

AT&T Cybersecurity

# 2023 Edge Ecosystem



Focus on  
Healthcare

## Focus on Healthcare

### About this Report

This report is a special industry report with a focus on healthcare and derived from the quantitative and qualitative research and analysis conducted for the full 2023 AT&T Cybersecurity Insights Report: Edge Ecosystem. For additional information and details about securing the edge, we encourage you to download a free copy of the full report at: [cybersecurity.att.com/insights-report](https://cybersecurity.att.com/insights-report).

### About the Research and the Focus on Healthcare Report

The research was conducted during July and August 2022. We surveyed 1,418 security practitioners from the United States, Canada, the United Kingdom, France, Germany, Ireland, Mexico, Brazil, Argentina, Australia, India, Singapore, and South Korea. Respondents come from organizations with 1,000+ employees except for 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 involves new technologies such as 5G and IoT devices. For certain questions, participants could choose more than one response. In these cases, the responses do not round to exactly 100%. Where indicated, this report focuses on the data collected from healthcare respondents.



# The Edge Ecosystem in Healthcare

In the past, IT typically made technology decisions based on business and computing requirements they understood. Thanks to ongoing advances in computing, things are changing.

Welcome to edge computing in 2023.

Edge computing is a transformative technology that brings together various stakeholders and aligns their interests to drive integrated business outcomes. The emergence of edge computing has been fueled by a generation of visionaries who grew up in the era of smartphones and limitless possibilities. In this paradigm, the role of IT has shifted from being the sole leader to a collaborative partner in delivering innovative edge computing solutions. In addition, we found that healthcare leaders are budgeting differently for edge use cases. These two things, along with an expanded approach to securing edge computing, were prioritized by our respondents in the 2023 AT&T Cybersecurity Insights Report: Edge Ecosystem.

---

## Topline research findings

In 2023, the primary use case reported by respondents is tele-emergency medical services, which involves accelerating diagnosis and providing initial care remotely to non-urgent cases by extending telemedicine capabilities to emergency medical staff in field situations. This represents a shift from the primary use case in the 2022 AT&T Cybersecurity Insights Report: Securing the Edge, which was focused on consumer virtual care. The driving force behind this change is the goal of enabling emergency personnel to make faster and more informed decisions.

Regarding endpoints, mobile devices are the top choice, accounting for 53% of the device category. Additionally, 74% of respondents utilize 4G/LTE cellular networks for edge connectivity. It is worth noting that 52% of the respondents are using a combined cybersecurity and networking function that is located on-premises. The top perceived threat in this context is an insider threat, highlighting the importance of addressing internal vulnerabilities in edge computing environments.

## AT A GLANCE

Edge computing in healthcare is taking off. The ability to provide positive patient outcomes while simultaneously delivering increased financial margins is the reality.

Cross-functional collaboration among groups that don't normally work together and building-in security from the start is the only way the potential of these exciting use cases will meet the high expectations of stakeholders.

The research found that balanced budgeting and security built-in at the point of conception are key factors for use case success.



# Devices are changing healthcare

## And it's just the beginning

One of the most promising aspects of edge computing is its potential to leverage real-time data for patient care, revolutionizing healthcare outcomes and operational efficiency. The 2023 AT&T Cybersecurity Insights Report highlighted two notable use cases: hospital-at-home providing remote care and autonomous mobile robots/drones.

- The concept of hospital-at-home, enabled by emerging edge computing technologies such as remote sensors and videoconferencing, presents a revolutionary approach to patient care. By providing care at home instead of occupying a hospital bed, healthcare practitioners can alleviate the strain caused by the nursing shortage. This allows nurses to focus on patients who genuinely require in-person care. Patients can access healthcare providers through the Internet, eliminating the need for physically seeking care within hospital premises.
- Autonomous mobile robots and drones represent another exciting application of edge computing in healthcare. These robots can navigate hospitals without human intervention, performing tasks such as disinfecting patient rooms and delivering supplies. Additionally, autonomous drones have the potential to provide lifesaving medicines and equipment swiftly.

While mobile devices and personal computers are still extremely popular in healthcare, their ubiquitous availability and connectivity make them vulnerable to cyberattacks. Successful cyberattacks can disrupt services, highlighting the need for robust cybersecurity measures.

## Collaboration is critical for development

The edge ecosystem in healthcare requires collaboration among various stakeholders, including the line of business leaders, research and development, innovators, legal, compliance, practitioners, consumers, and experts in networking, cybersecurity, and IT. Each stakeholder brings a unique perspective, represented by different points of view, frameworks, and priorities.

