AT&T CYBERSECURITY INSIGHTS™ REPORT

AT&T Business

AT&T Cybersecurity

2022 SECURING THE EDGE

FOCUS ON HEALTHCARE

FOCUS ON HEALTHCARE

About This Report
This report is a special industry report with a focus on healthcare and 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.

Healthcare Report Methodology Overview
This healthcare 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 line of business leaders. It was conducted during September 2021, and respondents span a variety of market segments that are nearly equally represented at 16.4–17%: the public sector, consisting of higher education and state/local government in the United States; energy and utilities; finance; healthcare; manufacturing; and retail. For certain questions, participants could choose more than one response. In these cases, the responses do not round to exactly 100%. To download the master report, A*T&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 "things 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 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

The promise of extending healthcare beyond clinical walls to the edge has and will be life changing, but security concerns will need to be constantly addressed to keep patient care confidential and compliant.

KEY TAKEAWAYS

There is not a one-size-fits-all security plan for the variety of use cases that are being deployed. Security teams need to be aware of all the security oversights and pitfalls that could impact the quality of care and the privacy implications of edge use computing.

INTRODUCTION

This report is related to the broader and more comprehensive 2022 AT&T Cybersecurity Insights Report: Securing the Edge and highlights specific healthcare industry findings. The evolution and greater reliance of healthcare providers on technology is becoming increasingly apparent to the consumers of these lifesaving capabilities. 5G technologies transform healthcare to be delivered at the edge in a variety of groundbreaking ways.

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 that healthcare providers are obligated by regulatory bodies to protect. Today, healthcare cybersecurity practitioners seek to improve their abilities to ward off ransomware attacks that have adversely impacted hospitals and the ability to provide patient care. With edge, they must now apply different cybersecurity controls to safeguard the data and other digital assets that reside outside of the proverbial four walls of the hospital or providers' locations that are traditionally defended.

It is worth noting how valuable and at risk the data is in healthcare edge computing. The protected health information (PHI) entrusted to healthcare providers is more valuable than other "soft" information such as credit card numbers or social security numbers that may be easily found and purchased on the dark web. It is difficult, but possible, to change a social security number or a credit card number, but a medical fact such as a birthdate or prior medical history cannot be changed. The immutability of most PHI can lead to it becoming weaponized when it is leaked or stolen and provides valuable insights that can be used for nefarious deeds.

The immutability of most PHI can lead to it becoming weaponized when it is leaked or stolen and provides valuable insights that can be used for nefarious deeds..

THE STATE OF HEALTHCARE EDGE

ADOPTION RATES VARY

The survey data behind the 2022 AT&T Cybersecurity Insight Report reveals a wide variety of edge computing use cases in a world where pandemic-related news is top of mind and accelerating digital transformation. Many of these use cases are particularly helpful in situations where physical separation and isolation of people are much more common and needed than in the pre-pandemic life.

For context, the study examines three stages of edge compute adoption in six industries and industry-specific use cases. Of all the possible adoption phases studied, the ones that were farther along were of the most interest. Planning and proof of concept stages are grouped together as mid-stage phases. Partially implemented and fully implemented are in the mature stage. Edge computing is a relatively new technology, so even fully implemented use cases are ripe for change as new standards and regulations come to fruition. Given this reality, "full implementation" may be transitory.

Industries studied in this survey – energy, finance, manufacturing, retail, public sector, and healthcare – are not uniform in their deployment stages. Overall, healthcare shows the second lowest ranking in the mature stage category. However, it has the second highest ranking in the mid-stage category, which indicates a lot of forthcoming activity as healthcare practitioners start to roll out edge computing strategies.

