NTT DATA

Navigating the new world of network security in manufacturing

Network as a service addresses business risk

Security and networking, along with cloud-first solutions and a move to identity-based security, will be key to the manufacturing network of the future.

Change and complexity pose unprecedented challenges to network security

Hybrid and distributed working, along with ongoing digital transformation, have become significant instigators of change and complexity in modern manufacturing networks. Both create unprecedented challenges to network security.

Threats can now come from anywhere. Heightened by recent global geopolitical tensions and ongoing supply-chain disruptions, they are particularly impactful in manufacturing. Yet many manufacturing organizations lack the know-how to chart a way forward with confidence.

According to the NTT DATA 2022–23 Global Network Report, the highest number of newly discovered security vulnerabilities on record was recorded in 2021.[1]

The report finds that amid geopolitical tensions and supply chain disruptions, attacks on the technology, telecommunications, and transportation and distribution sectors — all critical to manufacturing operations — have more than doubled. Cybersecurity experts and attackers alike are focusing intently on discovering new targets and methods.

More recently, high-profile security incidents have kept occurring across countries and industries. For example, in Australia, hackers posted customer data from health-insurance provider Medibank on the dark web.[2] In a separate incident, telecommunications firm Optus reported that the personal identification numbers of 2.1 million Australians had been compromised.[3]

Applications under attack

The wholesale migration of on-premises applications to the cloud has helped mitigate attacks. Cloud providers have been strengthening their infrastructure and security services to counter infrastructure-level vulnerabilities. However, applications within manufacturing mostly remain under the control of manufacturing organizations.

The nature of modern manufacturing applications is increasingly distributed and interconnected. This, combined with the number of ways in which application users interact with these applications (through user interfaces and application programming interfaces [API], for example), has increased the size of the attack surface. An overlooked public-API endpoint in a manufacturing application can be enough to cause significant harm to an organization. It can disrupt production and compromise sensitive manufacturing data.

Manufacturers are clear that the convergence of security and networking, along with cloud-first solutions and a move to identity-based security, will all be key to the network of the future.

NTT DATA 2022-23 Global Network Report[1]

Security concerns prompt a preference for outsourced network operations

According to the NTT DATA 2022–23 Global Network Report, more than 90% of organizations agree (over 40% strongly) that ever-increasing security and compliance risks are a challenge across their information technology (IT) and network operations.

The latest report classifies top-performing organizations as those with higher revenue growth (up by more than 10% in the latest fiscal year) and a stronger operating profit as a percentage of revenue (more than 15% in the latest fiscal year). Underperformers are those organizations with 0% or less revenue growth and an operating profit as a percentage of revenue of less than 5%.

The research finds that:

- 87% of top-performing organizations are investing in their cybersecurity capabilities, compared with just 41% of underperformers.
- 91% of all organizations are focusing on the move from perimeter-based security to identity-based security.
- After budget constraints — a logical concern, as 95% of organizations are already investing in their cybersecurity capabilities — vendor capability and rigidity are the top challenges to achieving network success.
- The need to improve security and compliance is one of the top three network-related motivators for CEOs in the next two years.

The results show that 89% of C-suite executives have operational concerns about running complex, intelligent networks that comply with security and regulatory requirements. It's precisely because of this complexity that 87% of senior IT security leaders would prefer to outsource their entire network, from end to end, to a single partner rather than multiple vendors.

Almost every manufacturer used a technology partner to deploy additional cybersecurity in the 12 months preceding the survey. However, most struggled to find a partner with the right experience and capabilities.

They also want to sidestep vendor lock-in and rigidity. Our research shows that most respondents cite their own lack of expertise in security as a main consideration when selecting a managed security service provider.

Underinvestment in the network creates risks

According to the report, 93% of organizations believe new threats will increase security demands, requiring deeper levels of access control and inspection. However, just 59% of IT leaders agree strongly that their organization is investing enough in cybersecurity capabilities.

Surprisingly, amid these prevalent concerns about increasing security and compliance risks challenging all areas of their network, 16% of organizations still have no structured processes in place for cybersecurity or remain in the very early stages of addressing this need.

Fewer than one in four respondents have optimized their security posture despite the rapid increase in critical threats. As an additional layer of risk mitigation, 91% of organizations insure specifically against cybersecurity risks. Doing so can address the potential financial impact of a cybersecurity incident, but it cannot repair reputational harm.

Even so, the research indicates that the security risks of underinvestment in the network — or, even worse, taking no action at all — are clear:

- Security policies are inconsistent, posing reputational, financial and compliance risks.
- Outdated infrastructure creates a broader attack surface.
- Typically, the security posture focuses on the network perimeter rather than across users and applications.

