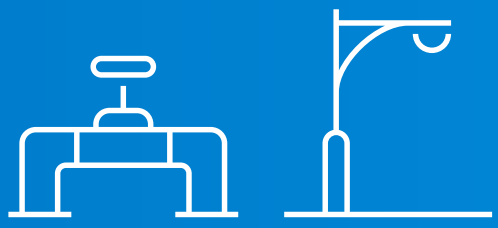
AT&T CYBERSECURITY INSIGHTS™ REPORT

AT&T Business

AT&T Cybersecurity

2022 SECURING THE EDGE



FOCUS ON ENERGY AND UTILITIES

FOCUS ON ENERGY AND UTILITIES

About This Report
This report is a special industry report with a focus on energy and utilities. 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*.

Energy and Utilities Report Methodology Overview
This energy and utilities 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%: manufacturing, healthcare, finance, retail, energy and utilities, and SLED in the United States. 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 sounds familiar, it is. Consider what happened when cloud first emerged. Cloud was a momentous shift in IT and security, and so is edge, which moves computing from a centralized model to a decentralized model. The change is occurring in these motions:

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

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

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

Edge networks are being implemented for specific use cases to help drive business. A useful approach for decision makers is to think about this transition through the lens of security, risk appetite, innovation goals, and network strategy — considerations that carry forward from previous AT&T Cybersecurity Insights reports. In *5G and the Journey to the Edge*, for example, 56% of survey respondents said they understood that 5G will require a change to their security approach to accommodate network changes. In the 2022 core report, *AT&T Cybersecurity Insights Report: Securing the Edge*, respondents weighed in on security controls and anticipated investments within their chosen edge network, the perceived associated risk, and benefit/cost considerations.

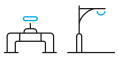
AT A GLANCE

KEY STATS

- 79% of energy and utilities respondents believe there is a high or very high likelihood of a compromise in one of the use cases intended for production within the next three years.
- The geographic infrastructure exploration, discovery, and management edge computing use case has the highest maturity adoption (63%) in the energy and utilities industry.

KEY TAKEAWAYS

There is no one-size-fits-all security plan for the various use cases that are being deployed. Security teams need to be aware of all the security oversights and potential pitfalls that could impact the innovation enabled by edge computing in the energy and utilities industry.



INTRODUCTION

This report is related to the broader *2022 AT&T Cybersecurity Insights Report: Securing the Edge* and highlights specific findings in the security-sensitive energy and utilities industry. Energy and utilities firms' increased utilization of and reliance on technology to provide for the safe acquisition of energy supplies on the front end of the supply chain, the proper monitoring of the consumption of energy on the back end, and the various functions that lie between these two phases rely on a variety of technologies. The survey data behind the report revealed insights related to the following edge computing use cases in the energy and utilities market:

- Intelligent grid management
- Connected field services
- Infrastructure leak detection
- Geographic infrastructure exploration, discovery, and management
- Mission-critical voice, data, and video
- Remote-control operations
- Self-healing assets
- Video-based site surveillance and inspection

The preceding list provides just a subset of the growing number of use cases in this vital sector that are being enabled through technologies such as 5G that allow for a high concentration of Internet of Things (IoT) devices such as sensors, devices, and endpoints in low-latency environments.

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, will continue to increase the attack surface that manufacturers need to protect. Today, cybersecurity practitioners in the energy and utilities industry seek to improve their abilities to ward off threats, including attacks against users and endpoints, ransomware, and attacks against applications, servers, and data at the network edge. With edge, cybersecurity controls are applied differently to safeguard the data and other digital assets and ensure the various use cases are resilient to attacks. The mix of controls will include those used historically as well as new and evolving technologies such as extended detection and response (XDR) and secure access service edge (SASE), which are better suited to distributed/cloud-based networks and edge use cases.