It is crucial to involve the line of business in the early planning stages to make informed decisions and accelerate implementation. Given the emphasis on regulation and privacy in healthcare, leveraging experts who can navigate these complexities expedites development time. Furthermore, considering an endpoint strategy that prioritizes user experience and secure data transfer may require intentional devices, as off-the-shelf consumer devices often fall short in terms of security requirements.

The research found that engaging trusted advisors from internal and external sources is a priority for those embarking on an edge computing path. The report reveals that most respondents (64%) rely on external expertise for project planning, and 71% seek guidance from outside trusted advisors during production. Seeking external advice can streamline processes, save time, and reduce costs, whether designing an access management approach, ensuring data integrity, or selecting the appropriate tools for data movement and protection.

The healthcare edge ecosystem requires collaboration among various stakeholders, from the line of business to compliance, security to user experience, and front line providers to patients.

# The common characteristics of edge computing

**Based on the research, respondents agreed that the following characteristics are common elements of most use cases.**

## Use cases are data-driven.

Edge computing is different from traditional computing. In edge computing, data is created and consumed at or very near the consumer or business of the specific use case. That means it's often happening outside traditional environments. In healthcare, this usually means it's happening in homes, laboratories, or in the field. In addition to data creation and consumption, decisions are often made closer to healthcare consumers, ideally resulting in better outcomes because it's personalized, near real-time, and allows for rapid analysis.

The challenge is that edge data creates different security requirements. It is potentially more vulnerable and could even include physical theft (if a device is stolen or lost). For example, suppose data is stored and collected at a bedside or in a robot performing heart surgery thousands of miles away from the cardiothoracic surgeon. In that case, there are increased opportunities for a breach. Data created, analyzed, and disposed of at the edge increases the need for dynamic cybersecurity. In other situations, healthcare organizations must keep and send data via the cloud. Organizations are responsible for the safe transmission of this data and likely do so through encryption, with appropriate network and cyber controls in place.



## What are the common characteristics of edge computing?

### Data driven

Closer to user creation and consumption

### Software defined

Private, public, on-premise, or cloud

### Distributed configuration

Intelligence, networks, and management



## Edge computing is software-defined

Edge computing changes the network and applications, driving a digital-first experience. Workloads, hosting, and applications are closer to where data is generated and consumed. This means the cybersecurity framework needs to adapt.

Imagine a world where healthcare practitioners are pulled into a crisis, such as a crowded hospital during a major catastrophe. The coordination of all the components needed to provide care; bed availability, routing doctors, sending nurses and supplies to where they are needed, performing and processing tests, etc. If a centralized system could make all the decisions that need to be made, along with system performance monitoring – that is a formidable effort tied to critical outcomes. That is a strong analogy explaining how a software-defined architecture's capabilities can deliver fast, reliable results in near real-time.

The elasticity of demand means that resources are available and utilized efficiently based on need. This flexibility extends to software-defined networking (SDN), which enables dynamic scaling of networking throughput to match varying demand levels. SDN can allocate more resources during peak usage, scale up for busy periods, and scale down during low activity. Additionally, SDN allows for centralized network configuration, reducing costs by minimizing the time needed to configure individual devices. This improvement in operational efficiency can lead to significant cost savings, particularly in the context of a shortage of network experts.

## Decision-making is closer to the data

With edge computing, the intelligence required to make decisions, the networks used to capture and transmit data, and the use case management are distributed. Distributed means things work faster because nothing is backhauled to a central processing area such as a data center and delivers the near-real-time experience. Rapid decision-making is also supported by machine learning powered by multi-access edge computing (MEC) devices. Some use cases rely on a mix of MEC for immediate decisions and then transmit detailed or summary findings back to a cloud environment for further processing.

The introduction of these capabilities raises concerns regarding regulatory compliance. It is important to consider whether private health information (PHI) is stored away from its final destinations, such as cloud computing platforms or data center servers. If the data is being transferred from the edge site to a different location, it is crucial to make sure that it remains private and encrypted throughout the process.

# The Challenge

## Securing It is non-linear, dynamic, and unconventional

To help ensure the success of healthcare edge use cases, organizations should break down the silos that have traditionally separated network, application development, cybersecurity, and lines of business. Like patient care, decision-making in healthcare requires input and collaboration from various disciplines. This teamwork is also necessary for planning, deploying, and operating edge computing environments.

