



Cybersecurity for manufacturers in the Industry 4.0 era:

Solving for the air-gap conundrum



Cybersecurity
Progress. Protected.

Manufacturing Security at a Crossroads

Security leaders in the manufacturing industry are being pulled in two directions. On the one hand is the requirement to secure the OT network against the growing array of threats that target those networks, which are often filled with legacy hardware for which no patches are available.

On the other hand is IT/OT convergence and digital transformation, where interconnectedness between IT and OT drives all manner of new business efficiencies and is a key underpinning of Industry 4.0.

Historically, OT networks were purpose-built, ran designed-for-industry protocols, and were effectively secured via “security through obscurity” and air-gapped separation from other business networks. Enhancing them with internet connectivity exposes them to cyberthreats.

Plus, the ability of threat actors to penetrate the OT networks has become easier with the use of network protocols built on top of publicly documented internet protocols, human/machine interfaces and other computing devices that run familiar operating systems, and adoption of industrial internet-of-things devices.



Given the changed threat landscape, Rockwell Automation, a provider of industrial automation and digital transformation technologies, reiterated its prior guidance to customers to disconnect devices from the internet:

Due to heightened geopolitical tensions and adversarial cyber activity globally, Rockwell Automation is issuing this notice urging all customers to take IMMEDIATE action to assess whether they have devices facing the public internet and, if so, urgently remove that connectivity for devices not specifically designed for public internet connectivity.

Consistent with Rockwell Automation’s guidance for all devices not specifically designed for public internet connectivity (for example, cloud and edge offerings), users should never configure their assets to be directly connected to the public-facing internet. Removing that connectivity as a proactive step reduces attack surface and can immediately reduce exposure to unauthorized and malicious cyber activity from external threat actors.

Echoing the Rockwell Automation advisory, in May 2025, CISA published “Primary Mitigations to Reduce Cyber Threats to Operational Technology.” Among the steps suggested were removing OT connections from the public internet, securing remote access to OT networks, and segmentation between the IT and OT networks.

How air gapped is air gapped?

Maintaining an absolute, 100% separation between the IT and OT networks is certainly possible, but in the age of IT/OT convergence and Industry 4.0, it's increasingly rare. In fact, according to Sean McGurk, the former Director, National Cybersecurity and Communications Integration Center (NCCIC) at the [Department of Homeland Security](#):

“In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network.”

If the needs of the business are such that a full air gap isn't possible, best-practice security for separating the IT and the OT networks is, at minimum, network segmentation with a firewall.

In a more secure version, the two are segmented from each other by a demilitarized zone where no traffic is allowed to pass directly through the firewall, but only indirectly through servers in the DMZ. Is either of these scenarios a true air gap, in the historical meaning of the term? Probably not, but in the practical sense, many would describe it as one.

Moreover, it's also common for equipment vendors to have remote access to the OT network via a VPN as part of a service-level agreement. Even if the VPN has the highest level of encryption and the world's most advanced authentication, these are connections and potential pathways into OT nevertheless.

In short, an air gap isn't necessarily what an air gap used to be. Even if the historical 100% air gap were fully maintained, in the present day it's no longer absolute security. In an OT network, there are files that need to be introduced to maintain equipment such as configuration files, software patches, and various files from vendors such as system integrators and contractors.

A laptop plugged into the OT network might be infected. Resourceful attackers can use spearphishing to dupe staff or contractors into injecting malware into the OT network via a USB drive. In fact, a review of attack frameworks directed at [air-gapped networks](#)

found that they all use USB drives as the physical transmission medium to transfer data in and out of the targeted network.

Moreover, studies have shown that despite having plant operators and staff who are trained regularly on cybersecurity issues, [60% will insert USB drives even when they were dropped in the parking lot](#), and the number rises to 90% if the drive has an official-looking logo on it.

Attacks that Made Headlines: Threat Actors Take Aim at Manufacturers

HONDA MOTOR CO. (2020)

Honda was hit by Snake ransomware. Early reports indicated that the customer service and financial services networks were impacted; however, production operations at some U.S. manufacturing facilities were also affected.