Considering the volatile geopolitical environment, energy and utilities stakeholders need to pay extra attention to securing technology platforms such as edge computing to ensure this technology is used for the designed purposes and not maliciously weaponized.

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

THE STATE OF ENERGY AND UTILITIES EDGE COMPUTING

ADOPTION RATES VARY

The survey data behind the *2022 AT&T Cybersecurity Insights Report* reveals a variety of edge computing use cases that accelerate digital transformation.
For context, the study examines three stages of edge compute adoption in nine industry-specific use cases. Of all the possible adoption phases studied, the ones that are farther along are of the most interest. Planning and proof-of-concept stages are grouped together as mid-stage phases, and partially implemented and fully implemented are in the mature stage. Of all general use cases expected to be in production within three years, industrial Internet of Things (IoT) or operational technology (OT) functions top the list. Edge computing is a relatively new technology, so even fully implemented use cases may change as new standards and regulations emerge. Given this reality, "full implementation" may be transitory.

Industries studied in this survey — energy and utilities, finance, manufacturing, retail, U.S. public sector (SLED), and healthcare — are not uniform in their deployment stages of edge use cases. Retail, SLED, and manufacturing lead the mature stage, with 52%, 52%, and 50%, respectively, while the energy and utilities sector lagged with only 40% of the surveyed use cases falling into the mature stage. This last place ranking in the mature stage should not be taken as a lack of interest; the energy and utilities market segment led the survey field in having the highest ranking in the mid-stage. Given the critical importance of this sector to well-being and safety, it could be argued that higher levels of maturity may justifiably take more time to safely achieve. Globally and across industry use cases, remote-control operations in the energy and utilities sector has the highest rate of mature stage adoption (47%). Video-based site surveillance and inspection (41%) is the highest use case in the mid-stage.

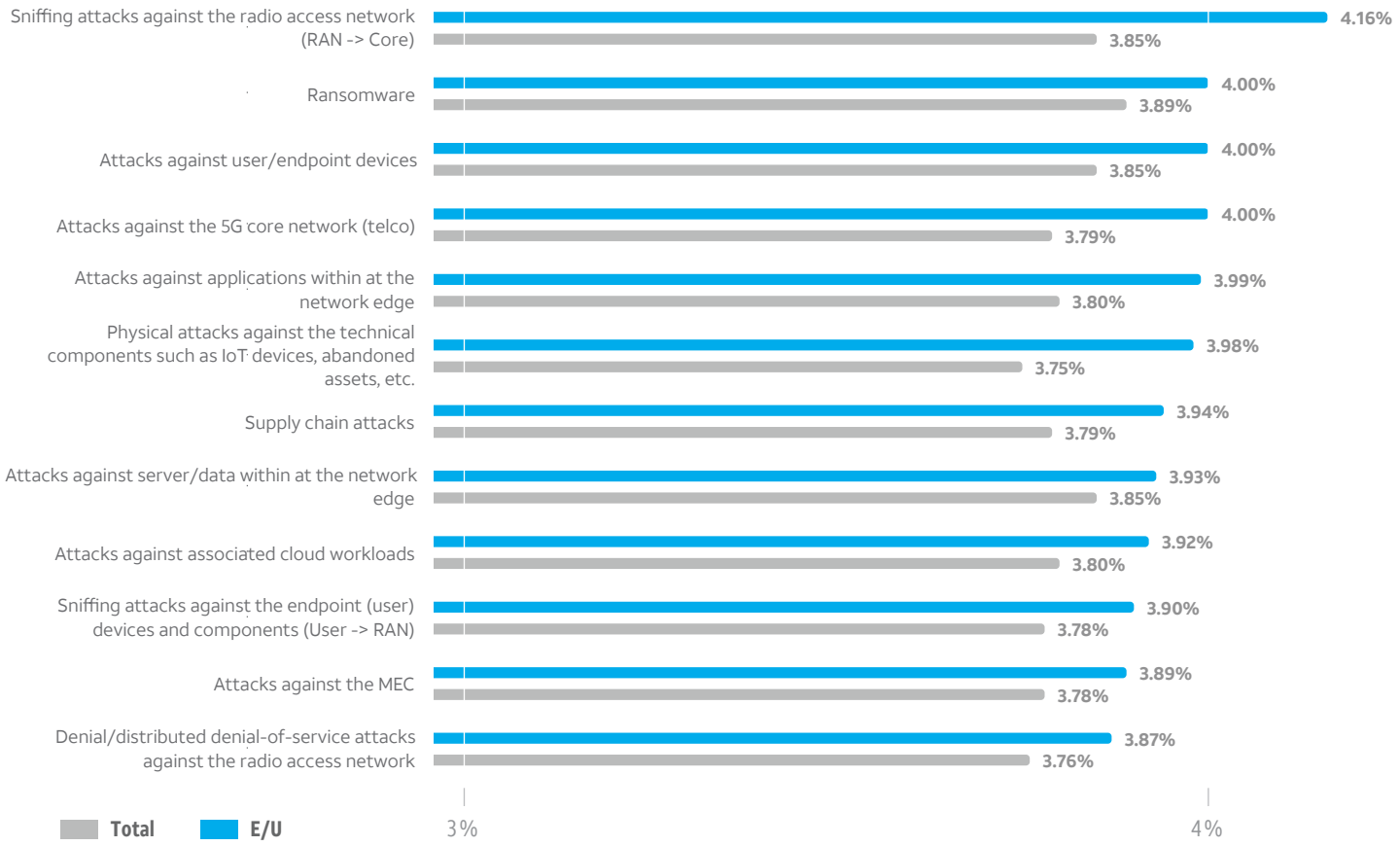
Combining the mid-stage and mature stage adoption rates reveals that the use of edge computing in infrastructure leak detection has the highest combined adoption (82%) among survey respondents.

