part of the use cases planned to be in production within three years.

EDGE NETWORK ENVIRONMENTS

The networks chosen for edge use cases are ubiquitous across the study. These networks include public and private cellular 5G, non-5G cellular such as 4G and LTE, remote office/branch office, cloud, and both industrial and consumer IoT networks.

Private 5G and cloud garner the highest aggregate responses from survey respondents. Public 5G is a close third (see Figure 6). These findings aren't surprising since last year's report found that over 93% of respondents were researching, implementing, and completing 5G implementations and 58% believed that the cellular edge would enable near-real-time cloud services.

The cloud environment is associated with retail's omni-channel commerce use case. Industrial and consumer IoT environments rank lower than other edge network choices, perhaps because IoT has existed for a long time and specific 5G and edge requirements are still being defined.

Legacy non-5G cellular and other edge network choices also have a role in a hybrid approach. For example, remote office/branch office network is associated with the telepresence robot use case in healthcare, the automation of public services use case in the public sector, and the AR/VR training, building management, and research and development use cases in the education segment of the public sector.

Several factors influence the choice of edge network environment:

- Private cellular may be preferred to eliminate dependency on a third-party network, but private 5G still needs to interoperate with commercial 5G infrastructure. Organizations acquire critical infrastructure, and those that transport highly sensitive data need the option of owning their own infrastructure and maximizing control over their data.
- Other factors include existing communications infrastructure, urban or rural locations, regulations, branch offices, and public venues such as hospitals, schools, and sports arenas that require a high level of connectivity.

IT SYSTEM COMPONENTS IN PRIMARY USE CASES

Edge computing is happening close to familiar IT system components (see Figure 7). Traditional endpoints (general-purpose computers) top the list, followed by individual components (smartphones and wearables) and MEC devices. The top three types of components in use and anticipated for use appear to be selected based on "most familiar" and/or "most advertised." MEC is purpose built for the edge. By defining and promoting MEC, the European Telecommunications Standards Institute (ETSI) helped MEC become known as the route to edge with 5G.

India reports the highest number of use cases involving MEC (56.6%), and according to the survey data, India is a frequent outlier that often outpaces other countries. Millimeter wave trials, for example, have commenced in India. Perhaps a bit later than some countries, but India is making up for lost time.

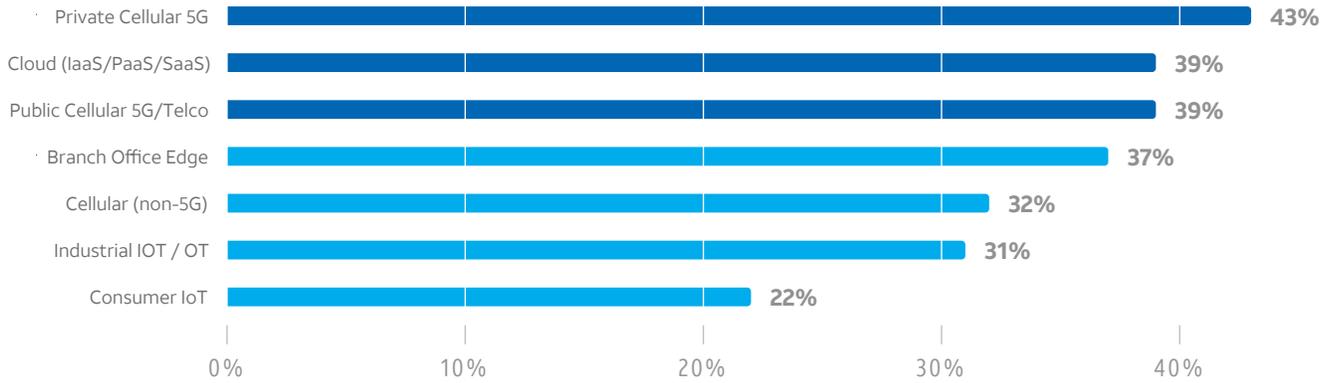
FIGURE 6

5G AND CLOUD ARE PREFERRED EDGE NETWORKS

Q. Which EDGE NETWORK environments do you expect to have supporting your primary use cases in the next 3 YEARS?

% of respondents

Networks Selected for Primary Use Cases



N= 1520

BASE All respondents

SOURCE AT&T Cybersecurity Insights™
Report: Securing the Edge - Survey, September 2021

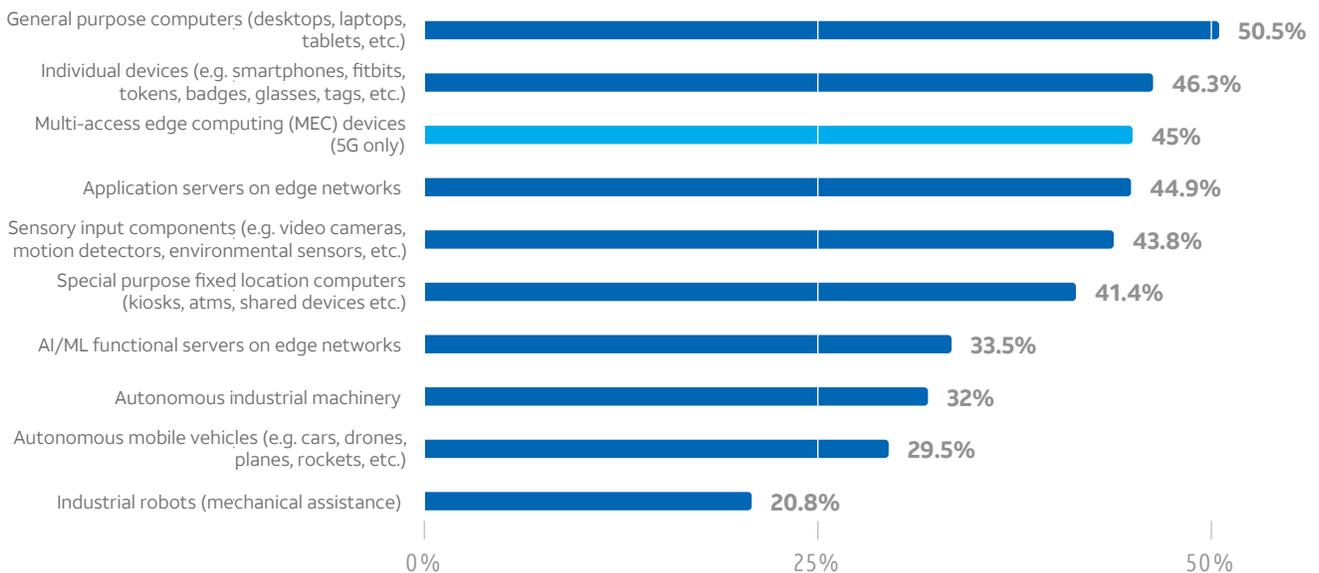
FIGURE 7

EDGE COMPUTING RELIES ON FAMILIAR COMPONENTS

Q. For your primary use case, which types of components are being/will be used? (select all that apply)

% of respondents

Components in Primary Use Cases



CYBERSECURITY CONTROLS

SASE is the new growth engine because organizations are moving from on-premises to cloud-based solutions. But certain industries may not want to route all of their data through cloud, so on-premises security solutions will continue to exist in areas such as OT.

Perhaps the most challenging task in cybersecurity is determining the selection and mix of controls to deploy based on a risk assessment. Often, there isn't a lot of directly pertinent information available to assess risk properly. The determination of potential likelihood and impact associated with a particular use case relies heavily on the experience and background of the assessors. The variability is evident in the final assessments. Likewise, there is little direct relationship between risk and security at the individual control level. Cybersecurity professionals therefore rely on experience and knowledge when they design an approach.

A common starting point involves best practices and the availability of existing security controls. Organizations often have their own cybersecurity standards to which they must adhere. But preferences for cybersecurity controls also are affected by the use case functionality and architecture, as highlighted later in this section.

As use cases develop into projects and architectures are evaluated, the networks and components are typically maintained in their own environment. Accordingly, the first decision about network edge cybersecurity controls typically focuses on determining how to apply an appropriate set of minimum controls. Decision making evolves to include broader considerations. For example, over time, security practitioners have evolved their perimeter cybersecurity architecture after debates about technology (e.g., software versus appliance) or administration

(e.g., best-of-breed single purpose or combined functions in solutions such as unified threat management [UTM]). Now cybersecurity control debates revolve around two topics: whether to deploy cybersecurity solutions on premises or in the cloud and whether to combine cybersecurity and network functionality into a single solution (see Figure 8).

The data clarifies that the days of single-function on-premises security solutions are numbered. But there is a sizable portion of holdouts (27%). Because participants were allowed multiple responses, the findings may be linked to two scenarios: organizations that have somewhat basic needs, such as branch office connectivity that backhauls network traffic, or organizations that are risk averse and have deployed highly customized technologies in their environments.