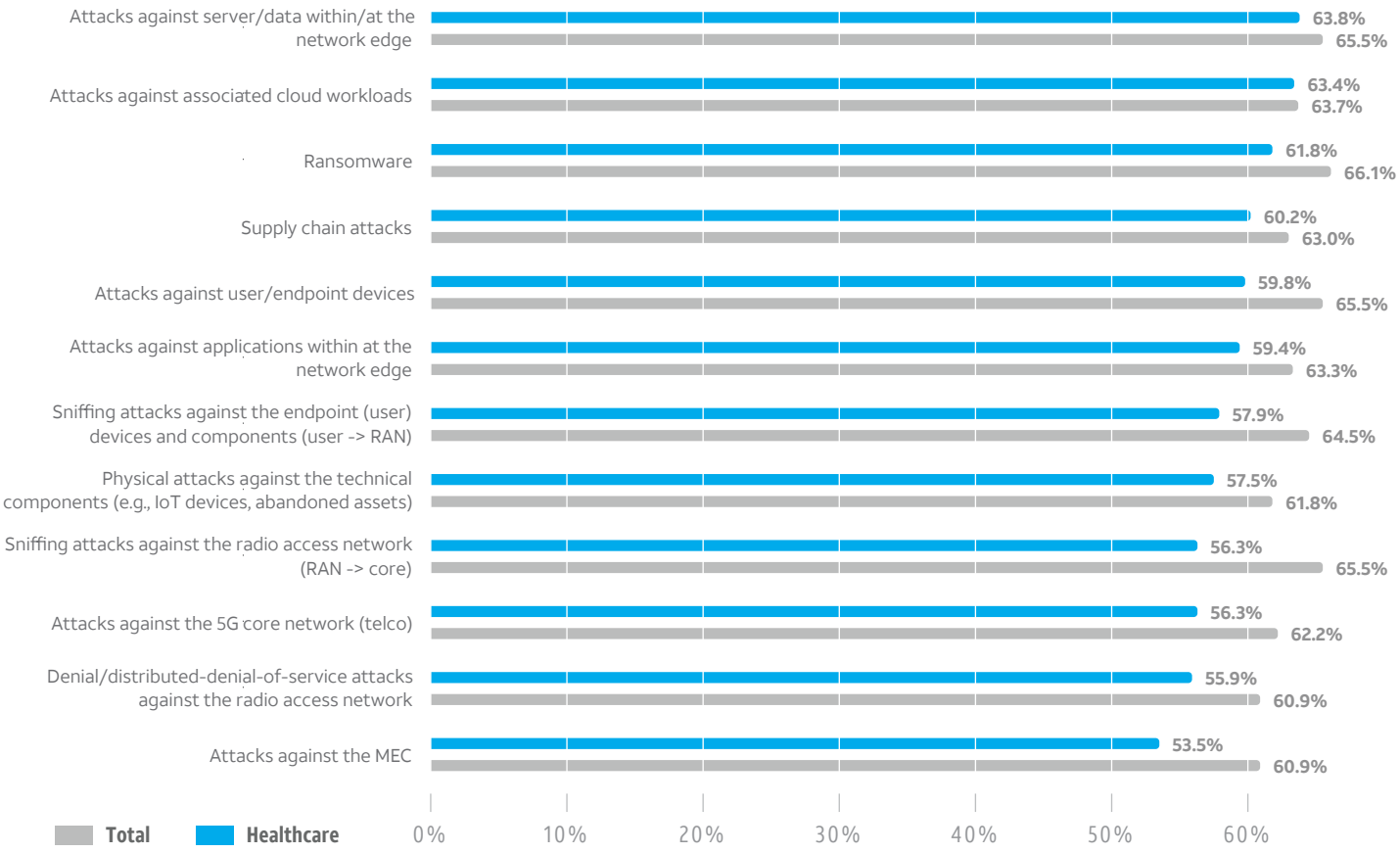
It should not be surprising to see consumer virtual care as the top use case in the mature stage for healthcare. This use case largely revolves around the capability of healthcare consumers to see a clinician anytime and anywhere from a secure device using a combination of video, mobile, cloud, and IoT technologies. Prior to the pandemic, a doctor would close the door when seeing a patient to create privacy and allow for completely open conversations. With the pandemic, new safeguards are needed to meet concerns for privacy and security of protected health information (PHI).