FIGURE 1

THE ENERGY AND UTILITIES INDUSTRY PRIORITIZES ATTACKS SLIGHTLY DIFFERENTLY THAN OTHER INDUSTRIES

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.

% of respondents that rated these categories as a 4 or 5



N= 1520

BASE 1,520 (total); 251 (E/U)

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

An example of applying edge use cases to infrastructure leak detection is utilizing sensors to gauge the flow of water in a municipal water system. Accurately capturing in real time the flow of water with any drops or spikes in water pressure can help detect leaks and save time and money on necessary repairs. This near-real-time detection showcases the power of low latency at the edge.

Pairing the leak detection example with a smart meter edge case, which has the second highest combined mid-stage and mature stage use case, provides visibility into how edge computing can impact the full life cycle of water flowing from city source to the residence or business for consumption. Just as the changes in water pressure have an ROI for the utility company (finding leaks more quickly), the cybersecurity CIA (confidentiality, integrity, and availability) triangle comes into play for the end user who pays the water bill.

The confidentiality principle is kept when the smart meter is accessible only by authorized users. Integrity is kept when the meter is accurately read and the information is transmitted back to the systems that ultimately produce their bill in a secure manner using controls such as encryption. The availability principle is kept when the entire life cycle of capturing the utility usage is resilient to attacks or outages of any of the potential network connections.