The latest developments in combined security and network solutions also may make organizations reluctant to change in the short term as the debates about on premises versus cloud and cyber versus security plus network continue, and technologies continue to evolve. The path forward in this dynamic space will be unique to each organization. Scrutiny of the environment, architecture, and use cases is vital to decisions about direction and controls.

The latest innovation in the controls arena is the secure access service edge (SASE) solution currently on the radar of many organizations across industries. SASE combines network and security capabilities in a cloud architecture, but no single vendor offers a complete SASE solution.

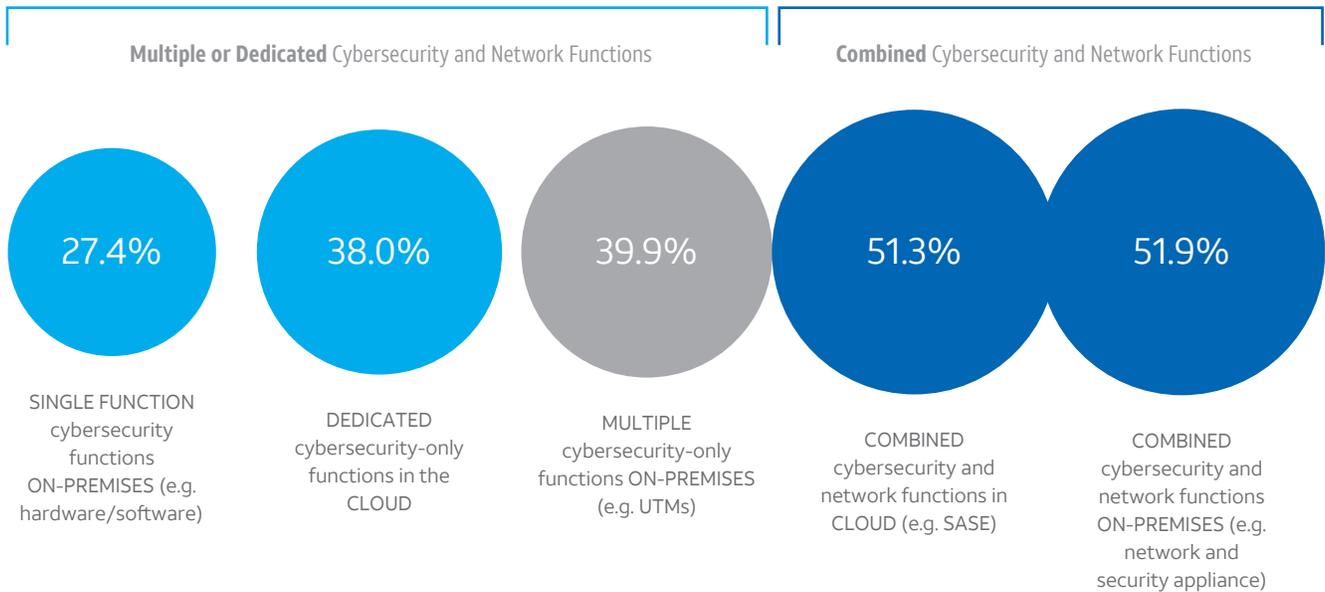
Currently, about the same number of respondents are interested in either

FIGURE 8

MANY COMPANIES ARE MOVING TOWARDS COMBINED CYBERSECURITY AND NETWORKING FUNCTIONALITY

Q. How will you implement your CYBERSECURITY functions for your primary use case?

% of respondents



N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

deploying an on-premises solution that mirrors the security plus network capabilities and/or deploying a similar solution in the cloud (SASE). In fact, from the two survey options of combined network and security in the cloud (SASE) and on-premises network plus security, SASE is preferred nearly equally by line of business and IT security stakeholders — a pointer to a potential lockstep approach. Most customer segments show a preference for SASE except for the smallest firms, which prefer SASE the least. Networking interoperability with cloud security in a multivendor environment can create challenges that will need to be solved as organizations move to SASE.

This statistical tie between on-premises and cloud-based solutions highlights an ongoing debate. But given the long head start that on premises has had, the

finding also points out the strength of the movement toward a cloud solution.

Cloud solutions can quickly negate traditional concerns about performance and bottlenecks since the architectures of cloud solutions are elastic and can be rapidly provisioned as needed. They can also be configured in many ways to address performance issues. The biggest potential downside to cloud-based solutions is lack of control. Depending on the cloud service model (IaaS/PaaS/SaaS), enterprises lose the technical freedom to architect various layers — a disconcerting situation for some decision makers, particularly those outside of the United States.

While security deployment methods currently seem to dominate discussions, the decisions about which cybersecurity controls to deploy are more important. Two types of controls are distinguishable.

First, controls “on” the edge at the ingress-egress point can be grouped into general-purpose traditional controls (firewall, virtual private network [VPN], intrusion detection systems [IDSs]), and special-purpose controls that can serve specific needs. Second, controls “in” the edge protect individual devices to fulfill a Zero Trust strategy and architecture. Figure 9 presents cybersecurity controls by network type.

EDGE SECURITY X PUBLIC SECTOR

In the US public sector, 82% of respondents are planning, have partially, or have fully implemented an edge use case.

TOP USE CASE

The public safety and enforcement (gunshot detection and surveillance) use case ranks highest in the US public sector for full or partial implementation. It has an average perceived level of risk.

EDGE RISK

Public safety and enforcement technologies have been in use for many years and still include human verification — even at the edge — which can raise concerns about data vitality. Automation of public services is second in adoption maturity and has a much higher perceived risk. These services use robotic process automation (RPA), chatbots, ML, AI and, in some cases, blockchain.

SECURITY CONTROLS

Public sector respondents in North America rank Zero Trust network access control, data encryption at rest, traffic encryption (internal to the network and external at a gateway/proxy), multi-factor authentication, and device authentication among the most efficient and effective security controls at their disposal.

SURVEY INSIGHT

69%

of respondents in the public sector perceive attacks against servers/data as the most likely route of an attack.



EDGE SECURITY X MANUFACTURING

In manufacturing, 78% of respondents globally are planning, have partially, or have fully implemented an edge use case.

TOP USE CASE

The video-based quality inspection use case ranks highest within manufacturing for full or partial implementation. It is also one of the lowest in perceived risk.

EDGE ADVANTAGE

Edge computing offers reduced bandwidth, lower latency, and proximity of data, enabling companies to efficiently deploy specialized AI-inspection models across multiple, global facilities that can handle the large number of files and formats typically found in a modern workflow.

SECURITY CONTROLS

Manufacturing respondents rank intrusion and threat detection, device authentication, and data leakage monitoring among the most efficient and effective security controls at their disposal.

