AT&T

AT&T Cybersecurity

# 2022 SECURING THE EDGE

# FOCUS ON SLED

# FOCUS ON SLED

**About This Report**
This report is a special industry report with a focus on state and local government and education (SLED). It is derived from the quantitative and qualitative research and analysis conducted for the 2022 core AT&T Cybersecurity Insights Report: Securing the Edge. For additional information and detail about securing the edge, we encourage you to read this industry report as well as the core AT&T Cybersecurity Insights Report.

**SLED Report Methodology Overview**
This SLED report is based on the AT&T Cybersecurity Insights Report: Securing the Edge, published in January 2022. The report is based on data from a global survey of 1,520 security practitioners, IT practitioners, and operations leaders. It was conducted during September 2021, and respondents span a variety of market segments that are nearly equally represented at 16.4–17%: SLED in the United States; energy and utilities; finance; healthcare; manufacturing; and retail. For certain questions, participants could choose more than one response. In these cases, the responses do not round to exactly 100%. To download the core report, AT&T Cybersecurity Insights Report: Securing the Edge, click here.

# EXECUTIVE SUMMARY

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

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

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

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

Edge networks are being implemented for specific use cases to help drive business. A useful approach for decision makers is to think about this transition through the lens of security, risk appetite, innovation goals, and network strategy — considerations that carry forward from previous AT&T Cybersecurity Insights reports. In AT&T's 2021 report, 5G and the Journey to the Edge, for example, 56% of survey respondents said they understood that 5G will require a change to their security approach to accommodate network changes. In the 2022 core report, AT&T Cybersecurity Insights Report: Securing the Edge, respondents weigh in on security controls and anticipated investments within their chosen edge network, the perceived associated risk, and benefit-cost considerations.

## AT A GLANCE

WHAT'S IMPORTANT

Edge computing has arrived in SLED. However, as organizations increasingly deliver services via digital channels and use edge computing to their advantage, security and IT leaders will need to continuously assess and manage security risks to maintain the public's trust.

KEY TAKEAWAYS

There is not a one-size-fits-all security plan for the variety of use cases that are being deployed. Security and IT teams will need to conduct security posture assessments as they roll out edge use cases, identifying gaps that could impact the safety and privacy of data and users. This will likely require a revisiting of approaches to security, including technology, processes, and the expertise of employees who are managing security risks across an increasingly complex and distributed attack surface.

# INTRODUCTION

This paper is related to the broader and more comprehensive 2022 AT&T Cybersecurity Insights Report: Securing the Edge and highlights specific SLED (state and local government and education) edge computing. This report includes research and analysis of higher education and state/local government (K-12 is not included). The effective use of technology in SLED, including new technology used in edge computing, is deeply dependent on citizens trusting that their digital interactions are safe and secure.

Edge computing allows for a wide variety of innovative use cases that at their core, consume, process, and create data. The location of this data, regardless of the length of time it resides there, creates a much wider attack surface for typically understaffed IT and cybersecurity teams to protect. In addition, the proper management and monitoring of that attack surface becomes even more critical with the use of near-real-time analytics on data, which allows for decisions to be made, such as:

When should a traffic light turn red or green?

Was that loud noise on a college campus a gunshot that requires police notification or simply noise from a party?

What history do voting machines have with being connected to a network while at a polling site?

How do we share network infrastructure between campuses and protect data?

As communities become more reliant on the digital delivery of services, SLED will continue to be a prime target for organized cybercrime. The public is certainly concerned about the uninterrupted and safe operation of digital services and other edge computing use cases. In addition, governmental and institutional leaders are concerned with the potential political fallout should cybercriminals exploit the edge applications and technologies used to deliver these services.

The effective use of technology in SLED, including new technology used in edge computing, is deeply dependent on citizens trusting that their digital interactions are safe and secure.

These and numerous other edge computing use cases require careful planning. Security architects need to be aware of the full life cycle of data in order to secure it. Protection of the raw data that is collected at the edge, the applications that turn that data into meaningful information, and the end state of that data either in the cloud or the traditional datacenter requires a holistic approach involving input from multiple stakeholders.

