illumio

INDUSTRY BRIEF

Illumio: Maintaining Manufacturing Operations During a Breach

How Zero Trust Segmentation (ZTS) can deliver cyber resilience in manufacturing

Digital transformation and new cyberthreats

If manufacturers cannot build, ship, or invoice their goods, the potential losses can be catastrophic. Cyberattacks add to the list of potential threats to the manufacturing and logistics process.

Two distinct cybersecurity issues face manufacturers currently:

- How to update security for legacy equipment that relied on a Purdue model and is vulnerable to low-level lateral movement.
- How to secure the migration to Industrial IoT or Industry 4.0.

As cyberattacks become more sophisticated, traditional network-based security approaches have become insufficient to prevent the spread of an attack. The focus needs to shift to a more agile approach of protecting the individual asset. The only way to maintain services is to be able to contain an attack while remediation and restoration take place.

The manufacturing industry must take a Zero Trust approach as more functions become virtualized and concentrated onto fewer physical systems. This means building least-privilege access based on verified identity so that only verified communications are allowed on an asset-by-asset model.

By doing this, manufacturing organizations remove the capability of a cyberattack to move easily through the network, containing an attack to its point of entry.

Resilience and the cyber physical threat

"The character of cyberthreats has changed. Respondents now believe that cyberattackers are more likely to focus on business disruption and reputational damage."

– World Economic Forum's 2023 Global Cyber Security Outlook

"Manufacturing had the highest number of extortion-based attacks in 2022."

– IBM Security X-Force Threat Intelligence Report 2023

Attacks on manufacturers fall into 3 distinct groups:

- Data theft of critical customer or business information
- Generic ransomware that can be either directed or viral to attack information systems or operational technology
- A targeted cyber-physical attack on a specific system to cause maximum disruption

A large majority of these attacks will begin as phishing attacks and quickly propagate to their intended target. Reducing this movement can reduce the impact of an attack.

Challenges

There are some high-profile cybersecurity challenges that the security teams in manufacturers need to address:

- Identifying legacy and unknown IT and OT devices
- Mapping communications between applications, systems, IT and OT devices
- Containing ransomware attacks
- Mitigating the risk of known and unknown vulnerabilities

The key to surviving any attack is to reduce the impact and to make sure that it doesn't reach the most critical parts of the network.

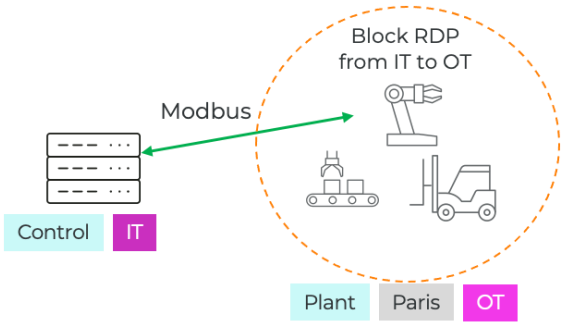
Many critical infrastructure regulators are recommending the following the steps of the NIST Cybersecurity Framework:

1. Identify

Illumio generates a simple map to show all devices and the flow of their communications to external computing resources, such as applications, servers, databases, the Internet, or even smart devices. With this knowledge, generating the required security policies is a much simpler process.

2. Protect

To prevent the cross contamination of malware from the IT to OT environments and vice versa, it's important to only allow communication between necessary devices. With Illumio, you can block specific ports that ransomware and breaches typically use.



Any patching limitations can be managed by limiting the systems that can communicate and which protocols they use.

3. Detect

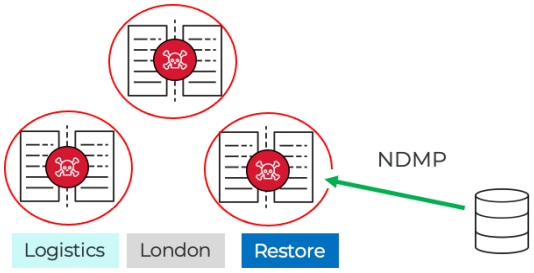
Detecting an attack is key to neutralizing the threat — and the quicker the better. Segmenting the network is shown to improve the performance of EDR systems by restricting the spread of an attack, thereby reducing the area required for detection.

4. Respond

You must respond instantly once an attack is detected. As soon as an attack starts, it needs to be stopped. With Zero Trust Segmentation (ZTS), you can effectively lock down attacks to help maintain services while the code is removed.

5. Recover

Security and IT teams can set up protection around individual departments and systems, so they can resume operations while shielded from the attack. Any attempts to reinfect can be prevented by only allowing connection with an immutable data source during the recovery phase.



Improve cyber resilience

Learn more about how Illumio helps protect critical systems.
illumio.com/products

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.