AT&T CYBERSECURITY INSIGHTS™ REPORT

TWELFTH EDITION 2023

AT&T Business

AT&T Cybersecurity

2023 Edge Ecosystem

AT&T CYBERSECURITY INSIGHTS™ REPORT

TWELFTH EDITION

2023

About the AT&T Cybersecurity Insights Report

The *2023 AT&T Cybersecurity Insights Report: Edge Ecosystem* focuses on connecting and securing the entire edge computing ecosystem. Previous yearly reports focused more squarely on the security component of the journey to edge computing: ***Securing the Edge*** and ***5G and the Journey to the Edge***.

The AT&T Cybersecurity Insights™ Report is an annual research report published by AT&T Cybersecurity. Currently in its twelfth 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 research, 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 attain a resilient and holistic cybersecurity approach that evolves with the business.

Contents

Executive summary 2

Introduction 3

Anticipated Edge Use Case Investments 4

The State of Edge 11

Edge Use Case Overview 13

Risk Considerations Associated with Edge Types 22

Likelihood of Attack, Compromise, and Impact 25

Changing Risk Perceptions 31

Cybersecurity Controls 33

Conclusion 41

Appendices 42

Executive summary

Ideally, the journey to edge aligns with an organization's long-term vision and short-term objectives. It's a collaborative endeavor that can span years. The right edge ecosystem partners bolster resilience and security, which are critical elements of each edge computing solution.

Consider the following primary edge characteristics to make the journey smoother and provide a consistent framework for the edge ecosystem:

- A distributed model of management, intelligence, and networks
- Applications, workloads, and hosting closer to the users and assets that are generating or consuming the data, which can be on premises and/or in the cloud
- Software defined

Together, resilience and security address risk, support business needs, and drive operational efficiency at each stage of the journey.

Key Takeaways

Understand that edge use cases are evolutionary not revolutionary. Edge use cases are pervasive, and many use existing connectivity, networking, and security elements. As use cases evolve, resilience gains importance and the competitive advantage that edge applications provide can be fine-tuned. Future evolution will involve more IoT devices, faster connectivity and networks, and holistic security tailored to hybrid environments.

Organization

- Collaborate across silos and communicate cross-functionally. When IT, network, security, development, and line-of-business organizations are not in sync, vulnerabilities inevitably occur. Collaboration enables a holistic view of developing edge use cases and reduces risk.
- Achieve consensus among internal stakeholders who hold varied perspectives. Engage an edge ecosystem trusted advisor to facilitate discussions and decisions.
- Explore perceptions of and assumptions related to value. Organizations and edge use cases are at different maturity levels, and maturity is an important decision variable.

Planning

- Plan to pivot. Change is inevitable. Expect edge requirements and standards to evolve over the coming years. Evaluate resource allocations continuously with flexibility, responsiveness, extensibility, and resilience in mind.
- Plan for extraordinary volume, velocity, and variety of data. Determine what a data life cycle means for the organization.
- Secure the edge. Bolster risk management by identifying and classifying the value of assets that reside in, travel to, or are processed at the edge. Then apply appropriate cybersecurity controls that are likely to be a use case-specific mix of traditional and new controls.
- Get outside help. Edge ecosystem partners are essential to edge use case success. Their experience and best practices can impact many facets, including strategy, decisions about the use of existing and legacy infrastructures, and cybersecurity.
- Recognize the importance of getting an edge computing framework as right as possible so that the edge computing framework can evolve in response to business requirements.

Budget

- Invest early. Think of the edge ecosystem as a new opportunity to drive competitive differentiation and business outcomes. Investing in and developing an edge ecosystem sooner rather than later can drive results faster.
- Invest first in the fundamentals of strategy, planning, network, and security before application development. However, make sure application development is part of the core team's planning and exploration of edge use cases.
- Support overall edge ecosystem fiscal responsibility. Clarify business, technology, security, and operational objectives. When used properly, edge computing can provide cost advantages. During deployment planning, study objectives with edge use case permutations in mind to understand how various components and partnerships affect outcomes.

Future evolution will involve more IoT devices, faster connectivity and networks, and holistic security tailored to hybrid environments.

Introduction

This AT&T Cybersecurity Insights report focuses on connecting and securing the entire edge computing ecosystem (see Figure 1). Previous reports focused more squarely on cybersecurity: ***Securing the Edge*** (2022) and ***5G and the Journey to the Edge*** (2021)This report highlights the dramatic shift in computing that is enabled by:

High-speed, low-latency networks such as 5G and edge architectures

+

the convergence of network functions and cybersecurity controls

This report presents a perspective that recognizes the essential characteristics of and key differences among edge architectures and provides a realistic picture of the state of edge. The report invites decision makers to think holistically about edge ecosystem strategies by providing insights into:

- Anticipated edge use case investments
- The intersection of edge computing, networking, and cybersecurity
- Observations about the state of edge, including project life-cycle management
- Edge use cases, including industry-specific primary use case snapshots
- Edge risk, which encompasses types of edges and perceived edge use case risk
- Cybersecurity controls and their perceived cost benefit

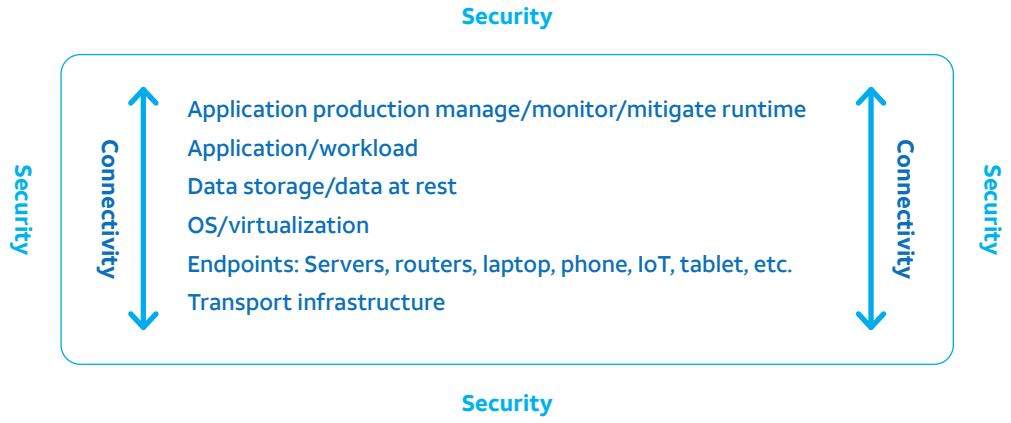
In addition, this report explores themes that are central to edge computing:

- **Partner ecosystem.** In-house IT, security teams, and line-of-business owners may lead the charge to the edge, but they engage ecosystem partners throughout all stages of use case creation and implementation — from network design/architecture through management, monitoring, and mitigation.
- **Cost efficiency.** During an edge journey, decision makers will scrutinize budgets, edge use case costs, and potential returns on investment. Digital transformation thinking is shifting to digital operations thinking, which focuses on essential business processes to achieve desired outcomes and ultimately to build an aura of digital trust among users.
- **Network and security resilience.** As organizations operate with far-flung edges, the distributed footprint of edge computing offers survivability advantages. Resilience depends heavily on designing edge architectures capable of evolving as business conditions change. Experienced edge ecosystem partners can save time and cost related to architecture design. Security at the edge needs to have a survivability mindset architected in to make cyber-resilience a pillar of the design.

This report concludes with recommendations to safeguard digital assets and workloads that traverse wired or wireless networks and advice for working with edge ecosystem trusted advisors. Ecosystem advisors encompass consultants, systems integrators, telcos, hyperscalers/cloud providers, managed services partners (SPs), and managed security services providers.

Figure 1

The Edge Computing Ecosystem



The Essence of an Edge Computing Ecosystem
Edge computing solutions include hardware, software, and services (provisioned, professional, support, and managed) that enable organizations to utilize a distributed architecture across core, cloud, edge, and endpoints. By placing IT resources closer to where data is generated and consumed, organizations can more effectively drive business, technology, and operational outcomes.

Anticipated Edge Use Case Investments

Think of the edge ecosystem as a new opportunity for competitive differentiation and business outcomes.

As organizations mature in their edge use case strategies and implementations, stakeholders can move from simple use cases using basic data analysis to more sophisticated use cases. Sophistication involves greater amounts of data and intelligence in the form of enriched machine learning (ML). Analytics-based use cases, however, need increased processing power. Fortunately, major server manufacturers are responding to the need for specialized, small form factor, rugged devices with enterprise-level features designed for edge.

As maturity increases, stakeholders benefit from the following edge accelerators:

- Experience, which minimizes the bespoke nature of early deployments that were likely not well integrated or built using the same standards as those followed by datacenters or cloud service providers
- Transfer of responsibility from internal groups to a collaborative edge ecosystem, validated reference architectures, pretested solutions, and off-the-shelf components (Stakeholders can rethink brownfield and greenfield technology investments to leverage these cost-saving elements and turnkey technologies such as the latest cloud service provider platforms that support innovation with attractive pricing.)

Edge use cases will become increasingly strategic and mission critical as organizations fine-tune the competitive advantage that edge applications provide. Explore core investment discussion threads, such as resilience, security, and brownfield and greenfield technology, in the context of how the network, applications, and data will continue to evolve. Aim for adaptable security solutions that can serve as a foundation for current and future applications. The edge timeline is provided in Figure 2.

Investment Nuances

As implementations continue, there's likely to be greater integration and cross-dependency among applications and more enriched data to analyze. Accompanying this trend is an expanding viewpoint that takes two forms:

- Inward focus on how to improve operations and the overall business; for example,

Figure 2 **Edge Timeline**

2019 - 5G is officially introduced to provide lower latency, higher bandwidth, and inherent network security.

2020 - Edge use cases increase in proof of concept with the expectation that edge will continue to evolve. The pandemic accelerates the need for edge adoption along with the convergence of cybersecurity controls and network functions.

2021 - Edge use cases advance quickly because of competitive differentiation demands.

2022 – Edge is evolving. Initial use cases are successful, and the next generation of edge is quickly being built. Organizations see the need for both a technology ecosystem as well as tight-knit operational ecosystem. Decades-old silos are beginning to erode and businesses realize the necessity of working with trusted advisors to assist with edge innovation.

2023 - Expectations:

- Organizational changes to enhance collaboration – a key element for edge
- Edge standards and best practices to emerge
- Preferred network types for edge
- Software engineering practices to focus on ephemeral and headless applets vs. GUI-based transactional apps.

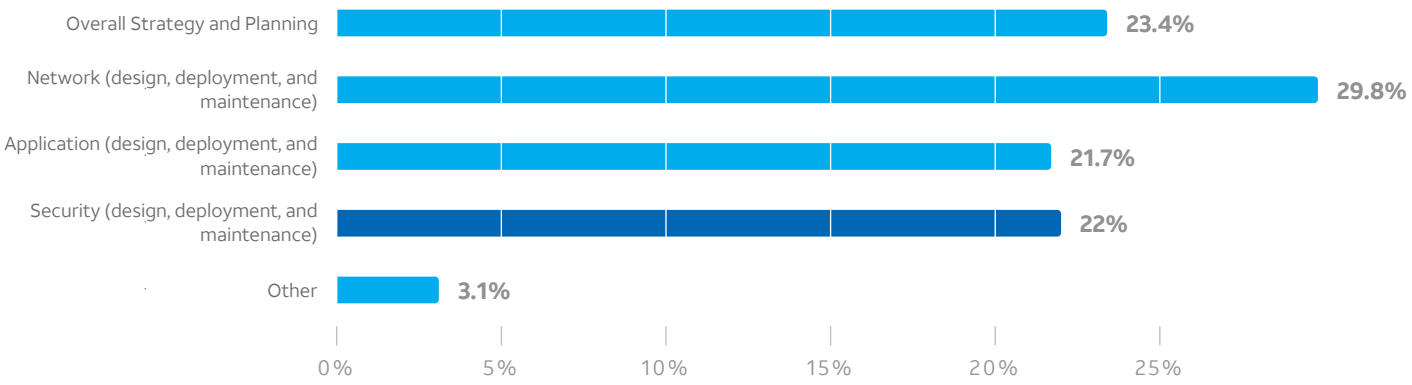
Figure 3

Security is an integral investment for edge

Q. What percent of your organization's total COMBINED investment for your primary edge use case (in production within 3 years) do you anticipate being allocated to the following services?