For example, tele-emergency medical services are widely utilized in use cases that benefit from the capabilities of 5G networks, such as improved speed and cybersecurity features, including

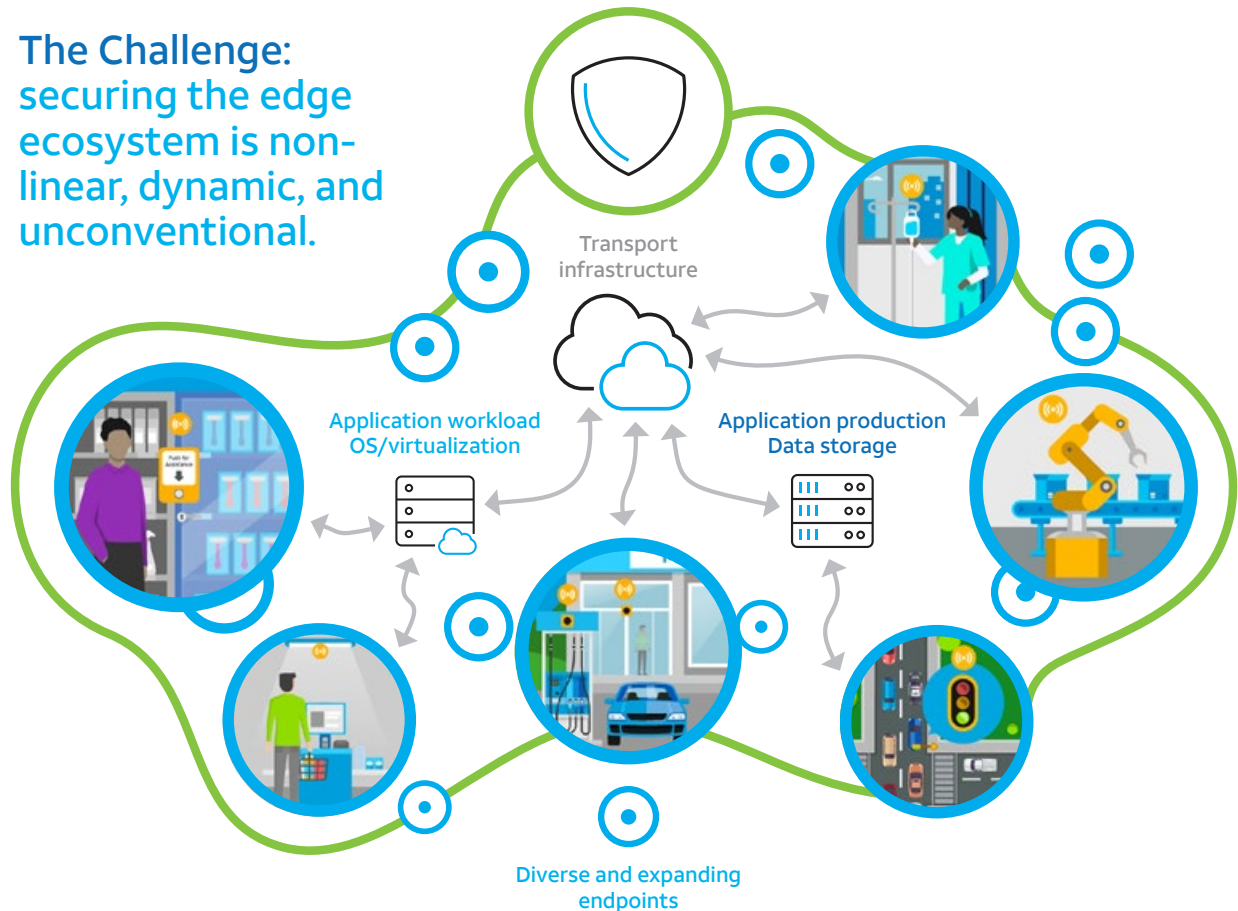
network slicing and enhanced encryption. However, when 5G is unavailable and legacy 4G is utilized, organizations can build resilience into their solutions by adopting compensating controls. These may include further use of multi-factor authentication, data-at-rest encryption, and software-defined networking (SDN) technologies that offer dynamic routing capabilities.