Manufacturers are willing but not able to ramp up security

When asked about their greatest challenges in optimizing their organization's network infrastructure, CIOs and CTOs list managing data security and the complexity of cost control across multi-cloud environments as their top obstacles. The operational complexity of multi-cloud and getting multiple service providers to work together follow these issues.

The research finds that security, identity, access and privilege management tools are the most prevalent network-platform tools in place for manufacturers at all levels of network maturity. Secure connectivity is next. Furthermore:

- 94% of organizations agree that the adoption of cloud solutions is compelling new connectivity and security architectures, including secure access service edge (SASE).
- Nearly nine in 10 (88%) agree that zero-trust security enables secure and transparent network delivery, and 92% agree that implementing privileged access and identity management for audited just-in-time network-management tasks is critical to their security posture.
- Automation levels are rising in line with digital optimization, network satisfaction and profitability. Among respondents, 44% now say they have a highly or fully automated security posture and another 45% say it has been partially automated.

However, many manufacturing organizations may lack the skills to implement and manage all these security improvements in the most optimal way. It's clear that complexity is a common stumbling block when trying to address these challenges internally.

Why network as a service is gaining traction

A key challenge for more than nine in 10 organizations is that their cybersecurity teams are only partly involved in network architecture decision-making and vendor selection. However, the propensity to include these teams rises sharply among top performers. For those with advanced network maturity and well-aligned business and network strategies it more than doubles.

Also, only two in five IT security teams say their security strategy fully aligns with business needs.

It is therefore unsurprising that 98% of organizations are open to network as a service as a simpler way of addressing their deepening business risk. This can help address complexity and security concerns while providing access to skilled resources to build a modern, agile network with security at its core, not bolted on as an afterthought.

Additionally, the subscription nature of these solutions helps manufacturers avoid future technical debt, as the barriers to network transformation and modernization are significantly lower.

Recommendations for outsourcing network management

Beyond price, senior executives say they consider a service provider's range of skills, track record, operational support, flexibility and scalability, and coverage as their key considerations. The research highlights that manufacturers looking to successfully outsource their network should:

1.

Evaluate the capabilities of service providers, which should be able to manage both the current state of the network and its ongoing evolution. This includes incorporating new network technology with improved security, analytics and AIOps. Such a partnership addresses a lack of in-house skills in this area and frees up time for in-house IT and OT teams to focus on translating key business transformation initiatives into technology strategies, rather than being bogged down by routine network maintenance.

2.

Engage with a single vendor to minimize contract complexities. Doing so also eliminates the lack of interoperability between vendors and the need to maintain multiple software versions. For example, the convergence of networking and security is leading organizations away from having separate vendors in these areas.

3.

Consider the network-as-a-service model, as this can save time and money. According to the research, more than 90% of senior executives prefer this model.1 They cite the flexibility to scale up and down, followed by supply-chain certainty, a single consumable model, and a balance between operational and capital expenditure as their main reasons for this choice. Top-performing organizations are almost twice as likely to strongly prefer this model than underperformers.

4.

Get guidance from the experts

Our network consulting services can help you transform and improve infrastructure performance and develop a clear, comprehensive security strategy that addresses business risks. Register for a complimentary network assessment and get recommendations from our experts on network operations models, platform-delivered service operations and next steps to advance your digital initiatives.

Work with a service provider that takes a platform-based approach to technology management (using AIOps capabilities to cluster and correlate feeds of metrics from multiple technology types) to overcome the siloed nature of individual tools in a multivendor network environment. The vendor should also provide an MSP AI aggregation layer that builds on vendor-specific AI capabilities (where they exist) in the network infrastructure.

Take the next step

We work with manufacturing organizations around the world to shape and achieve outcomes through intelligent technology solutions, including network management and security. Contact us now for more information on how we can help you secure your manufacturing network and achieve your business goals.

Sources

1. NTT DATA. "2022–23 Global Network Report." https://services.global.ntt/en-us/insights/2022-23-global-network-report

2. Josh Taylor. "Medibank hackers announce 'case closed' and dump huge data file on dark web." The Guardian. November 30, 2022. https://www.theguardian.com/australia-news/2022/dec/01/medibank-hackers-announce-case-closed-and-dump-huge-data-file-on-dark-web

3. Jason Firch. "Australian Telecom Optus Exposes Data Of 2.1 Million Customers." PurpleSec. May 4, 2024. https://purplesec.us/breach-report/optus-data-breach/

Visit us.nttdata.com to learn more.

NTT DATA is a trusted global innovator of business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have diverse experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.