AT&T Business

AT&T Cybersecurity

2023 Edge Ecosystem

Focus on Manufacturing

Focus on Manufacturing

About this Report
This report is a special industry report with a focus on manufacturing 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**.

About the Research
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 202 manufacturing respondents.

The Edge Ecosystem in Manufacturing

n 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 leaders in manufacturing are budgeting differently for edge use cases. These two things, along with an expanded approach to securing edge computing, were prioritized by the respondents in the *2023 AT&T Cybersecurity Insights Report: Edge Ecosystem*.

Topline research findings

In 2023, the manufacturing respondents' primary edge use case is smart warehousing, which involves deploying computing resources close to or on the warehouse floor. The enhanced productivity of warehouse employees, flexible logistics, and better optimization of warehouse space are some benefits of edge computing. This represents a shift from the primary use case in the 2022 AT&T Cybersecurity Insights Report: Securing the Edge, which focused on video-based quality inspection as the primary manufacturing edge computing use case.

As manufacturing has evolved, the need for efficiency and speed is focused on moving goods out of warehouses and onto the next stop of either consumption or integration. The rising cost of labor and customer expectations for next-day or same-day deliveries drive the need for greater investments in rapidly understanding which products are most likely needed to fulfill a sales pipeline or supply chain.

AT A GLANCE

Edge computing in manufacturing is still emerging. The ability to provide new services for the public and quality outcomes for educators and students is a new reality. But it does not happen by accident or in isolation. Cross-functional collaboration among groups that don't normally work together and building-in security from the start is a smart way to tap the potential of these exciting use cases that will meet the stakeholders' expectations.

ATCR CYBERSECURITY INSIGHTS™ REPORT 2023

Devices are changing in manufacturing

Industrial robots are the top endpoint, accounting for 55% of the device category. In addition, 78% of respondents utilize private cellular 5G networks for edge connectivity on-premises. Notably, 55% of the respondents use a combined cybersecurity and networking function in the cloud. The top perceived threat in this context is the concern of a DDoS attack. A DDoS attack can bring down operations, causing a potentially catastrophic ripple effect throughout the supply chain.

And it's just the beginning

One of the most promising aspects of edge computing is its potential to cost-effectively benefit environmental, social, and governance (ESG) goals at both an institutional and a personal level. The 2023 AT&T Cybersecurity Insights Report highlighted two notable use cases: augmented reality for maintenance and intelligent inventory programs.

- Augmented reality (AR) can provide maintenance technicians with a visual overlay of real-time information and instructions needed to complete their jobs. Improved employee safety, better utilization of resources, and reduced downtime can improve overall metrics.

- Using edge computing for inventory intelligence aligns with ESG goals. Near real-time data analytics optimizes inventory levels, resulting in less waste and more efficient use of resources.

Collaboration is critical for development

The edge ecosystem in manufacturing requires collaboration among various stakeholders, including line-of-business leaders, research and development, innovators, legal, compliance, manufacturing and warehouse employees, and networking, cybersecurity, and IT experts. Successful edge computing in manufacturing is more likely to succeed when stakeholders, with all their unique perspectives, frameworks, and priorities, are engaged early and often – throughout research, ideation, proof-of-concept, and implementation.

Edge computing is new and different – it requires input from various stakeholders with possible conflicting priorities. As manufacturing teams continue to innovate with edge computing, aligning stakeholders and architect use cases as one entity with a stated and agreed-upon business outcome is critical. Across all stakeholders, issues such as data regulations, compliance, and

security need to be considered holistically. This means proper planning, budgeting, and collaboration is central to delivering a successful edge computing use case.

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 53% of manufacturing respondents rely on external expertise for project planning and 68% for 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 common characteristics of edge computing

Based on the research, respondents agreed that these edge-computing 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 manufacturing, data sources are collected and instantly analyzed, such as the industrial robots on the shop floor, the sensors measuring heat, humidity, and vibrations in chip manufacturing, or the motion-sensing devices in a warehouse that allow humans and robots to interact. In addition to data creation and consumption, decisions are made closer to where the process occurs, resulting in better outcomes because it is personalized and near real-time, allowing for rapid analysis and response..

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, lost, or damaged. The quantity and length of time that data resides on an edge device impacts the potential risk if the device ends up in the wrong hands. Informed and logical decisions need to be made about whether data should be kept on the device or transferred to other systems for further analysis or auditing.