With this level of complexity, it's common to re-evaluate decisions regarding security, data storage, or networking. Decisions are often revisited based on insights gained during the initial pilot stage and when consulting outside expertise. Moreover, regulatory bodies are becoming increasingly prescriptive with minimum standards. For instance, the Food and Drug Administration (FDA) now

requires medical devices to meet specific cybersecurity guidelines and updates them every two years. This means that doctors performing robotic-assisted surgeries on patients remotely need to make sure their network-connected infrastructure is effectively managed and secured. Newer devices often include the ability to install security patches.

IT and cybersecurity teams should establish a collaborative relationship to make sure all devices, including servers, computers, sensors, and robots, are regularly patched. Research indicates that most healthcare edge cases rely on in-house IT staff for patch management, but managed security service providers (MSSPs) are the second most likely group to have primary responsibility for device patching.

**The Challenge: securing the edge ecosystem is non-linear, dynamic, and unconventional.**





# The Opportunity Securing the Ecosystem

## Proactive investing

### Respondents anticipate change and allocate resources accordingly.

When examining investments in healthcare edge computing, the saying “follow the money” holds true. The research reveals that the allocation of investments across overall strategy and planning, network, application, and security for the anticipated use cases that organizations plan to implement within three years is almost equally distributed. Each use case will have its unique investment breakdown based on the scenario’s specific nature.

Figure 2 illustrates the variation in investment allocation among the top five primary healthcare use cases analyzed. Overall, spending is approaching a balance not typically seen in conventional computing. Where there are differences, it is likely tied to the requirements associated with the use case.

For example, the hospital-at-home use case shows a relatively lower percentage

of spending on upfront strategy and planning. A portion of that investment is shifting toward the network segment, which is nearly twice as large. This shift can likely be attributed to requiring sensors to be constantly operational and transmitting data back to healthcare providers during monitoring.

Overall, these investment allocations exemplify the dynamic nature of healthcare edge computing, where there is no one-size-fits-all approach.

## Cross-functional collaboration

### Respondents report value by getting outside help in the edge ecosystem.

Healthcare practitioners prioritizing patient well-being typically work collaboratively rather than in isolated silos. This collaborative approach becomes evident when dealing with serious medical conditions, where a diverse team of professionals comes together to triage, diagnose, and provide care for the patient.

The same principle of collaboration applies when designing healthcare edge computing use cases. Given the critical nature of the healthcare industry, there are significant consequences when things go wrong. Fortunately, despite edge computing being a relatively new technological approach, a growing ecosystem of experienced edge partners can provide valuable insights and expertise.

In fact, the research reveals that 64% of healthcare organizations involved external firms in crucial project planning processes, and 71% relied on external expertise during production. Organizations can minimize the risk of costly mistakes or missteps by using outside expertise as needed.

## Dynamic cyber resilience

**The edge ecosystem requires new thinking.** It’s constantly evolving, and legacy thinking won’t solve emerging challenges. Cyber resilience is crucial, encompassing various disciplines beyond cybersecurity. While cybersecurity is a top concern, other factors should also be considered:

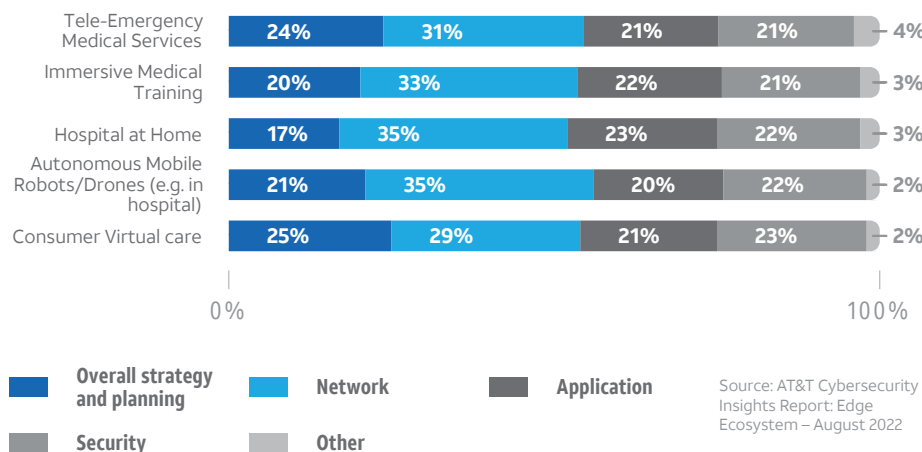
Network resilience plays a vital role in supporting edge devices, whether it’s a sensor monitoring a patient’s vital signs at home or a robot disinfecting hospital rooms. Edge architects must incorporate forward-thinking strategies to accommodate advancements in network technologies.

