Prevention First

6 Ways to Prevent Cyberattacks in Manufacturing

Digital Security
Progress. Protected.

Navigating cybersecurity risks in manufacturing

The following paper will explore exactly what risks manufacturing organizations are facing across multiple threat vectors. And it will explain how a multi-layered prevention-first strategy can be effectively implemented in a manufacturing environment.

As IT complexity increases and threats continue to grow in volume and sophistication, the best way to manage these challenges is from a single, unified platform and pane of glass. When change is the only constant, finding a cybersecurity partner you can trust will be critical.

The world is changing fast. And technology is the agent of this change—transforming how global businesses operate and interact with their supply chains and customers. But the cost of this digital transformation is a quickly expanding cyberattack surface.

Amidst the challenges of legacy systems and Industry 4.0, email inboxes, endpoints, SaaS applications, mobile devices, networks and other assets present growing targets for threat actors. Many organizations are struggling to manage a dynamic set of risks. A recent Verizon report states that 83% of breaches in manufacturing were represented by system intrusion, social engineering and basic web application attacks. According to Infosecurity Magazine, the manufacturing sector is top-targeted industry by cyber extortion campaigns. Another statistic reveals that over half (52%) of organizations don't know how much of their attack surface is secured—and **none are confident that they are fully in control of that attack surface.**

20%

of all extortion campaigns

targeted the manufacturing sector.

More than

52%

of companies

don't know how much of their attack surface is secured.

Layering Up Protection Across Attack Vectors

Manufacturers are faced with daily attempts to steal sensitive internal, customer or employee data, hijack IT assets or encrypt critical systems. Here are the **six essential layers** you should address from a cybersecurity perspective.

ENDPOINT

The endpoint represents the intersection of human and machine. That makes it a popular target for attack, as threat actors look to exploit vulnerabilities in endpoint devices/machines, or human fallibility (via phishing), to gain a foothold into networks. Fileless malware is particularly dangerous as it doesn't leverage traditional executable files.

1 PREVENTION AT THE ENDPOINT LEVEL

Endpoint protection must go beyond traditional AV to feature AI-powered behavioral analysis, which can help stop fileless exploits executed via scripts. Such technology can investigate and classify suspicious samples at scale to streamline threat prevention. Look for solutions that **continuously update in real time** and **apply multiple layers of protection**. Endpoint protection should also work across multiple operating system and machine or device types.

In the manufacturing, **securing operational technology (OT) and industrial IoT devices** is essential. **Detecting vulnerabilities and eliminating them, or mitigating their exploitation**, by installing the latest patches for apps and operating systems remain crucial prevention measures. Organizations should prevent any potential risk caused by postponed patching, and **seek an automated solution**.

MOBILE

The trend toward hybrid and remote working means that more users are accessing corporate resources from mobile devices. In manufacturing environments they can even reduce costs. But these are increasingly targeted with phishing attacks and malware, and are at higher risk of loss or theft.

2 PREVENTION AT THE MOBILE LEVEL

Organizations need multi-layered protection that works across all their corporate devices. Where possible, it should include **anti-theft** (including remote wipe and lock), **app control**, **web security** and **anti-phishing**, as well as the ability to remotely **enforce password policies**, and more. All of this must be manageable from a single console for enhanced visibility and control.

CLOUD PRODUCTIVITY APPS AND EMAIL

Email continues to be a popular conduit for threats such as phishing attacks, advanced ransomware, business email compromise (BEC) and more. In fact, phishing was the most common initial access vector in data breaches in 2023.

The most popular cloud email and productivity platforms, Microsoft 365 and Google Workspace, include a host of cloud-based productivity applications such as cloud storage and collaboration, which can be targeted for data theft and extortion.

Organizations shouldn't rely on the cloud providers' native security controls alone to keep them safe.