For example, when traffic enters toll roads, a photo of the driver and car license plate are identified. The public or private operators of the monetized toll road are obligated to safeguard the picture of the driver, the address associated with the license plate, and the prepaid toll bank account number. The immutability of the driver's facial features or the address that the toll bill goes to can lead to this data becoming weaponized when it is leaked or stolen.

Drivers and pedestrians use of roadways require trust that the edge applications directing traffic systems to change lights from red to green are secure from malicious cyberactivity. With edge, CISOs need to deploy different cybersecurity controls to safeguard the data and other digital assets that fall outside of the cloud or on-premises systems they normally protect.

# THE STATE OF SLED EDGE COMPUTING

## ADOPTION RATES VARY

The survey data behind the 2022 AT&T Cybersecurity Insights Report reveals a wide variety of edge computing use cases currently being deployed by state or local governments and higher education, especially where organizations are accelerating to digital-first operating models.

For context, the study grouped adoption phases into early stage (ideation and researching), mid-stage (planning and proof of concept), and late stage (partial and full implementation). It examines three stages of edge compute adoption in six industries and industry-specific use cases. This report focuses on the survey results of the mid- and late-stage adoption phases for SLED in the U.S. (higher education and state/local governments).

Edge computing is a new compute paradigm underpinned by 5G technology. As edge computing evolves with new standards and regulations, the security controls used to secure the early, fully implemented use cases may need to be updated to reflect more current practices or more stringent regulations that may emerge. The increased recognition of the need to protect data such as student grades or patient information transmitted by a city-operated ambulance, for example, partially explains the top ranking of data leakage monitoring solutions for higher education and the state/local government sectors.

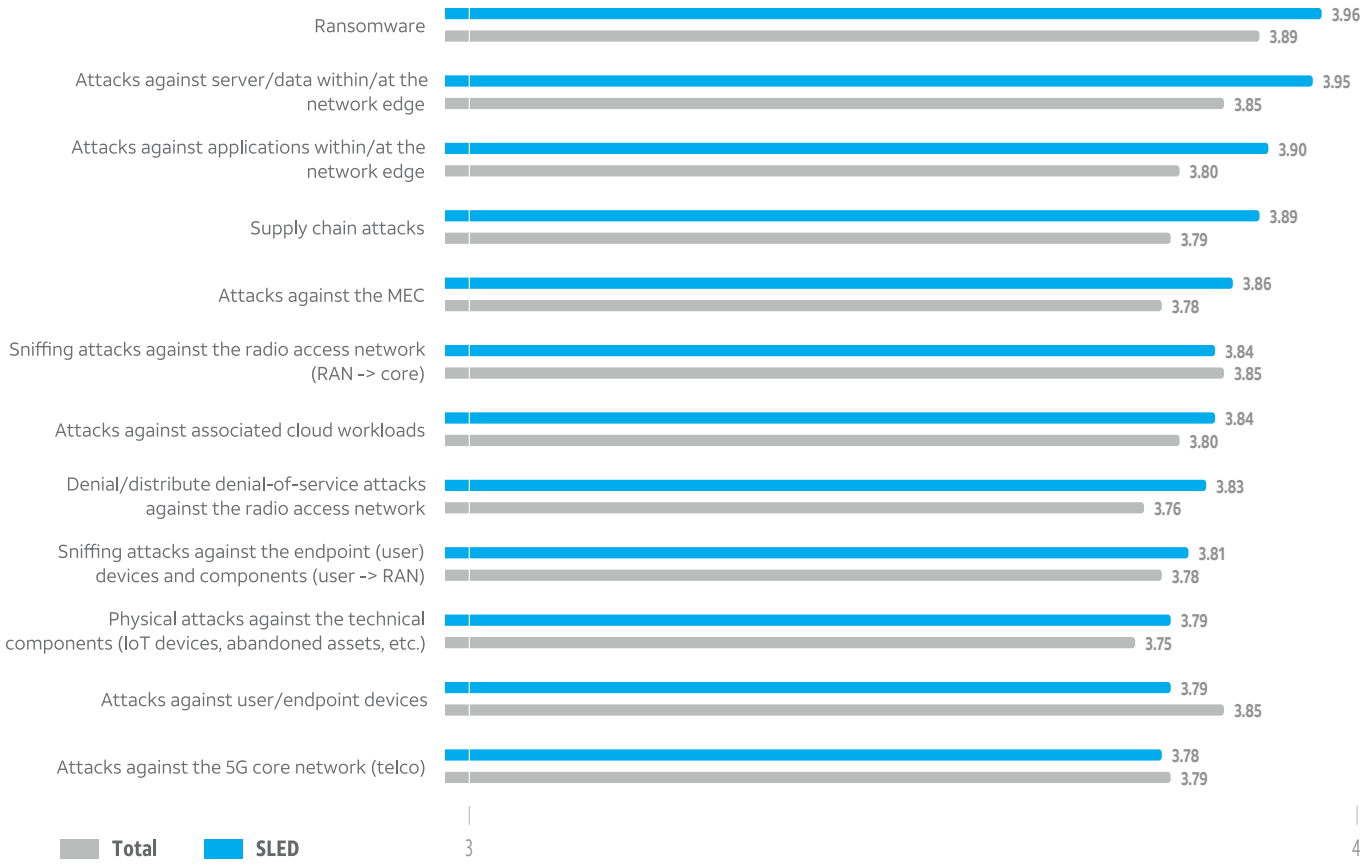
Industries studied in this survey – energy, finance, manufacturing, retail, SLED, and healthcare – are not uniform in their deployment stages. Of all the industries surveyed, SLED shows the highest ranking for industries with edge use case deployment in the mature-stage and a respectful third highest in mid-stage.

