SOLUTION BRIEF

Manufacturing

Cybersecurity and Risk Management for Digital Transformation

FORESCOUT

Manufacturing

Cybersecurity and Risk Management for Digital Transformation

Industrial operations are more connected and reliant on digital systems and extended supply chains than ever before. The business priority is keeping production up 365/24/7. But all this integrated automation technology operates with some amount of cybersecurity risk. Many of the systems and devices used on the plant floor were not designed with security in mind — and cybercriminals are aware of your vulnerabilities.

Today's attack surface is evolving faster than most organizations can keep up. Gaps in visibility, siloed tools, and slow response times are no longer acceptable. Every minute of downtime comes at a cost. The responsibility for preventing cyber incidents, such as a ransomware attack, now extends beyond security teams to senior executives and board members.

To stay ahead, manufacturing organizations must shift from reactive defense to proactive control. That requires the ability to uncover every asset and system across the industrial environment, assess risk in real time, and execute a coordinated response at scale.

Two of the most difficult challenges in securing manufacturing environments today are:

Incomplete Visibility Across Assets, Connectivity, and Risk

Most manufacturers operate with partial visibility into their environments. IT, OT, and IoT assets are often discovered and monitored using disconnected tools, making it difficult to:

- Understand how devices communicate
- Know where vulnerabilities exist
- Determine the risks these interconnections pose

Without a complete picture, it's nearly impossible to assess exposure or enforce consistent security policies across the enterprise.

Fragmented Detection and Response Across Technologies and Sites

Threat detection and response are typically spread across multiple tools and vendors, each with limited reach into the full environment. Security teams struggle to correlate threats across diverse technologies, device types, and locations — and often lack the ability to act quickly across systems. This fragmentation delays containment, complicates remediation, and puts uptime at constant risk.

How much is 'visibility' really worth if you can't act on it? If your security stack only shows you what's wrong, but can't help you to fix it, you're not managing risk, you're documenting failure. That's the trap most OT security tools fall into: A pretty dashboard, a pile of alerts, and zero context or control. Forescout breaks that cycle.

The Forescout 4D Platform™ isn't just another passive OT monitoring tool with nice traffic maps and zero bite. It's a unified, enterprise-grade security platform built to do one thing: protect industrial operations, at scale, in real time, and without gaps. It's what other point solutions wish they could be.

With patented deep packet inspection, anomaly detection, and the industry's largest ICS threat intelligence library, Forescout is a remediation powerhouse. Our platform helps you understand risk, prioritizes your mitigation efforts, and executes the response. Assets are mapped, flows are analyzed, risks are scored based on cyber impact and operational relevance. Actions are automated and orchestrated across your existing tools — from isolating compromised engineering workstations to enforcing segmentation policies. While others give you a snapshot of what's happening in your OT environment, Forescout delivers dynamic, real-time intelligence across your entire industrial footprint. We're not limited to OT or reliant on third-party visibility for IT: We see it all – IT, OT, IoT – and make it work together.

Our platform automates security workflows across disparate products by sharing rich device, user, and network context with your broader IT and security stack. Pre-built integrations allow you to bridge the gap between tools, enforce policies in real time, and accelerate response. The result? Better visibility, faster response, and stronger compliance, all without replacing what you already have in place.

From Visibility to Industrial Resilience:
What the Forescout 4D Platform™ Delivers

Forescout goes beyond visibility and network monitoring. It's the only OT security platform that unifies asset intelligence, network security, risk management, and automated response across IT, OT, and IoT systems. Whether you're starting with asset inventory or scaling to enterprise-wide risk exposure management and incident response, Forescout delivers the depth, context, and control needed to secure complex industrial operations without ripping and replacing your existing infrastructure.

Asset Intelligence & Change Management

Continuously discover and monitor every device type across all Purdue levels with 30+ discovery methods and support for over 350 industrial protocols. Choose between passive, active, agent-based, agentless, and API-driven. Automatically detect any asset on the network, including non-responsive devices, and track asset lifecycle events, such as changes in risk posture, behavior, and compliance. Advanced device profiling captures hundreds of asset properties, not just vendor, model, OS, or IP — but also the exact physical location (down to the switch port), compliance posture, and risk history. This level of context improves operational awareness and decision-making. Interactive dashboards and persona-based views help security teams focus on what matters, improving visibility across departments and streamlining daily tasks.