SURVEY INSIGHT

71%

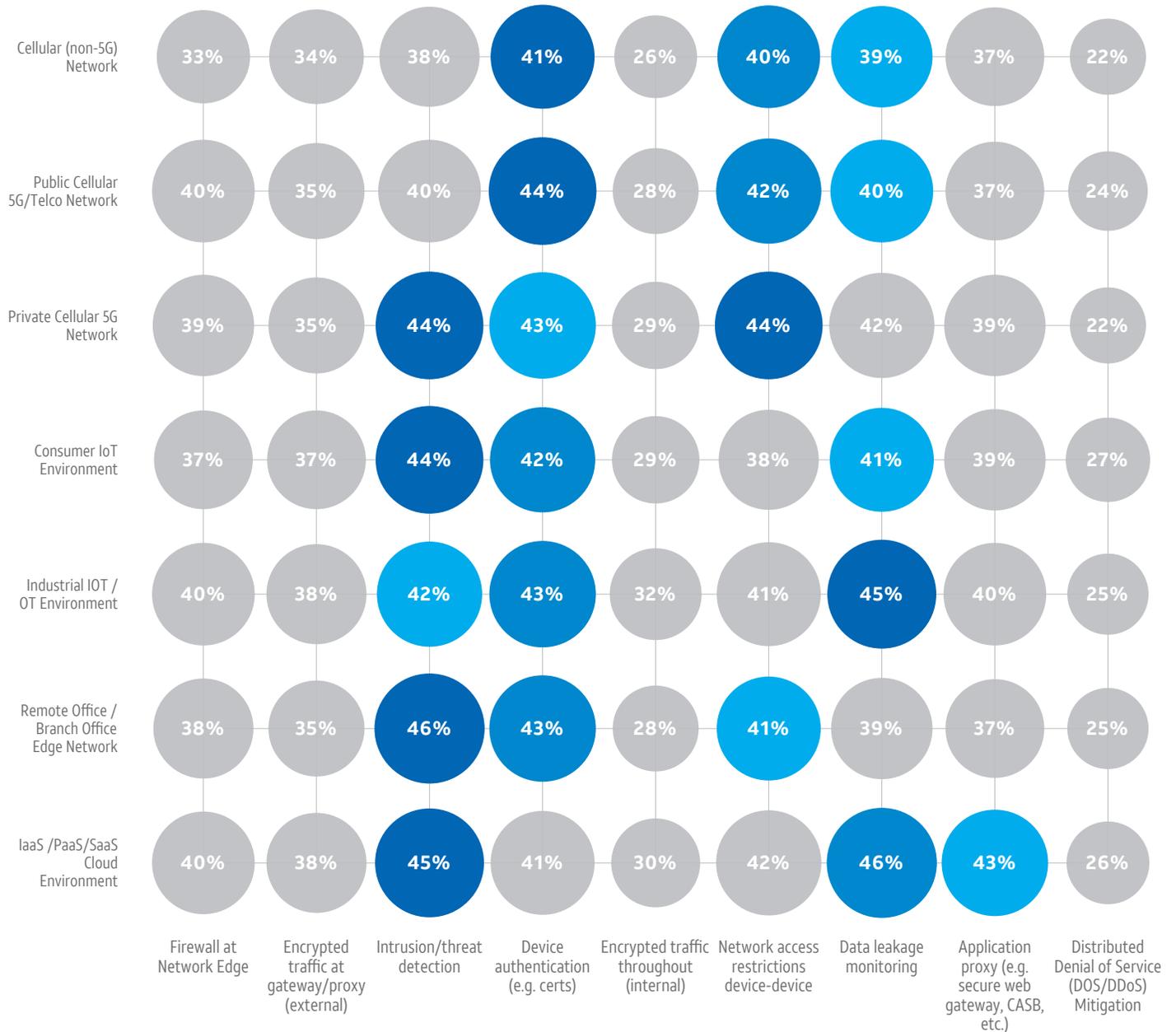
of respondents in manufacturing are most concerned about attacks against user and endpoint devices

FIGURE 9

CYBERSECURITY CONTROLS BY NETWORK

Q. Which of the following CYBERSECURITY CONTROLS will you deploy to protect the NETWORKS of your primary use case?

% of respondents



N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

CYBERSECURITY “ON” THE EDGE

When SASE and legacy on-premises solutions are combined, they have capability beyond security. The security focus of these two together revolves around:

- Traditional firewall, VPN, and IDS functionality for general cybersecurity needs
- Special-purpose functionality like data loss prevention (DLP) for privacy-oriented data
- Application firewalls for more distributed ephemeral application architectures

Legacy cellular garners the fewest number of security controls, probably due to an assumption that the proprietary technology in use by the carriers is difficult to break into. As 5G develops further, network security will become shared in the sense that cloud, network operators, and telcos will work in parallel to secure the data in motion, and the enterprise will secure the data at rest wherever the data resides. In legacy non-5G cellular, there also is a much lower need for gateway firewalls than in other environments.

Public 5G has a lower need for enterprise network security controls than private 5G or non-cellular networks because they are embedded in the network operation. This is due most likely to lack of enterprise network ownership versus the private 5G network, which many stakeholders, especially those in critical infrastructure, may own. In public 5G, enterprises are responsible for their device and network security, although they don't own “5G network security.”

Healthcare uses both public and private 5G for its top use cases. Private 5G is predominant for hospital at home, for which the network and the most frequently used component — general-purpose computers — are secured by legacy network security tools such as firewalls, IDS, multifunction authentication (MFA), and passwords.

Fraud and data leakage monitoring and network access restrictions are preferred for public cellular 5G/telco. IDS and network access restrictions are preferred for private cellular 5G, for which organizations potentially have more control over the setup of the network. The use of IDS is strong across all edge networks but is thought of most often

in branch and private 5G architectures. If there are virtual network functions (VNF) in private 5G, IDS is likely an extra layer of protection in front of the VNF.

The low concern about DDoS may recognize that DDoS is on the northbound side of the user plane, which lowers the probability that DDoS can overwhelm the RAN. DDoS, however, still is a real threat to enterprises beyond 5G networks.

CYBERSECURITY “IN” THE EDGE (NETWORK)

Zero Trust for networks, a key security consideration within edge networks, encompasses device firewalls, full VPN, and the network side of network access control. This approach extends traditional firewall and VPN capabilities into the more granular device-to-device firewalls, full internal VPN, and network segmentation of a Zero Trust approach.

Zero Trust is most popular in industrial IoT environments. Both cloud and IIoT networks are more dynamic than other networks and often have shared tenancy, making them ripe for Zero Trust.

Dependence on cloud networks and, to some extent, the focus on fraud prevention also may be the reason retail respondents (think e-tailers) value data leak monitoring, or DLP, the most of all industries — a sensible choice given the presence of personally identifiable information and credit card information.

IDS, followed by DLP, is preferred for industrial IoT/OT. Application proxy, followed by network access restrictions, is preferred for consumer IoT.

Zero Trust hasn't caught on in 5G and cellular environments as much as in other networks. Zero Trust is low in branch as well as in consumer IoT. This finding may reflect a couple of factors. One is the traditional inability to secure the complete connection from user to service and to stabilize connectivity. The other is latency issues, which cause hesitation to see value today. Survey findings reveal that encrypted connections (full VPN) are not always an appealing option for security practitioners, even at the edge. Still, there is a need for encryption in transit and for IDS. The lower rating for encryption may reflect the need for clear (unencrypted) data for packet analysis performed by IDS and DLP solutions.

Some devices will be deployed in a Zero Trust architecture and some devices won't. Different policies are needed to manage different types of devices.

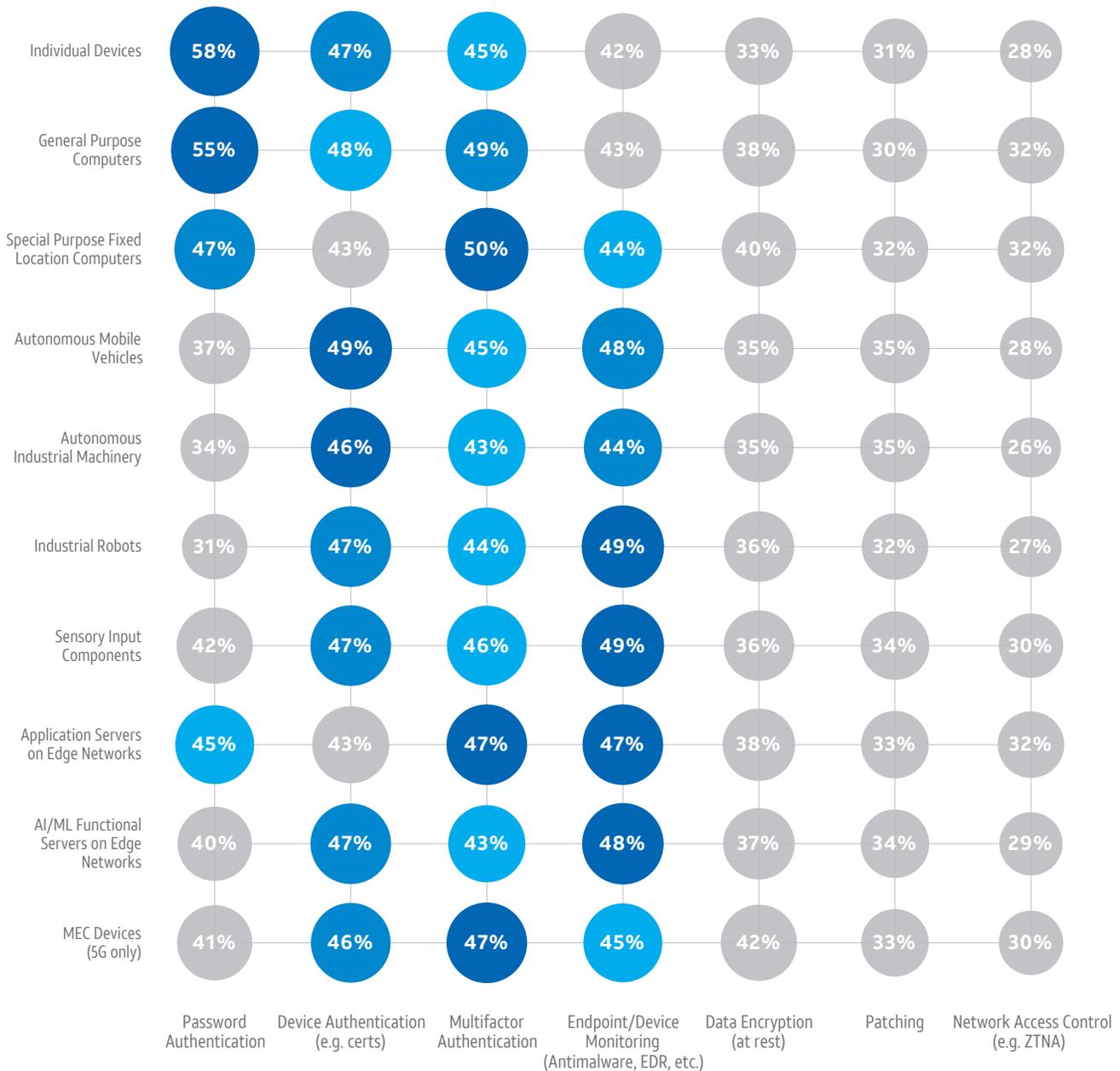
Finance focuses on access control through firewall solutions, which are more preventative than other controls.