Public safety and enforcement (gunshot detection and surveillance) was the top use case in the mature stage of deployment for SLED. The need for real-time or near-real-time information to aid and speed response is critical in potentially life-saving situations. In addition, the potential future pairing of the immediate analysis and notification of first responders with the capability of speeding up police, fire, and ambulance response with real-time traffic analysis and control can usher in much-needed changes to

FIGURE 1

## SLED EDGE COMPUTING RANKS RANSOMWARE AS THE TOP CONCERN

Q. In your opinion, how likely are the following attack vectors? Note: Mean rating is based on a scale of 1 to 5, where 1 = very unlikely and 5 = very likely.




N= 1520 BASE 1,520 (total); 251 (SLED) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

help with time of detection and time to respond.

The automation of public services is the highest-ranking use case in the mid-stage for SLED edge computing. Smart meters for utilities such as water, gas, or electricity are increasingly being rolled out, and the uptime and accuracy of the various metrics the devices gather need to be securely captured and transmitted.

## PERCEIVED THREAT VECTORS TO CONSIDER

SLED security architects and leaders need to be informed and aware of the types of potential cyberattacks as various use cases are planned, piloted, and rolled out.

When asked how likely SLED respondents view each of the attack types presented in the survey, the higher education and state/local government respondents had higher overall concerns about the likelihood of attacks than other industries, with an average score of 3.84 and 3.86, respectively. These scores align more closely to the score of 5 which represents the belief that an attacks is "very likely". In comparison, the overall average across all industries was 3.81. (For more on how SLED views attack vectors compared with other industries, see Figure 1.)

Understanding why SLED ranks attacks more likely may have to do with following:

- Experience matters. The higher maturity rates of the various use cases make it more likely that practitioners have been exposed to, have considered, or have put in place

# EDGE SECURITY x SLED

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

**TOP USE CASE**
The public safety and enforcement (gunshot detection and surveillance) use case ranks highest in SLED for full or partial implementation. It has an average perceived level of risk.

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

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

**SURVEY INSIGHT**

# 69%

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

the security controls, processes, and people needed to guard against a cyber miscreant.
- Regulations matter. This study did not focus on the federal government space, but there is no denying that local and state IT and cybersecurity leaders pay attention to and are influenced by legislation, regulations, and executive orders enacted at the federal level.
- It only takes one. All attacks have the potential to cause disruption, regardless of where the attacks occur. A DDoS (distributed denial of service) attack hitting the cloud workload that a 911 call center is utilizing can be just as devastating as an attack that hits the onboard computer in a police car. In public safety situations, all types of attacks matter.