FIGURE 1

HEALTHCARE PRIORITIZES ATTACKS SLIGHTLY DIFFERENTLY THAN OTHER INDUSTRIES

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

% of respondents



N= 1520

BASE 1,520 (total); 254 (healthcare)

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

The hospital-at-home concept has the highest usage in the mid-stage category. As hospital bed usage and availability statistics are business-critical statistics to monitor, the innovators providing this capability are freeing up in-hospital capacity. More patients may receive treatment at home thanks to wearables, telemedicine, virtual care platforms, and other edge computing technologies.

PERCEIVED THREAT VECTORS TO CONSIDER

Healthcare security architects and leaders need to be aware of the numerous types of attacks as various use cases are planned, piloted, and rolled out. News of ransomware attacks is unavoidable, and so it is not surprising that across all industries surveyed, ransomware is a top concern. Healthcare practitioners express two top-of-mind threats ahead of ransomware: the potential for attacks against servers or data at the network edge and attacks against associated cloud workloads. After ransomware, supply chain attacks and attacks against user/endpoint devices round out the top 5 (see Figure 1).

EDGE SECURITY x HEALTHCARE

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

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

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

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

SURVEY INSIGHT

63%

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

CYBERSECURITY CONTROL OPTIONS

There is no single control that is a panacea to instantly secure healthcare applications, workloads, assets, and data. On the contrary, survey results show a mixed bag of security controls in use.

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 could potentially be used. For example, low-power specialized CPUs that power many of the edge case devices common in healthcare cannot support security endpoint agents, and so other compensating controls need to be put into place.

The CPU cycles needed to encrypt or decrypt data often mean that sensitive data is not always encrypted. IDS is one example of a control that can be utilized to partially make up for the lack of total encryption.

In addition, where healthcare organization are deploying their security controls — on premises, in the cloud (public and private), or through a hybrid deployments — impacts the mix of controls they use and flexibility the organization has in scaling up or down to the needs of the organization, fine-tuning, and even managing those controls. Figure 2 shows the mix of preferred healthcare security controls. 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 that broadly, organizations are adopting cloud deployments, while still maintaining some on-premises presence. This could be for a variety of reason, including but not limited to: legacy infrastructure that is not yet ready to be retired, concerns about data residency (especially in Europe where EU GDPR and specific countries have strict regulations about data residency), or even yet-to-be assuaged fear of the efficacy of putting workloads in the cloud.

It is important to note the relatively low current or planned use of patching as one of the layers of protection. IT and security teams may have less visibility in environments where edge devices are used, lack resources to test and validate that patches will not impact patient care, or even lack a systematic way of deploying patches to devices using niche operating systems. It may also be that IT and security teams are using alternative ways of mitigating versus remediating vulnerabilities, such using segmentation and managing or changing securing policy to shield assets.

Security architects need to recognize the challenges in keeping their edge devices properly patched. Having "good bones" in their healthcare edge computing networks means incorporating compensating controls to proactively make up for known weaknesses in areas such as patching.

SECURITY INVESTMENTS

Cybersecurity leaders for the most part have made inroads in gaining increased budgets over the years. During the COVID-19 pandemic, IDC research has shown that cybersecurity budgets have generally increased. The general awareness of the need for security investments over the years, along with the need to secure data regardless of where it resides, has aided CISOs in seeing a significant percentage of edge computing budgetary dollars allocated to security (see Figure 3).

Given the highly regulated nature of healthcare and the need to secure connections for delivery of care, it is encouraging to see that this industry has the highest percentage of respondents investing at least 21% or more of the total use case investment in security.

BENEFIT-COST ANALYSIS

Healthcare cybersecurity controls have the lowest anticipated total cost of ownership (TCO) rating overall compared with other industries surveyed. Of all controls available, passwords appear to earn the best TCO, but industries disagree on its effectiveness.

When measuring effectiveness of individual controls, IDS had the highest rating for all industries. Healthcare agrees and rates it as the most effective control. Multifactor authentication (MFA) is perceived as the next best level of effectiveness in healthcare.