3 PREVENTION AT THE CLOUD APP AND EMAIL LEVEL

Best practice dictates enhancing Microsoft's or Google's built-in controls with dedicated, multi-layered protection for cloud-hosted email, collaboration and storage. **Integrated cloud email security** or a cloud-native, API-enabled email security solution should include **spam filtering**, **anti-malware scanning**, **anti-phishing** and **behavioral analysis**. It will automatically scan for any new and changed files in shared storage to prevent malware from executing or spreading. And ideally, it should be manageable from a single, centralized console.

4 PREVENTION AT THE ON-PREMISES EMAIL LEVEL

Organizations that, for various reasons, still operate on-premises mail servers must deploy comprehensive anti-phishing, anti-spam and anti-malware protections **to filter unsolicited or malicious messages**. In addition, they need to protect the server as a host. The best solutions combine AI with human expertise, and feature support for clustering, which allows products to communicate with each other and exchange configurations, notifications, greylisting and more, for enterprise-grade protection.

HARDWARE & DEVICES

As endpoints proliferate, so does the attack surface. And very often, it's corporate data that threat actors are after. They may attempt to compromise machines via vulnerability exploitation, or—more frequently—by using legitimate credentials. The average cost of data breach in industrial sector is $5.56m today. Protecting industrial control systems (ICS) and operational technology (OT) is crucial, as these systems are integral to production processes and supply chain management.

5 PREVENTION AT THE HARDWARE LEVEL

Organizations can put in place layered protection, but it's not 100% foolproof. If the worst-case scenario does occur, they also need **strong encryption of data** to render it useless to any would-be thief. This will also help to ensure compliance with ISA/IEC 62443 series of standards, CCPA and other regulations and cyber insurance requirements. Organizations should look for a solution that applies 256-bit Advanced Encryption Standard (AES) to system disks, partitions and entire drives—ensuring that nothing is exposed. For ease of administration and utility, it should work across Windows/macOS, and enable management of multiple devices from a single console.

IDENTITY

Increasingly, threat actors are dispensing with malware and vulnerability exploitation altogether, and using legitimate credentials to impersonate users and glide past endpoint defenses. According to the Verizon report, 58% of attacks in the manufacturing sector compromised clients' personal data.

The work of threat actors is made easier because of password reuse and poor password management. You should conduct regular cybersecurity awareness training that covers phishing, password management, and secure data handling. Encouraging employees to report suspicious activity without fear fosters an open, prevention-first security culture.

6 PREVENTION AT THE IDENTITY LEVEL

Multifactor authentication (MFA) is essential in preventing credential misuse, especially on privileged or administrative accounts and it reduces the risk of unauthorized access. Solutions should support **mobile-based, one-tap authentication** that works seamlessly across Android and iOS devices, integrating with biometrics and supporting push authentication. Native support for network access, VPNs, Remote Desktop Protocol (RDP), Outlook Web Access, VMware Horizon View and RADIUS-based services would also enhance back-end efficiency. Comprehensive MFA solutions should also work with hardware tokens if the organization uses them.

Going beyond with MDR

Alongside protection at each of these points across the attack surface, manufacturers should consider the value of Extended Detection and Response (XDR) that offers proactive, prevention-first cybersecurity. XDR reveals poorly configured systems, unpatched vulnerabilities, and hidden threats, enabling prompt action and building cyber resilience.

But for organizations with understaffed or underqualified security personnel, MDR might be an even better option. ESET MDR can provide around-the-clock security, alleviating risks stemming from solutions such as EDR. All of this is achieved without the need for heavy investment into internal resources, while still maintaining production efficiencies. MDR helps organizations:

- **Strengthen security readiness with threat detection, investigation and response capabilities with cybersecurity expertise**
- **Achieve cost-efficient, always-on, 24/7 expert-led threat hunting**
- **Reduce costs of maintaining in-house skilled workforces while minimizing the incident response times to minutes**
- **Get ready for compliance; EDR/XDR and MDR are becoming critical components of cybersecurity insurance and regulatory requirements**

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

EXPLORE

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

Digital Security
Progress. Protected.