The types of valuable data that universities often contain as a result of research programs can make them an enticing target. Ransomware attacks are often launched after some or all of the data the targets contain has been exfiltrated. CISOs and other security leaders in higher education and government are aware of the potential damaging impact this could have, hence Figure 1 shows ransomware as the top attack concern for SLED.

State/local government respondents identified the threat of attacks against servers and data and attacks against applications at the edge as the top two respective concerns, with ransomware concerns dropping to the eighth position. The immediate needs of defending an attack against the data utilized at the edge is a likely driver for this high ranking.

## CYBERSECURITY CONTROL OPTIONS

Unsurprisingly, there is no single cybersecurity control believed to be a panacea to instantly secure SLED applications, workloads, assets, and data. Our survey participants identify a variety of cybersecurity controls in use.

Controls "on" the edge at the ingress-egress point can be grouped into general-purpose, traditional controls (such as firewall, virtual private network [VPN], intrusion detection systems [IDS]), and special-purpose controls that can serve specific needs. Controls "in" the edge protect individual devices (such as the laptops, tablets, IoT devices, and sensors) and to fulfill a Zero-Trust strategy and architecture.

Different controls are more applicable to some device types than others. Multifactor authentication, for example, was the top control choice for fixed location devices such as kiosks. It makes sense to use an identity-type control in the higher traffic areas of higher education. For state and local governments, patching for computers used at the edge continues to be seen as a highly relevant control. (However, this contradicts the overall percieved effectiveness of patching as a control throughout all IT systems.)

The types of devices utilized "in" edge computing can limit some of the security controls that could potentially be used. For example, low-power, specialized CPUs that power many of the edge case devices common in SLED, such as sensors or cameras, are unable to support security endpoint agents. For some of these devices, the high CPU cycles required to encrypt or decrypt data often result in that sensitive data being left unencrypted. Therefore, security architects need to utilize different compensating controls, such as the use of intrusion detection systems (IDS) to partially make up for the lack of total encryption.

Where SLED organizations are deploying security controls — on premises, in the cloud (public and private), or through hybrid deployments — will also impact the mix of controls used. Figure 2 shows the mix of preferred security controls for state and local governments and higher education. The high ranking of a need for on-premises security may be surprising to some when cloud computing generates so much attention and awareness. However, data from the survey across industries indicates organizations are adopting cloud deployments while still maintaining some on-premises presence. The rationale behind this hybrid approach may include legacy infrastructure not yet ready to be retired, concerns about data residency, or even yet-to-be assuaged fears of the efficacy of putting workloads in the cloud.

It is important to note that survey respondents overall (across all industries, except state and local government) perceived patching as having the second-to-highest cost of ownership and lowest effectiveness of all security controls. Cybercriminals often exploit vulnerabilities within applications and hardware to execute an attack, and poor patching hygiene practices often put organizations at risk. Despite this knowledge, respondents rank the patching of those vulnerabilities (patch management) lowest among security controls.

IT and security teams may have less visibility into environments where edge devices are used, lack resources to test and validate that patches will not impact critical systems, or even lack a systematic way of deploying patches to devices using niche operating systems. The low emphasis placed on patching may also be a result of IT and security teams using alternative mitigations for vulnerabilities versus remediating them with a patch. For example, they may use segmentation and managing or changing security policies to shield assets.

Security architects need to recognize the challenges their IT counterparts face in keeping edge devices and applications properly patched in a timely manner. Therefore, best practices in architecting and securing SLED edge computing environments requires incorporating compensating controls to proactively address known weaknesses caused by exposed vulnerabilities that have not or cannot be patched.