Security researchers who examined the Snake ransomware noted that when executed, it kills processes related to industrial control systems on the OT network before encrypting files on the impacted server. Reporting at the time indicated that the company resumed operations within a few days, presumably because there were backups.

BASSETT FURNITURE (2024)

Virginia-based furniture manufacturer and retailer Bassett Furniture was targeted in a ransomware attack that disrupted the company's production lines. It reported in a filing with the SEC that as a result of its containment measures, the company was not operating its manufacturing facilities. Customers were able to place orders and purchase available merchandise, but order fulfillment was impacted. The factory shutdown lasted a week.

KEYTRONIC (2024)

Keytronic, an American contract manufacturer for technology companies, detected a ransomware incident after disruptions at its Mexico and U.S. sites impacted business applications supporting robotic operations and corporate functions.

Data was also exfiltrated during the attack, as the perpetrators leaked screenshots of employees' passports and social security cards, customer presentations and corporate documents on their dark web site. In a filing with the SEC, Keytronic reported it had incurred approximately \$2.3 million of additional expenses and believes that it lost approximately \$15 million of revenue during the fourth quarter.

KOJIMA INDUSTRIES (2022)

A manufacturer of plastic parts and electronic components for the automotive industry, Kojima Industries was attacked by threat actors who penetrated the systems of a Kojima third-party business partner, giving them the means to attack Kojima's file servers and encrypt data.

The incident left Kojima unable to ship deliveries to Toyota, and the next day Toyota announced it was suspending the operation of 28 production lines in 14 plants across Japan. Although the lines were restarted the next day, the result was a loss of production of 13,000 vehicles.

VISSER PRECISION (2020)

A precision parts manufacturer based in Denver, Colorado that supplies the automotive, aeronautics and aerospace industries, Visser Precision suffered a ransomware attack. The company was tight-lipped about specifics of the attack and any ransom demand, and a spokesperson said the business was operating normally.

Data, however, was exfiltrated. NDAs with Tesla, SpaceX and General Dynamics appeared online, along with a portion of a schematic for a missile antenna. The gang later published stolen personnel information of corporations, government officials and subcontractors.

ESET Security for Air-Gapped Networks

If you're a manufacturing organization with IT and OT networks that are separated from each other by either a 100% air gap or a hybrid air gap (network segmentation enforced by strict sets of firewall rules), then ESET has some solutions for you.

These same solutions also apply on the IT network, if you have individual computers or groups of them that are segmented or air gapped because they have extremely sensitive information related to personnel, R&D or trade secrets.



For hybrid air-gapped networks: ESET Managed Detection and Response (MDR)

ESET MDR is a 24/7 cybersecurity service that continuously monitors your environment for threats, blocks and contains them before they can execute malicious behavior, and removes and remediates them.

If you have networks that contain highly sensitive information that are separated from your main business IT networks by a hybrid air gap that allows specific traffic through the firewall by exception, the [ESET MDR](#) service can protect those networks.

In the special case of a hybrid air-gapped OT network, some ESET manufacturing customers who use our MDR service have opted to extend ESET MDR to the devices on the OT network that our service is able to support. Practically speaking, this means devices running Microsoft Windows.

This solution uses our MDR Ultimate service in conjunction with ESET Inspect, enabling the XDR capability that powers the consoles for our MDR service in an air-gapped environment. Locating ESET Inspect on the OT network bolsters its security in a number of ways:

ESET security teams are familiar with the specialized security environments of OT networks. They track the CVEs and monitor and analyze the threat reports and indicator-of-compromise lists related to OT. ESET also tracks the threat actors targeting industrial control devices, both the larger APT groups and smaller crime groups that aren't classified as APTs but are known to target manufacturing.

