Rearchitecting manufacturing for IT security

The manufacturing sector is a prime target for hackers and bad actors of all kinds. In 2021, manufacturing was the most attacked sector of the economy, even more so than the financial services industry.[1]

Every modern enterprise is a target. The reasons manufacturers top the list are complex. There are aspects of both the business of manufacturing and the IT environment that contribute to its target profile for bad actors of many types.

Business model factors

Manufacturing is an asset-heavy industry. One of the key assets it possesses is intellectual property (IP). Manufacturing IP can cover a wide range of sensitive categories, from trade secrets around managing difficult scientific matters such as materials science to process flows and other insights that only come from experience and investment. Industrial spies or nation state actors looking to take advantage of someone else's hard-earned knowledge will try to infiltrate systems to steal that IP.

It's time to rethink security in the manufacturing industry.

Manufacturing is also a 24/7 business. In addition to the traditional three-shift workforce structure, automation enables near-constant operations. Manufacturers make commitments to their customers based on that schedule. Time is money, as the saying goes. According to IDC, every hour of downtime costs $113,099 on average.[2]

Ransomware is a scourge that targets those who cannot operate without their data and applications – and have significant risks over any disruption. This extortion racket has targeted hospitals, municipalities and now has set its sights on manufacturing. Manufacturers might not feel they have much in common with hospitals, but they look similar to ransomware hackers.

Distributed Denial of Service (DDoS) attacks seek to overwhelm systems with access requests. Typically, this involves a corporate website or e-commerce site. DDoS has unfortunately evolved. Because hacker networks have gotten so good at launching such attacks, DDoS can be a diversionary tactic. A manufacturer's corporate website could be under attack to get IT staff focused there, while the firm's IP is going out the virtual backdoor.

1. Security Management Magazine Article
2. International Data Corp InfoBrief

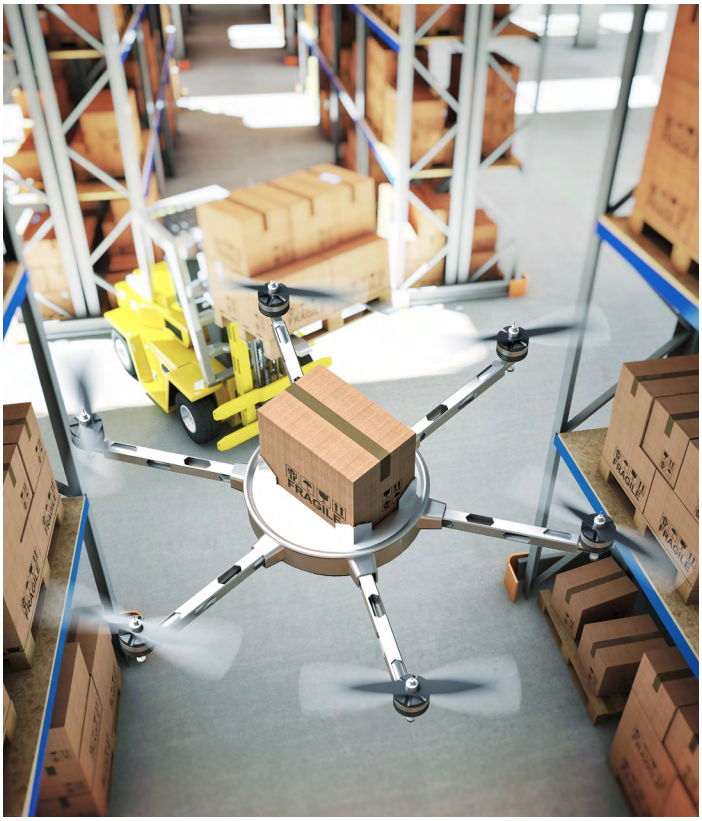
LUMEN® TECHNOLOGIES

Unique environments

Manufacturers also operate unique IT environments. In addition to all the usual office devices, manufacturers operate thousands of endpoints producing data and feeding it into other parts of the system. With the Internet of Things (IoT), these endpoints stretch from the factory floor to external networks. From the hacker's perspective, there is a huge attack surface to exploit.

A single piece of manufacturing equipment can cost millions of dollars. So manufacturers will seek to keep that machine going as long as possible before having to budget for replacing it. This can create an odd mix of old and new equipment, some of which might not be patchable with the latest security technology – yet they are vital to production. Each machine must be secured in the best way possible.

Manufacturers often have deep supply chains, warehouse management systems, connections to customers and a torrent of real-time data running throughout that system. It is all tied together with application programming interfaces (API). Those APIs are doorways between companies that hackers might walk through once infiltrating someone else in the chain. Those APIs must be protected and the data running across them inspected.



Your security must be holistic and proactive. It cannot begin with an incident.

Why Lumen

Staying secure in a fast-moving world requires a strategy, security partners and ongoing vigilance. Your security must be holistic and proactive. It cannot begin with an incident.

Lumen is a key security partner for many manufacturing firms. Lumen brings an array of professional services in addition to the Lumen platform of adaptive networking, edge cloud, connected security and collaboration services. Our professional services consultants can perform assessments and penetration tests to determine where you are vulnerable. Our security services include the capability to monitor and analyze traffic across the APIs that knit together the modern enterprise.

Lumen's platform and ecosystem model also allows an agnostic approach to the technologies a customer needs, integrating the best of breed tools and services from a variety of partners. This allows new measures such as Zero Trust Access and Secure Access Services Edge (SASE) to be smoothly implemented. These and other new security concepts are really frameworks where different technologies must work together.

Lumen's edge compute capability can aid in processing and securing real-time data. As a major carrier of the global Internet backbone, Lumen's network also acts as a threat sensor for organized attacks. Our threat intelligence operation, Black Lotus Labs®, constantly analyzes this traffic looking for anomalies and patterns indicating dangers such as DDoS attacks and other exploits. In many cases, we can neutralize these attacks before customers see an impact. The Lumen network is secure by design and we can add layers on top of that foundation.

Lumen can help the modern manufacturer secure its business in a fast-moving threat landscape.

Lumen® Connected Security

Network and application protection	Threat intelligence, detection and response	Security consulting
Keep the business running and stay aware of risks	Protect from continually evolving threats	Partner with experts to leave no security risk unaddressed
• Secure Access Service Edge • DDoS Mitigation Services • Application protection • Perimeter Security • Managed Zero Trust Network Access	• Managed Detection and Response • Incident response • Rapid Threat Intelligence • SOCaaS • Managed SIEM • Vulnerability Assessment	• Advisory services • Workshops and planning • Compliance and framework assessments • Vulnerability management • Security assessment

LUMEN® TECHNOLOGIES