Access Control & Authentication

Continuously enforce access policies across all users, devices, and sessions using risk, role, and context-based controls. Authenticate and authorize identities before granting access to OT, IoT, and IT systems, leveraging integrations with IAM, MFA, and directory services. Prevent the use of default credentials, insecure authentication methods, and unmanaged service accounts. Detect and block suspicious behavior, policy violations, and over-privileged access in real time. With Forescout you can enforce least-privilege access using existing switches, firewalls, and network infrastructure, simulate and test your policies before to apply them, without disrupting operations.

Network Segmentation & Communication Monitoring

With the Forescout 4D Platform™, you can continuously monitor traffic across all Purdue levels to baseline communications, detect anomalies, and enforce segmentation policies aligned to IEC 62443-3-3 or Zero Trust principles. We automatically map asset by device type, communications, and role to define logical zones and control east-west traffic. Forescout gives you the ability to enforce segmentation across your existing switch and firewall infrastructure. Users can visualize traffic flows and understand interdependencies and simulate policy impact before deploying them. It allows you to block unauthorized communications in real time to contain threats and maintain operational continuity. With Forescout, you can detect the use of insecure protocols, weak encryption algorithms, poor password practices, failed authentication attempts, and privileged escalation, before they lead to compromise.

Vulnerability & Risk Exposure Management

Stay ahead of cyber and operational risk with enterprise-wide visibility into device configuration, behavior, risk exposure, and compliance. With the Forescout 4D Platform™ you can prioritize remediation based on business impact, targeting the systems most exposed, most exploitable, or most critical to operations. We enable security teams to handle the slow and complex patch management in industrial environments with advanced features suppress false positives, manage exceptions, or virtually patch with direct case management, either within the platform or through the service management tools already in place. Using industry-standard metrics, such as CVSS, EPSS, and KEVs from CISA, and Forescout Vedere Labs, security teams can identify the most impactful threats and respond with precision. The platform brings IT and OT risk into a single, clear view that no other solutions can offer. Backed by practical KPIs and detailed metrics, we help teams understand, communicate, and reduce risk effectively.

Threat Detection & Response

Monitor network traffic flows and system behavior in real time to identify cyber and operational threats before they impact production. The Forescout 4D Platform™ correlates multiple data sources across IT and OT environments, aligning detected events with the MITRE ATT&CK framework for a deeper and more accurate threat analysis. This helps teams to respond faster, triage events more effectively, and make better decisions — even when resources are stretched. With deep packet inspection (DPI), anomaly detection, and our Industrial Threat Library (ITL) backed by Vedere Labs intelligence, security teams can uncover sophisticated attack patterns. From malware infections and IOCs to unauthorized PLC changes and suspicious outbound traffic, Forescout exposes threats that others miss. With a dedicated analyst interface, enhanced by Gen AI and operational playbooks, Forescout streamlines investigations to support faster, more confident responses.

Compliance & Policy Management

Forescout helps organizations stay ahead of compliance issues by identifying policy violations before they impact operations. Whether a misconfigured device, unauthorized access, or an outdated control, early detection ensures teams can act before risks escalate. With a flexible policy engine at its core, the platform makes it easy to align enforcement with internal policies and industry standards, such as IEC 62443 and NIST CSF 2.0. Security teams can build policies from a library of ready-to-use templates or create their own, with the option to test and validate them before deployment, giving security and operations teams the confidence to enforce policies without risking downtime or interfering with critical processes. With Forescout you can apply policies consistently across all device types and vendors, using the infrastructure already in place, so policies can be enforced consistently, at scale, without rearchitecting your environment or adding operational overhead.