What are the common characteristics of edge computing?

Software defined
Cloud - public or private, or on-premises

Distributed configuration
Intelligence, networks, and management

Data driven
Closer to user creation and consumption

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.

Consider using edge computing on a manufacturing floor, because of the need for performance, many applications and devices are sensitive to network latency. Edge computing utilizes quality of service (QoS) principles to prioritize latency-sensitive network traffic. Different traffic routes can be utilized, and less latency-sensitive network traffic can be downgraded to handle surges in network traffic. Optimized network routing capabilities are imperative for the critical time-sensitive decision-making that needs to occur.

The elastic capabilities of software-defined networking (SDN), which enables dynamic scaling of networking throughput to match varying demand levels, recalibrate during peak demand situations, such as managing a warehouse during a peak shopping season. SDN can allocate more resources during peak usage: scale up for busy periods and scale down during low activity. In addition, 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 thus delivers a 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 personally identifiable information (PII) 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 manufacturing edge use cases, organizations should break down the silos that have traditionally separated network, application development, cybersecurity, and IT operations.
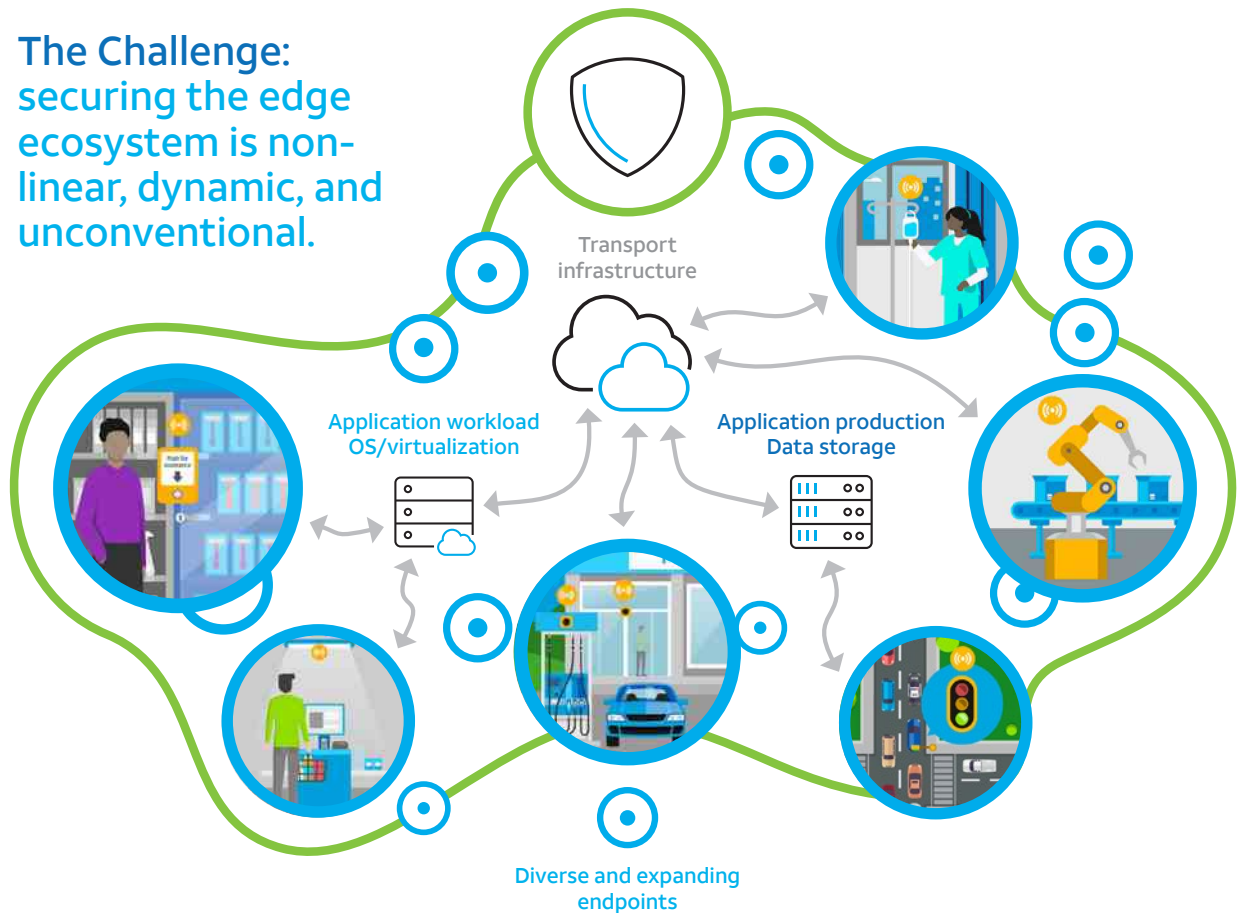
For example, the increased use of sensors and cameras on a production line to reduce defects and increase manufacturing yield can benefit from the capabilities of 5G networks, such as improved speed and cybersecurity features, including network slicing and