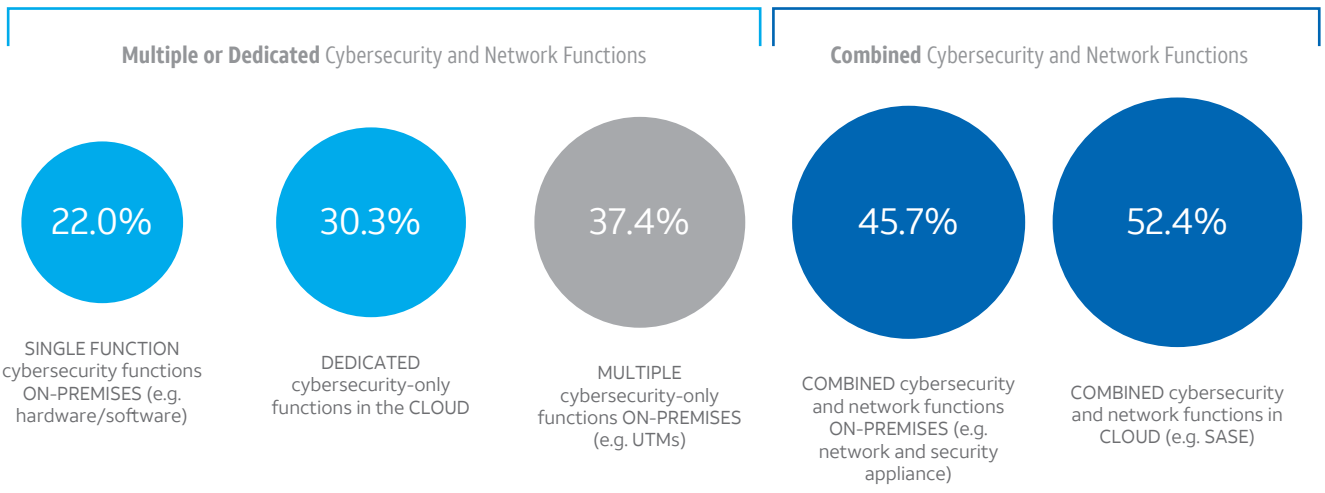
Firewalls at the network edge, IDS, network access restrictions, data leak monitoring, and password authentication are the top 5 controls for all industries combined as well as for healthcare. Surprising unanimity for the top 5 controls!

FIGURE 2

CYBERSECURITY CONTROLS WILL BE A MIX OF CLOUD AND ON-PREMISES FUNCTIONS

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

% of respondents



N= 1520 BASE 254 (healthcare) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

