SOLUTION BRIEF

From Zoning to Zero Trust

Securing Manufacturing Networks

FORESCOUT

From Zoning to Zero Trust
Securing Manufacturing Networks

Welcome to the future of manufacturing, where data is the new fuel, automation is the engine, and hyper-connected systems power factories that fine-tune production in real time. From robotic assembly lines to smart sensors and digital twins, modern operations are evolving into a smart but complex industrial ecosystem.

But there's a catch. The same systems that drive efficiency and innovation also introduce new types of risk.

In manufacturing, where patching OT devices is often impractical or impossible, segmentation isn't just an option, it's a necessity. Isolating insecure-by-design assets limits exposure, reduces risk, and creates a safer path to monitoring and detecting threats without affecting production.

The convergence of IT and OT, the proliferation of new devices, remote access, cloud-connected services, and extended supply chains create a level of complexity that most organizations are not prepared to handle. To keep this complexity under control and ensure operational resilience, manufacturers need a new kind of security foundation. One that doesn't just defend the perimeter but actively controls who and what can move within the network. This is where visibility, network access control, and segmentation come together as a layered defense strategy: **It needs to be designed to contain threats, reduce exposure, and secure every connection, device, and user — across every asset type and Purdue level**.

Why We Need Robust Network Security

All it takes is one malicious file or a misconfigured device to bring production to a halt, expose critical data, and undermine the entire operation. The reality? Most industrial environments aren't built to contain modern threats.

- **Perimeter defense is no longer enough:** Industrial Control Systems require secure internal communication between devices and subsystems to keep processes running.
- **Remote access is expanding:** Engineers, SCADA vendors, and system integrators routinely connect on-site or remotely, increasing risk and exposure.
- **Legacy systems are a serious risk:** Many OT assets are running outdated, un-patchable software or firmware — and are often networked with IoT devices with direct internet connectivity.
- **Flat networks expose everything:** Once inside, attackers can move freely between systems with little to stop them moving freely across systems.
- **Physical access bypasses cyber controls:** Unsecured ports, devices, and insider actions can compromise even well protected networks.

Challenges in Securing ICS Networks

In manufacturing environments, Zero Trust starts with access control and segmentation. These are essential for isolating assets, enforcing least privilege, and limiting lateral movement. However, putting these principles into practices presents significant challenges.

- **Lack of authentication methods:** Many field devices and controllers lack basic authentication features, making it hard to verify or limit access to critical systems.
- **Complex interdependencies:** ICS components span multiple zones and locations and have interdependencies hard to understand, leaving teams hesitant to enforce restrictions.
- **IT tools don't fit industrial security needs:** Traditional routers and firewalls can't understand or block unsafe industrial traffic like abnormal process values or dangerous commands.
- **Inconsistent environments:** Multi-vendor systems with proprietary protocols and different security requirements make it difficult to enforce unified policies across locations, roles, and devices.
- **Limited visibility into ICS traffic:** Many organizations lack real-time insight into industrial communications, resulting in delayed detection and extended triage times.

The Forescout Solution:
Built for Industrial Security

If these challenges sound familiar, it's time to take a closer look at the Forescout 4D Platform™, purpose-built to secure complex industrial environments. We leverage our NAC and enterprise policy management capabilities to enable Zero Trust. The Platform leverages your existing IT and security ecosystem, giving you the visibility, segmentation, and automation you need to stay secure and in control.

Advanced Asset and Traffic Visibility Forescout continuously discovers and classifies every connected device and maps communication flows across OT and IT networks. The Platform gives you the clarity and confidence to identify risks and take action without disrupting operations.

Integration with Existing Tools Forescout leverages your current security stack and orchestrates response actions across your existing IT and security systems, helping you maximize value from past investments, extending the protection without adding complexity.

Threat Detection and Correlation Forescout correlates threat intelligence from multiple data sources across IT and OT to improve detection accuracy, reduce false positives, and accelerate investigations with clear, actionable insights.

> "Organizations need to implement comprehensive information security and resiliency practices for Zero Trust to be effective. When balanced with existing cybersecurity policies and guidance, identity and access management, continuous monitoring, and best practices, a Zero Trust Architecture can protect against common threats and improve an organization's security posture by using a managed risk approach."
>
> **—from NIST Special Publication 800-207 "Zero Trust Architecture"**

Enterprise Policy Management The Forescout 4D Platform enables you to design, validate, and enforce security policies from a single point and apply them across multi-vendor environments to streamline compliance and maintain a consistent security posture.

Threat Containment and Access Control Our Platform helps you identify and stop insecure or unauthorized activity by detecting, isolating, or blocking risky network traffic, unapproved access attempts, and non-compliant devices before they can impact operations.