EDGE SECURITY x ENERGY

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

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

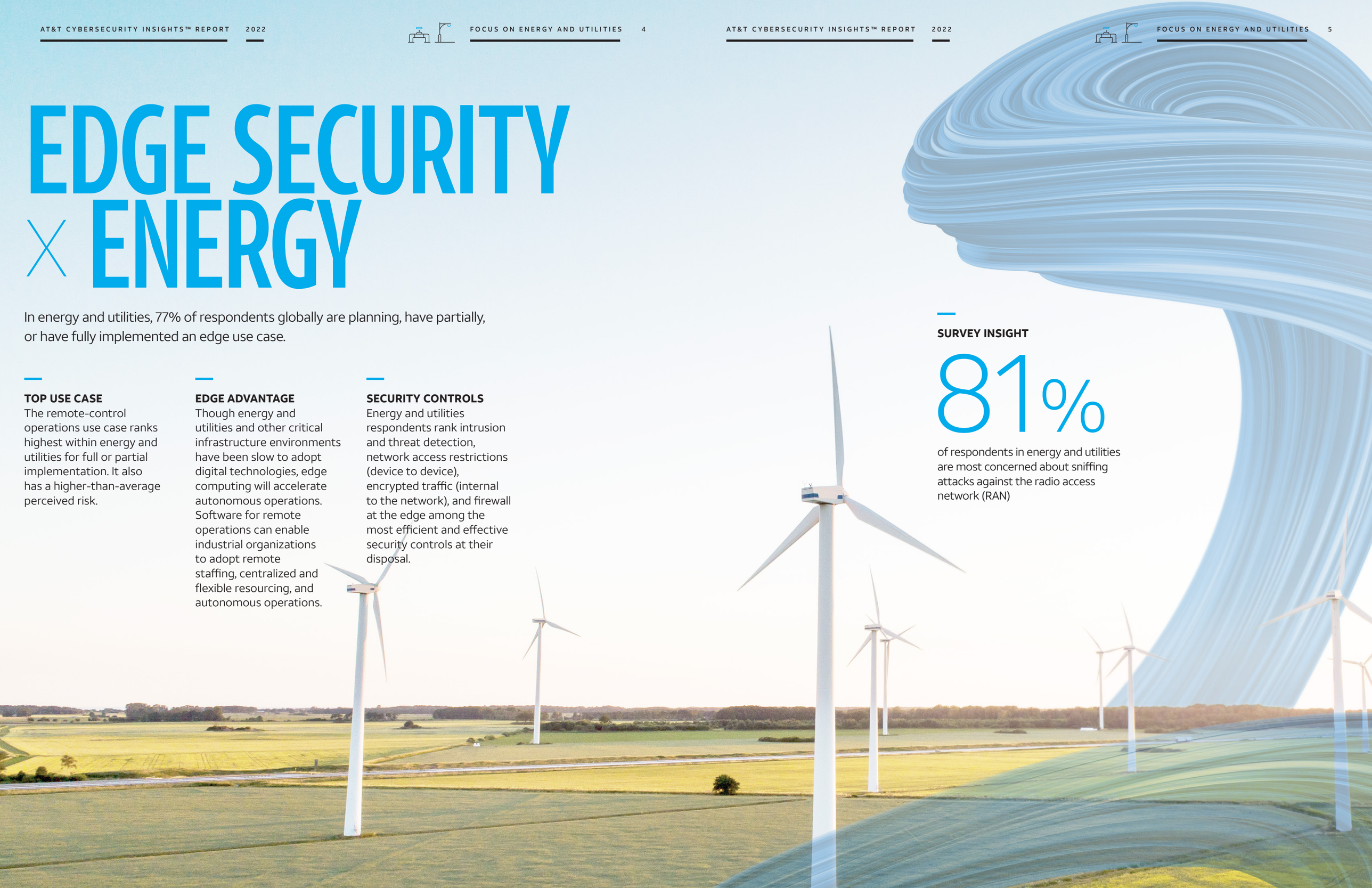
EDGE ADVANTAGE
Though energy and utilities and other critical infrastructure environments have been slow to adopt digital technologies, edge computing will accelerate autonomous operations. Software for remote operations can enable industrial organizations to adopt remote staffing, centralized and flexible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

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

SURVEY INSIGHT

81%

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



THREAT VECTORS TO CONSIDER

Energy and utilities security architects and leaders need to be aware of various types of potential attacks as edge use cases are planned, piloted, and rolled out. IT and OT networks historically were air gapped from each other. OT environments, arguably a bit naively, were thought to be secure and more immune from the types of cyberattacks that have historically been more focused on the open IT systems. The coming together of IT and OT requires that OT leaders and their partners in cybersecurity get aligned on the best practices for securing the OT environment.