% of overall spend

Areas of edge investment (percentage of overall spend)



N= 1418 Base All respondents

inventory management in retail and video-based defect tracking in manufacturing

- Outward focus on the use of edge computing oriented to improving customer and/or partner experience; for example, contextual promotions and retail recommendation engines

Investment decisions can benefit from a study of the inward-outward balance in context of business objectives. When edge use cases are implemented properly, they reduce traditional constraints such as bandwidth capacity planning and associated operational costs. More data can be filtered and processed at the edge, thereby reducing traffic to and from the datacenter. Data management methods can help reduce cost. For example, allow point-in-time data to expire where it is and switch from "all data" collection to event-driven collection. Instead of sending temperature every five seconds, send temperature only when it changes.

Another investment nuance is future platform consolidation. It can be hard to predict, but a good concept to keep in mind is that software-based functions and controls will likely be easier to upgrade and more easily accommodate future enhancements than a hardware-based, single-function device.

Think of the edge ecosystem as a new opportunity for competitive differentiation and business outcomes. Edge use cases require edge ecosystem partners that help organizations strike the right balance at the right time and avoid common mistakes by applying best practices. It's all too easy to focus on technical conversations about fixed locations, mobile locations, connectivity, bandwidth, and security and zero in on solving technical issues. The business conversations are about growth opportunities and outcomes dependent on applications and data. The earlier stakeholders can come together and bring along the right edge ecosystem partners, the sooner they can start driving value.

A Focus on Fundamentals

Figure 3 shows the total combined expected investment in primary use cases. Findings are generally consistent across regions, but some industry variations exist. Network investments lead in all regions, followed by overall strategy and planning, security, and applications.

Some applications are 100% at the edge, but a distributed application approach is more common. Expect headless, ephemeral applications such as those in industrial IoT/OT environments to proliferate. Machine-generated data never stops and has different characteristics than human-generated data. Plan for extraordinary volume, velocity, and variety of data, and continue to explore cross-functional opportunities to find value.

Healthcare Edge Ecosystem

Primary use case:

Tele-Emergency Medical Services

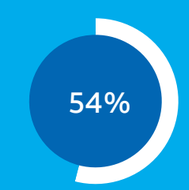
Accelerate diagnosis and initial administration of non-urgent care by extending telemedicine to emergency medical staff in field situations.

Business need:
Make faster and more informed decisions for emergency personnel.

Security approach:
Combine on-premises network and security to mitigate insider threats.

Primary use case snapshot:

Implementation Stage



Planning

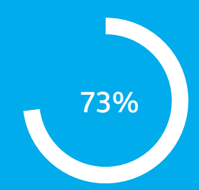
Top Endpoint

Mobile Devices

Data Rate

Enhanced Mobile Broadband (embb)

Edge Network Connectivity



4G/LTE Cellular

Top Perceived Threat

Insider Threat

Cybersecurity Approach

Combined Cybersecurity and Networking Functions On-premises

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 205

Manufacturing Edge Ecosystem

Primary use case:

Smart Warehousing

Enable augmented and autonomous execution in warehouses through integrated demand and consumption insights, process workflows, and physical automation.

Business need:

Manage warehouse output efficiently while adjusting to seasonal capacity fluctuations.

Security approach:

Combine network and security functions in the cloud to mitigate DDoS attacks.

Primary use case snapshot:

Implementation Stage

61%

Partial

Top Endpoint

55%

Industrial Robots

Data Rate

38%

Enhanced Mobile Broadband (embb) and Massive Machine (mmtc)

Edge Network Connectivity

78%

Private 5G

Top Perceived Threat

3.3/5

DDoS

Cybersecurity Approach

55%

Combined Cybersecurity and Networking Functions in the Cloud

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 202

North America expects to spend the most on applications (22.8%).

Network investments lead globally with an average of 29.8%.

Organizations appear to be focusing rightly on the fundamentals before they turn to application development. However, be sure to include application development teams in planning efforts. Strategy and planning investments can contribute to cost efficiency by exploring value opportunities and avoiding rip-and-replace scenarios. The balance across investment areas suggests progress in cross-functional communication, collaboration, and breaking down of silos, all of which in turn help unify go-to-market efforts and hone competitive advantage.

In last year's study, one-third of respondents expected to spend 6–10% and half expected to spend 11–20% on security. This year, security is on par with other investment areas, which are all within the range of 22–30% of overall spend, as shown in Figure 3. This shift indicates that security has become integral to edge use case deployment instead of being an afterthought. Security strategies need to address this reality, particularly in view of the predominance of hybrid environments at the edge and the fact that IT and OT environments are merging and connecting devices of varying functionality, standards, and purpose.

The anticipated security allocation of the U.S. state, local, and education (US SLED) at 24% of overall spend suggests a greater concern about security than other industries (20.8–22.6%). The emphasis on strategy and planning in transportation and retail may indicate these industries are in more of a disruptive mode than other industries.

A three-year outlook on edge strategies and investments points out that industries don't have a single focus. All expect to invest in all studied investment areas. The US SLED expects to make the highest investment in applications (23.8% versus a range of 20.2–22.6% for other industries). Healthcare expects to invest 31.5%, the highest of all industries, in the network category.

Edge is an ongoing investment. Each organization is on a journey to augment existing systems with edge infrastructure and applications. As edge increasingly plays a strategic role in achieving business objectives, edge will follow a life cycle similar to its datacenter and cloud counterparts.

The Intersection of Edge Computing, Networking, and Cybersecurity

All of an organization's edges and edge use cases by design will connect across an increasingly distributed network architecture. Gone are the days in which enterprise network architecture included two distinct places in the network: the campus and the datacenter. Network technologies included the LAN, WLAN, WAN, and the datacenter network, which elegantly connected the campus to the datacenter. Today's enterprise has an expanded geographic footprint, along with increasingly global dispersion of applications, workloads, and employees. This reality requires reexamination of network architectures and how network architectures align to current business dynamics.

The expansion of new networking technologies, topologies, and operating models introduces new challenges for enterprises:

- Using complex network topologies that can impede standardization (Use open standards to increase interoperability.)
- Managing the increased need for observability and management considering heterogenous environments, diverse hardware, multiple types of connectivity, and security controls
- Rethinking the impacts of network design, policies, and operational models in context of converging network functions and security
- Determining how traditional silos, such as IT and OT, and specialized technologies influence network design and operations (Budgets and teams remain siloed, but they're moving toward convergence.)
- Building a "cloud ready" network that provides secure connectivity to applications regardless of residence or access.

The State of Edge

The enterprise edge network infrastructure needs to be inclusive of campus, branch, datacenter, devices, and remote/hybrid work connectivity. As a result of connecting various locations, applications, devices, and things, securing this expanded landscape is an IT imperative and strategic priority. Security can't be an afterthought. Network technologies, like Wi-Fi 6/Wi-Fi 6E, SD-WAN, and multi-gigabit Ethernet switching, are key to edge journeys. Network technologies contain certain levels of embedded security, but IT and security professionals need to be thoughtful about the edge use case– and architecture-specific security policies and controls.

Brownfield Edge Use Cases

A brownfield approach involves reevaluating networks, equipment, systems, and security with an eye to modernization. Evaluation of new technology and new architectural approaches helps determine which assets should be retained and which should be updated or replaced. Modernization of network, equipment, systems, and security at the edge is an ongoing, collaborative effort that avoids rip and replace but likely involves refactoring. An example is the IoT journey:

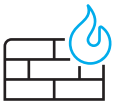
- Step 1. Collect and communicate data from simple use cases. For example, how many times a temperature reading exceeded a certain threshold. The intelligence is in the cloud. The edge serves as data aggregator and processing happens elsewhere.
- Step 2. Apply enriched machine learning to allow better understanding of the data. Remote infrastructures are upgraded to enable distributed processing, which can be moved to where the data resides or data can be moved to where the processing is located.
- Step 3. Use real-time automation to analyze new information to identify actions.

Greenfield Edge Use Cases

Greenfield initiatives differ from brownfield in areas such as decision points, the amount of integration, and accelerated timing. In a greenfield scenario, the IoT journey begins with a clean sheet of paper. Decision makers can leverage collective learnings (internal and external expertise) and increase the chances of getting the use case right the first time. Up-front assessments and gap analysis set a baseline and enable stakeholders to think in terms of phases and required decisions. Common decision points are related to people, resources, deployment, testing, training, continuous assessment, and ongoing optimization.

Project Life-Cycle Management

The edge through line story encompasses both network and cybersecurity as well as two implementation plotlines: brownfield or modernization of existing/legacy infrastructure and greenfield or net-new investments.



State of Edge at a Glance

- Across all edge types, the majority of survey respondents (56%) consider themselves in partial implementation.
- Industrial IoT/OT is the leading edge type (65.4%), followed by IaaS/PaaS/SaaS cloud datacenter (60.4%).
- On-premises private cellular 5G is the leading edge network connectivity (77.1%).
- Personal computers are the leading endpoint type (48.1%), followed closely by mobile devices (47.8%).
- DDoS edges out business email compromise and personal information exfiltration as the most likely perceived threat for primary use cases (mean rating of 3.03 on a scale of 1 to 5).
- Firewall at the network edge continues to be perceived as delivering the most significant cost benefit (38.6%).
- Anticipated edge use case investments are relatively balanced across the strategy/planning (23.4%), network (29.8%), security (22.0%), and application (21.7%) categories.

Edge cloud can be delivered as IaaS/PaaS/SaaS. In the case of retail and SaaS, examples include premade components for people counting/queue management, a smart shopper retail mobile app, and in-store video management systems.

The study data reveals that both in-house resources and a systems integration partner (52.2%) or a consultant (63.5%) collaboratively deliver life-cycle services.

Edge use cases are designed to address specific challenges or opportunities, with business objectives in mind. Ideally, edge use cases involve stakeholders across the organization, including executive leadership, line-of-business managers, and IT/security teams. Line-of-business stakeholders are tasked with achieving business objectives, and they own the data and outcomes. IT and security teams own operations, maintenance, security posture, compliance, and delivery of continuous uptime to support the business. As the to-do list grows, IT teams with limited resources need to balance daily operations and the ability to innovate and accelerate business objectives.

As edge momentum increases and use cases proliferate, in-house IT and security resources may find themselves short of hours, skills, and resources. The study participants were asked who is responsible for specific edge project life-cycle activities such as strategy, planning, design and architecture, integration, adoption, optimization, management and monitoring, and support. Surprisingly, respondents identify in-house resources as the top group responsible for management of these life cycle activities.

Dependence on in-house resources may be viable in early pilot stages for single use cases or deployments of a few endpoints. But they are untenable as use cases become more strategic to the business, involve more complex endpoints, and require a broad partner ecosystem. The study data reveals that in-house resources plus a systems integration partner (52.2%) or a consultant (63.5%) collaboratively deliver life-cycle services. Similarly, in-house resources plus a systems integration or a consultant partner (63% and 70.9%, respectively) collaboratively provide monitoring and management of the edge solution.

Consider an edge project life cycle that encompasses the plan, build, and run/manage phases delivered by an ecosystem of partners. The project lead must demonstrate how investments in people, processes, tools, and technologies help accelerate and de-risk an edge solution deployment. It's highly unlikely that a single vendor can provide everything needed for an end-to-end edge use case. Look for vendors with strategic relationships in the ecosystem. Generally, use cases are assemblies of custom and industry-available technologies offered by hardware, software, and service providers.

