illumio

INDUSTRY GUIDE

# Zero Trust Segmentation for Manufacturing

Manufacturers are turning to Zero Trust Segmentation to maintain operations and build cyber resilience against attacks

## Manufacturing is the top-attacked industry

Manufacturers are increasingly becoming a target for cyber criminals, with ransomware attacks and breaches on the rise in the industry. And if manufacturers cannot build, ship, or invoice their goods, the potential losses can be catastrophic.

Ransomware attacks can disrupt operations and lead to significant financial losses. Data breaches, on the other hand, can result in sensitive information being stolen, causing harm to the organization and its customers.

Supply chain cyberattacks, where adversaries infiltrate the organization through third-party vendors, have emerged as a major concern due to their potential to compromise entire systems. Manufacturers should also be aware of security risks like phishing attacks, DDoS attacks, and insider threats.

As these kinds of attacks become more sophisticated and frequent, manufacturing organizations are facing immense pressure to strengthen their cybersecurity measures and protect their critical systems and data.

> “
>
> For three years in a row, manufacturing is the top-attacked industry.
>
> **IBM X-Force Threat Intelligence Index 2024**

## The impact of Industry 4.0

Manufacturers worldwide are benefitting from more automated, connected manufacturing operations. Most are at some point of transformation, whether at full automation or at just an initial step.

In fact, many organizations are probably more transformed than they think. Nearly everything is now overseen by an enterprise resource planning (ERP) system which controls everything from order management to what is being produced in each factory.

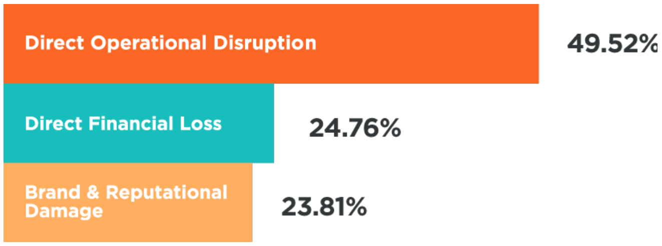
The efficiency of the system is limited by how smart the industrial control system (ICS) is. The more information it can feed the ERP, the more streamlined the supply chain and the more efficient the manufacturing process becomes. This is further enhanced by the ability to create a virtual digital twin of each machine to model exact adjustments in operations.

Modern deployments also address previous challenges of legacy systems in the ICS. New controllers can run on standard ruggedized servers implemented in a virtual- or container-based system. From a patching perspective, this means that many parts of the ICS can be treated and managed the same as IT.

## Security threats to production

The biggest challenge to any manufacturer is loss of production. In the 2024 World Economic Forum Global Cybersecurity Outlook, cyber leaders highlighted disruption as the biggest concern.

Cyberattacks like ransomware can cripple manufacturing systems, halting production lines, disrupting supply chains, and causing significant operational downtime. These disruptions can lead to delayed order fulfilment, lost production time, and significant financial losses including the costs of remediation and restoring systems.



However, other threats are always lurking:

- **Intellectual property theft:** Manufacturers invest heavily in research and development to innovate and maintain competitive advantages. Cyberattacks, such as espionage and data breaches, can lead to the theft of intellectual property (IP) such as patents, designs, formulas, and manufacturing processes. This not only results in a direct loss of competitive edge but can also have long-term impacts on market position and profitability.

> 45% of leaders say that operational disruption is their greatest concern with regard to suffering a cyber incident.
>
> **2024 World Economic Forum Global Cybersecurity Outlook**

- **Damage to physical assets:** Attacks on industrial control systems (ICS) and operational technology (OT) can lead to physical damage to machinery and equipment. Attackers can manipulate control systems to operate machinery in unsafe conditions, leading to equipment failure, destruction of goods, and potentially endangering human lives. Such incidents not only require costly repairs but can also lead to extended downtime and safety investigations.

- **Data breach and loss of confidential information:** Manufacturers often hold sensitive data, including customer information, vendor details, and employee records. Cyberattacks targeting this data can lead to breaches, resulting in legal liabilities, fines, and a loss of trust among customers and partners. The cost of a data breach extends beyond immediate financial implications, impacting brand reputation and customer relationships in the long term.