## SECURITY INVESTMENTS

Over the years, cybersecurity leaders have made inroads to attain a greater portion of IT budgets. During the COVID-19 pandemic, research from IDC, a global market intelligence firm, has shown that more cybersecurity budgets have increased than have decreased. The high priority organizations are giving to security investments, especially over the past two years, directly relates to increasing awareness of the need to secure data regardless of where it resides and to ensure operational resiliency. This is especially true as organizations move to a digital-first mindset where applications and software — especially software as a service (SaaS) — are dominating compute. It has also aided CISOs in seeing a significant percentage of edge computing budgetary dollars allocated to security (see Figure 3).

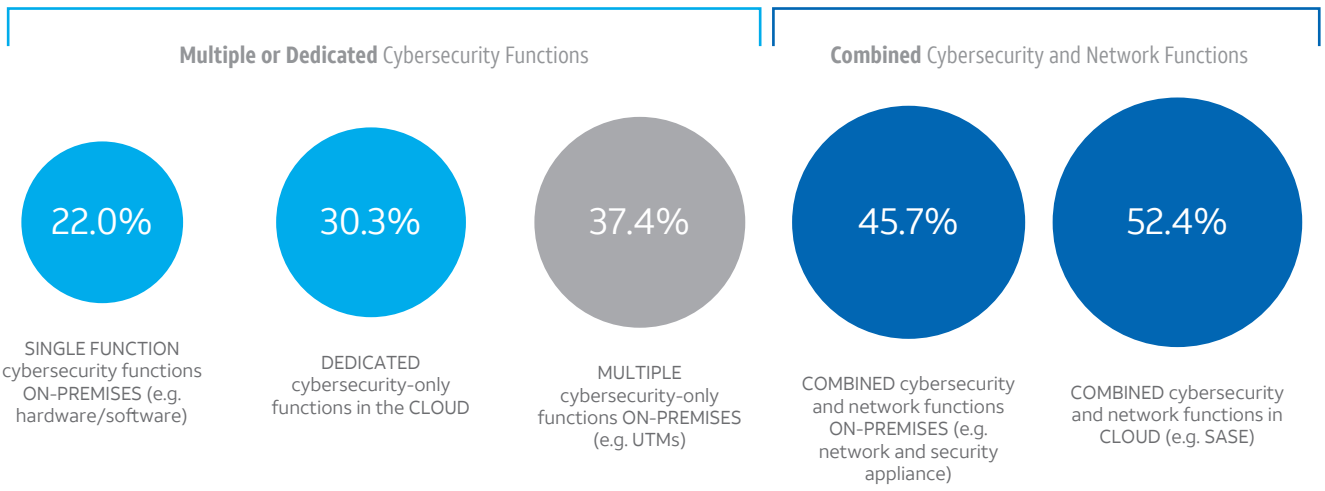
Federal funding made available through the Infrastructure Investment and Jobs Act (IIJA ) and the American Rescue Plan Act (ARPA) may help state and local governments defray the expense of cybersecurity initiatives. The IIJA has specified funding for state and local entities to enhance cybersecurity protections and processes as well as incorporated funding in many other infrastructure programs as a condition of the award.