FIGURE 10

CYBERSECURITY CONTROLS BY COMPONENT

Q. Which of the following CYBERSECURITY CONTROLS will your organization deploy to protect the COMPONENTS of your primary use case?

% of respondents



N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

CYBERSECURITY AT THE COMPONENT LEVEL

The final target of cybersecurity architecture is the component-level security. Figure 10 displays findings about expected use of security controls applied to various components that are part of edge network computing.

Multifactor authentication leads in protection for fixed location computers and is also the third most popular control. Desktops and laptops are generally equipped with more security features than other components. The features are inexpensive and often built in, except they won't work with components that don't have keyboards (e.g., vehicles, machines, and robots).

Patching ranks low, as it does elsewhere in the survey, although patching is often top of mind for protecting IT architectures. Across the board, respondents do not value patching. Patching is a reactionary, manual, time-consuming control that isn't suitable for the edge, where controls need to be automated and seamless. Practitioners haven't done a good job with hygiene or patching for years. Now organizations are moving into networks that must always be available and networks that feature accelerated bandwidth, low latency, sensors everywhere, and constantly flowing data. Organizations cannot put firewalls in front of sensors.

The low value that is placed on patching signals the direction of organizations intent on securing the edge: automation, integration, and real-time alerts. In addition, the essential characteristics of edge discussed previously strengthen the case for thinking through security from the start as a business requirement with a focus on limited access, network segmentation, and SASE.

Autonomous vehicles have built-in MFA in key fobs. It makes sense that passwords, MFA, and device authentication are utilized. There are no direct inputs into vehicle networks; therefore, endpoint detection and response (EDR) and managed detection and response (MDR) are seen much more often as a requirement in this environment and the IoT environment. Monitoring is important, but authentication is critical to help prevent

an attacker from breaking into the connection and taking over a vehicle.

Device authentication is ubiquitous across all manufacturing use cases. Energy and utility organizations also use device authentication as their second favored control after EDR for remote control operations. Smart meter components are secured with passwords, MFA, and device authentication.

Data encryption, while not rated the highest overall by component, is seen as the most important in MEC, especially in healthcare, which rates data encryption as third overall. Manufacturing places data encryption as fourth, and both are above the average. Some security experts believe data in public cloud, which often is multitenant, should always be encrypted in transit to help prevent side-channel attacks.

The US public sector has the lowest levels of security for any device type. MFA and encryption were supposed to be in place by November 8, 2021, but many agencies were expected to miss the deadline. Decision makers in public sector may want to take a note from manufacturing and retail. These industries have had to ramp up quickly to address the onslaught of ransomware attacks in manufacturing and credit card attacks in retail.

Of all industries, finance typically has the largest, most mature security programs. Survey findings, however, place finance in the middle of the pack in edge security, indicating a possible security optimization approach that reduces the types of controls being deployed.

The US public sector has the lowest levels of security for any device type and may want to take note from manufacturing and retail, which have had to ramp up quickly due to ransomware attacks.

Security experts recommend the encryption of data between MEC applications regardless of the chosen transport to restrict access to services.



PERSPECTIVE ON PATCHING

Many stakeholders in 5G and edge are using open source software, a known target for attackers. But because the software is embedded, dependencies aren't always apparent. As a result, enterprises may want to prioritize the design of a clear process for receiving notifications about vulnerabilities or patches.

Patching isn't always an option. But when patching is an option, stakeholders should patch software in the infrastructure as quickly as possible. Yet they won't always know the threat source, especially of zero-day attacks. The reality of this situation may be one reason why patching is the lowest ranked control.

INVESTMENTS IN EDGE USE CASE CYBERSECURITY

One heuristic for measuring and understanding the risk associated with edge use cases is to look at associated cybersecurity spending expectations.

The total investments in use cases act as a proxy for the minimum expected value to be derived. While organizations usually expect much higher return on investment from use cases after deployment, they likely proceed based on the assumption that they will at a minimum cover costs. The relative amount of an investment associated with cybersecurity can therefore provide insight into the anticipated level of risk at a high level.

Figure 11 shows the distribution of spending expectations for industries. An average number related to these ranges is approximately 13%. This corresponds with the third of respondents who expect to spend 6–10% and the half who expect to spend 11–20%.

The variability, or mix of responses, is noteworthy. Healthcare has the highest level of variability, with both a larger percentage (7%) of organizations investing only 1–5% and a significantly higher level of respondents (17%) who expect to spend more than 20%. Finance also reveals a bit more variability than the other industries.

While these variances may be slightly unsettling, they aren't surprising. At the business level where compliance interests reign, use cases and decisions about cybersecurity control decisions follow a predictable pattern. But at the architectural level, a program consists of many elements, such as networks, components, and volume of activity. Multiple elements lead to considerable variation in the cybersecurity strategies and investment associated with edge use cases.

The variability in cybersecurity spending may be an indicator of confusion. Some respondents may answer based on personal experience or insight, and some respondents may recognize more nuanced differences in risk among the various industry use cases. The outcomes of risk assessment will play out over time.

CYBERSECURITY CONTROLS EFFICIENCY AND EFFECTIVENESS

The lack of agreement associated with total cost of ownership versus effectiveness of controls is another example of variability playing out in the study (see Figure 12). Most Zero Trust technology fares well in effectiveness and is fairly high in TCO, but greater cost-effectiveness leads to better benefit. Firewalls at the network edge and IDS are viewed as expensive but deliver the highest perceived benefit.

Controls with low cost of ownership and low perceived effectiveness include password authentication, application proxy, multifactor authentication, encrypted traffic throughout, endpoint/device monitoring, and data encryption (at rest).

Patching, in keeping with earlier findings, offers the lowest cost of ownership and also rates lowest in effectiveness. Device authentication is on the line between low and high cost but earns a low effectiveness rating.

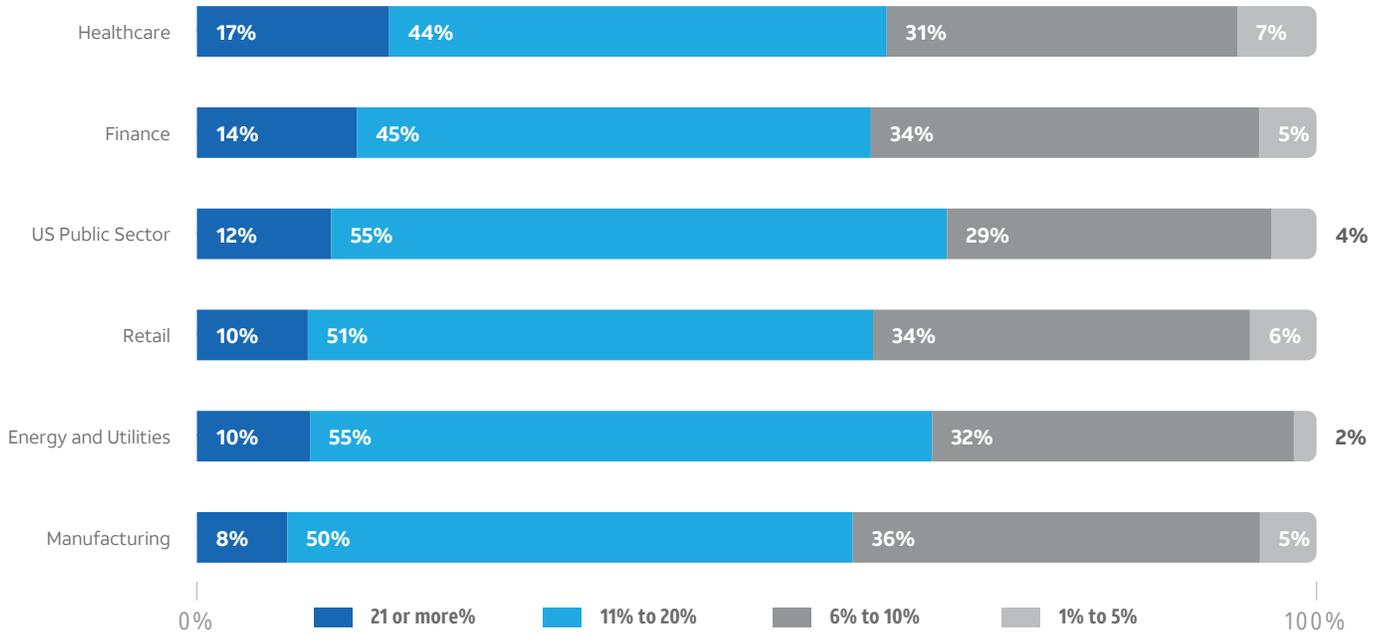
Controls viewed as expensive with low effectiveness include encrypted traffic at gateway/proxy, DDoS mitigation, data leakage monitoring, and network access control. In this group, data leakage monitoring was ranked the highest in terms of benefit-cost analysis.