- **Compliance violations and legal ramifications:** Manufacturers operating in regulated industries may face additional consequences from cyberattacks in the form of compliance violations. Regulations like GDPR, HIPAA, and others require stringent data protection measures. Failure to protect data due to a cyberattack can result in heavy fines, legal actions, and increased scrutiny from regulatory bodies.

- **Supply chain compromise:** Attackers increasingly target manufacturers as a way to access broader supply chains. Compromising a single manufacturer can provide attackers with a backdoor into the systems of connected suppliers, partners, and customers. This not only amplifies the impact of the initial breach but can also strain business relationships and lead to loss of business.

## Smarter, more complex systems are more vulnerable

There has been a significant shift in the types of attacks seen in ICS environments. Traditionally, they were limited to basic malware and known vulnerabilities, but with the introduction of smarter systems, attackers have now found ways to exploit the complex interconnections and communication protocols used in these systems. This has led to a rise in sophisticated attacks such as zero-day exploits and targeted attacks, as well as an increase in the use of social engineering tactics to gain access to critical systems.

The interconnectedness of these systems with the Internet has made them vulnerable to a wider range of cyber threats. Threat actors can now find and exploit existing weaknesses quicker and more easily evade detection systems.

As a result, it's easier to execute attack scenarios like:

- Unauthorized command message
- Modification of process or controller parameters
- Compromise HMI
- Data Historian Compromise
- Unauthorized device detection
- Unauthorized connection

While the Purdue Model is still valid as a concept, the way it's implemented needs to be updated. Traditionally, each layer would be built as a demilitarized zone (DMZ), with a firewall or digital diode separating the layers. This makes each layer effectively a trusted network — and means that there's nothing stopping successful attacks that have entered the trusted network.

The network can be used to further segment each layer, but this just adds layers of complexity and the potential for errors to cause outages in the system. The high levels of OT systems' availability may not be able to support many security functions and protocols.

For example, installing high-power endpoint detection and response (EDR) software on an OT system could take too many resources and generate too much traffic which could interfere with its basic function. A better option could be to use network detection and response (NDR) which would place no load on the system itself.

Industry 4.0 is making systems so interconnected that the traditional trust-based model no longer applies. Manufacturers must move to a Zero Trust security model to protect modern industrial control systems.

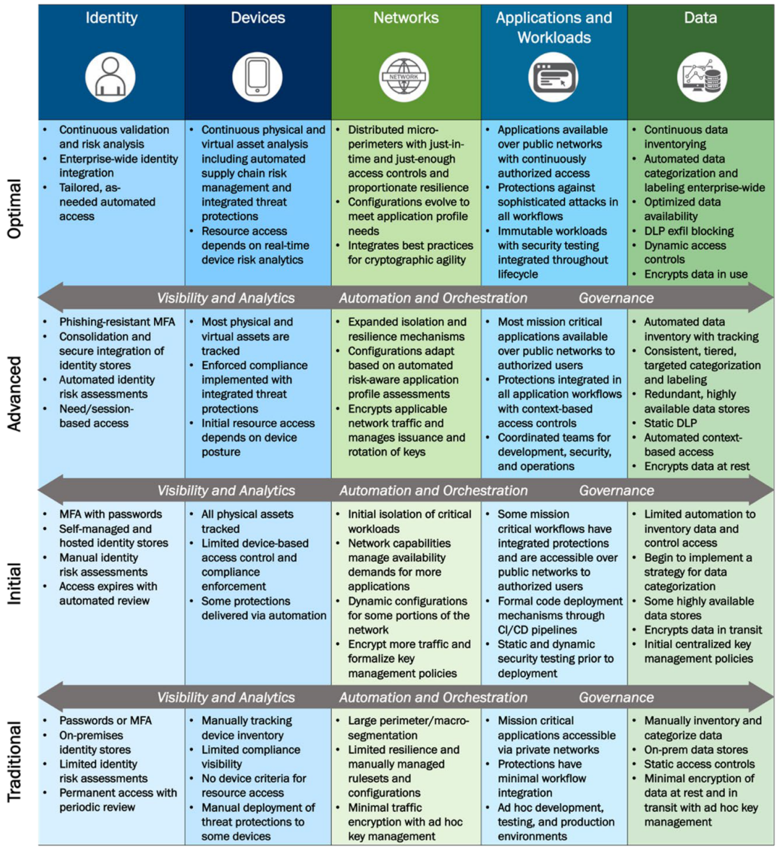
# A Zero Trust approach to manufacturing security

NIST defines Zero Trust as “an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources.”