Systems integrators, managed service providers, and professional services arms of telcos possess the skills, resources, and technical expertise to lead edge projects, vet ecosystem partners, support interoperability, test configurations in labs, or use new techniques such as digital twins to bring edge use cases to life. These providers have developed defined and repeatable methodologies for deployment and operations as well as best practices and reference architectures that are aligned to specific industries to provide consistency and reliability. A comprehensive solution approach includes assigning responsibilities to professional services, a hybrid role (professional services/client/third party), and clients and/or third parties.

Edge Use Case Overview

Edge use cases are an ideal portal to understanding the state of edge and the importance of holistic thinking about edge, networking, and security. This report explores both general cross-industry use cases and industry-specific primary use cases. Figure 4 shows the general use cases expected to be in production within three years. Industrial IoT/OT functions rank highest this year, as they did last year.

The study also examines six stages of edge compute adoption (ideation, research, planning, proof of concept [POC], partial implementation, and full implementation) in seven industries. For simplicity, the six stages are conflated to three, and this report focuses on mature stage primary use cases:

- Low stage: Ideation and research
- Midstage: Planning and POC
- Mature stage: Partially implemented and fully implemented

Implementation stages are fluid, given evolving regulations, industry standards, ancillary use cases, and modernization and optimization efforts. Figure 5 shows the distribution of edge use cases expected to be in production within the next three years across implementation stages. Organizations in the earlier stages will quickly begin to understand the complexities and intricacies of implementing and managing an edge solution and build

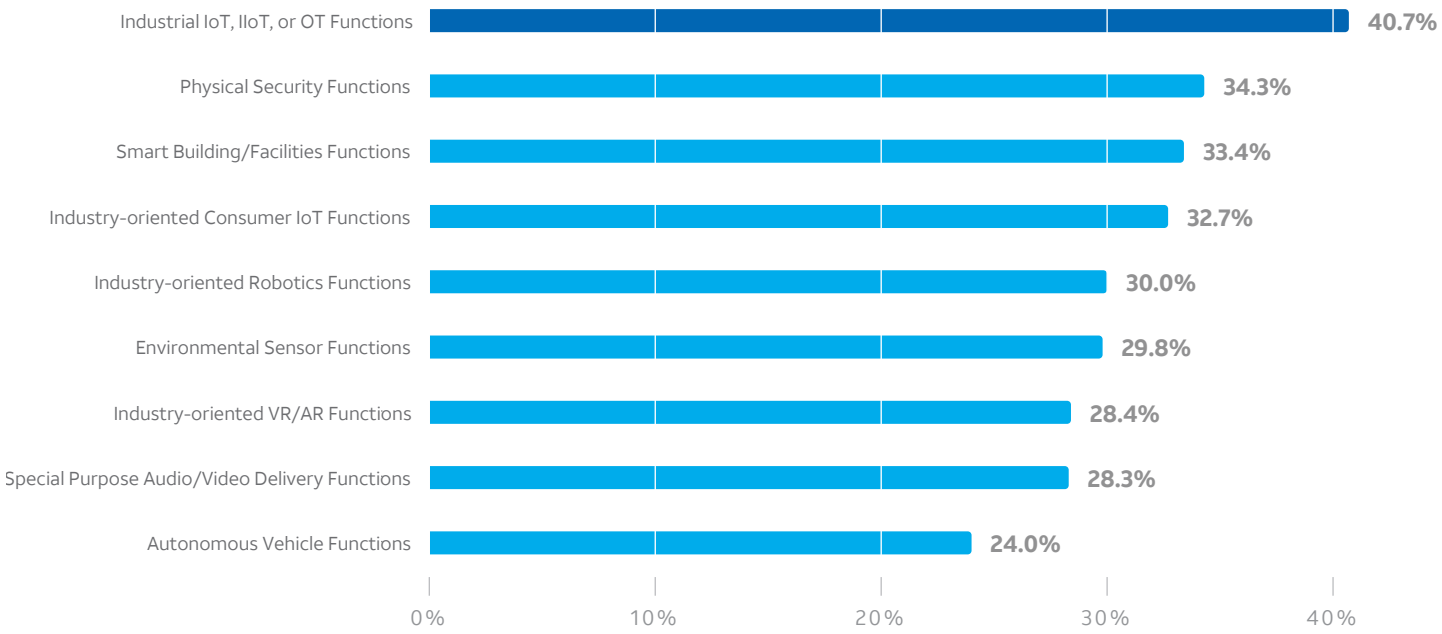
Figure 4

IoT and OT functions lead use case initiatives

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

% of respondents

Production use cases anticipated within the next three years



N= 1418 BASE All respondents

a partner ecosystem to help complete or accelerate project deployment.

Partially implemented use cases are most prevalent, which matches findings from the 2022 research. In 2023, 56% of respondents (data not shown) have at least one partially implemented edge use case.

Of all use cases, 61% are in the ideation, research, planning, and proof-of-concept stages. Nearly 40% of use cases are partially or fully implemented. Compared with 2022, the ratio of use cases in early stages versus later stages has shifted, potentially giving the impression that companies are falling behind in their deployments. This is not the case. The overall volume of use cases under development has increased, meaning that successful implementations led to the addition of more use cases in early stages as these deployments expand in scope and reach.

The US SLED sector has the highest combined number of use cases considering the midstage and mature stage, followed by manufacturing. This mirrors the top two industries noted last year. The maturity of US SLED reflects in part the record revenue that state governments experienced in FY22. The types of edge computing use cases in the US SLED area, such as mass transit management and optimization or the automation of public services, have received broad bipartisan support.

Edge Use Cases by Industry

Seven industries are studied in this report: finance, healthcare, retail, manufacturing, energy and utilities, US SLED, and transportation. The industries naturally support a highly distributed deployment model, and they've emerged as early developers of edge use cases. Against this backdrop, development and implementation commonalities emerge although implementation stages vary among industries.

How do this year's primary use cases compare with last year? Across all industries, the primary use cases are different (see Table 1). Shifts may occur due to organizational maturity, including the use of enriched machine learning and analytics, as well as decisions about resource use and business objectives.

Edge Network Connectivity Choices

Edge solutions present various connectivity choices, and enterprises must carefully evaluate which connectivity solution will deliver the best results from a bandwidth, security, cost, and operational perspective.

While private 5G is the new shiny technology, it may not be right for every use case. Technologies such as 4G/LTE and Wi-Fi/Wi-FI 6 may be good enough. One dynamic to consider is that private 5G networks deliver a high-speed, low-latency, closed-loop network that does not allow access to the public internet.

Highly sensitive industries, such as finance and energy and utilities, require a closed-loop function for security reasons. Industries such as manufacturing and retail use a private 5G network for its ability to deliver low latency for real-time insights as well as security benefits. Transportation, healthcare, and US SLED utilize 4G/LTE cellular, as this may be their best fit because public 5G is not regionally pervasive at this time.

In most implementations, networks for edge use cases will be a hybrid model that combines public and private or hybrid 5G models along with 4G/LTE cellular and even Wi-Fi in certain cases. Why? Because organizations have already made investments, and they adopt higher-speed networking solutions. Speed, low latency, security, availability, and cost all factor into connectivity choices.

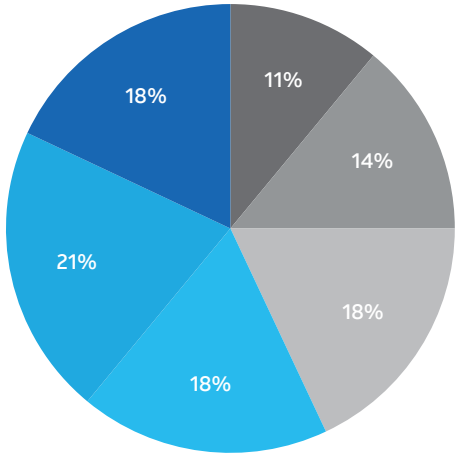
Figure 5

Initial success accelerates development of more use cases

Q. You indicated your organization expects to be using the following EDGE 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 use cases

Stages of edge use case deployment



Ideation
Researching
Planning
Proof-of-concept
Partial Implementation
Fully Implemented

N= 1418 BASE All respondents

Figure 6 shows anticipated solutions for supporting edge use cases in the next three years. On-premises private cellular 5G is the edge network connectivity choice that leads overall, and 4G/LTE is the second choice in several industries. Notable exceptions include:

- Healthcare, transportation, and US SLED expect to deploy 4G/LTE as their primary type of connectivity.

Table 1

Primary use cases changed in all industries

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

Primary use cases changed in all industries

Industry	Primary Use Case 2023	Primary Use Case 2022
Healthcare	Tele-emergency Medical Services	Consumer Virtual Care
Manufacturing	Smart Warehousing	Video-based Quality Inspection
Retail	Real-time Inventory Management	Loss Prevention
Energy and Utilities	Intelligent Grid Management	Remote-control Operations
Finance	Real-time Fraud Prevention	Concierge Services
US SLED	Building Management	Public Safety and Enforcement
Transportation	Fleet Tracking	N/A

N= 1418 BASE All respondents

- Finance, retail, and manufacturing expect to deploy hybrid private cellular 5G as their second choice following on-premises private cellular 5G.
- Within US SLED, more than one-quarter of respondents choose Wi-Fi 6 and 40% choose public network. Wi-Fi 6 technology is robust and can be managed easily in the cloud. Cost is a significant consideration, and the expense of building and operating another high-speed network without a specific use case is difficult to justify. In addition, leveraging the public network is appropriate for public-facing use cases (those that may not require a closed-loop private function).

Considering all edge types planned to be connected in the next three years, the majority of respondents consider themselves in partial deployment. All industries anticipate connecting all edge types in the next three years (see Figure 7). Industrial IoT/OT environments lead, followed by IaaS/PaaS/SaaS cloud datacenters. Consumer IoT/OT edges rank lowest, which is consistent with last year's finding.

US SLED stands out with highest anticipated IaaS/PaaS/SaaS cloud connectivity.

Retail Edge Ecosystem

Primary use case:

Real-Time Inventory Management

Enable near real-time visibility of product inventory in physical and virtual environments via IoT and collaborative edge ecosystem partner relationships.

Business need:
Improve omni-channel orchestration and inventory fulfillment service levels.

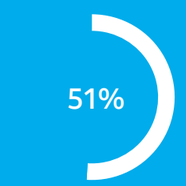
Security approach:
Combine network and security functions in the cloud to thwart potential DDoS attacks.

Primary use case snapshot:

Implementation Stage

Partial

Top Endpoint



Personal Computers

Data Rate

Enhanced Mobile Broadband (embb)

Edge Network Connectivity

Private 5G

Top Perceived Threat

DDoS

Cybersecurity Approach

Combined Cybersecurity and Networking Functions in the Cloud

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 201

Energy and Utilities Edge Ecosystem

Primary use case:

Intelligent Grid Management

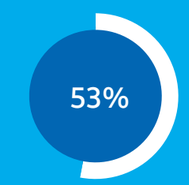
Achieve improved power flow management and predictability, quality, and asset performance through detailed models and simulations of grid performance.

Business need:
Improve security posture, cost management, and asset performance.

Security approach:
Combine network and security functions on-premises to protect against exfiltration of personal information.

Primary use case snapshot:

Implementation Stage



Partial

Top Endpoint

Mobile Devices

Data Rate

Massive Machine (mmtc)

Edge Network Connectivity

Private 5G

Top Perceived Threat

Personal Information Exfiltration

Cybersecurity Approach

Combined Cybersecurity and Networking Functions On-premises

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 203

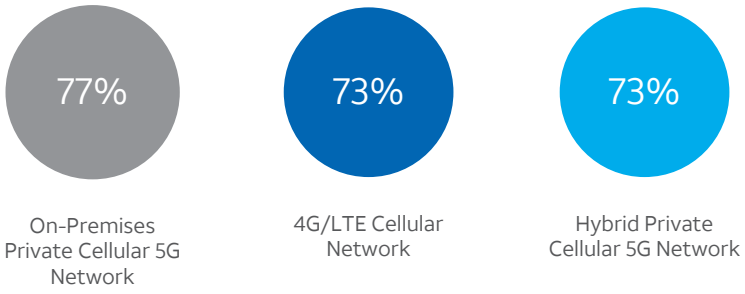
Figure 6

Private cellular remains leading edge network environment

Which EDGE NETWORK CONNECTIVITY solutions do you expect to deploy to support these use cases in the next 3 YEARS?