FIGURE 11
COMPANIES PLAN SIGNIFICANT INVESTMENTS TO SECURE EDGE USE CASES

Q. What percent of your organization's total COMBINED investment for ALL of these use cases (in production within 3 years) do you anticipate being allocated directly to security?

% of respondents

Combined Investment Allocated to Security by Industry



N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

Note: This data does not include 'don't know' survey responses.

Latin America rates nearly all controls above 70% effectiveness. Retail rates nearly all controls above 70% effectiveness. Public sector and healthcare rate data leak monitoring the lowest in effectiveness. India rates all controls at 4 out of 5 in effectiveness.

EDGE SECURITY X RETAIL

In retail, 78% of respondents globally are planning, have partially, or have fully implemented an edge use case.

TOP USE CASE

The loss prevention use case ranks highest in retail for full or partial implementation. Its risk is perceived as lower-than-average.

EDGE ADVANTAGE

As retailers build loss prevention at the edge using advanced cognitive tools, the use case will benefit from big data analytics and real-time video analytics to move it from reactive, where it identifies a loss, to proactive and preventive.

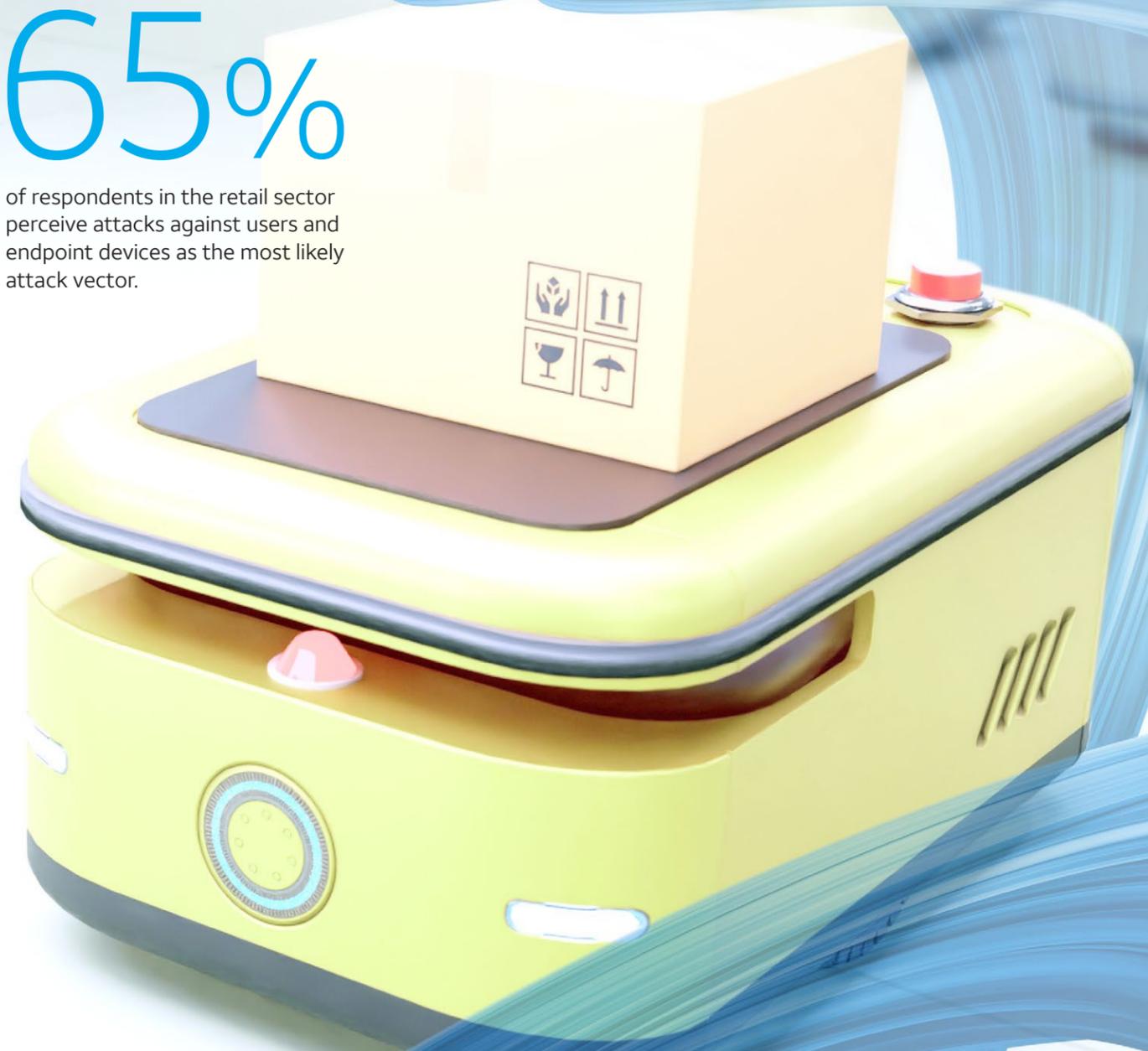
SECURITY CONTROLS

Retail respondents rank network access restrictions (device to device), intrusion and threat detection, and traffic encryption (both internal to the network and external at a gateway or proxy) among the most efficient and effective security controls at their disposal.

SURVEY INSIGHT

65%

of respondents in the retail sector perceive attacks against users and endpoint devices as the most likely attack vector.



EDGE SECURITY X ENERGY

In energy and utilities, 77% of respondents globally are planning, have partially, or have fully implemented an edge use case.

TOP USE CASE

The remote-control operations use case ranks highest within energy and utilities for full or partial implementation. It also has a higher-than-average perceived risk.

EDGE ADVANTAGE

Though energy and utilities and other critical infrastructure environments have been slow to adopt digital technologies, edge computing will accelerate autonomous operations. Software for remote operations can enable industrial organizations to adopt remote staffing, centralized and flexible resourcing, and autonomous operations.

SECURITY CONTROLS

Energy and utilities respondents rank intrusion and threat detection, network access restrictions (device to device), encrypted traffic (internal to the network), and firewall at the edge among the most efficient and effective security controls at their disposal.

SURVEY INSIGHT

81%

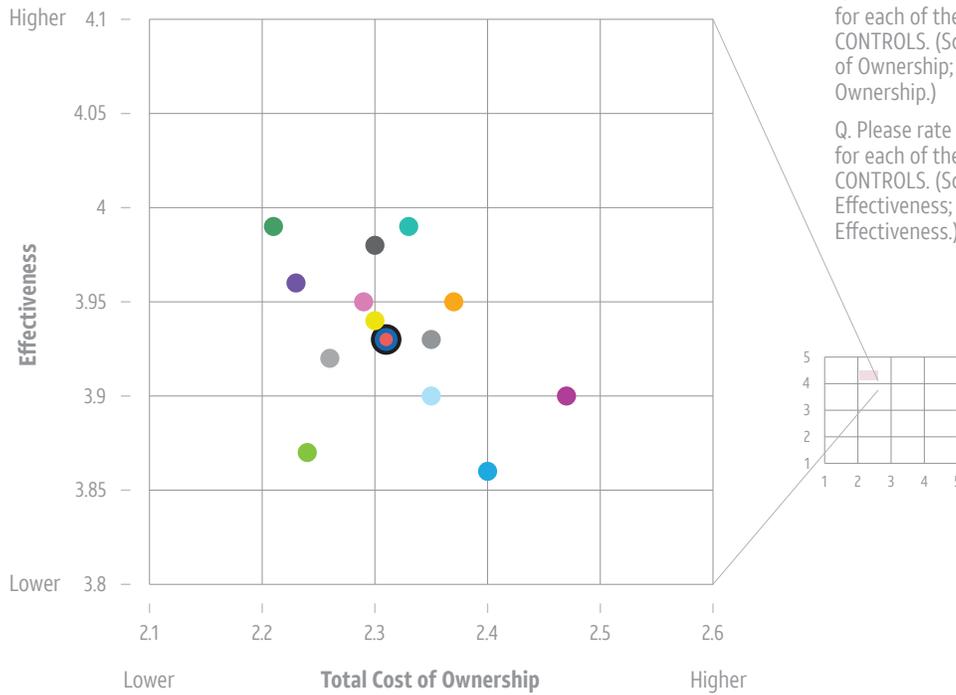
of respondents in energy and utilities are most concerned about sniffing attacks against the radio access network (RAN)



FIGURE 12

PERCEIVED COST OF OWNERSHIP AND EFFECTIVENESS OF CONTROLS

Scale of 1-5



Q. Which of the following CYBERSECURITY CONTROLS will you deploy to protect the NETWORKS of your primary use case?

Q. Please rate the total cost of ownership for each of the following CYBERSECURITY CONTROLS. (Scale: 1=Very Low Total Cost of Ownership; 5=Very High Total Cost of Ownership.)