The heightened awareness of cybersecurity requirements that OT leaders gain needs to be a two-way communication effort. Classic cybersecurity controls, such as patching systems when a vulnerability is discovered, does not work when that patch requires bringing down an entire oil refinery or wastewater treatment facility. Further, it may be challenging to collect and normalize data for monitoring purposes given the increase in data across merged IT/OT networks.

Across all industries surveyed (shown in Figure 1), ransomware is a top concern. However, it is the second highest concern in the energy and utilities sector. For the energy and utilities sector, sniffing attacks against the radio access network (RAN) rank the highest. The three types of attacks tied for the second highest concern were attacks against the 5G core networks, attacks against the user/endpoint devices and, not surprisingly, the concern around ransomware attacks. Consider the types of attacks energy and utilities respondents identified as a concern. These concerns paint a picture of the need to protect (and the challenge of protecting) the most critical components of the network, supporting infrastructure, and OT devices. As energy and utilities organizations plan their cybersecurity controls for edge use cases, understanding what peers consider the biggest risks can help in understanding what controls should be prioritized and may help with efficiency gains as organizations plan and continue use case implementation.

Ransomware, as an outcome or objective of an attack, becomes media worthy when executed. Energy and utilities organizations should proactively address ransomware at the tactical level as well as the board level to have a plan in place in the event of falling victim to a cyberadversary. The tactical groups include line-of-business and IT leaders who can provide input on the ramifications and costs of a successful ransomware attacks, while the C-suite and the board need to consider the potential liabilities of paying a ransom versus attempting a cyber-recovery.

It is interesting that all industries identified DDoS attacks as the area of least concern. For use cases where artificial intelligence (AI) is a key technology to make decisions at the edge, it is understandable that DDoS attacks may not be as destructive in comparison with other attacks. Stakeholders need to factor in how long a given edge computing use case can remain functional while under a sustained DDoS attack. How long can the AI systems make the appropriate decisions in a vacuum without having access to the back-end IT systems that maintain their configurations?

For edge cases, such as remote-control operations, a DDoS attack could be devastating, and thus different compensating controls may be required to survive this type of attack.

CYBERSECURITY CONTROL OPTIONS

No single control is a panacea to secure edge computing assets, applications, and data. On the contrary, survey results show that the organizations in the energy and utilities sector use a combination of controls in their approach to securing business at the edge.

First, controls “on” the edge at the ingress-egress point can be grouped into general-purpose traditional controls (firewall, virtual private network [VPN], intrusion detection systems [IDS]), and special-purpose controls that can serve specific needs. Second, controls “in” the edge protect individual devices to fulfill a Zero Trust strategy and architecture. Controls that are put in place are dependent on the use case in question, and the networks that need to be secured are tied to the use case.

The types of devices that are utilized “in” edge computing can limit some of the security controls that potentially can be used. For example, not all of the device types used by energy and utilities organizations can support security endpoint agents, so other compensating controls need to be put into place. In situations where sensitive data is not or cannot be encrypted completely, IDS is one example of a control that can be utilized to partially remediate the lack of complete encryption.

Figure 2 shows the mix of preferred energy and utilities security controls, along with types of controls and where they will be deployed. The high ranking of combined cybersecurity and network functions on premises may be surprising to some when cloud computing garners so much attention. However, given the critical nature of so many of the use cases, as well as the varied locations of energy and utilities edge computing, on-premises security controls will be a part of the mix of security controls going forward.