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 multifactor authentication, data-at-rest encryption, and SDN technologies that offer dynamic routing capabilities.

With this level of complexity, it's common to reevaluate decisions regarding security, data storage, or networking. Decisions are often revisited based on insights gained during the initial pilot stage of an edge computing use case and when consulting outside expertise.

IT and cybersecurity teams should establish a collaborative relationship to ensure all devices, including servers, computers, sensors, and robots, are regularly patched. Regular, routine, and pro-active patching is critical in edge computing use cases and should be part of an overall ongoing maintenance plan.

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

Transport infrastructure

Application workload OS/virtualization

Application production Data storage

Diverse and expanding endpoints

The Opportunity Securing the Ecosystem

Respondents identified three key initiatives they're embracing as they evolve their edge ecosystem. These initiatives are described in the sections that follow.

Proactive investing

When examining investments in manufacturing 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 manufacturing 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.

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

Cross-functional collaboration

Technology-focused disciplines like IT or networking have often led prior technology revolutions. The mishaps that occurred because the consumers of the technologies were not adequately part of the planning process have caused issues. Prior technology revolutions that did not consider the consumers of the new products led to some unintended consequences, such as the proliferation of shadow computing.

The same principle of collaboration applies when designing manufacturing edge computing use cases. There are significant consequences when things go wrong for many of these use cases, such as employee safety or hampered transportation. Fortunately, despite edge computing being a relatively new technological approach, a growing ecosystem of experienced edge partners can provide valuable insights and expertise.
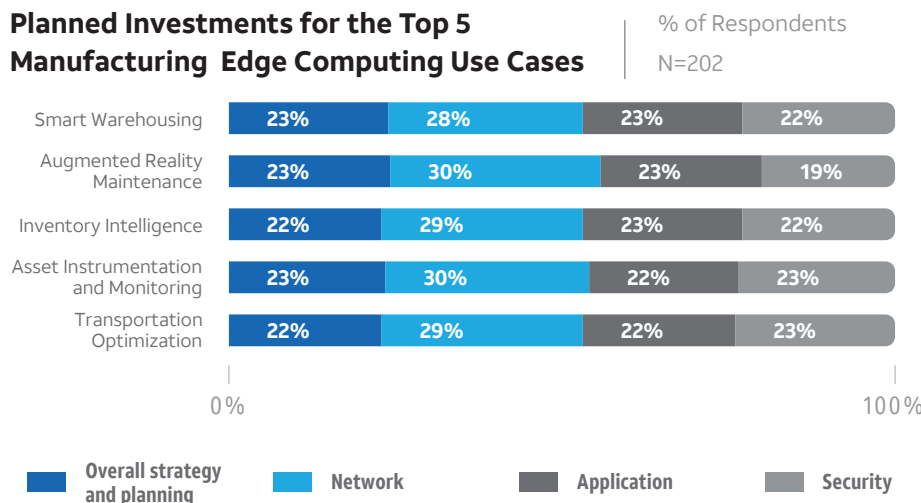
In fact, the research reveals that 53% of manufacturing use cases involved external firms in crucial project planning processes, and 68% relied on external expertise during production. Organizations can minimize the risk of costly mistakes using outside expertise and gain knowledge from trusted advisors implementing edge computing use cases for other clients. Taking advantage of third-party expertise is an added benefit when embarking on new types of computing, especially edge computing, where complexity is high, and the margin for error is low.