Q. Please rate the efficiency/effectiveness for each of the following CYBERSECURITY CONTROLS. (Scale: 1=Very Low Efficiency/Effectiveness; 5=Very High Efficiency/Effectiveness.)

- Average
- Application proxy (e.g. secure web gateway, CASB, etc.)
- Data encryption (at rest)
- Data leakage monitoring
- Device authentication (e.g. certs)
- Distributed Denial of Service (DOS/DDoS) Mitigation
- Encrypted traffic at gateway/proxy (external)
- Encrypted traffic throughout (internal)
- Endpoint/device monitoring (antimalware, EDR, etc.)
- Firewall at network edge
- Intrusion/threat detection
- Multifactor authentication
- Network access control (e.g. ZTNA)
- Network access restrictions device-device
- Password authentication
- Patching

N= 1520

BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

CYBERSECURITY CONTROLS BENEFIT-COST ANALYSIS

IDS is the overall benefit-cost analysis winner, with best effectiveness and neutral TCO. Passwords garner best TCO overall, with moderate effectiveness.

Passwords have the best TCO across all controls, but industries disagree on cost-effectiveness.

A benefit-cost analysis of the survey data reveals at the highest level a greater variability in opinions on effectiveness than on TCO. Control effectiveness is rated far above the middle (3.93) on average on a scale of 1–5 and across all industries studied. Control TCO, on the other hand, is rated below the middle (2.31) on average. The perception of high cost may exist in the absence of attacks, a situation in which the controls are doing their job. But when attacks occur, organizations are more willing to spend money to increase cybersecurity controls. In both scenarios, perception may lead to thinking that controls are too expensive.

Decision makers at all levels and departments of organizations routinely compare benefits with costs. Whether the effort is cost justification or full-on benefit-cost analysis, organizations expect some analysis that provides insight into the worthiness of a project or an initiative. But it can be challenging to articulate the benefits and costs of cybersecurity. Often decision makers look for benefits such as obvious increases in revenue or clear reductions in expenses. But in cybersecurity, benefits accrue in terms of reducing risk — an ephemeral concept.

Cybersecurity preferences, however, arise over time as organizations make decisions and experience the outcomes associated with preferences. Company size, industry, and geographic region play a role, so preferences will vary by organization. For specific cybersecurity control decisions, the networks and components of an architecture are likely to play an even larger role.

Variability in expectations persists, so it's useful to look at different industries and how they rate the benefits and costs

of the same set of available controls as in Figure 12. Figure 13 shows the perceived benefits and costs of all controls.

Across industries, expectations of the cost of security controls are similar (Figure 13) shown by the approximate vertically aligned points. Interestingly, healthcare and finance respondents again are the outliers. Healthcare anticipates slightly lower TCO and finance anticipates slightly higher TCO than other industries. Meanwhile, the reverse is true in terms of benefit. Healthcare expects lower benefits than finance. Historically, finance has been more risk averse compared with healthcare, although healthcare has adjusted its stance due to privacy concerns. Decision makers will need to ponder whether cost drives benefit or benefit drives cost.

Retail and manufacturing have experienced more than their fair share of publicized breaches in recent years, but they also recognize strong cybersecurity control benefits. Historically, these industries have not had the highest levels of risk awareness.

At the aggregate level, IDS solutions are the clear winner in terms of effective controls by industry. IDS is followed closely by both data encryption at rest and internally encrypted traffic. The last two are less costly and nearly equal in effectiveness. IDS solutions are costly but highly effective, though not all industries agree, given the high degree of rating variability. The highest effectiveness rating for IDS across all industries comes from retail. In fact, the rating is one of the two highest control effectiveness ratings for retail next to full firewall.

While passwords appear to earn the best TCO of all controls, industries disagree on cost effectiveness. For example, healthcare and manufacturing

believe passwords have the best TCO among all industries and across all controls studied. Energy and utilities and public sector believe that passwords provide a good TCO but rate the TCO 15 points lower than healthcare and manufacturing.

The benefit-cost analysis of traditional firewalls aligns with average TCO and effectiveness. Firewalls still are critical as

organizations move to the edge, but there is a high degree of variability by industry on both TCO and effectiveness. Network access restrictions through device-to-device firewalls rate similar to firewalls at the network edge, and retail seems to prefer firewalls at the network edge most for their effectiveness next to IDS. And, according to retail, network access firewalls provide decent TCO.

DLP doesn't shine as an edge control. DLP receives poor TCO and effectiveness marks. Unsurprisingly, retail — a top target of cybercriminals attracted by large caches of personal and credit card data — states the highest effectiveness of DLP. Retailers require data leakage monitoring and insight into data storage vulnerabilities to stem exploitation of personally

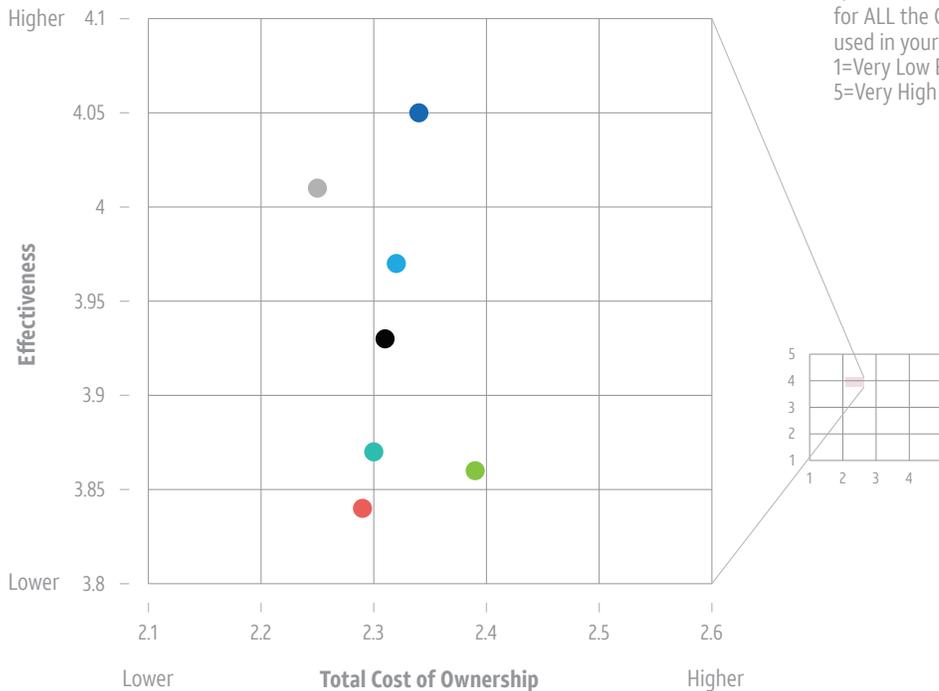
FIGURE 13

PERCEIVED BENEFITS AND COSTS OF ALL SECURITY CONTROLS IN USE BY INDUSTRY

Scale of 1-5

Q. Please rate the total cost of ownership for ALL the CYBERSECURITY CONTROLS used in edge use cases. (Scale: 1=Very Low Total Cost of Ownership; 5=Very High Total Cost of Ownership.)

Q. Please rate the efficiency/effectiveness for ALL the CYBERSECURITY CONTROLS used in your edge use cases. (Scale: 1=Very Low Efficiency/Effectiveness; 5=Very High Efficiency/Effectiveness.)



- Energy/Utilities
- Finance
- Healthcare
- Manufacturing
- Overall
- US Public Sector
- Retail

Along with passwords, patching has the best TCO and the worst effectiveness. Patching also receives the worst benefit-cost rating overall.

Cloud is viewed as needing the most security, followed by IoT networks.