% of respondents

Edge network connectivity solutions expected to be in use within the next three years



N= 1418 BASE All respondents

Trends in Endpoint Development

Edge use cases may require highly engineered, purpose-built endpoints such as robotic arms or sensors that are products of extensive research and development. As the development of edge use cases advances, diverse types of endpoints will become available. The introduction of new endpoints depends on the availability of enabling chipsets such as 5G chips. However, in this study, the predominant endpoints today across all industries are personal computers and mobile devices. Certain industries show fairly high use of special-purpose fixed-location endpoints (see Figure 8).

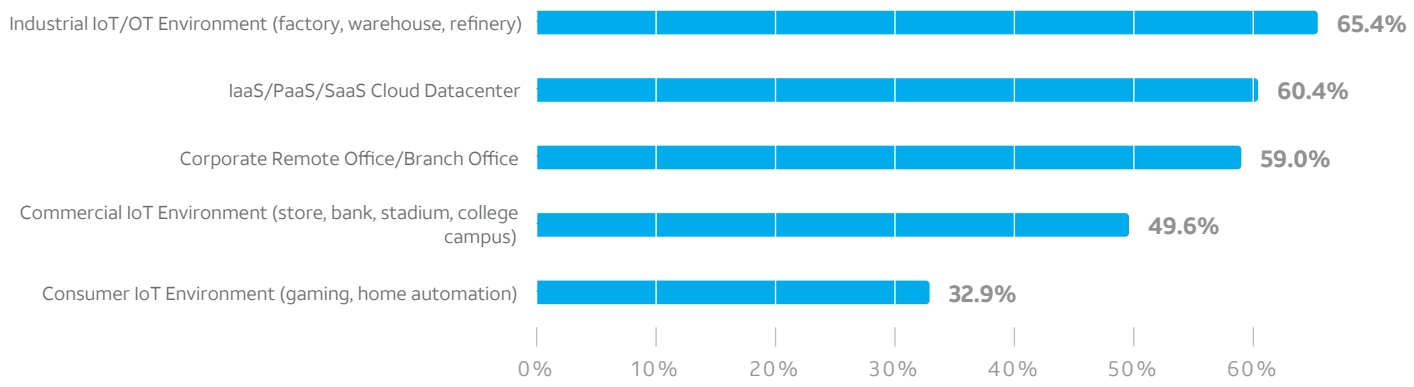
Multi-access edge computing (MEC) devices are an area of continuing interest. Small form factor appliances bring compute and storage capabilities closer to where the data is being generated, thereby eliminating the need for the data to be backhauled to a datacenter to be acted upon. The high speed and low latency of 5G networking will only accelerate MEC use cases, such as robotics for manufacturing, traffic intelligence for public safety, or high-speed trading on a financial exchange trading floor.

Figure 7

Plans in place to connect all edge types

Q. What type of "EDGES" are you planning to connect in the next 3 years?

% of respondents



N= 1418 Base All respondents

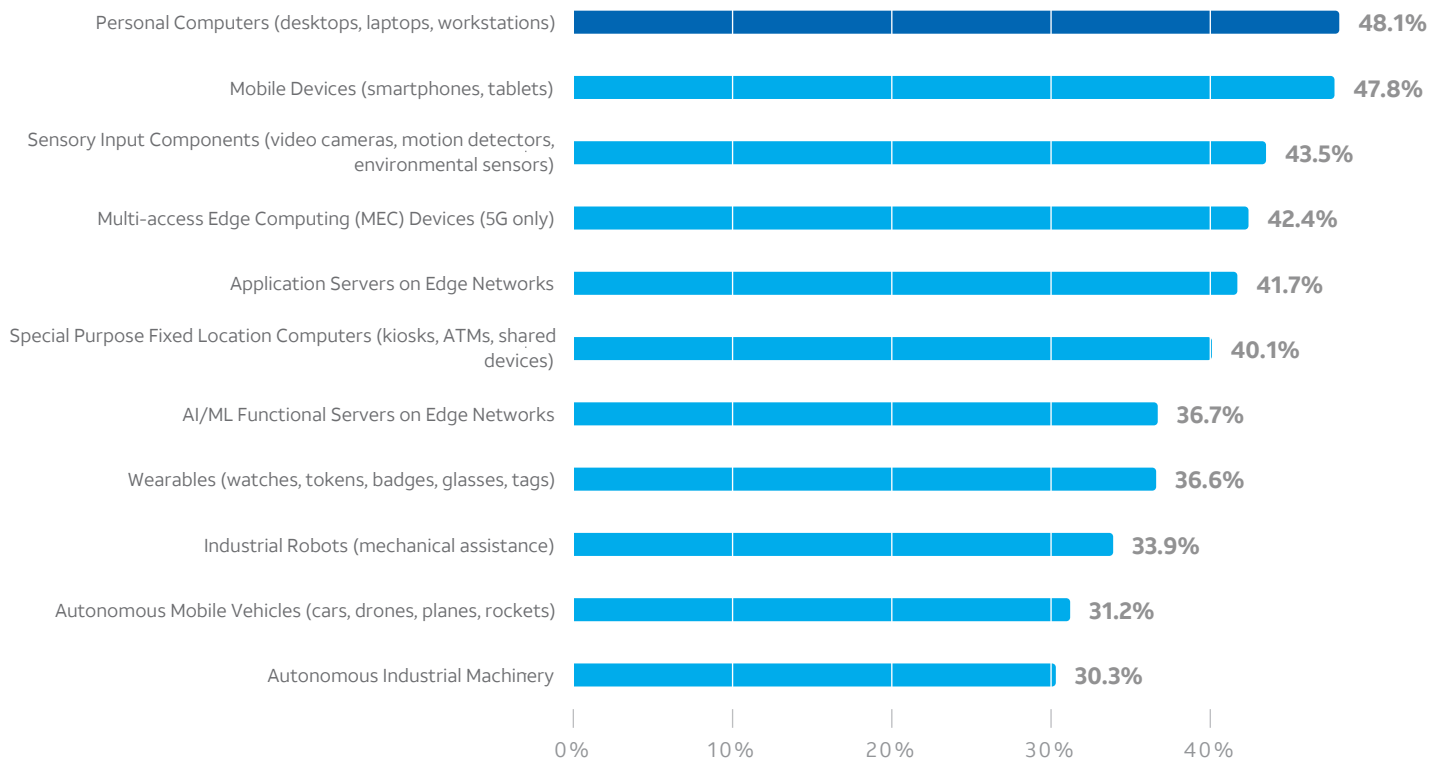
Figure 8

PCs and mobile devices remain the prevalent endpoint types

Q. For your primary use case, which types of endpoints will be used?

% of respondents

Endpoints planned for primary use case



N= 1418 BASE All respondents

Risk Considerations Associated with Edge Types

Industrial IoT/OT is the top edge type planned for connection, followed by cloud datacenters.

Risk considerations are specific to each type of edge. Stakeholders will want to explore risk tolerance and security controls specific to each edge use case, particularly when they connect new edge types.

Each edge use case faces different risks, new and legacy, that need to be on the radar of risk management programs and solution architects. Some edge use cases simply extend existing risks that are inherent in classic environments — for example, protecting the privacy of a customer who enters a grocery store loyalty number into a cashierless checkout or a staffed cashier station, or implementing cashierless scenarios that use technology such as video analytics and machine learning to determine the accuracy of the total. In both cases, the loyalty information needs to be protected during transmission and verification.

For all edge types, consider risk associated with the software in edge use cases. Software bills of material (SBOMs) are an increasingly critical and required element of the software life cycle. SBOMs show exactly what is in the software package and its origin. As software packages change, accurate SBOMs can support accurate logs of modifications and potential impacts to the edge ecosystem. When IoT devices are widely used, SBOMs make it possible to complete a full software inventory. Teams can check for vulnerabilities in one domain, such as the introduction of an application with open source components, prior to deploying an edge use case. Consider the complete SBOMs during triage of new vulnerabilities and risk evaluation.

The industrial IoT/OT edge, which is the top edge type that respondents plan to connect in the next three years, has changed significantly. Use cases in this area are likely to see greater regulatory oversight. The CIA triad of confidentiality, integrity, and availability flips upside down with availability becoming more prominent. Confidentiality and integrity are still valid, but edge use case criticality elevates availability or lack thereof.

Some edge computing device operating systems (OSs) lessen the likelihood of attacks due to the uniqueness of the OS. A more popular OS such as Contiki or RIOT is less costly for cybercriminals to attack as their underlying code can be utilized against a larger potential list of devices. Economics matter, especially for criminal gains that are seeking monetary gains.

The XorDdos Linux malware, for example, is architected to work on multiple chipsets. The XorDdos Linux malware gains an initial foothold on the targeted IoT devices through brute force attacks. When enough devices are infected, they are used to launch DDoS attacks.

Older Windows systems such as Windows 7 and Windows XP typically don't have up-to-date, embedded protections. IoT/OT environments also contain older communications protocols and data formats that must be translated before connecting to external applications. Owing to their age, these devices can be difficult to patch, in part because the manufacturers may be out of business. Replacement conversations with the chief financial officer or chief operating officer can be difficult, considering the large capital investment in potentially obsolete but critical equipment. Consider the use of endpoint detection and response (EDR) and extended detection and response (XDR) platforms to monitor and detect attacks when patching is no longer a viable option.

Compensating controls such as increased monitoring or network segmentation can make up for the lack of available embedded cybersecurity controls and the inability to patch. Consider a scenario in which an IoT/OT edge computing use case relies solely on the ability to patch onboard/embedded systems. This presents a risk that the next published common vulnerabilities and exposures (CVE) that mentions the device may be a wake-up call for defense in depth.

Cloud datacenters, the second most common planned edge type, are generally more resilient by nature. Diverse network connections and virtualized computing devices help reduce

Table 2 **Likelihood of attack types for primary use case**

Rank	Attack	What Is It	Potential Damage
1	Distributed Denial of Service (DDoS)	Disruption of normal traffic of connected devices, applications, or websites that degrades or shuts down an organization's ability to conduct normal operations.	Business income losses due to downtime. Remediation to distinguish between legitimate and attack traffic.
2	Business E-mail Compromise	Typically leverages compromised credentials of email accounts in order to impersonate a person of authority and attempt to trick a staff member into transferring funds to a fraudulent account.	Acquisition of sensitive information such as account numbers, credit card details, company trade secrets, or privately held information such as personally identifiable information (PII) or protected health information (PHI).
3	Personal Information Exfiltration	The unauthorized transfer of information from an organization to places outside of the organization through downloads to unsecure devices, social engineering, or transmission of information by insecure/unencrypted means.	Costs associated with extortion and loss of intellectual property.
4	Phishing	A common entry point for other attacks, phishing prompts a recipient to open an attachment or click on a URL that can either deposit a malicious executable or be utilized to capture credentials by mimicking legitimate websites.	Loss of PII, credential theft, or destructive results of a ransomware attack.
5	Insider Threat	A person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.	The theft or leakage of sensitive information, whether accidental or with malicious intent can incur forensic and remediation financial costs, as well as institutional losses due to the unauthorized access of sensitive information.
6	Account Takeover	An attempt through social engineering or brute force attacks to gain the credentials of the target.	Running up charges for computing when done in a cloud environment.
7	Nation-state Cyber Attack	Attacks by organized crime groups, often with tacit backing of governments or groups sympathetic to the government.	Espionage/spying activities, ransomware, and physical damage due to the disruption of normal IT activities.
8	Ransomware Attack	Involves actual attack or threat to block access to IT systems and data unless a ransom is paid. The ransom request is often sent after sensitive data has been exfiltrated. The ransomware actor threatens to divulge the data, permanently block access, or both unless the ransom is paid.	Financial losses due to ransom payment, downtime due to systems not available, institutional reputational damage, costs of remediation, and cyber insurance deductibles.