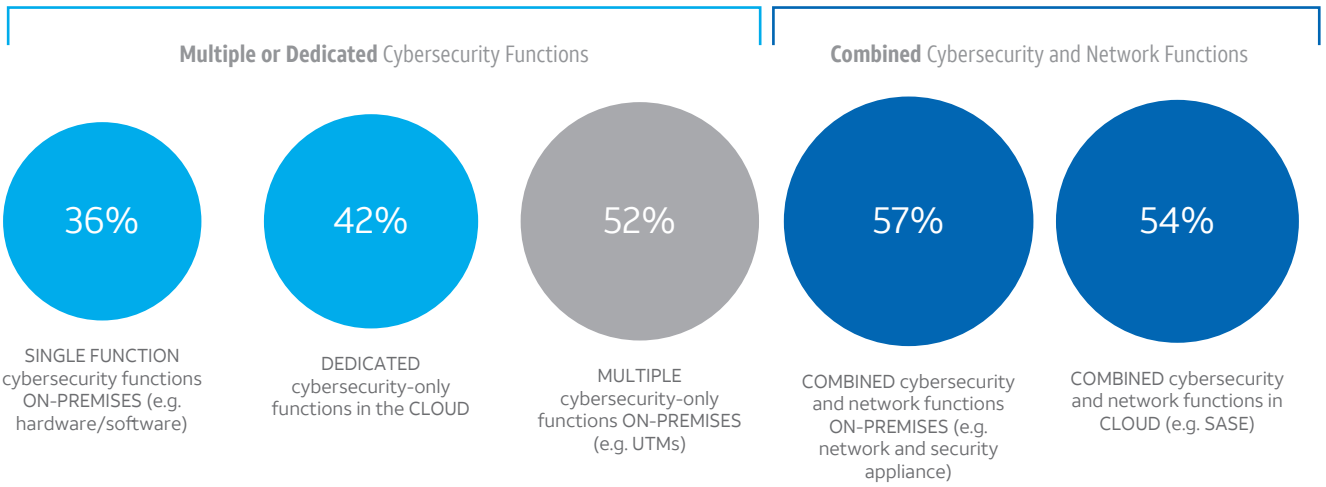
The attention that the energy and utilities sector has received from governmental bodies, due to their inclusion in the “critical infrastructure” category, is arguably a top-of-mind concern among the respondents when asked about how they plan to implement their cybersecurity functions for their primary use case. The consistently higher rates of inclusion in their answers could be an indication of increased maturity and awareness of the dangerous threats that face this industry. When respondents were asked about the impact that a successful compromise would have, energy and utilities industry respondents were the most concerned of all industry respondents. Conversely, there could be a concern that an all-of-the-above thinking may be at work here, rather than a thoroughly vetted plan that applies a finite source of funding to the best mix of controls that secures the use case.

FIGURE 2

ENERGY AND UTILITIES 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 (E/U) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