N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

identifiable information, meet PCI standards, and manage the explosion of big data that’s driving personalized buyer experiences. Retail’s emphasis on and experience with DLP is something other industries may want to consider as data privacy regulations increase globally, fines rise, and attackers change their goals and tactics in pursuit of data access and exfiltration.

The effectiveness of gateway VPN is one of the more debated controls across industries given the 15-point rating variance. All industries believe gateway VPN control demonstrates poor TCO. Finance and retail highly value the effectiveness of the control — in fact, finance rates gateway VPN as number 1 and retail as number 3 for effectiveness across all controls. Full

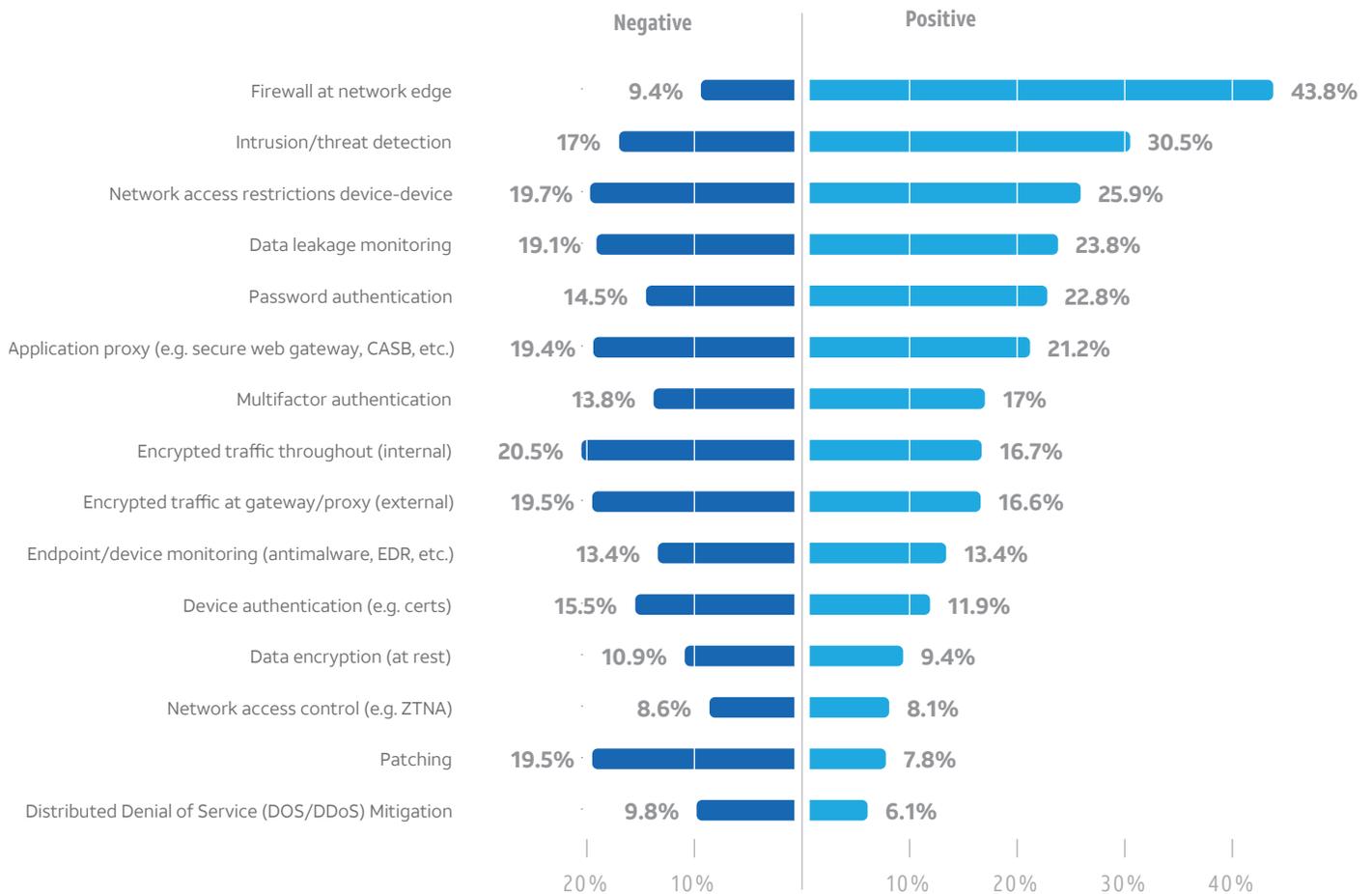
VPN doesn’t receive the best TCO rating but is perceived as one of the most effective controls overall, especially by retail and finance. Manufacturing also places gateway VPN among its top choices.

All industries agree that MFA isn’t a great TCO story, but they are at odds regarding effectiveness. Though not the top control overall for retail and

FIGURE 14
PERCEIVED COST-BENEFITS OF SECURITY CONTROLS FOR EDGE USE CASES

Q. In your opinion, which of the following would provide the most significant cost-benefit for your EDGE SECURITY and which would not be worth deploying.

% of respondents



N= 1520 BASE All respondents

SOURCE AT&T Cybersecurity Insights™ Report: Securing the Edge - Survey, September 2021

Manufacturing finds DDoS to have the worst TCO but also the highest effectiveness.

In a software-defined networking world, organizations need to know the building blocks of the cellular network and how it works. Organizations can't stop at the edge of cellular networks or take security vendors for granted.

healthcare, these industries find MFA the most effective control across all industries. Considering all controls, healthcare values MFA the highest after IDS. MFA is rated lowest on cellular of all networks studied, likely because the technology is viewed as proprietary and difficult to break. Autonomous motor vehicle key fobs have built-in MFA.

Device authentication is perhaps the biggest loser in the benefit-cost analysis overall. It makes sense, however, that manufacturing above all other industries believes that device authentication (the use of certificates) is highly effective. Device certificates are tools used by manufacturers to secure devices before shipment and by the enterprises that use these devices within their environments to secure the devices on their networks. Retail also believes in device certificate effectiveness and follows manufacturing in giving the control a strong TCO.

EDR used at the edge is seen as average in both cost of ownership and effectiveness. Finance and retail rate its effectiveness and TCO better than other industries, but EDR still is not a top choice for finance and retail.

Finance and retail appear to be early users of Zero Trust network access (ZTNA) for edge. While one of the worst in TCO overall, ZTNA is actually one of the best in effectiveness. ZTNA is not a top control for either finance or retail, but both believe ZTNA to be higher in effectiveness than other industries.

Distributed denial of service has very poor TCO and low effectiveness. The perception of high cost and low effectiveness may be because DDoS works behind the scenes and blocked attacks are "invisible." Manufacturing states DDoS has the worst TCO but also the highest effectiveness. DDoS is still not a top choice for this industry but perhaps is seen as a necessary preventative measure.

Overall, public sector appears to be the most skeptical of cyber controls' effectiveness and overall benefit-cost analysis. Healthcare has the highest opinion that cybersecurity is expensive.

Are cybersecurity controls worth the investment? Figure 14 shows negative and positive responses for each control studied.

Cybersecurity at the edge is necessary regardless of cost and sometimes regardless of perceived effectiveness. This is likely because true effectiveness at the edge is not yet understood generally or by a particular industry, or because compliance regulations haven't yet matured to clarify which cybersecurity controls should be mandated at the edge. Also, familiarity can influence the perception of effectiveness. Security leaders may want to look to industries outside their own for guidance on the importance and effectiveness of controls. Just as cybersecurity controls at the edge are expected to be implemented in next-generation forms, best practices can evolve based on collaboration and cross-industry thinking.

CONCLUSION

Edge may mean different things to different people, but this doesn't alter the fact that organizations are adopting edge computing and implementing edge use cases. The ongoing transition from a centralized to a decentralized computing model is a sea change that calls for next-generation thinking about security.

Securing the edge is top of mind, as reflected in concern about all attack vectors and perceived risk. But the decisions about which controls to use where vary and are dependent on several factors, including whether edge is an extension of cloud or on premises, the edge network environment, whether controls are on or in the edge network, familiarity, regulations, and benefit cost.

This report presents a realistic view of the state of edge and edge security by highlighting edge use cases both at a high level and by industry. It also provides survey findings that may prompt decision makers to think differently about edge network and edge security strategies and plans. This effort may be challenging in an immature edge computing market. Discerning decision makers gather information, evaluate multiple viewpoints and technologies, and make decisions that take into account an organization's risk appetite, network strategy, innovation goals, and security.

A proactive, preventive approach to security at the edge considers a hybrid network model that is likely to persist for a long time. 5G adoption is increasing, but organizations can leverage legacy networks where it makes sense to do so for specific use cases and as dictated by the realities of existing communications infrastructure, regulations, and location. As the number of IoT devices and access points rises, sensors and data will be everywhere in different network

environments. The shared security responsibility model is more relevant than ever before.