Dynamic cyber resilience

Cyber-resilience is crucial, encompassing various disciplines beyond cybersecurity. While cybersecurity is a top concern, other factors should also be considered:

- Embrace network resilience as vital in supporting edge devices, such as providing a 4G backup to a private 5G network used in an augmented reality maintenance use case. Edge architects should incorporate forward-thinking strategies to accommodate advancements in network technologies.

- Plan for the unexpected with edge computing. Edge computing use cases need to be built with redundancy to allow for the possible failure of endpoints or sensors. This ties back to the need for cross-functional communication and collaboration to help with physical engineering needs that may be out of the scope of traditional computing.

Figure 2

Planned Investments for the Top 5 Manufacturing Edge Computing Use Cases

% of Respondents
N=202

Use Case	Overall strategy and planning	Network	Application	Security
Smart Warehousing	23%	28%	23%	22%
Augmented Reality Maintenance	23%	30%	23%	19%
Inventory Intelligence	22%	29%	23%	22%
Asset Instrumentation and Monitoring	23%	30%	22%	23%
Transportation Optimization	22%	29%	22%	23%

0%   100%

Manufacturing Edge Ecosystem

Primary use case:

Smart Warehousing

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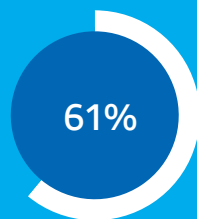
Business need:

Manage warehouse output efficiently while adjusting to seasonal capacity fluctuations.

Security approach:

Combine network and security functions in the cloud to mitigate DDoS attacks.
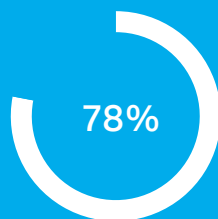
Implementation Stage	Top Endpoint	Data Rate
61%	**55%**	**38%**
Partial	**Industrial Robots**	**Enhanced Mobile Broadband (embb) and Massive Machine (mmtc)**

Edge Network Connectivity	Top Perceived Threat	Cybersecurity Approach
78%	**3.3/5**	**55%**
Private 5G	**DDoS**	**Combined Cybersecurity and Networking Functions in the Cloud**

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

Prepare to Secure the Ecosystem

The 2023 AT&T Cybersecurity Insights Report reveals best practices and recommendations that manufacturing edge computing practitioners can follow to help secure current and future use cases.

Develop your edge computing profile

It is essential to break down the barriers that typically separate the internal lines of business, application development, network, and security teams. Technology decisions should not be made in isolation but instead 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 this expertise from the broader manufacturing edge ecosystem increases the chances of outstanding performance and alignment with organizational goals.

Develop an investment strategy

During manufacturing 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 budget. 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 multilayered approach to address the unique security challenges of each use case.

Increase your compliance capabilities

Manufacturing regulations can vary significantly across different jurisdictions, including countries, states, and municipalities. This underscores the importance of doing more than a simple checkbox approach. Conducting regular reviews helps ensure compliance with the growing number of regulations. 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, respondents report using outside help from experts.

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. Manufacturing is experienced at working with outside experts to optimize operations; edge use case development shouldn't be any different. Involving outside SMEs in edge computing can help prevent costly mistakes and accelerate deployment. 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. During the planning stages of development, it's crucial to thoroughly analyze and address these potential disruptions. The proof-of-concept phase is essential for uncovering any unforeseen issues before full-scale implementation. 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 manufacturing edge computing implementations require a holistic approach encompassing collaboration, compliance, resilience, and adaptability. By considering these factors and proactively engaging with the expertise available, manufacturing organizations can unlock the full potential of edge computing to deliver better outcomes, operational efficiency, and cost-effective solutions.

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

About AT&T Cybersecurity

We simplify securing valuable business assets by providing broad cybersecurity experience and award-winning services for network security, extended detection and response, and endpoints. From traditional computing to edge computing, we're focused on business innovation. We help make complexity easy to understand and navigate.

By providing affordable, strategic services, our clients rely on us as trusted advisors. Our cybersecurity consulting is product neutral, so you get unbiased answers for your business. Our managed security services, threat awareness, and ground-breaking research are dedicated to help keep you protected today and prepared for tomorrow.

AT&T Cybersecurity manages the risk. You reap the reward.

Contributing Organizations

AT&T Business

IDC

Akamai

CISCO

ivanti

SentinelOne

Edge computing in manufacturing is here, providing new ways to make operations more efficient, reduce expenses, and meet ESG goals.