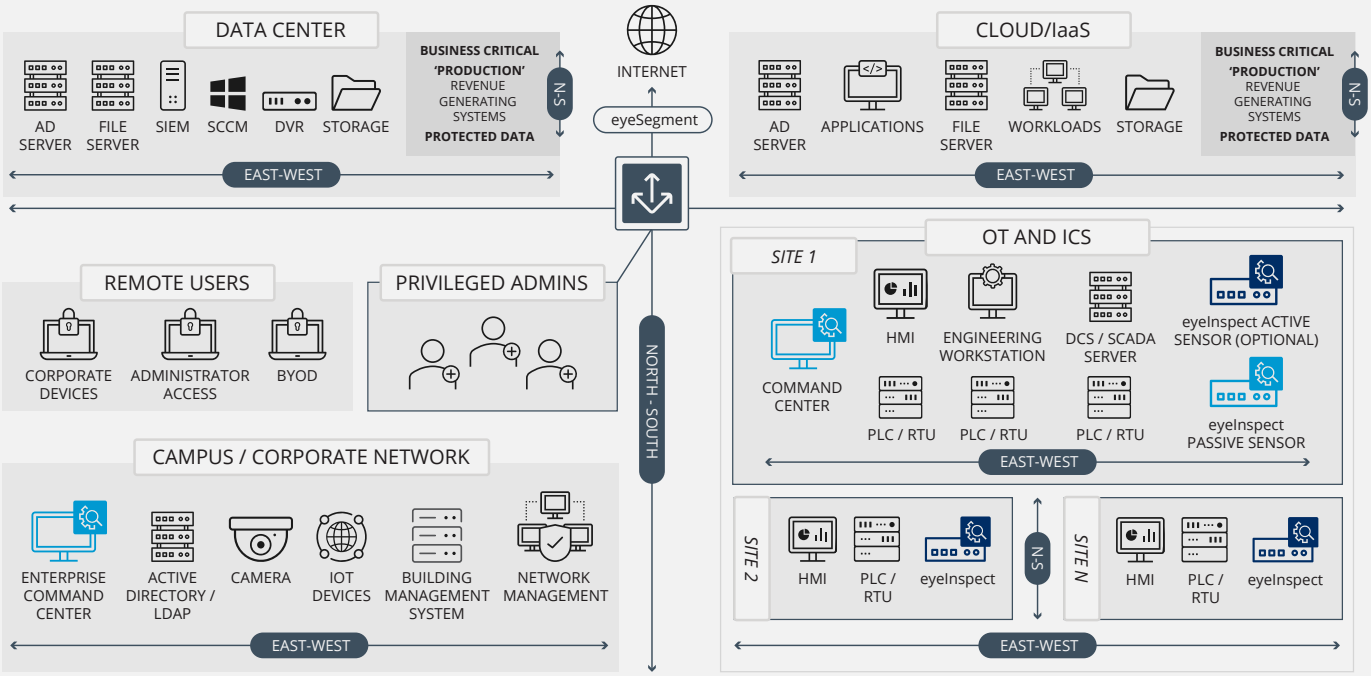
Automated Remediation Forescout enables you to orchestrate and automate response actions across your existing security ecosystem, accelerating threat containment, reducing manual workload, and minimizing the impact of incidents on operations.

Building Secure Zones Without Breaking Operations

The Forescout 4D Platform enables agentless, real-time mapping of traffic flows by user, device, function, location, and risk level — making it easy to design, model, and deploy Zero Trust segmentation without re-architecting your network. With patented anomaly detection, deep packet inspection, and a rich library of ICS threat indicators, the platform continuously monitors communications, baselines asset behavior, and automates policy enforcement to isolate vulnerabilities and contain threats without disrupting operations.

Forescout gives you the tools to move from flat networks to Zero Trust without starting from scratch or ripping out what you've already built. Whether you're designing segmentation for the first time or refining an existing access control strategy, the Platform simplifies the entire process. You can create user, device, and asset profiles in minutes, apply them to existing policy templates, and simulate enforcement before a single rule is pushed live. This means no blind changes, no trial-and-error disruptions, and no guesswork.

With Forescout, you don't need to standardize or rebuild to get started. Our Platform works with over 100 makers of switches, firewalls, and network systems, to let you manage and enforce policies from a single interface across different vendors. Zero Trust in manufacturing doesn't require a rip-and-replace, it starts with better visibility and faster control, using the infrastructure you already have in place.



Forescout's dynamic segmentation solution supports a broad range of OT and IoT use cases. The platform's adaptability helps reduce the risk of operational impact while lowering the cost and complexity of segmentation efforts. Key use cases include:

- Continuously monitoring and validating the security posture vendors or contractors, whether on-site or remote, and restricting access to only the necessary network zones.
- Separating IT, IoT, and OT environments, and isolating un-patchable or high-risk assets to limit exposure.
- Simulating segmentation policy changes and visualizing traffic impacts in advance, so you can refine enforcement strategies without interrupting production.

Why Choose Forescout

The Forescout 4D Platform™ provides complete asset intelligence and control across IT, OT, IoT, and IoMT environments. For more than 20 years, Fortune 100 organizations, government agencies, and large enterprises have trusted Forescout as their foundation to manage cyber risk, ensure compliance, and mitigate threats with seamless context sharing and orchestration across more than 180 fully featured security and IT product integrations. With Forescout, every cybersecurity investment is more effective.

Learn more at **forescout.com**

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com