N= 1418 BASE All respondents

the need to keep data in other remote locations. Data in transit, however, requires protection. Sending data to the cloud from remote locations may require a path that includes a mix of more secure methods such as private 5G and less secure methods such as 4G. Consider piggybacking off SD-WAN rollouts in the enterprise or initiating an SD-WAN solution to achieve greater control over routing and path selections. After the data is in a cloud datacenter, use cybersecurity controls such as a next-generation firewall (NGFW) or an XDR platform to monitor signs of an attack.

A corporate remote office/branch office (ROBO) priority is securing data that's being processed. ROBO edges can be attack targets since ROBO edges typically don't have the full-scale protections of a corporate main office, nor are ROBO edges managed by local IT staff. Lower operational visibility in ROBO locations calls for extra attention to security function governance.

Commercial IoT environments generally lack the resilience of a virtualized cloud datacenter environment. Commercial IoT environments can carry increased risk due to public exposure, which suggests physical security considerations to prevent physical attempts to steal or destroy data. This risk can be addressed by locked cabinets and chassis intrusion detection sensors. Future choices, based on edge infrastructure supplier experiments, may include onboard GPS tracking to help prevent compromise. Ideally, data is created, processed, and moved quickly to its final destination.

Consumer IoT edges offer rich, exposed attack surfaces. In retail or other uncontrolled environments, for example, the public nature of these devices can lead to potential compromises. Electronic access or physical access to certain people can be limited more easily in other edge types compared with consumer IoT. Solution architects need to consider the possibility of physical theft of the devices deployed in use cases. Encryption of data at rest becomes a requirement when sensitive data potentially can be extracted physically.

Edge Use Case Risk

If money was no object, organizations could apply resources to all attack vectors for every conceivable type of attack. Budget limitations require more likely attack vectors to receive more funding than less likely attack vectors. Decision makers who are familiar with types of attacks can better understand likelihood and potential impact.

Table 2 describes common attack types for which survey respondents rate the likelihood of attack. Table 3 lists the attack types ranked by the survey respondents' answers in descending order.

Likelihood of Attack, Compromise, and Impact

As shown in Table 3, types of attacks vary by industry, with notable variances in some edge use cases. Overall, survey participants perceive DDoS as the most likely attack, followed closely by business email compromise and personal information exfiltration. Retail is most concerned about DDoS, and finance is a close second.

Surprisingly, ransomware is viewed as having the lowest overall perceived likelihood of attack. Every industry ranked ransomware the lowest except for US SLED. There isn't a huge spread (3.03 versus 2.80) between DDoS and ransomware. This seeming lack of concern for ransomware may point to organizational spending during the past 24 months to fortify against ransomware and educate users. However, ransomware's continued assault against targets is relentless. Perhaps the threat actors are cycling with the rise and fall of different types of attacks. While ransomware ranks low as an attack type, ransomware remains a concern for edge.

A possible explanation for the lower perceived likelihood of ransomware attacks against edge computing devices relates to the operating systems. OSs embedded in edge IoT devices make it costly for financially motivated ransomware operators to write and deploy destructive code. For example, the cost is higher to target an IoT edge computing infrastructure that runs an embedded-altered version of Linux than it is for a Windows-based device.

Businesses in the finance industry historically have invested heavily in cybersecurity due to the sensitive financial information they handle. The higher level of spending hasn't resulted in a lower level of concern related to the perceived likelihood of an attack. Finance has the highest attack concern of all industries. Healthcare respondents exhibit the lowest concern of an attack.

Healthcare's tele-emergency medical services use case shows ransomware is a low concern — 2.11 on a 5-point scale (5 is the highest likelihood of an attack). The lower concern may be due to the specialized types of devices in use, along with the specialized operating systems that make launching ransomware attacks cost prohibitive, and potential use of stringent network segmentation schemes. Insider threats and the possibility of exfiltration and sale of personal health information are top concerns for healthcare.

Time sensitivity factors into retail's real-time inventory management and finance's real-time fraud prevention. These use cases can't fulfill their missions when the network is degraded or brought down by a DDoS attack. It follows logically that DDoS is perceived as the most likely and second most likely attack type, respectively, for these use cases. Respondents suggest they are concerned about both perceived likelihood of an attack and perceived impact of an attack.

Real-time inventory management shows the largest combined drop-off of close to 25% in 2023 compared with 2022 related to assessing the impact of a successful compromise. Some of the supply chain worries that gripped countries in 2021 and early 2022 have eased, allowing for more breathing room on inventory management. But supply chain issues are far from over. Increased supply chain resilience may be easing concerns of the edge use case stakeholders that previously had the highest fears of the perceived impact of a successful compromise.

Real-time fraud prevention reveals the smallest drop in the combined grouping of perceived likelihood of compromise and perceived impact of a successful compromise. The speed at which transactions occur is accelerating. Computing resources need to detect the literal "needle in a haystack" in real time, making this use case particularly sensitive to disruption. The return on investment of making real-time fraud detection resilient to cyberattacks can be measured by assessing the cost of the fraud that can occur during downtime.

The use of cyber as a geopolitical weapon has forced government regulators and security leaders to be aware of possible destructive nation-state cyberattacks. Yet building management in US SLED and fleet tracking in transportation are the only use cases for which nation-state cyberattacks crack the top 3 in perceived likelihood. It's urgent for chief risk officers to engage IT, security, and line-of-business leaders to be sure that proper resources and attention are paid to this attack vector. Multiple threat intelligence sources, for example, can provide specific guidance and warnings on possible hostile actors.

Ransomware is viewed as having the lowest overall perceived likelihood of attack on primary use cases.

Finance Edge Ecosystem

Primary use case:

Real-Time Fraud Prevention

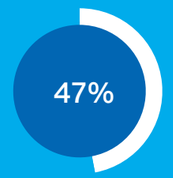
Monitor bank accounts, financial transactions, accounting invoices, purchase orders, and other financial documents and analyze data through enriched machine learning techniques.

Business need:
Improve the ability to identify potentially fraudulent activity in near real-time.

Security approach:
Combine network and security functions in the cloud to help prevent phishing.

Primary use case snapshot:

Implementation Stage



Full

Top Endpoint

Fixed Location Computers Such as Kiosks

Data Rate

Enhanced Mobile Broadband (embb)

Edge Network Connectivity

Private 5G

Top Perceived Threat

Phishing

Cybersecurity Approach

Combined Cybersecurity and Networking Functions in the Cloud

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 204

US SLED Edge Ecosystem

Primary use case:

Building Management

Provide visibility into a building's energy and operational status through advanced technologies that help automate energy and operational functions to optimize performance and cost.

Business need:

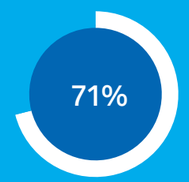
Optimize building management performance and energy efficiency through increased automation.

Security approach:

Combine network and security functions on-premises to thwart perceived ransomware threats.

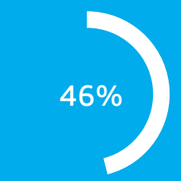
Primary use case snapshot:

Implementation Stage



Partial

Top Endpoint



Mobile Devices

Data Rate

Enhanced Mobile Broadband (embb)

Edge Network Connectivity

4G/LTE Cellular

Top Perceived Threat

Ransomware

Cybersecurity Approach

Combined Cybersecurity and Networking Functions On-premises

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 201

Table 3

DDoS attacks seen as most likely to occur

Q.In your opinion, how likely are the following attacks to occur for your primary use case?

Scale:
1=Very Unlikely;
5=Very Likely.

Perceived likelihood of attack types for primary use case

	Total	Finance	Healthcare	Retail	Manufacturing	Energy	Transportation	US SLED
DDoS (disrupt website availability and/or functionality)	3.03	3.28	2.93	3.33	3.15	3.00	2.82	2.67
Business Email Compromise (financial gain via fraud)	3.00	3.41	2.92	3.26	3.00	2.89	3.06	2.47
Personal Information Exfiltration (financial gain, espionage, extortion)	3.00	3.34	2.70	3.13	3.02	2.91	3.00	2.91
Phishing (credential theft)	2.98	3.33	2.86	3.12	3.02	2.85	2.93	2.78
Insider Threat (personal gain or vendetta)	2.97	3.27	2.75	3.22	2.90	2.86	2.94	2.87
Account Takeover (hijack network and/or compute resources)	2.96	3.31	2.71	2.95	3.00	2.91	3.11	2.76
Nation-state Cyber Attacks (disrupt/corrupt critical infrastructure, cause public distrust, conduct espionage)	2.95	3.17	2.74	2.99	2.95	2.99	3.00	2.80
Ransomware Attack (financial gain via extortion)	2.80	3.11	2.42	2.90	2.84	2.78	2.69	2.85

N= 1418 BASE All respondents

Changing Risk Perceptions

It's somewhat perplexing that every size of organization in every industry in every country perceives a lower concern about likelihood of edge use case compromise this year compared with last year (see Figure 9). A similar decline appears in perceived concern about the impact of a successful compromise this year compared with last year.

Has the cybersecurity maturity level of organizations increased markedly in one year? Some of the optimism likely comes from maturity associated with one more year of edge computing experience. Lessons learned and investments in edge computing resilience may give stakeholders some relief. Still, the 28% increase in optimism in the perceived likelihood of a compromise and the 26% optimistic shift downward of perceived impact of a successful compromise deserve a dose of realism.

Respondents may be expressing optimism regarding perceived impact because certain edge use cases were necessary during the COVID-19 pandemic. Home healthcare, for example, was a life-saving necessity during a time when someone who walked into a hospital might come down with COVID-19. Fast forward one year, and remote healthcare is viewed by many as a convenience more than a necessity. If a DDoS attack takes down the ability to provide remote care, healthcare circa 2019 still works. On the contrary, if an attack spreads inside a hospital's IT systems, the consequences can range from delayed appointments and procedures to serious life and death repercussions. The dependence of healthcare systems on the ability to communicate remotely with patients and remote specialists means that DDoS attacks, like ransomware attacks, can also have life and death consequences.

Increased communication between IT, the C-suite, and cybersecurity also plays a role in easing some fears. Many edge use cases expand organizational capabilities in areas distant from the traditional office or datacenter. Some new capabilities require significant funding. When the push to the cloud first occurred, the security ramifications of the expanded attack surface were sometimes not taken into account. The results of not bringing cybersecurity into that mix are apparent. Edge computing is a benefactor of the lessons (and the pain) caused by insecure digital transformation. Stakeholders are increasingly aware they need to take a holistic view of the expanded attack surface associated with edge computing.