Security That Adapts to Your Needs

Cloud, On-Prem, Hybrid, or Air-Gapped

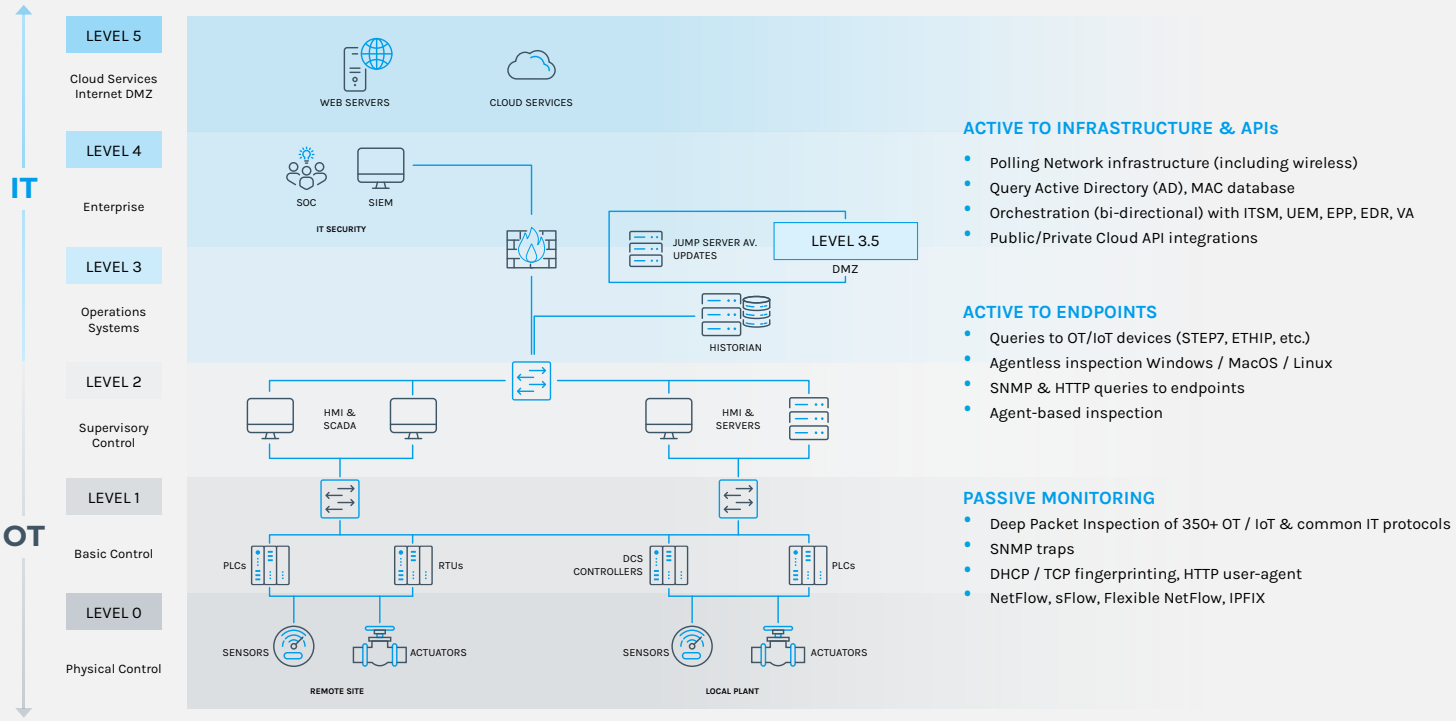
Every industrial environment has its own constraints and realities. What works in one facility might cause issues in another. Installing new switches, accessing external services, or configuring SPAN ports isn't always an option. That's why deployment flexibility is a critical capability. Forescout supports different deployment options across cloud, on-prem, hybrid, and air-gapped sites — while overcoming SPAN and passive monitoring limitations. The Forescout 4D Platform™ delivers full visibility and control without disrupting operations or requiring major infrastructure changes.

- **Cloud, On-Prem, and Hybrid:** Forescout supports different deployments options, whether you're operating fully on-prem, expanding into the cloud, or managing a mix of both. We seamless adapt to industry requirements, operational, and compliance needs.
- **Direct Infrastructure Integration:** Deploy Forescout sensors directly onto existing network equipment, routers, switches, or packet brokers solutions, without the need for major network changes or downtime. For environments where SPAN ports is not an option, we provide the flexibility to use selective active queries and API-based discovery to offer a practical alternative, delivering full visibility without disruption.
- **Form Factors That Match Your Infrastructure Needs:** Forescout supports a wide range of deployment options to seamless adapts to your environment. Choose from physical appliances, virtual machines, or container-based deployments, all designed to integrate with your existing infrastructure and minimize disruption.
- **Scalable, Multi-Tier Management:** Forescout supports a flexible management approach that fits your needs and operations. Sensors can be administered locally, managed centrally through the Command Center, or integrated into a broader enterprise view spanning multiple local Command Centers.
- **Fly Away Kit for Air-Gapped Sites:** Self-contained and portable, built for disconnected or sensitive environments, delivering full asset visibility and threat detection, even in segregated, remote, or mission-critical locations.

Forescout OT Deployment Model

This diagram shows a typical deployment architecture of the Forescout solution for industrial plants and manufacturing deployments. Various sensor deployment options are available, ranging from high performance appliances for centralized deployments to ruggedized and lighter low-cost models as well as deployment on existing network infrastructure equipment for use in decentralized or segmented networks with limited throughput.

FROM CLOUD TO DIRECT INFRASTRUCTURE INTEGRATION WITH FORESCOUT 4D PLATFORM™



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