Many regulatory organizations around the world define a series of principles that include:

- Know your architecture
- Use policies to authorize requests
- Authenticate and authorize every connection
- Don’t trust any network including your own
- All communication is secured regardless of location
- Access to individual enterprise resources is granted on a per-session basis
- No resource is inherently trusted

CISA have defined a Zero Trust Maturity Model (ZTMM) which will not only allow you to identify which stage you have reached but also have a roadmap for your Zero Trust journey.



| | Identity | Devices | Networks | Applications and Workloads | Data |
|---|---|---|---|---|---|
| Optimal | • Continuous validation and risk analysis<br>• Enterprise-wide identity integration<br>• Tailored, as-needed automated access | • Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections<br>• Resource access depends on real-time device risk analytics | • Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience<br>• Configurations evolve to meet application profile needs<br>• Integrates best practices for cryptographic agility | • Applications available over public networks with continuously authorized access<br>• Protections against sophisticated attacks in all workflows<br>• Immutable workloads with security testing integrated throughout lifecycle | • Continuous data inventorying<br>• Automated data categorization and labeling enterprise-wide<br>• Optimized data availability<br>• DLP exfil blocking<br>• Dynamic access controls<br>• Encrypts data in use |
| | Visibility and Analytics | | Automation and Orchestration | | Governance |
| Advanced | • Phishing-resistant MFA<br>• Consolidation and secure integration of identity stores<br>• Automated identity risk assessments<br>• Need/session-based access | • Most physical and virtual assets are tracked<br>• Enforced compliance implemented with integrated threat protections<br>• Initial resource access depends on device posture | • Expanded isolation and resilience mechanisms<br>• Configurations adapt based on automated risk-aware application profile assessments<br>• Encrypts applicable network traffic and manages issuance and rotation of keys | • Most mission critical applications available over public networks to authorized users<br>• Protections integrated in all application workflows with context-based access controls<br>• Coordinated teams for development, security, and operations | • Automated data inventory with tracking<br>• Consistent, tiered, targeted categorization and labeling<br>• Redundant, highly available data stores<br>• Static DLP<br>• Automated context-based access<br>• Encrypts data at rest |
| | Visibility and Analytics | | Automation and Orchestration | | Governance |
| Initial | • MFA with passwords<br>• Self-managed and hosted identity stores<br>• Manual identity risk assessments<br>• Access expires with automated review | • All physical assets tracked<br>• Limited device-based access control and compliance enforcement<br>• Some protections delivered via automation | • Initial isolation of critical workloads<br>• Network capabilities manage availability demands for more applications<br>• Dynamic configurations for some portions of the network<br>• Encrypt more traffic and formalize key management policies | • Some mission critical workflows have integrated protections and are accessible over public networks to authorized users<br>• Formal code deployment mechanisms through CI/CD pipelines<br>• Static and dynamic security testing prior to deployment | • Limited automation to inventory data and control access<br>• Begin to implement a strategy for data categorization<br>• Some highly available data stores<br>• Encrypts data in transit<br>• Initial centralized key management policies |
| | Visibility and Analytics | | Automation and Orchestration | | Governance |
| Traditional | • Passwords or MFA<br>• On-premises identity stores<br>• Limited identity risk assessments<br>• Permanent access with periodic review | • Manually tracking device inventory<br>• Limited compliance visibility<br>• No device criteria for resource access<br>• Manual deployment of threat protections to some devices | • Large perimeter/macro-segmentation<br>• Limited resilience and manually managed rulesets and configurations<br>• Minimal traffic encryption with ad hoc key management | • Mission critical applications accessible via private networks<br>• Protections have minimal workflow integration<br>• Ad hoc development, testing, and production environments | • Manually inventory and categorize data<br>• On-prem data stores<br>• Static access controls<br>• Minimal encryption of data at rest and in transit with ad hoc key management |

*Figure 4: High-Level Zero Trust Maturity Model Overview*

## How Illumio benefits manufacturers

**1. Enhanced security through microsegmentation:** Illumio provides microsegmentation, also called Zero Trust Segmentation, capabilities that break down the network into smaller, manageable segments. By applying fine-grained access controls to these segments, Illumio can limit the movement of potential threats within the network. This approach is particularly effective in protecting sensitive areas of the manufacturing process and ensuring that an attacker cannot easily move laterally across the network, thereby protecting intellectual property and sensitive data.