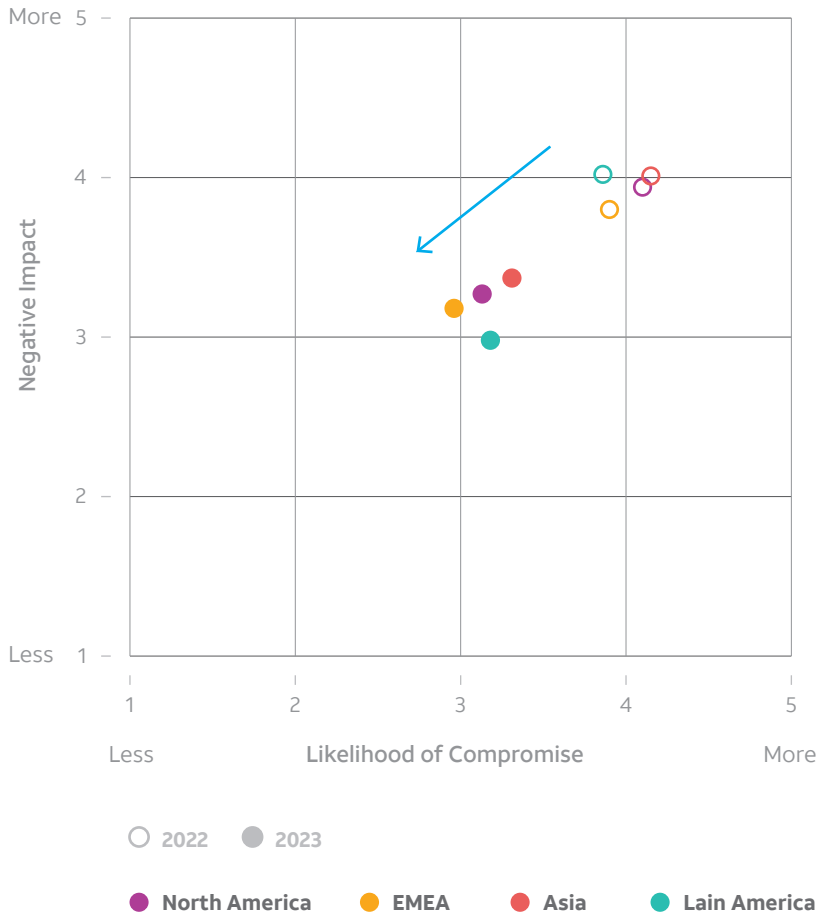
At the country level, the United Kingdom shows a 6% decrease in the perceived likelihood of compromise, a finding that is significantly lower than the 28% average for all countries. The United Kingdom shifted from the bottom tier of being less concerned about the perceived likelihood of a compromise in last year's study to being the second most concerned in this current study. In part, the shift may be explained by a heightened awareness of the risk of fallout from geopolitical activities on the European continent, including the potential use of cyberattacks in kinetic warfare.

Concerns related to the likelihood of a compromise, as well as the impact of successful compromise, are significantly lower in 2023 compared with 2022.

Figure 9

Concerns around the likelihood and impact of a compromise have declined

Scale: 1=low likelihood/low impact; 5=very likely/very impactful.



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. Please use your best judgement.

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. Please use your best judgement.

N= 1418 BASE All respondents

Cybersecurity Controls

Edge use case maturity sets the stage for cybersecurity controls, a topic on which survey respondents have significantly different perspectives. The respondents represent a range of edge use case experience that is consistently distributed across all sizes of organizations.

Stages of implementation also have a clear relationship to use case maturity. The findings suggest that organizations with four mature use cases (use cases either partially or fully implemented) are farther along in their edge journeys than organizations with fewer mature use cases.

Cost-Benefit Overview

Network cybersecurity controls are viewed as most beneficial by the highest number of organizations surveyed, but perspectives vary. Figure 10 indicates that many of the controls have equal representation between most beneficial and not worthy. Overall, respondents perceive that standard network controls and monitoring capabilities provide the greatest benefit. However, similar to last year's findings, the first three controls — firewall at network edge, intrusion/threat detection, and network access restrictions — stand out for their most beneficial ranking, potentially because of their highly practiced use. IPS/IPD systems, for example, provide advance threat notifications that allow security teams to take countermeasures before disruptions occur.

In last year's study, patching received the worst cost-benefit rating overall. Again this year, patching hovers near the bottom of cost-benefit ratings. Perhaps the rating reflects the imprecision in measuring the full benefit of security practices such as disciplined, automated patching that reduce exposure. This practice proactively reduces exploitability and cyberincidents by removing known vulnerabilities in an organization's IT estate. In addition, patching can reduce the volume of alerts, leading to a time savings for security teams.

A contrasting finding is that DDoS is perceived as the most likely attack threat, but the perceived benefit of DDoS mitigation ranks low. Like patching, DDoS mitigation may not be viewed by survey respondents in its full, proper context. DDoS mitigation is a form of insurance for organizations' public-facing websites. But rather than paying out after a DDoS attack, DDoS mitigation pays out during the attack by defusing DDoS attacks as they unfold. When DDoS mitigation solutions operate as designed, they help organizations avoid website-affecting incidents. In addition, an effective DDoS mitigation solution acts as a deterrent by indirectly signaling to would-be attackers that their cost to attack will be higher and their likelihood of success lower.

DDoS is perceived as the most likely threat overall to primary use cases, but the perceived benefit of DDoS mitigation is low.

Implementation of Cybersecurity Functions

Organizations commonly employ multiple implementation approaches for cybersecurity functions in their primary edge use cases. Respondents weigh in on these choices:

- Single-function on premises, such as dedicated hardware or software firewall
- Multiple cybersecurity-only functions on premises, such as unified threat management
- Combined cybersecurity and network functions on premises, such as network + security appliance
- Combined cybersecurity and network functions in the cloud, such as SASE as a service
- Dedicated cybersecurity-only functions in the cloud

Two-thirds of organizations (67.4%) use at least two implementation approaches. One-third of organizations (33.5%) use three or more implementation approaches. The use of multiple implementation approaches is even higher for organizations with more edge use cases that are either partially or fully implemented (79% of organizations use two or more implementation approaches and 45% of organizations use three or more implementation approaches).

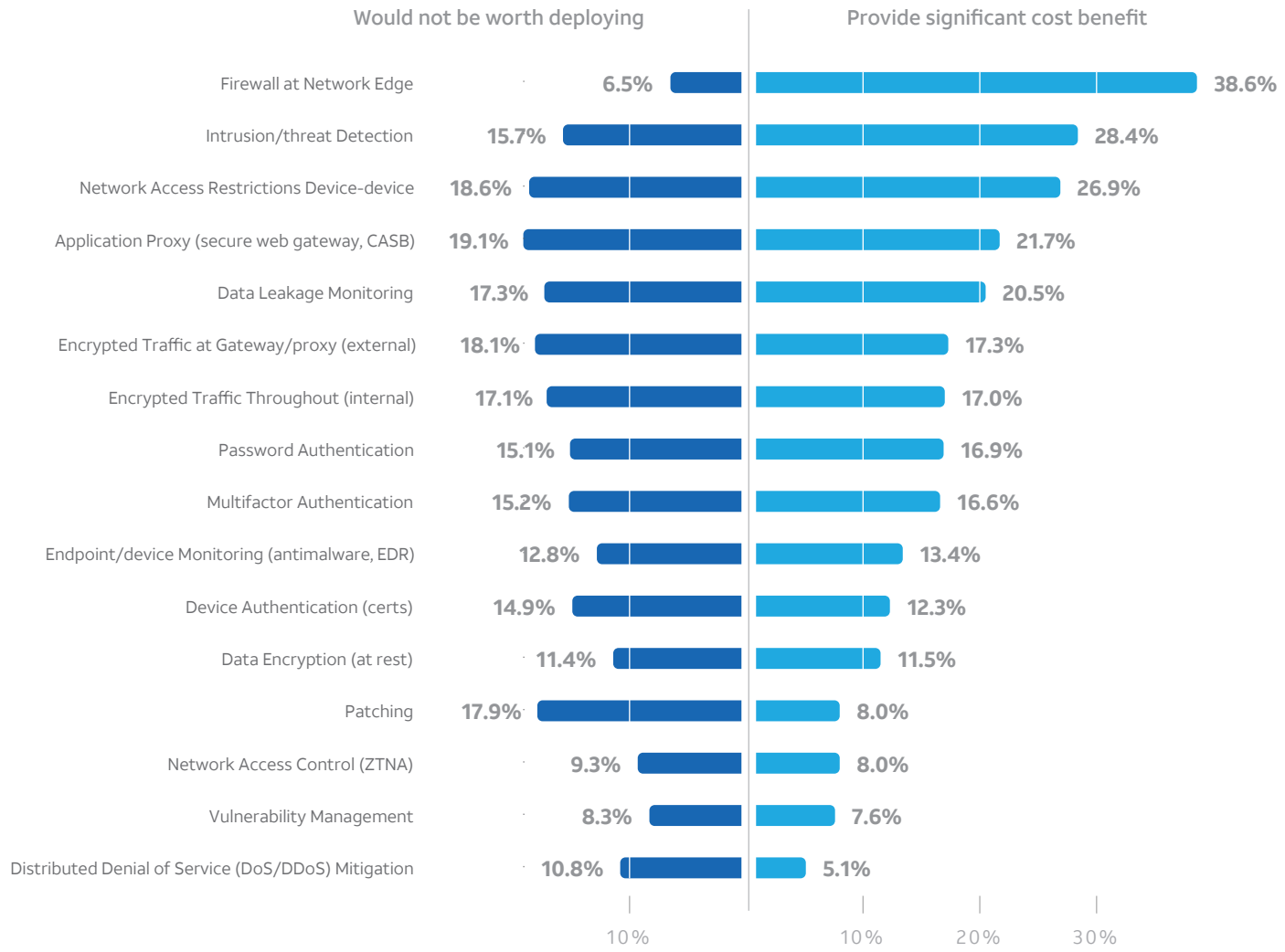
67% of total respondents implement at least two types of cybersecurity functions. One-third of respondents implement three or more types of cybersecurity functions.

Figure 10

Edge firewalls offer greatest perceived cost-benefit

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= 1418 BASE All respondents

Organizations with more partially or fully implemented edge use cases tend toward cybersecurity implementation approaches that combine multiple cybersecurity functions or combine cybersecurity and networking functions into a single location. For example, organizations may opt for on-premises or as-a-cloud service versus an on-premises appliance for a single cybersecurity function or a cloud service only for cybersecurity functions. On average, 58% of organizations with four partially or fully implemented use cases use one or more of the combined approaches versus 42% of organizations with zero partial or fully implemented use cases.

What drives the use of multiple implementation approaches? One reason is experience. Edge-experienced organizations find there isn't one best implementation approach for cybersecurity functions across all of their edge use cases. Another reason is history. An organization starts with one implementation approach and determines