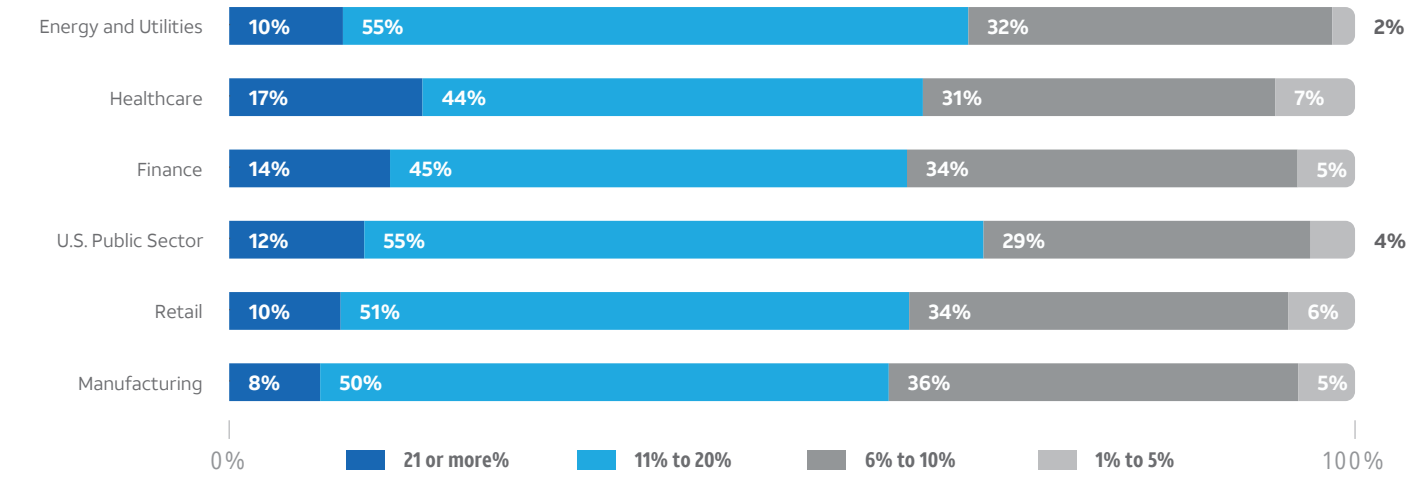
FIGURE 3

ENERGY AND UTILITIES 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 (E/U) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

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

SECURITY INVESTMENTS

In addition to the immediate monetary damage of an attack, the economic damage that can occur outside of the organization that gets hit by a successful cyberattack can be widespread. Industry executives have seen, and should continue to see, extensive attention to the industry by governmental bodies that are tasked with protecting critical industries such as the energy and utilities industry.

Regardless of the potential benefits of the particular use case, there will be no extra grace granted to good intentions to secure the use cases. Good intentions need to be backed up by real investments of time, attention, and finances. Protecting the ability of an organization's customers to have reliable electricity, accurate bills, and safe pipelines requires good cyber hygiene inside the classic four walls as well as proper risk management and cyber controls applied to the external assets that are needed to receive the benefits of the edge computing use cases.

Cybersecurity leaders for the most part have made inroads in gaining increased budgets over the years. IDC research found that during the COVID-19 pandemic, cybersecurity budgets generally increased. Overall, organizations have become increasingly aware of the need for security investments over the years and have gained a better understanding of the business impact of a cyberattack, including the need to secure data regardless of where it resides. This awareness has led CISOs to allocate a significant percentage of edge computing budgetary dollars to security (see Figure 3).

The criticality of security for so many of the use cases in the energy and utilities sector likely plays a role in the funding of the reported security-related expenditures. With regard to investments allocated to security, and specifically those industries that are investing 11% or more of their budget into security, the energy and utilities industry has the second highest commitment to major security investments.

CYBERSECURITY CONTROLS: TOTAL COST OF OWNERSHIP AND EFFECTIVENESS

Total cost of ownership (TCO) and effectiveness are core considerations for security decision makers as they evaluate the mix of cybersecurity controls. Of all controls studied and across all industries, passwords have the lowest TCO and intrusion detection solutions have the highest TCO.

Based on survey responses, the energy and utilities sector perceive the combined stack of cybersecurity controls as having the third lowest TCO compared with other industries. Patching is first in terms of the lowest cost of ownership. The next top two cybersecurity controls are encrypting data at rest closely followed by the use of application proxies such as secure web gateways and CASBs.

Respondents who noted the use case of geographic infrastructure exploration, discovery, and management provide valuable insights regarding the higher TCO of device restrictions such as network access restrictions between devices as well as device authentication using certificates. Both of these controls tied for first in having the highest TCO, likely due to the very unique types of devices used in this particular edge use case ecosystem.

There was surprising unanimity in the energy and utilities industry regarding the efficiency and effectiveness ratings for the top 2 cybersecurity controls that are utilized. Intrusion/threat detection and encrypted networks ranked first and second for all industries combined and the energy and utilities industry. A point could be made that these types of controls have some maturity — a rare word in the cybersecurity industry — within the security operations centers (SOCs) that have handled the IT cybersecurity side of the house. Migrating these skills to handle edge computing security is made easier by prior knowledge of how to utilize these controls.