**2. Protection of industrial control systems (ICS) and operational technology (OT):** Manufacturers rely heavily on ICS and OT for their production processes, but these systems are often vulnerable to cyberattacks due to their specialized nature and the difficulty of applying traditional security measures. Illumio helps secure these critical systems by allowing manufacturers to segment their networks and control which devices can communicate with each other, reducing the risk of disruptions caused by cyberattacks.

**3. Compliance with regulatory standards:** Manufacturers are subject to various regulatory requirements that mandate strict cybersecurity measures to protect sensitive data and ensure the integrity of their production processes. Illumio helps manufacturers meet these compliance requirements by providing detailed visibility into network traffic and enforcing security policies that protect sensitive data, thereby aiding in compliance with standards such as GDPR, NIST, and others.

**4. Visibility and control over network traffic:** Illumio offers a real-time, interactive map of network flows, giving manufacturers detailed visibility into the traffic within their networks. This visibility allows for better control and understanding of how applications and systems are communicating, facilitating the identification and isolation of potentially malicious activity. Such insights are crucial for proactive threat detection and response.

**5. Reduced attack surface:** By enforcing strict access controls and segmenting the network, Illumio significantly reduces the attack surface available to attackers. This minimizes the chances of a successful breach and helps protect against both external attacks and insider threats, thereby safeguarding critical manufacturing processes and data.

> “Regardless of which industry you’re in, technology is essential to business growth. And to grow quickly and responsibly, leadership must be able to trust that the organization’s technology and data is secure. Illumio makes not only our technology team, but also our entire business confident that our operations are secure and resilient to inevitable cyberattacks now and as we scale.”
>
> **Jamie Rossato**
> **Chief Information Security Officer**
> **Lion**

**6. Operational resilience:** In the event of a breach, Illumio can contain it to a small segment of the network, preventing it from spreading and causing widespread disruption to manufacturing operations. This containment capability is critical for ensuring operational resilience and maintaining production uptime, which is vital for meeting customer demands and protecting the manufacturer's bottom line.

**7. Scalability and flexibility:** As manufacturers grow and evolve, their network architectures and security needs change. Illumio's platform is designed to be scalable and flexible, accommodating new devices, technologies, and production processes without compromising security. This ensures that manufacturers can adapt to new challenges and opportunities without exposing themselves to additional cyber risks.

## Aligning with the NIST Cybersecurity Framework

Many directives have been created to address cybersecurity risks and build cyber resilience. The common factor is that in some way they are all based on the NIST Cybersecurity Framework (NIST CSF).

Like most directives, the NIST CSF and the associated Guide to Operational Technology Security (NIST SP 800-82r3) recommendations are comprehensive and contain a full list of actions to improve the security of organizations.

However, there are some simple steps from the framework that can be taken to improve cyber resilience while a full implementation takes place. These can easily be aligned with the five steps of the NIST CSF.

Illumio provides the technology to use this model to build resilience in the manufacturing system.

## How Illumio maps to the NIST CSF

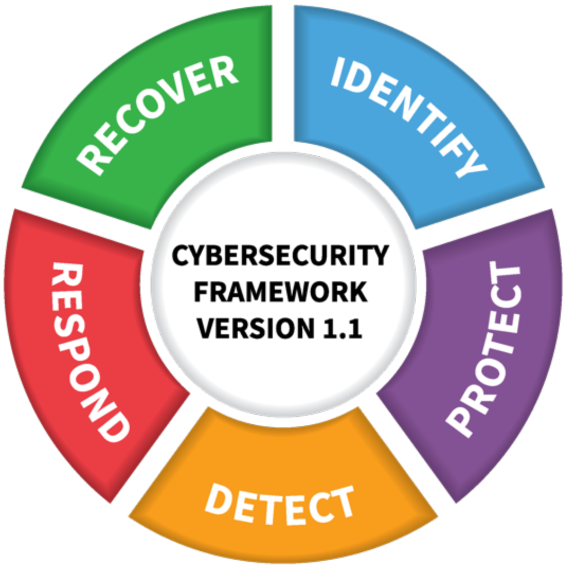
### 1. Identify

The first step is a simple audit to identify which systems will have the biggest impact on maintaining services. In other words, what are the minimum resources required to keep the production flowing? Most national cybersecurity directives include the requirement to map the interdependencies of all systems.