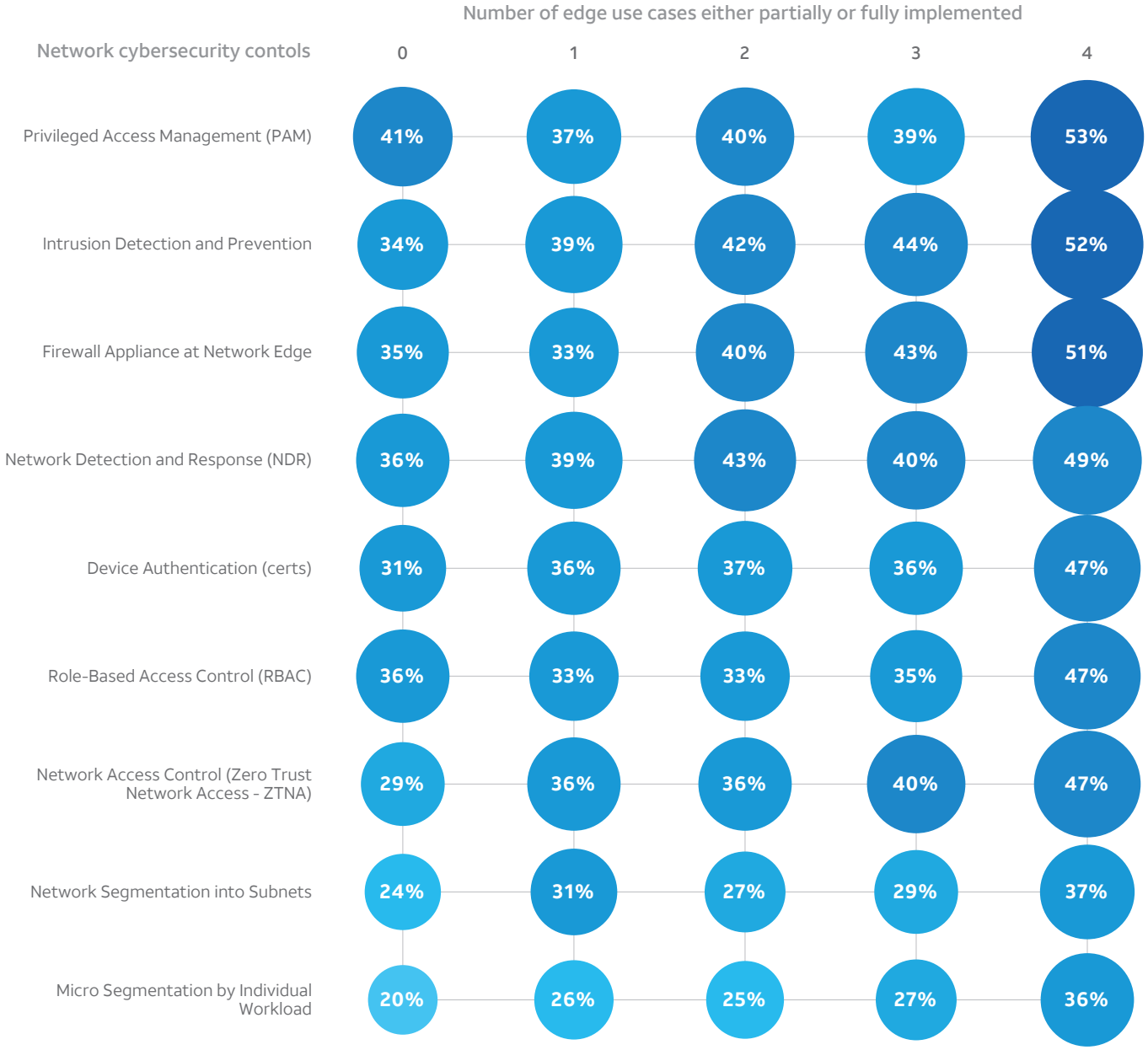
Figure 11

Network cybersecurity controls increase with use case implementations

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

% of respondents

Edge implementation maturity brings increasingly complex network cybersecurity controls. Network Cybersecurity control stack increases with the maturity of Edge implementation.



N= 1418 BASE All respondents

Transportation Edge Ecosystem

Primary use case:

Fleet Tracking

Use GPS tracking and telematic software to enable near real-time monitoring of fleet vehicles, drivers, and other equipment.

Business need:

Efficiently track fleet assets to improve safety and reduce costs.

Security approach:

Deliver combined network and security functions both on-premises and in the cloud.

Primary use case snapshot:

Implementation Stage

62%

Partial

Top Endpoint

46%

Mobile Devices

Data Rate

46%

Enhanced Mobile Broadband (embb)

Edge Network Connectivity

77%

4G/LTE Cellular

Top Perceived Threat

3.2/5

Business Email Compromise

Cybersecurity Approach

47%

Combined Cybersecurity and Networking Functions in the Coud and On-premises

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 202

The use of cybersecurity controls for networks increases in number and variety as the number of partially or fully implemented edge use cases increases.

The use of cybersecurity controls for endpoints/devices and data increases in number and variety as the number of partially or fully implemented use cases increases.

later that a different approach is superior. Unable or unwilling to change approaches on their original edge use cases, the decision makers juggle multiple approaches with some being less than optimum.

The survey findings show a lack of consensus about which groups are responsible for providing cybersecurity functions (see Appendix for a list of the groups). For example, individuals with line-of-business roles lean slightly more on existing in-house security staff than individuals in other roles. This preference may reflect business profitability objectives and the use of in-house security staff as a means to minimize external expenditures.

The survey reveals that 60% of organizations, on average, rely on two or more groups to oversee (two or more groups that are responsible for) the nine cybersecurity functions surveyed. And, 33% rely on three or more groups.

Cybersecurity Controls to Protect Networks

Organizations rely on a stack of cybersecurity controls for their primary use cases (see Figure 11). The largest stacks appear in "end-user present" edge environments, particularly corporate/remote office/branch office and consumer IoT. Survey respondents give virtual network functions (VNFs) and cloud-native network functions (CNFs) the lowest projected deployments.

Notably, the use of cybersecurity controls for networks increases in number and variety as the number of partially implemented or fully implemented edge use cases increases. For example, privileged access management (PAM) is used by 53% of respondents with four mature use cases compared with 41.1% of respondents with no mature use cases. Perhaps the more experienced decision makers build a collection of controls into their plans, or they realize through experience that more controls are needed.

Cybersecurity Controls to Protect the Endpoints/Devices and Data

Similar to network controls, edge use case maturity correlates to a greater number and variety of controls to protect endpoints/devices and data, although there's a greater focus on securing endpoints and devices versus data (see Figure 12).

Digitally transformed organizations need to safeguard data while permitting its fluid movement to support business operations. This effort has been a long-term struggle. For this reason, organizations rely more heavily on protection strategies and detect-and-respond cybersecurity controls. These aren't bulletproof, however. As threat actors advance their sophistication and evasiveness, organizations are starting to embrace the principles of Zero Trust in their security approaches as part of their overall cybersecurity strategies.

Other approaches permit visibility into the flow of sensitive information in end users' communication streams. These include access and communication controls such as email security gateway, secure web gateway, cloud access security broker, and antiphishing. These types of solutions are predominantly cloud based due to attractive attributes such as scalability, reliability, and proximity to a distributed end-user community.

Vulnerability management appears at the low end of the list of controls for legitimate reasons. An immense number of known vulnerabilities in operating systems, applications, firmware, and hardware can exist in an organization's IT estate. Consequently, organizations struggle to identify all systems containing vulnerabilities and to patch or update thoroughly and rapidly. Also, older devices still in service, particularly OT and IoT devices, may have reached end of life, and patches and updates to address vulnerabilities are not available. In addition, it's time consuming to test patches and software updates to be sure a business process won't be broken. And testing may not produce 100% coverage. Consequently, patches and updates may not be deployed so as not to risk an operational disruption.

Instead, organizations may rely on compensating controls to limit their exposure to known vulnerabilities in unpatched and unupdated systems. Stakeholders also can leverage threat intelligence feeds and attack surface management assessments. These help pinpoint vulnerabilities most at risk of being exploited and clarify business implications. Challenged to stay current in patching and updating, organizations are better off when they can prioritize and sequence patching-based reliable threat intelligence and use of compensating controls.

Figure 12

Endpoint and data protection increases with use case implementations

Q. Which of the following CYBERSECURITY CONTROLS will you deploy to protect the ENDPOINTS/DEVICES and DATA of your primary use case?

% of respondents

Endpoint cybersecurity contols	Number of edge use cases either partially or fully implemented				
	0	1	2	3	4
Endpoint Protection (antivirus, next-generation AV)	37%	32%	38%	43%	49%
Mobile Threat Defense	35%	31%	34%	33%	47%
Endpoint Detection and Response (EDR)	35%	32%	34%	39%	47%
Mobile Device Management	35%	31%	34%	38%	46%
Cloud Access Security Broker (CASB)	27%	30%	30%	33%	45%
Mobile Application Management	32%	30%	30%	33%	45%
Multifactor User Authentication	29%	32%	32%	34%	43%
Secure Web Gateway (SWG)	27%	28%	36%	32%	42%
Data Loss Prevention (DLP)	25%	28%	32%	26%	38%
Email Security Gateway	26%	27%	31%	30%	37%
Anti-phishing Software	24%	28%	29%	30%	36%
Sensitive Data Discovery and Classification	20%	25%	26%	29%	36%
Virtual Private Network (VPN)	22%	26%	29%	30%	36%
Data Access Governance	20%	24%	30%	26%	35%
Disk, File, or Folder Encryption	15%	22%	26%	24%	28%
Vulnerability Management	14%	19%	20%	23%	27%

N= 1418 BASE All respondents

The transportation industry relies the least on in-house security staff.

Latin America shows the highest use of in-house security staff for cybersecurity services.

Responsibility for Cybersecurity Functions and Services

Across all cybersecurity functions, in-house security staff is the most responsible group, followed by managed security services providers and managed services providers. The listed functions principally relate to an organization's assets (devices, users, and applications) that require recurring oversight — a likely reason why these groups are identified by the highest percentage of organizations.

The high ratings of in-house security staff by company size suggest that smaller organizations lack the scale of larger organizations (individuals must be responsible for a wide range of functions) and larger organizations can justify more functions in-house and therefore can scale.

Across all cybersecurity functions, Latin America shows a higher use of in-house security staff. On average, manufacturing, slightly more than finance, indicates the highest reliance on in-house security staff. Conversely, the transportation industry relies the least on in-house staff.

The outside provider versus in-house staff decision isn't unique to edge computing. Cybersecurity discussions at some point touch on the sizable shortage of cybersecurity practitioners. Some organizations don't have a choice. The lack of available and/or affordable talent makes the decision moot. Industries such as finance that historically paid higher salaries for cybersecurity talent may be able to tap in-house talent, while manufacturing or transportation might have a greater need to use outside help.

The lack of readily available cybersecurity talent continues to be a friction point in securing the edge. Strategy and architectural help on the front end can be supplied by outside experts who have "been there, done that." These experts often are the ones that recognize, for example, that a SASE-based approach to securing the edge infrastructure requires security, IT, and network teams to work together. Siloed edge computing can result in costly do-overs and gaps in capability, security, and resiliency.

Responsibilities for cybersecurity services are consistent with cybersecurity functions. The highest percentage of respondents across all functions say in-house security staff is most responsible. On average for these services, organizations with more than 10,000 employees show the highest reliance on in-house security staff. A notable exception is penetration testing. Companies with 5,000–9,999 employees rely less on in-house security staff. Perhaps they are sufficiently large to have the flexibility to use external groups but not large enough to have specialized skills in-house.

Industries vary in their ratings of in-house security staff as the primary responsible group for cybersecurity services. However, US SLED consistently shows a lower reliance on in-house security staff than other industries. Similar to cybersecurity functions, Latin America shows the highest use of in-house security staff for cybersecurity services. The relatively low use of in-house security staff in US SLED depresses the usage levels for North America.

Is there consensus among respondent roles about which groups are or will be responsible for providing cybersecurity services? No. Again, different perspectives, and no pattern emerges based on edge use case experience. Lack of consensus related to cost benefit and controls can be a risk factor. This suggests an opportunity to bring in an edge ecosystem partner to facilitate discussions, unify perspectives, and put stakeholders on a single path to meet requirements.

Conclusion

Another year of the edge journey reveals greater edge use case maturity. Two potential accelerators are experience and the transfer of responsibility from internal IT/security groups to an ecosystem of edge partners.

Collaboration is the keynote of the journey ahead. A collaborative approach is vital to business outcomes, cost efficiency, and resilience. Organizational silos are beginning to erode and converge. Edge partner ecosystems, which offer efficient routes to edge and competitive differentiation, are gaining recognition and acceptance.

Stakeholders are encouraged to take a holistic approach to edge computing, networking, and cybersecurity. This approach considers the project life cycle and how to optimize investments in people, processes, tools, and technologies. As edge use cases become increasingly strategic and business critical, holistic thinking ultimately can help reduce risk and shorten the distance to desired outcomes.

Anticipated edge investments are focusing rightly on the fundamentals of strategy, planning, networks, and security prior to application development. Security now is on par with other investment areas and viewed as integral to edge use cases instead of being an afterthought. This finding is a significant, welcome milestone.