The ability to update applications, operating systems, or firmware is happening. Healthcare CISOs have shared difficulties securing expensive MRI machines running outdated and unsupported software, which cannot be updated. Regulatory bodies are addressing these concerns by urging manufacturers to incorporate update and patch capabilities to address cybersecurity vulnerabilities. Healthcare organizations should anticipate changes that impact their edge computing use cases, evaluating how devices within the ecosystem, including PCs and remote sensors, can be patched, or upgraded.

Figure 2

### Planned Investments for the Top 5 Healthcare Edge Computing Use Cases

% of Respondents  
N=205



Source: AT&T Cybersecurity Insights Report: Edge Ecosystem – August 2022



# 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:

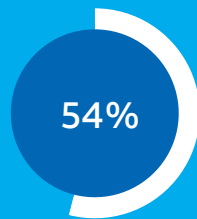
**Make faster and more informed decisions for emergency personnel.**

Security approach:

**Combine on-premises network and security to mitigate insider threats.**

Primary use case snapshot:

Implementation Stage



**Planning**

Top Endpoint



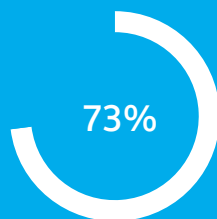
**Mobile Devices**

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**



# Prepare to Secure the Ecosystem

---

## Develop your edge computing profile

It is essential to break down the barriers that typically separate the internal line of business teams, application development teams, network teams, and security teams. Technology decisions should not be made in isolation but rather through collaboration with line of business partners. Understanding the capabilities and limitations of existing business and technology partners makes it easier to identify gaps in evolving project plans.

The edge ecosystem is expanding, and expertise is available to offer solutions that address cost, implementation, mitigating risks, and more. Including expertise from the broader healthcare edge ecosystem increases the chances of outstanding performance and alignment with organizational goals.

---

## Develop an investment strategy

During healthcare edge use case development, organizations should carefully determine where and how much to invest. Think of it as part of monetizing the use case. Building security into the use case from the start allows the organization to consider security as part of the overall cost of goods (COG). It's important to note that no one-size-fits-all solution can provide complete protection for all aspects of edge computing. Instead, organizations should consider a comprehensive and multi-layered approach to address the unique security challenges of each use case.

---

## Increase your compliance capabilities

Regulations in the healthcare industry can vary significantly across different jurisdictions, including countries, states, and municipalities. This underscores the importance of not relying solely on a checkbox approach or conducting annual reviews to help ensure compliance with the growing number of regulations impacting healthcare organizations. Keeping up with technology-related mandates and helping to ensure compliance requires ongoing effort and expertise. If navigating compliance requirements is not within your organization's expertise, seeking outside help from professionals who specialize in this area is advisable.

---

## Align resources with emerging priorities

External collaboration allows organizations to utilize expertise and reduce resource costs. It goes beyond relying solely on internal teams within the organization. It involves tapping into the expanding ecosystem of edge computing experts who offer strategic and practical guidance. The healthcare industry is familiar with the concept of engaging external subject matter experts (SMEs) to enhance decision-making. Involving outside SMEs can help prevent expensive mistakes and accelerate the deployment process. These external experts can help optimize use case implementation, ultimately saving time and resources.

---

## Build-in resilience

Consider approaching edge computing with a layered mindset. Take the time to ideate on various "what-if" scenarios and anticipate potential challenges. For example, what measures exist if a private 5G network experiences an outage? Can patient data remain secure when utilizing a public 4G network? How can business-as-usual operations continue in the event of a ransomware attack?

During the planning stages of development, it's crucial to analyze and address these potential disruptions thoroughly. However, it's not uncommon for certain situations to be overlooked. That's why the pilot phase is essential for uncovering any unforeseen issues before full-scale implementation. Seek input from industry peers and engage external expertise to identify vulnerabilities. Investing time and resources can yield significant benefits in preparedness and cost savings.

---

## Prepare for dynamic response

Edge computing is characterized by its data-driven nature, software-defined infrastructure, and distributed configuration. These key attributes highlight the dynamic nature of edge use cases, where constant data insights drive continuous improvements. By transitioning from a device-centric approach to a software-defined model, edge computing enables greater flexibility in network and security components, enhancing overall resilience. The distributed configuration allows organizations to choose where data is processed and stored, providing additional options for optimizing performance and efficiency.



