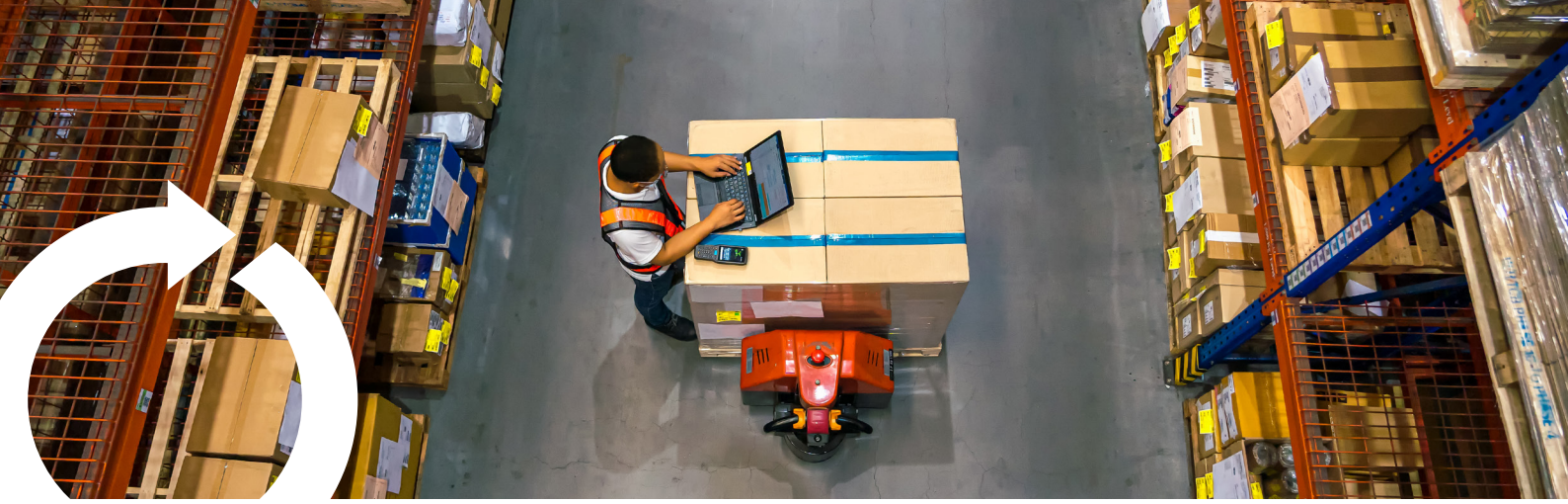
Ontinue

WHITE PAPER

Manufacturers: Outsource Your SOC to Outsmart Threat Actors



Production of nearly every type of product in today's world relies on some form of connected machinery to manufacture safely and efficiently. Chemical companies use specialized equipment to blend raw materials for their pharmaceutical customers, allowing them to create life-changing and life-saving medications. Robotics firms create smart machines that make it possible for automotive customers to automate and streamline production lines. Food service companies rely on custom machinery to process dairy and other beverages so they flow freely and are packaged safely.

Manufacturing companies like these and others around the world who rely on operational technology (OT) face a realm of threats never imagined when some of their most vital production equipment was manufactured 20, 30 or even 40 years ago.

Keeping that OT up and running 24/7 to fulfill production SLAs and other requirements is non-negotiable. Global manufacturers operate 24/7 around the world, so downtime isn't an option. For those manufacturers who take a "just in time" production approach, the impact of disruption is exacerbated, and only increases the probability of ransom being paid. But between 2018 and 2022, the manufacturing industry experienced the greatest share of cyberattacks — and given how costly potential downtime is for this industry, it's not surprising that extortion was involved in 30% of these incidents.*

While manufacturers deal with the same cybersecurity challenges other industries face, there are several challenges unique to the industry.

- **Equipment monopolies:** Manufacturers often require specialty equipment to produce their product, and generally in the manufacturing space there are few options to source that equipment. With a limited number of options for purchasing the equipment or machinery required to produce a company's product, this gives the company/companies who produce the machines a monopoly on the machinery, leaving customers with few options and little leverage—and nowhere else to turn if a supply chain falls victim to an attack.
- **OT compatibility:** Manufacturing equipment may have a life span of 20, 30 or even 40 years, yet it still needs to work with other newer systems and technology created in the past 10 years. Legacy debt support is a significant issue, and standards aren't changed or adopted as quickly as in the IT environment. In some cases, such machines have a vendor lock, so upgrades and new security updates are dependent on the vendor. If a vendor no longer exists or has stopped releasing security patches, that may leave you stuck with outdated and vulnerable equipment.
- **Supply chain threats:** With a larger attack surface than other verticals, detecting vulnerabilities in a manufacturer's OT equipment depends on the operating system, how accessible it is, and whether it responds to scans that could identify vulnerability issues — among other issues. Unfortunately, most OT environments are more of a black box and don't make it easy to scan vulnerabilities. Having the visibility to understand what the embedded operation system is, even if you can't scan or patch it, may make other compensating controls possible. Many global manufacturers are interconnected to other businesses in the supply chain, which increases the chance that an attack on one company can affect others in the chain.
- **Talent shortages:** While the global talent shortage is a problem in all industries, manufacturers seem especially challenged to find qualified cybersecurity talent. Manufacturers, due to their remote locations or their business models, often struggle to attract talent or pay the same salaries as banks or professional services firms, so building an in-house security operations center (SOC) simply isn't an option.
- **Global footprint:** Manufacturers with global production demand 24/7 availability — more so than in many other industries — so taking a machine