Recommendations to Safeguard Digital Assets

- Begin edge use case plans with one or more assessments to determine usability of current assets and to identify gaps in networking and security.
- Conduct continuous assessments within an agile framework.
- Evaluate organizational and use case objectives in the context of maturity related to edge, networking, and cybersecurity. A crawl-walk-run approach that considers all phases of the project life cycle is best.
- Consider engaging experienced edge ecosystem trusted advisors to streamline integration activities that encompass heterogenous environments, diverse hardware, multiple types of connectivity, and security controls.
- Eradicate silos by unifying IT and non-IT groups and promoting cross-functional communication. At the same time, look to edge ecosystem partners for guidance related to working with lines of business and board members.
- Seek assistance from a qualified firm to obtain risk and compliance capabilities if they aren't staffed internally.
- Bring in threat intelligence partners early in the project life cycle if threat intelligence isn't available internally. It's important to "paint the picture" of the types of attacks that have been seen and are being seen to aid decisions about risk and security controls. Threat intelligence providers can likely add current and potential edge computing use cases into their services.
- Implement edge security by orchestrating security controls tailored to each use case using an approach that balances the diverse viewpoints of stakeholders.

Advice for Working with Edge Ecosystem Trusted Advisors

- Consider important variables such as culture, relationships with providers, project scope, and in-house resources.
- Proceed on the assumption that multiple providers will make up an edge ecosystem. It's unlikely that a single vendor can provide everything needed for an end-to-end edge use case.
- Evaluate the pros and cons of working with different types of providers such as telco-driven, network-centric, software-centric, process-centric, and global systems integrators that have a world view.
- Understand provider roles and responsibilities and how a "prime partner" such as a systems integrator oversees and wrangles subpartners.
- Talk to ecosystem partners about dos and don'ts and responsibilities. Ecosystem partners are generally oriented to meeting their customers where they are.
- Compare internal skills sets and competencies to those of providers to clarify decisions about what to outsource.
- Explore network resilience and survivability throughout provider evaluations and proposed solutions.

Appendices

Appendix A

Methodology

This report is based on a survey of 1,418 security practitioners from the United States, Canada, the United Kingdom, France, Germany, Ireland, Mexico, Brazil, Argentina, Australia, India, Singapore, and South Korea conducted during July and August 2022. Respondents come from organizations with 1,000+ employees, with the exception of US SLED and energy and utilities verticals. Respondents were limited to those whose organizations have implemented edge use cases that use newer technologies such as 5G, robotics, virtual reality and/or IoT devices. Respondents are involved in decision-making for edge use cases including cybersecurity that involve new technologies such as 5G and IoT devices. Respondents' job titles include manager up to C-level, as well as architect/engineer, developer lead and networking administrator. Respondents' roles include IT/security/ cybersecurity (e.g., CISO, security architect, security engineer), IT Networking roles (Systems architect/ engineer, Network architect/engineer), other IT roles (non-security e.g., CIO, CTO, development), and line-of-business roles (e.g., president, CEO, CFO, HR, Marketing, Sales). Respondents span a variety of market segments that are nearly equally represented at 14.2–14.5%: US SLED, consisting of higher education and state/local government in the United States; energy and utilities; finance; healthcare; manufacturing; transportation; 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

2023 AT&T Cybersecurity Insights Report – Contributors and Authors

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 1,418 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

AT&T
Mark Freifeld
Tawnya Lancaster
Theresa Lanowitz

IDC
Carol D. Anderson
Becky Diercks
David McCarthy
Craig Robinson
Leslie Rosenberg
Michael Suby

Contributors

AT&T
Ryan Bearden
Christopher Boyer
Alicia Dietsch
Dan Feldstein
Mark Freifeld
Bob Gamiel
Dan Ghillone
Faisal Haidar
Robbie Harrell
Derrick Johnson
Leslie Johnson
Danessa Lambdin
Tawnya Lancaster
Theresa Lanowitz
Rita Marty
Jill Sanders
Eric Sineath
Ginny Smith
Lee Wagner
Todd Waskelis
Gillen Young

Altitude Management Inc.
Paul Cavanaugh
Beth Marshall
Bryan Reid

Akamai Technologies, Inc.
Patrick Sullivan

Check Point Software Technologies, Ltd.
Glen Deskin

Cisco
Omri Guelfand

Ivanti
Srinivas Mukkamala

Palo Alto Networks
Keith O'Brien

SentinelOne
Mike Petronacci

VMware
Michael Leonard

Appendix C

Contributing Organizations

Appendix D

Services and Functions

Network Services and Functions

Provider Choices	Network Services	Network Monitoring and Management Functions
In-house IT/networking staff Consultant Managed service provider Telco Vendor Systems integrator VAR, reseller Other	Strategy and edge business case development Design new architecture Assessment and planning Integration services Labs for innovation and use case development Testing and validation Adoption services Operations planning and development Integration of a dashboard/control plane for continuous visibility Management, monitoring, and reporting Optimization services Support of network, edge, and endpoint equipment Managed network services	Access management and control Patch management Configuration management Vulnerability scanning and remediation Encryption management (certificates, keys) Report generation Network optimization services Change management Application development Incorporation of automation platforms and tools for visibility

Cybersecurity Services and Functions

Provider Choices	Cybersecurity Services	Cybersecurity Functions
In-house security staff	Design and deployment new architecture	User account provisioning
Consulting firm	Application security	Device provisioning
Managed security services provider (MSSP)	Penetration testing	Patch end-user devices
Managed service provider (MSP)	SOC security monitoring	Patch app/server/network components
Telco	Incident response	Patch IoT/OT devices
Vendor	Vulnerability testing	Configuration management
Systems integrator	Tabletop exercises	Vulnerability scanning and remediation
VAR, reseller	Red/blue/purple team exercises	Encryption management (certificates, keys)
Other	Breach and attack simulation	Application development
	DevSecOps	
	Security training	
	Security audits	

Appendix E

Glossary

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 to device	Full FW	Network access restrictions device to 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 exfiltration 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 often are used interchangeably.
Application proxy (e.g., secure web gateway, cloud access security broker [CASB])	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 VPNs are encrypted traffic throughout the network from host to host.
Network access control (e.g., Zero Trust Network Access [ZTNA])	NAC	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 the "Zero Trust Network Access" row head for the definition of ZTNA.)
Distributed denial of service mitigation	DDoS	DDoS mitigation is a set of network management techniques and/or tools for resisting and mitigating distributed denial-of-service attacks.
Secure access service edge	SASE	SASE is the integration of networking and network security as a single unified, cloud-delivered service. Core security capabilities include firewall, intrusion prevention, secure web gateway, CASB, DLP, and VPN or Zero Trust Network Access (ZTNA) alternatives.
Zero Trust Network Access	ZTNA	ZTNA establishes secure connections from an authenticated user to only authorized applications based on context-aware, identity-aware, and device-aware policies. ZTNA solutions are designed for complex and distributed network environments featuring combinations of on-premises and remote users.

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	Multifactor authentication involves the combination of two or more types of proof of identity. Multifactor authentication can be something known like a password, something like a physical token for smartphone, or something like a biometric capturing device.
Device authentication (certificates)	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, or application.
Endpoint/device monitoring (antimalware, EDR)	EDR	Endpoint detection and response, also known as endpoint threat detection and response, continually monitors and responds to mitigate cyberthreats 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 patches usually referred to as 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.
Vulnerability management	VM	Scans of infrastructure and applications uncover security vulnerabilities in the form of known security holes (vulnerabilities) or configuration settings that can be exploited.
Extended detection and response	XDR	XDR is a cloud-native API-enabled platform that ingests and correlates telemetry from a variety of sources to detect cyberattacks. A unified XDR platform allows for the timely investigation, isolation, and containment of and response to attacks.

Zero Trust Components

Name	Abbreviated Name	Definition
Network access restrictions device-to-device	Full FW	Also known as packet filtering firewalls, these operate inline at junction points of routers and switches comparing packets received with 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 (Zero Trust Network Access)	NAC	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 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	Multifactor 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.
Software bill of materials	SBOM	This is a nested list of all of the components that are used to build a piece of software.

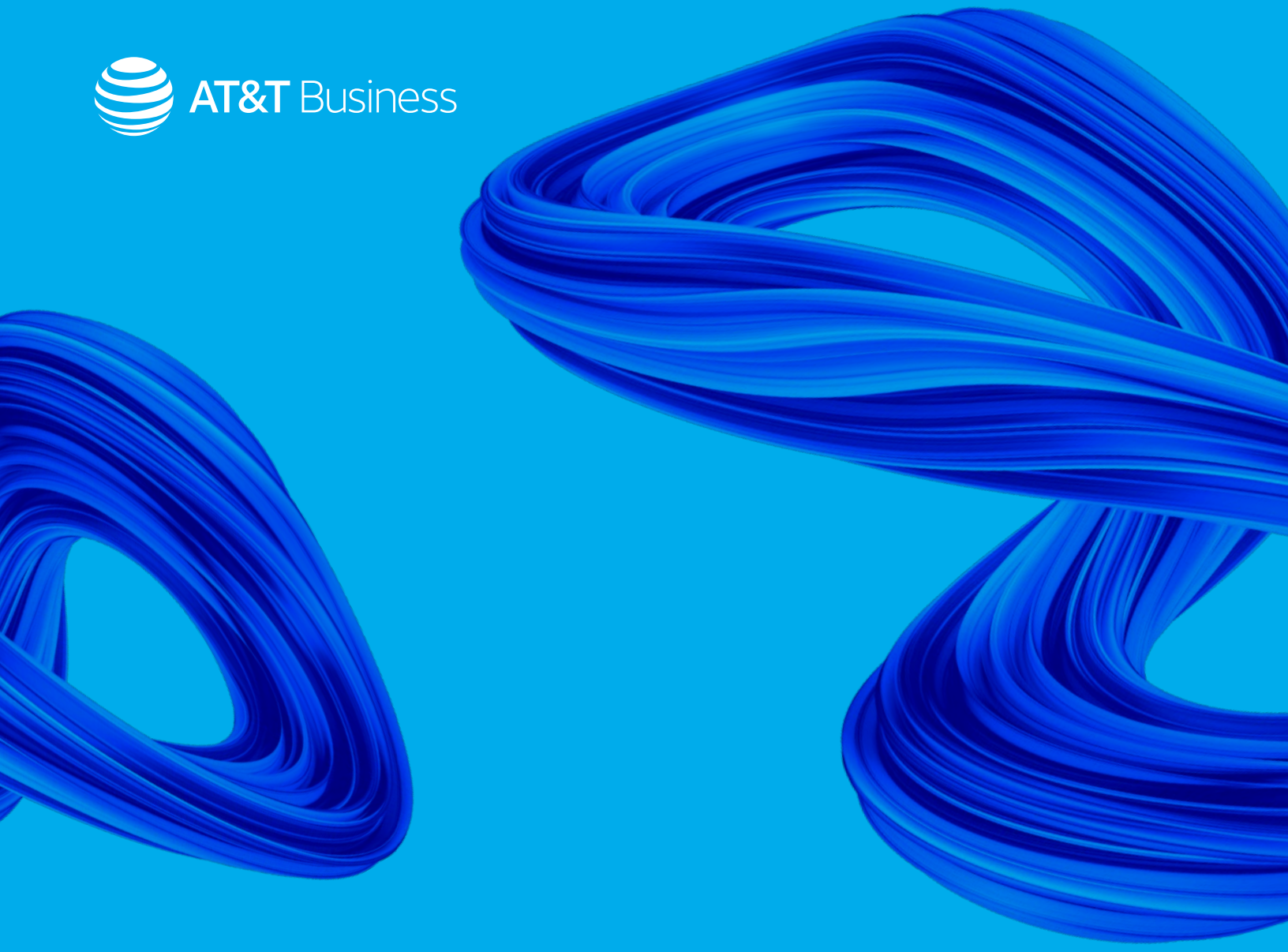
AT&T Cybersecurity

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 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.

© 2023 AT&T Intellectual Property. AT&T and globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

AT&T Business



Collaboration is key for the continuing journey to securing the edge – it is vital to creating partner ecosystems, optimizing investments, and building resiliency; all for stronger and more predictable business outcomes.