# Conclusion

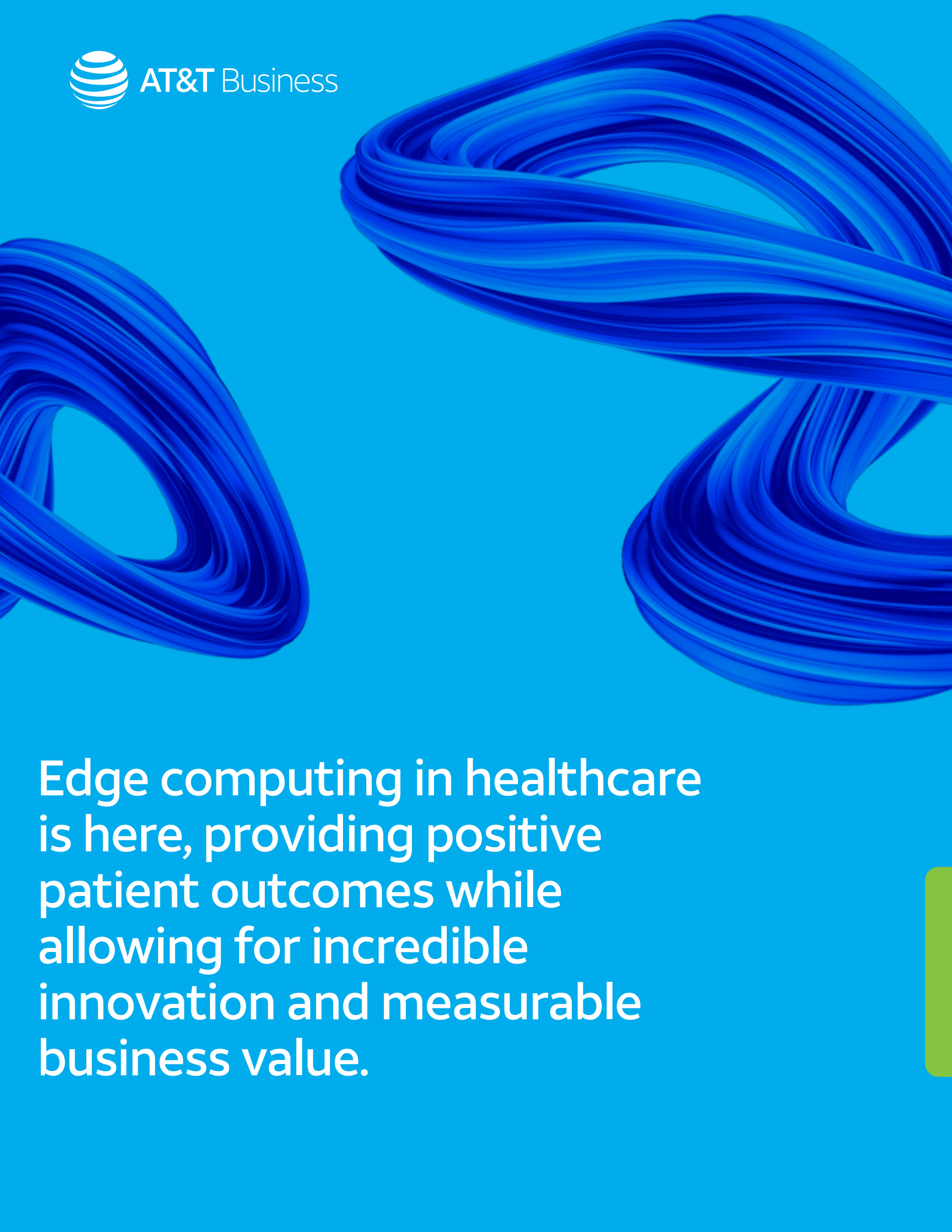
Successful healthcare edge computing implementations require a holistic approach encompassing collaboration, compliance, resilience, and adaptability. By considering these factors and proactively engaging with the expertise available, healthcare organizations can unlock the full potential of edge computing to deliver improved patient outcomes, operational efficiency, and cost-effectiveness in the ever-evolving healthcare landscape.

## 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.

# Contributing Organizations



The background features a vibrant blue gradient. Three large, abstract, swirling shapes made of many thin, overlapping lines are positioned in the upper half of the frame. One swirl is on the left, one is in the top right, and one is in the bottom right. A solid green vertical bar is located on the right edge of the page.

Edge computing in healthcare is here, providing positive patient outcomes while allowing for incredible innovation and measurable business value.