1. First, having MDR running on the IT network protects against the [75% of threats that reach the OT network by first gaining a foothold on the IT network](#).
2. ESET Endpoint Protection gives the MDR security analysts visibility to the inbound and outbound traffic on Windows servers, desktops and laptops on the OT network, and also monitors running processes and login attempts. If the Windows computers interface with non-Windows devices such as PLCs, this provides protection against attacks that take control of Windows devices and use them to attack industrial control systems, using tools such as the Pipedream/InController toolkit.
3. Similarly, this provides protection for segments of the IT network that serve industrial internet-of-things devices. Most of these sensors, actuators, and other devices do not have the resources to run endpoint protection, but if there are Windows devices on those networks, ESET Inspect monitors and detects malicious inbound and outbound traffic on them, including traffic that targets the IIoT devices. Also, the MDR service blocks and contains attempts to commandeer the Windows devices and use them as launch points for attacks.
4. ESET Endpoint Protection identifies and blocks known threats and suspicious/malicious behavior detected on USB drives inserted into ESET-protected devices. It can totally block devices by type, or scan them on insertion.
5. ESET Endpoint Protection and the MDR service are able to support and protect legacy Windows devices for which security patches are no longer available, because we continue to track the CVEs that impact them and detect those exploits.



For fully air-gapped networks: ESET Inspect managed by in-house security analysts

Some ESET manufacturing customers who are able to run a fully air-gapped network opt to install ESET Inspect and manage it with an in-house security team.

[ESET Inspect](#) can be installed in-cloud or on-premises, and its capabilities include incident detection, incident management and response, data collection, indicator-of-compromise detection, anomaly detection, behavior detection, policy violation detection, email notifications, reporting and more.

In-house teams have full use of the [ESET threat intelligence](#) that our own security analysts use, including updates on the latest tactics and techniques used by the attacker groups that target manufacturing.

ESET Inspect also supports individual computers with sensitive data or that control vital operations that are air-gapped at the machine level. When the ESET Inspect Agent is installed on those machines, they appear as “isolated from network” devices in the console when not connected. When they do connect, they become briefly visible and can be inventoried for management purposes.



For fully air-gapped or hybrid networks: ESET updating solutions

For devices that aren't allowed to connect to the public internet, ESET has implemented access to updates using a variety of delivery models to best fit organizational security policies.

Via USB drives. A scanner on a USB drive loaded with the current updates makes the process of detecting status and updating devices quick and easy for administrators.

Via a mirrored update server. For devices that are normally behind an air gap but sporadically allowed to connect locally, the [ESET PROTECT](#) console maintains a mirrored database of all the current updates. When an otherwise offline device becomes available in the environment, it retrieves the updates from the mirror.

Via an Apache proxy server. For a fully air-gapped network, devices can retrieve updates from an Apache proxy server located behind the air gap.

Two Tiers of MDR Service

Choose the one that's right for your organization.

MDR

The base tier of [MDR](#) is designed to be affordable for smaller manufacturers with as few as 25 seats. ESET experts immediately contain the threat, take action by blocking files and processes, and then notify you of the actions taken and any additional steps you need to take.

- Notification of incidents and actions taken
- Optimization of the ESET Inspect MDR console at the backend level
- Continuous threat hunting
- Feedback to incidents
- Weekly & monthly reports

MDR Ultimate

Larger manufacturers at the enterprise level tend to have dedicated IT security admins who want to work with our analysts through an incident. [ESET MDR Ultimate](#) works as a seamless extension of your IT function. We contain the threat and then interact with your internal security personnel on complete remediation.

- Joint response to incidents with remediation guidance
- Optimized ESET Inspect console for your environment
- Continuous and on-demand threat hunting
- 24/7 availability to analysts
- Periodical reports with human interpretation

Parting Thoughts

At its highest level, ESET MDR service builds on the work of world-class security analysts and threat researchers at 11 R&D centers around the globe and ESET's 30 years of cybersecurity experience. ESET monitors, tracks, and knows the activities of the threat actors and the telltale signs of their presence on your network.

The MDR service augments and extends their human effort with cutting-edge artificial intelligence that applies their knowledge and insight at scale to protect your manufacturing business and operations.

[LEARN MORE](#)

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.



**Multilayered,
prevention-first**



**Cutting-edge AI
meets human
expertise**



**World-renowned
threat intelligence**



**Hyperlocal,
personalized
support**



Cybersecurity
Progress. Protected.

© 1992–2025 ESET, spol. s r.o. – All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.