FIGURE 2

## SLED CYBERSECURITY CONTROLS WILL BE A MIX OF CLOUD AND ON-PREM FUNCTIONS

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

% of respondents




N= 1520 BASE 251 (SLED) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

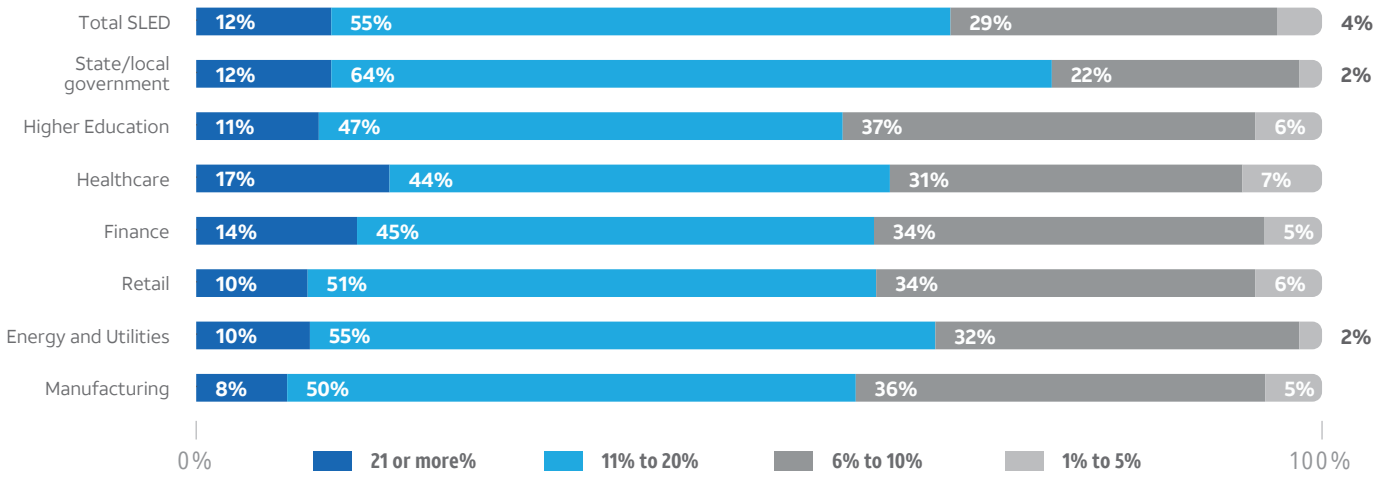
FIGURE 3

## SLED ORGANIZATIONS PLAN SIGNIFICANT INVESTMENTS TO SECURE EDGE USE CASES

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

% of respondents

**Combined Investment Allocated to Security by Industry**




N= 1520 BASE 1,520 (total); 251 (SLED) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

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

When asked about security investments for edge computing projects, the majority of respondents in SLED are allocating between 6% to 20% of their combined investment for edge use cases to cybersecurity. And, reflecting the general growth trend in cybersecurity budgets, 47% of respondents in higher education and 64% in state and local government indicated they are allocating between 11% and 20% of their total edge project budget to cybersecurity.

## BENEFIT-COST ANALYSIS

Respondents answered survey questions on the overall total cost of ownership (TCO) and effectiveness/efficiency for multiple security controls, including:

- Firewall at network edge
- Network access restrictions (device to device)
- Intrusion/threat monitoring
- Application proxy, e.g. SWG (secure web gateway), CASB (cloud access security broker), etc.
- Encrypted traffic at gateway/proxy (external)
- Encrypted traffic throughout (internal)
- Password authentication
- Multifactor authentication
- Device authentication
- Endpoint/device monitoring
- Patching
- Data encryption (at rest)
- Network access control
- Vulnerability management
- Distributed denial of service (DOS/DDoS) prevention/ mitigation

Respondents in SLED rank the overall cost for all the cybersecurity controls listed above as the second highest compared to other industries. This could be a result of IT and cybersecurity teams in state/local governments and higher education generally having smaller budgets and fewer resources than their counterparts in the private sector.

Of the individual controls listed above, SLED respondents perceive firewalls at the network edge as having the lowest TCO, multifactor authentication the second lowest, and password authentication the third lowest.

An analysis of the perceived effectiveness and efficiency of all the controls listed above shows that state/local government rank them 3.8 out of 5.0 (5.0 being very high and 1.0 being very low effectiveness/efficiency). Higher education ranks them 3.9 out of 5.0. This is lower, although not significantly, than other industries: retail (4.1), finance (4.0), manufacturing (4.0), and healthcare (3.9).

Security teams have always sought to rationalize the cost of security controls with their effectiveness when evaluating the mix that is necessary to secure applications and data — whether on-premises, in the cloud, or at the edge. To help identify where the cost may outweigh the benefit for a particular control, CIOs and CISOs should regulary assess their security program as their attack surface evolves. Identify measurable outcomes that can be tracked for each control, assess which technologies offer integrations that can provide added value beyond a single control, and consider the cost of managing and maintaining in-house technology versus outsourcing.