As previously noted, the very nature of some of the devices utilized in this industry make the effectiveness, and frankly even the possibility, of utilizing patching as a major control somewhat prohibitive. This likely explains the other match between the energy and utilities industry and the overall ranking for all industries as patching came in dead last for the lowest effectiveness.

RECOMMENDATIONS

- Cybersecurity architects, and the budgetary decisions makers who need to approve the funding for these designs, likely recognize that there is a balance between the best controls that should be put in place and those that fall within budgetary reality. Remember that cost savings might be found by utilizing existing controls that are used elsewhere within the organization as well as tapping into the knowledge base that current associates already have.
- Similar to the U.S. public sector, the energy and utilities industry is seeing extra attention paid to the cybersecurity posture for the various use cases by governmental and regulatory bodies. Having a fully vetted incident response plan that understands the particular trigger points that require specific communication to governmental agencies as well as various other stakeholders is something that should be documented and practiced on a regular basis.

- Some systems — especially in OT (ICS/SCADA) — can't have traditional endpoint-centric controls put in place. The cybersecurity infrastructure simply doesn't exist for your DOS 3.0 or Windows CE endpoint. Proactive controls such as microsegmentation, vulnerability scans, and threat hunting should be considered for these more difficult use cases.
- Consider getting professional guidance from service providers on the front end to evaluate road maps for current and proposed use cases. It is likely that a service provider can be found that has done all or most of what your organization is considering. Better to follow someone else who has been "on the bleeding edge" already than to be the pioneer that gets exposed.
- Your IT cybersecurity controls likely look quite different than they did three years ago. Your cybersecurity posture should look different in outlying years. Continuous reviews of what works, what doesn't work, and what needs to be put in place to future proof your edge computing use cases will likely require some outside expertise.
- The energy and utilities industry is not static. As technology continues to evolve and different use cases emerge,
- The exposed attack surface is likely to increase. Conducting regular vulnerability scans and offensive security testing (pen tests, breach and attack simulations, red, blue, and purple team exercises) on a regular basis garners increased cyber-resilience.

CONCLUSION

Technological advances in the use of edge computing in the energy and utilities industry has allowed the industry to come up with innovative use cases such as infrastructure leak detection and smart meters being widely deployed, but the efficiencies that stakeholders and society in general have gained are not cost free. Securing these cutting-edge use cases requires holistic views of the risks that these use cases expose and significant investments in the systems that are deployed to protect these critical use cases. It is not hyperbole to state that lives depend on having the new technologies in this vital industry secured in a resilient way. Conversely, the legacy technology from the 1970s and 1980s that has been exposed due to IT/OT convergence also requires the right mix of attention and cybersecurity controls now that the IT and OT domains are irrevocably joined together.

Securing these edge computing use cases is not a one-and-done occurrence. Security, IT, and business leaders need to make sure that reviews of proposed cybersecurity investments in this critical industry are not just check-the-box annual reviews but that they become standard agenda items as a matter of regular due diligence.

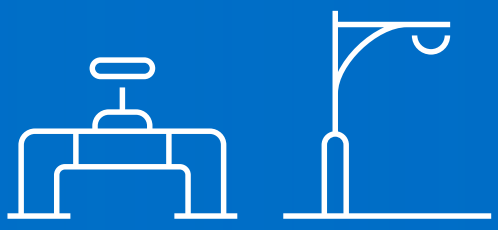
ABOUT AT&T CYBERSECURITY

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 Business



CONVERGENCE OF IT AND OT REQUIRES OT LEADERS AND THEIR PARTNERS IN SECURITY ALIGN ON THE BEST PRACTICES FOR SECURING THE OT ENVIRONMENT.