* X-Force Threat Intelligence Index 2023, IBM, 2023

offline because it's infected by ransomware has significant financial repercussions. With intellectual property theft the top cybersecurity concern among manufacturers, protecting IP across a global footprint becomes more challenging in areas that don't respect IP ownership.

Solving for the complexity of OT

Manufacturing as an industry has a significant OT footprint — among the largest of all verticals. Historically, that space has always been the least protected because it's the hardest to protect, and attackers have taken note. Because IT systems are well protected with cybersecurity solutions, attackers have taken the path of least resistance: homing in on OT devices that are more connected than ever and can provide an easier path into the broader network — or provide a ripe attack target themselves.

Traditionally OT protocols are less secure because production machines from 40+ years ago were created well before the age of the Internet, so there was no need to design them to thwart cyberattacks. In some ways, that's changed with the move to connected devices. Many have been designed with security in mind, although there are still device types that are severely lacking built-in security capabilities. And while you may have a good idea of how the OT systems work, the nature of those devices and the ways in which they communicate with each other, and the network mean it's often harder to determine the threats to and vulnerabilities of those assets.

Given the complexity of securing the manufacturing OT environment, the talent shortage, the impact an attack can have on the supply chain and with it, a company's ability to meet its SLAs, manufacturers have turned to managed extended detection and response (MXDR) service providers to manage their cybersecurity.

Outsourcing your SOC to the experts

As infrastructure grows in a manufacturing environment, its complexity grows, too. Between working with external vendors and procuring complete solutions for production systems, understanding how everything works together becomes ever more challenging. But automatic detection by an MXDR service provider can help you identify what assets exist in your organization's network, what software is supplied, and whether and how the OT works, and who needs access to what systems.

Once you understand what devices are integrated to which assets, you can then discuss vulnerability management. In terms of your systems: What is the most significant risk for your company, its livelihood and potential impact? Is there a single critical production machine producing your goods? Is it a production line whose failure would cause a lot of other machines to fail? Understanding the answer to these questions will identify the highly vulnerable pieces of equipment that demand the greatest protection. In most OT environments, just as in most IT environments, patching every single system and plugging every vulnerability is often impossible—being able to understand the risk posed by each vulnerability and prioritizing accordingly is crucial.

Driving business outcomes while doing more with less

Manufacturers who've standardized on the Microsoft Security product portfolio will want to identify an MXDR service provider that offers a security operations center (SOC) with sufficient expertise in Microsoft Security and collaboration tools, so they can help your business extract the greatest value from your investment. And if you're using Microsoft Sentinel, you'll want to find a service provider who can optimize your spending on Sentinel to improve ROI to increase time-to-value.

While manufacturing is among the most at-risk industries as a ransomware or malware target, look for an MXDR service provider who can help drive the outcomes you need:

- **Detect and respond quickly:** Because production lines don't stop, resolving security incidents can't slow you down. You'll need real-time collaboration and automation through AI, so efforts are focused on true threats and communication is in real time. A knowledgeable MXDR service provider who has

manufacturing expertise in house will factor in all of your assets, even decades-old systems and production equipment.

- **Maximize your Microsoft investment:** With budgets being what they are, improving the ROI of your Microsoft spending can speed time to value, as long as your vendor has the expertise to integrate new Microsoft detection capabilities into its coverage model. For manufacturers using Microsoft Defender, an MXDR service should offer the ability to leverage Defender for IoT, which can help you manage the security of thousands of connected devices, reducing the pressure on your internal team.
- **Gain a SecOps force multiplier:** Finding experienced cybersecurity professionals during a talent shortage makes it increasingly attractive to outsource your SOC to security experts. But that's just the beginning. Optimizing your day-to-day security operations is a critical part of the solution, and that can only happen if there is continual measurement and optimization and attentive partners.
- **Accelerate security program maturity:** Staying ahead of supply chain threats means you have to adopt a mindset of continuous improvement. But improving security program efficacy and scalability requires focusing prevention, detection and response efforts according to your company's risk profile. Seek a vendor who can continually reduce risk and mitigate threats—while measuring historical impact and identifying the most critical areas of potential risk.

Conclusion

To manage the requirements of a global manufacturing organization, an MXDR service provider needs to have dedicated teams of experts in threat hunting, vulnerability management, and threat intelligence. Enhancing that with AI-powered automation and data science will elevate your organization's capabilities and provide not only around-the-clock service, but a focus on the alerts that truly matter to your organization.