RECOMMENDATIONS

- Communicate with and educate stakeholders along a journey that will be both thrilling and challenging.
- Emphasize the importance of security by design throughout all stages of edge network discussions and use case implementation. Leverage legacy controls where they are effective, but keep up with next-generation approaches such as Zero Trust and SASE that are designed for 5G and edge.
- Talk with service providers and network operators prior to making decisions about edge networking. Discuss the pros and cons of public and private 5G cellular, legacy cellular, remote office/branch office, IaaS/PaaS/SaaS cloud environment, industrial IoT/OT, or consumer IoT environments. Develop realistic scenarios for incremental transitions to 5G.
- Delve into the shared security responsibility model with public cloud service providers and carriers to clarify roles and responsibilities at every stage of use case implementation.
- Think ahead about innovation, evolving technologies, and security at the edge. Use cases are the most practical way to proceed for now, given the immature, ambiguous state of edge. Specificity is better than generality in all things edge.
- Understand that implementing edge use cases may need to rouse stakeholders out of their comfort zones. Initial deployments involve familiar devices such as general-purpose computers and individual devices, and this makes sense. But other components may present opportunities for differentiation and competitive advantage.
- Classify data and maintain processes and procedures related to data privacy and data sovereignty. Current and emerging regulations will influence data management decisions and locations of security controls.
- Evaluate the benefit cost of security controls before implementing controls, keeping in mind the necessity of visibility across the entire attack surface. Scrutinize traditional assumptions about security controls that may influence perceptions of cost and/or effectiveness. Look to other industries for inspiration, guidance, and best practices.
- Conduct frequent security control reviews based on data travel routes and storage locations, beyond what's required for regulatory compliance. Perceived risk in all studied attack vectors is high, and increased spending on security may be both necessary and wise.
- Use multisourced, enriched threat intelligence to keep up with attacker tactics, techniques, and procedures. An industry-specific perspective helps prioritize threats and simplify resource allocation.
- Engage security services providers with broad, complementary capabilities to help reduce complexity, lower cost, enable rapid scalability, and increase business agility.

Assume that traditional security controls may still be relevant at the edge, but in a different, next-generation form.

APPENDICES

APPENDIX A

METHODOLOGY

This report is based on a survey of 1,520 security practitioners from the United States, the United Kingdom, France, Germany, Ireland, Mexico, Brazil, Argentina, Australia, India, Singapore, and South Korea conducted during September 2021. Respondents come from organizations with 1,000+ employees, with the exception of public sector and energy and utilities verticals. Respondents were limited to those with direct knowledge of their organizations' edge network plans or with decision-making responsibilities related to securing the edge as well as direct knowledge of IoT, cloud, edge and MEC, and Zero Trust. Respondents' job titles include manager up to C-level. Respondents' roles include IT/security/cybersecurity (e.g., CISO, security architect, security engineer), other IT roles (e.g., CIO, CTO, networking, development), and line-of-business roles (e.g., president, CEO, CFO, HR). Respondents span a variety of market segments that are nearly equally represented at 16.4–17%: the public sector, consisting of higher education and state/local government in the United States; energy and utilities; finance; healthcare; manufacturing; and retail. For certain questions, participants could choose more than one response. In these cases, the responses do not round to exactly 100%.

APPENDIX B

CONTRIBUTING AUTHORS AND 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 report. This includes the 1,520 security, IT, and business professionals who participated in the research of this report and subject matter experts who provided their technology insights, along with the writers, editors, designers, and project managers who shepherded this report from initial research through completion. Thank you, everyone!

Contributing Authors

IDC

Christina Richmond
Craig Robinson
Pete Lindstrom

AT&T

Tawnya Lancaster
Theresa Lanowitz

Contributors

AT&T

Ryan Bearden
Christopher Boyer
Lourdes Charles
Nora Cheseby Peskin
Rupesh Chokshi
Phillip Coleman
Alicia Dietsch
Will Eborall
Dan Feldstein
Jeff Hobbs
Jeff Huegel
Jason Inskeep
Leslie Johnson
Danessa Lambdin
Tawnya Lancaster
Maureen Langevin
Theresa Lanowitz
Rita Marty
Gerry Myers

Deon Ogle
Senthil Ramakrishnan
Carlos Salinas
Ginny Smith

Altitude Management Inc.

Paul Cavanaugh
Bryan Reid

Akamai Technologies, Inc.

Patrick Sullivan

Check Point Software Technologies Ltd.

Chris Federico

Cisco

Robert Albach

Digital Defense, by HelpSystems

Jon Hallber

Fortinet

Jonathan Nguyen-Duy

Juniper Networks

Albert Lew

Palo Alto Networks

Jason Georgi
Hari Srinivasan

RedShield
Matt Taylor

SentinelOne
Jared Phipps

VMware
Michael Leonard

APPENDIX C

CONTRIBUTING ORGANIZATIONS



APPENDIX D

GLOSSARY

CYBERSECURITY CONTROLS TO PROTECT COMPONENTS

NAME	ABBREVIATED NAME	DEFINITION
Password authentication	PWD	Passwords provide single factor authentication based on "something you know," usually a string of six to eight characters typed in a field by a user.
Multifactor authentication	MFA	Multi-factor authentication involves the combination of two or more types of proof of identity. It could be something you know like a password, something you have like a physical token for smartphone, or something you are like a biometric capturing device.
Device authentication (e.g. certs)	DevAuth	Certificate-based authentication is the use of a Digital Certificate to identify a user, machine, or device before granting access to a resource, network, application, etc.
Endpoint/Device monitoring (antimalware, EDR, etc.)	EDR	Endpoint detection and response, also known as endpoint threat detection and response, continually monitors and responds to mitigate cyber threats at the endpoint.
Patching	Patch	A patch is a set of changes to a computer program, or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bugfixes or bug fixes
Data encryption (at rest)	Crypt	Data encryption uses cryptographic algorithms to make data stored on hosts and endpoints unreadable unless a special key is provided to make it readable.

CYBERSECURITY CONTROLS TO PROTECT THE NETWORK

NAME	ABBREVIATED NAME	DEFINITION
Firewall at network edge	GW-FW	Firewall at network edge or gateway firewalls filter network traffic based on access control rules with source and destination IP addresses as well as the destination port.
Network access restrictions device-device	Full FW	Network access restrictions device-device or full firewall is the same as a firewall at the network edge except that full firewalls block at each individual host. Rather than blocking only at an entry or egress point to the network every component on the network performs the blocking.
Intrusion/threat detection	IDS	An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations.
Data leakage monitoring	DLP	Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use to prevent access to personally identifiable information (PII). The terms "data loss" and "data leak" are related and are often used interchangeably.
Application proxy (e.g. secure web gateway, CASB, etc.)	Proxy	Application proxies work at the application layer and filter based on the context of activities being performed.
Encrypted traffic at gateway/proxy (external)	GW-VPN	Gateway virtual private networks (VPNs) are devices at the network edge that encrypt traffic from one point to another.
Encrypted traffic throughout (internal)	Full-VPN	Full virtual private networks (VPNs) are encrypted traffic throughout the network from host to host.
Network access control (e.g., Zero Trust network access)	ZTNA	Network access control is an approach to computer security that attempts to unify endpoint security technology, user or system authentication and network security enforcement. (See below further definition of ZTNA.)
Distributed Denial of Service (DOS/DDoS) Mitigation	ADOS	DDoS mitigation is a set of network management techniques and/or tools for resisting and mitigating distributed denial-of-service attacks.

ZERO TRUST COMPONENTS

Network access restrictions device-device	Full FW	Also known as packet filtering firewalls these operate inline at junction points of routers and switches comparing packets received to a set of established criteria, such as allowed IP addresses, packet type, port number and other aspects of the packet protocol headers.
Network access control (e.g., Zero Trust network access)	ZTNA	Network Access Control is an approach to computer security that attempts to unify endpoint security technology, user or system authentication and network security enforcement.
Encrypted traffic throughout (internal)	Full-VPN	An internal virtual private network (VPN) is an Internet security service that creates an encrypted connection between user devices and one or more servers to securely connect a user to a company's internal network.
Multifactor authentication	MFA	Multi-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.

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.



BUSINESSES INNOVATING AT THE EDGE CANNOT BE REACTIONARY, ESPECIALLY WHEN IT COMES TO SECURITY. THE STAKES ARE TOO HIGH. SENSORS ARE EVERYWHERE, NETWORKS MUST BE ALWAYS AVAILABLE, AND DATA – IN MOTION AND AT REST – MUST BE PROTECTED. SECURITY AT THE EDGE CAN'T BE AN AFTERTHOUGHT OR PRESCRIBED BASED PRIMARILY ON PAST EXPERIENCE OR PRACTICES.