# RECOMMENDATIONS

- Communicate and educate stakeholders, including organizational leadership. Edge security is not the exclusive domain of cybersecurity departments. Work cross-functionally and engage with IT, legal, and industry practitioners with various job titles to move use cases and security forward.
- Be prepared and familiar with explaining the ROI for investments on security. Edge initiatives in SLED have the potential to attract more scrutiny on the spending and effectiveness of each use case. Mistakes and missteps can be newsworthy at a local, state, or national level. Consider additional independent reviews on edge planning to optimize costs without impacting safety.
- Align TCO with the effectiveness of the controls. Spending more time on the piloting phase of a use case, as well as taking into account the lessons learned from prior edge computing use cases will help to better align cost and effectiveness metrics.
- Emphasize the importance of security-by-design throughout all stages of edge network discussions and use case implementation. Leverage legacy controls where effective but keep up with next-generation approaches such as Zero Trust and SASE for 5G and edge.
- Talk with service providers and network operators prior to making decisions about edge networking and security. Discuss the pros and cons of public and private 5G cellular, legacy cellular, remote office/ branch office, IaaS/PaaS/SaaS cloud environment, industrial IoT/ OT, or consumer IoT environments. Develop realistic scenarios for incremental transitions to 5G.
- Delve into the shared security responsibility model with public cloud service providers and carriers to clarify roles and responsibilities at every stage of use case implementation.
- Think ahead about innovation, evolving technologies, and security at the edge. Use cases are the most practical way to proceed for now given the immature and ambiguous state of edge. Specificity is better than generality in all things edge.
- Have higher education utilize in-house talent and peer review of plans that can help to mitigate some of the initial cost outlays for security.
- Classify data and maintain processes and procedures related to data privacy and data sovereignty. Current and emerging regulations will influence data management decisions and locations of security controls.
- Evaluate the potential benefits and costs of security controls before implementing them, keeping in mind the necessity of visibility across the entire attack surface. Evaluate ahead of time and test where integrations between platforms can provide added value or potential cost savings. SLED budgets are more closely scrutinized relative to other industries; additional oversight by elected officials, and the public in general, means that any purchase is a truly “public” purchase. Scrutinize traditional assumptions about security controls that may influence perceptions of cost and/or effectiveness. Look to other industries for inspiration, guidance, and best practices.
- Conduct frequent security control reviews based on data travel routes and storage locations, beyond what’s required for regulatory compliance. Respondents of this survey perceive the risk in all studied attack vectors as high, and increased spending on security may be both necessary and wise.

- Use multisourced, enriched threat intelligence to keep up with attacker tactics, techniques, and procedures. An industry-specific perspective helps prioritize threats and simplify resource allocation.
- Engage security services providers with broad, complementary capabilities to help reduce complexity, lower cost, enable rapid scalability, and increase business agility.
- Reference complimentary resources such as the Center for Internet Security to assist in understanding cybersecurity best practices.

# CONCLUSION

Edge computing for SLED has accelerated due to the societal changes caused by the COVID-19 pandemic. While there is a clear desire to see many of these use cases used for the betterment of communities, appropriate cybersecurity controls to protect use cases such as mass transit optimization, building management, or electronic voting from being hacked and attacked require careful consideration. Privacy issues go along with security concerns when looking at how higher education enables hybrid learning or implements private campus networks.

CISOs and CIOs in SLED can lose the trust of constituents if their edge computing projects go over budget, but it is even harder to regain trust when the digital forensics show a lack of proper planning, testing, and oversight after an attack. Work and plan with success in mind by seeking out expert help in the planning and implementation stages of edge use cases.