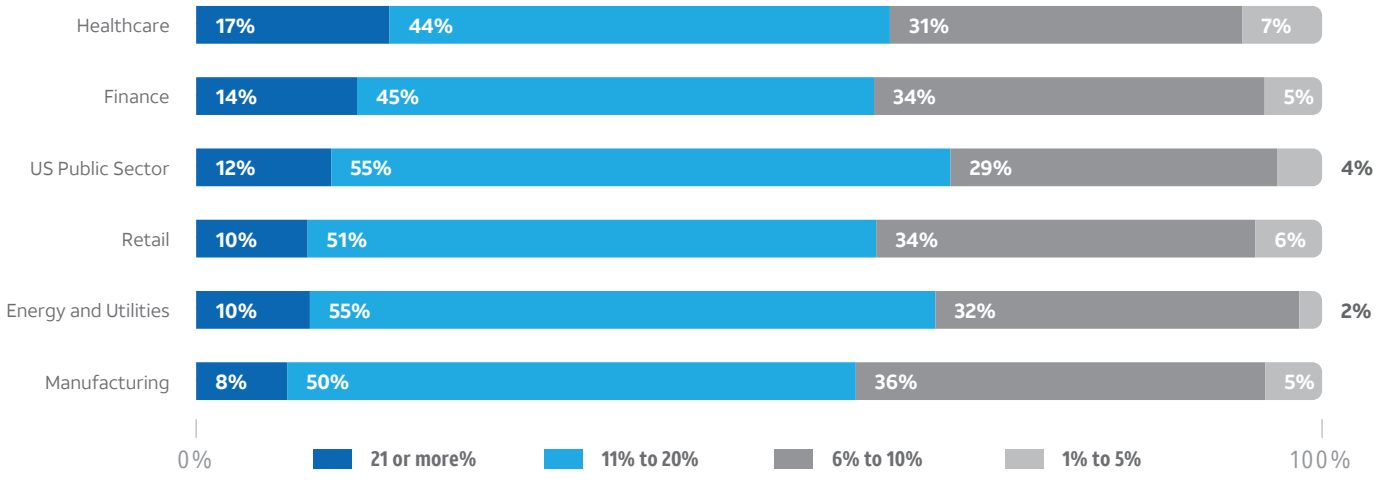
FIGURE 3

COMPANIES PLAN SIGNIFICANT INVESTMENTS TO SECURE EDGE USE CASES

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

% of respondents

Combined Investment Allocated to Security by Industry



N= 1520 BASE 1,520 (total); 254 (healthcare) SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge* - Survey, September 2021

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

RECOMMENDATIONS

- Communicate with and educate stakeholders along a journey that will be both thrilling and challenging. Healthcare edge security is not the exclusive domain of cybersecurity departments. Work cross-functionally and engage with IT, legal, and healthcare practitioners with various job titles to move healthcare use cases and security forward.
- Emphasize the importance of security by design throughout all stages of edge network discussions and use case implementation. Leverage legacy controls where they are effective, but keep up with next-generation approaches such as zero trust and SASE that are designed for 5G and edge.
- Talk with service providers and network operators prior to making decisions about edge networking. Discuss the pros and cons of public and private 5G cellular, legacy cellular, remote office/branch office, IaaS/PaaS/SaaS cloud environment, industrial IoT/OT, or consumer IoT environments. Develop realistic scenarios for incremental transitions to 5G.
- Delve into the shared security responsibility model with public cloud service providers and carriers to clarify roles and responsibilities at every stage of use case implementation.
- Think ahead about innovation, evolving technologies, and security at the edge. Use cases are the most practical way to proceed for now, given the immature, ambiguous state of edge. Specificity is better than generality in all things edge.
- Understand that implementing edge use cases may need to rouse stakeholders out of their comfort zones. Initial deployments involve familiar devices such as general-purpose computers and individual devices. Other types of components may present opportunities for differentiation and competitive advantage.
- Classify data and maintain processes and procedures related to data privacy and data sovereignty. Current and emerging regulations will influence data management decisions and locations of security controls.
- Evaluate the benefit cost of security controls before implementing controls, keeping in mind the necessity of visibility across the entire attack surface. Scrutinize traditional assumptions about security controls that may influence perceptions of cost and/or effectiveness. Look to other industries for inspiration, guidance, and best practices.
- Conduct frequent security control reviews based on data travel routes and storage locations, beyond what's required for regulatory compliance. Perceived risk in all studied attack vectors is high, and increased spending on security may be both necessary and wise.
- Use multi-sourced, 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.

CONCLUSION

Healthcare edge computing is accelerating because of a once-in-a-lifetime pandemic. Hospital at home and virtual home care are early leaders in the more mature adoption phases noted. Edge computing capabilities such as the processing of data where it is consumed or produced, along with lower latency, will enable other use cases such as tele-emergency medical services and autonomous mobile robots and drones in hospitals to learn from the pioneering healthcare edge computing use cases identified in this report. Improved quality of life and saved lives will be the headlines of future history books that describe this era of healthcare technology innovations.

ABOUT AT&T CYBERSECURITY

AT&T Cybersecurity helps make your network more resilient. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

CONTRIBUTING ORGANIZATIONS

AT&T Business

HEALTHCARE EDGE COMPUTING HAS ARRIVED. SECURING THESE INVESTMENTS WILL BE DIFFERENT DEPENDING ON EACH USE CASE.