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.

The detail on this map is provided by metadata from IT devices, information gathered from operational technology (OT) and Internet of Things (IoT) security platforms like Armis. It can also be enriched with data from a configuration management database (CMDB) like ServiceNow.

With this knowledge, generating the required security policies is a much simpler process.



### 2. Protect

Once you have built a plan around what to protect, you need to enforce that protection. The simple first step is to deploy Zero Trust Segmentation.

To prevent the cross contamination of malware from the IT to OT environments and vice versa, it is important to only allow communication between the necessary devices using the minimum of verified protocols. This is the principle of least privilege and should be applied across all communication.

With least-privilege security controls consistently deployed across a hybrid network, organizations can stop a cyberattack at its first point of entry — preventing any further movement across the network.

With Zero Trust Segmentation, you can block specific traffic routes and ports that attackers typically use. Or you can block all traffic on a given pathway while allowing only traffic from specific sources.

Many OT systems in manufacturing run on older versions of software and operating systems which oftentimes can't be patched to the latest version. This requires some mitigation to protect those vulnerable devices.

Zero Trust Segmentation helps manage patching limitations while reducing the systems that can communicate and protocols they use. This helps ensure that an organization can continue to deliver services even while undergoing a breach.

### 3. Detect

Detecting an attack is key to neutralizing the threat — and the quicker the better.

Detection covers several technologies. Tools like extended endpoint detection and response (EDR/XDR) and next-gen anti-virus (NGAV) monitor your computing systems looking for indicators of compromise (IoCs).

IoCs raise the suspicion that a piece of code could be malware. Other security tools like network detection and response (NDR) and user and entity behavior analytics (UEBA) monitor for activities on the network that fall outside of normal baselines.

The final part of the puzzle is detecting any connections that should not be allowed, such as the machine communicating with the Internet. Bishop Fox research shows that Illumio Zero Trust Segmentation stops the spread of breaches four times faster than EDR alone by restricting the spread of an attack and reducing the area required for detection.

### 4. Respond

Once an attack is detected, you must respond instantly. As soon as an attack starts, it needs to be stopped.

With Zero Trust Segmentation, you can effectively lock down breaches to help maintain services while the code is removed from your computing systems.

Illumio can be built as a manual response or automated within various incident response security systems, including security orchestration, automation, and response (SOAR) and security operation center (SOC) tools.

Your response process and configurations should be planned and tested for efficacy because any attack could be devastating with unknown consequences. Establishing a cyber resilience plan and practicing the response can make the difference between being able to maintain services and risking continuity of delivery.

As systems are determined to be safe, they can be added to a "clean" segment so that they cannot be reinfected.

**5. Restore**

The last action is to restore services. If the attack is still underway, any premature repair work could create new risks.

With Zero Trust Segmentation, security and IT teams can set up protection around individual departments and systems, so they can resume operations shielded from the attack. Individual systems can be labelled based on their status whether they are “Infected” or “Clean.” These labels rules can be applied to either keep them quarantined or give appropriate access back into the wider system.

And with knowledge gained during the unsuccessful attack, you can tune your policies to further tighten access and boost your organization's cyber resilience.

## Learn more about Illumio for manufacturing

The Illumio Zero Trust Segmentation Platform provides visibility into both your IT and ICS environment, allowing you to determine the risk posed by unauthorized connections and apply the required policies to protect all areas and maintain production in the event of an attack.

To learn more about how Illumio can strengthen the security and resilience of your operations:

- Explore the Illumio platform
- Schedule a demo and consultation with one of our security experts
- Test drive Illumio by registering for one of our hands-on virtual labs

## About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches 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.