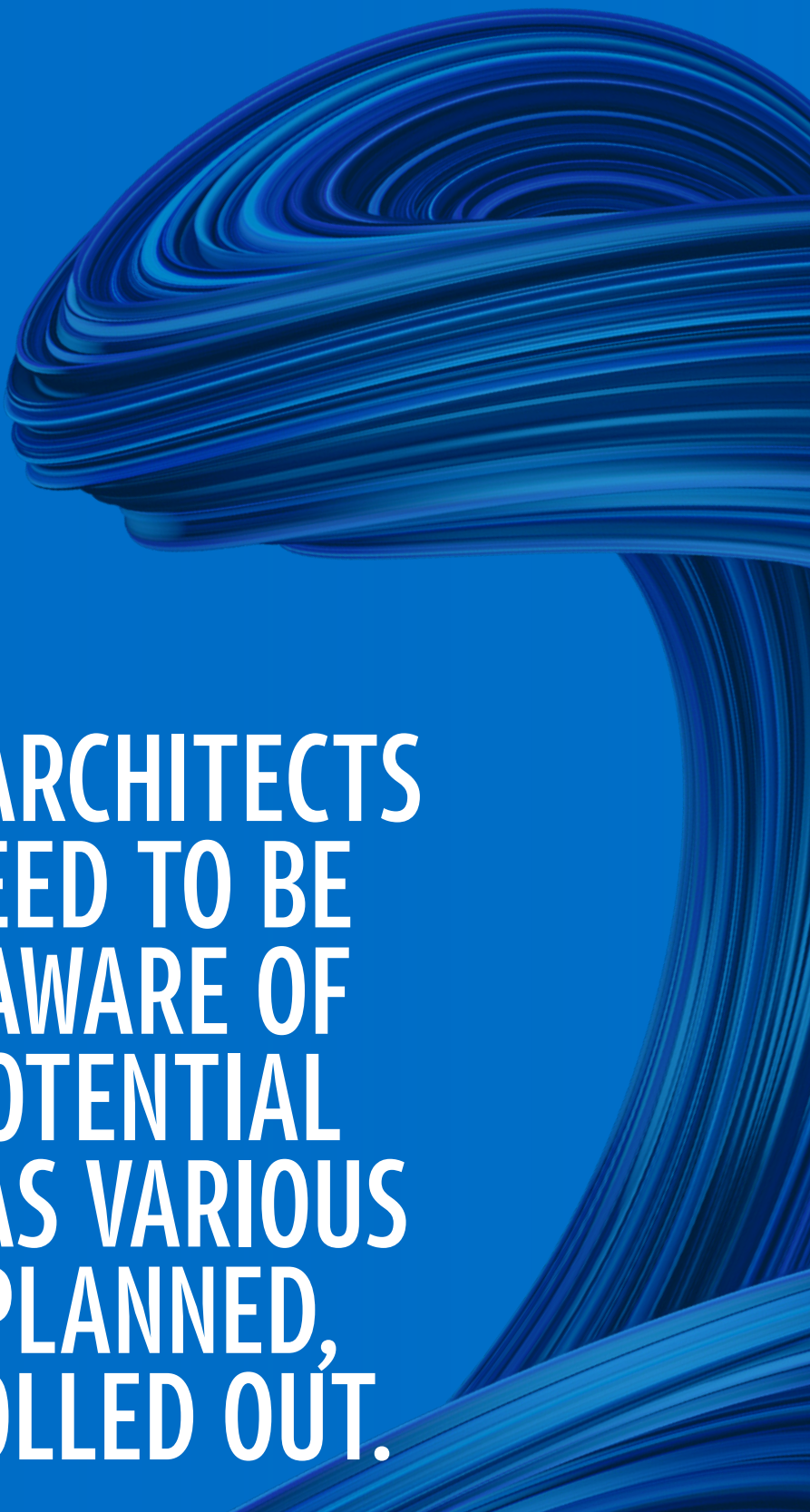
## ABOUT AT&T CYBERSECURITY

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 security operations center (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.

# CONTRIBUTING ORGANIZATIONS

AT&T IDC Akamai Experience the Edge Check Point SOFTWARE TECHNOLOGIES LTD cisco FORTINET paloalto NETWORKS SentinelOne vmware

AT&T



# SLED SECURITY ARCHITECTS AND LEADERS NEED TO BE INFORMED AND AWARE OF THE TYPES OF POTENTIAL CYBERATTACKS AS VARIOUS USE CASES ARE PLANNED, PILOTED, AND ROLLED OUT.