AT&T CYBERSECURITY INSIGHTS™ REPORT

AT&T Business

AT&T Cybersecurity

2023 The Edge Ecosystem

Focus on Manufacturing

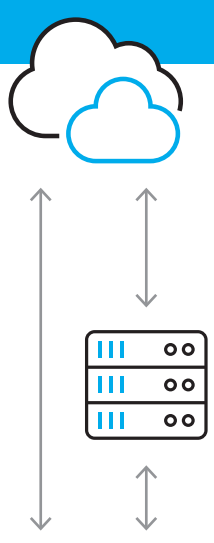
The edge ecosystem is rapidly developing in manufacturing. Our research uncovers the trends to help you start strategically planning and investing for securing this dynamic shift in computing.

Based on survey results from the 2023 AT&T Cybersecurity Insights Report: Edge Ecosystem.

What are the common characteristics of edge computing?

Software defined
Cloud - private or public or on-premise

Data driven
Closer to user creation and consumption



Distributed configuration
Intelligence, networks, and management

Think of the edge ecosystem as a new opportunity for competitive differentiation and business outcomes.

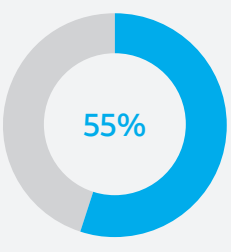
Manufacturing edge computing benchmarks

Primary use case

2022
Video-based quality inspection

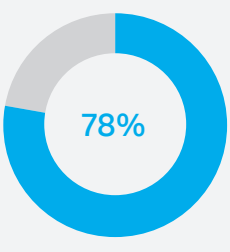
2023
Smart warehousing

Top endpoint



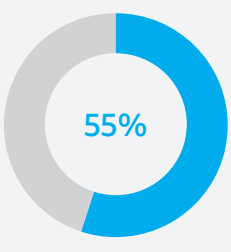
Industrial robots

Top network



Private 5G

Top configuration



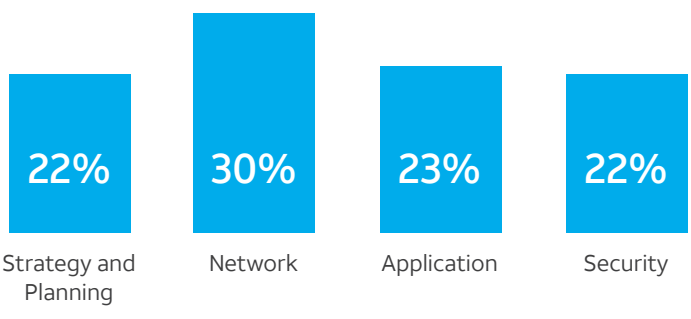
Cybersecurity and networking in the cloud

The Opportunity: creating a secure edge computing ecosystem in manufacturing

Three key initiatives emerged as respondents reported the changes they are making.

1

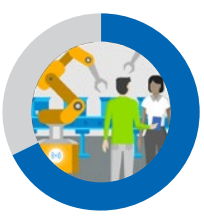
Proactive investing
Respondents anticipate change and are allocating resources accordingly.



2

Cross-functional collaboration
Respondents report value in tapping both internal and external ecosystem expertise.

53%
use external expertise in project planning



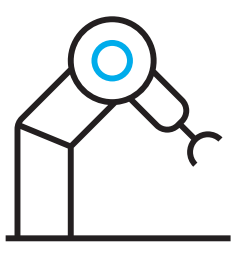
68%
use external expertise in production

3

Dynamic cyber resilience
The edge ecosystem requires new thinking. It's constantly evolving, and legacy thinking won't solve emerging challenges.

Use cases anticipated in next three years:

55%
of use cases are IoT, IIoT, and OT



Prepare to secure your edge ecosystem

Define your edge computing profile
Work with lines-of-business on use cases. Include business partners and vendors to identify which initiatives impact security.

Develop an investment strategy
Bundle security investments with use case development. Evaluate investment allocation and include a security budget.

Increase your compliance capabilities
Regulations can vary significantly. Keep up with tech mandates and compliance by tapping advisors with expertise.

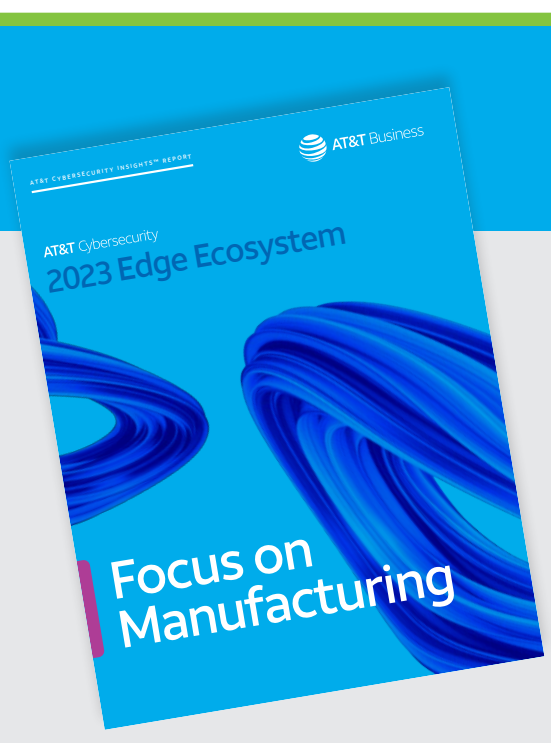
Build-in resilience from the start
Evaluate investment allocation as use cases multiply. Consider bundling security expense with use case development.

Align resources with security priorities
Collaboration expands expertise and lowers resource costs. Edge use case security experts can help streamline use case development.

Prepare for ongoing, dynamic response
Use cases require high-speed, low-latency networks; at the same time, network functions and cybersecurity controls will converge.

Get the 2023 AT&T Cybersecurity Insights Report: Focus on Manufacturing

Download



About the research

Research 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%. More information is available in the full report. https://cybersecurity.att.com/insights-report