Manufacturing

Cybersecurity and risk management for digital transformation

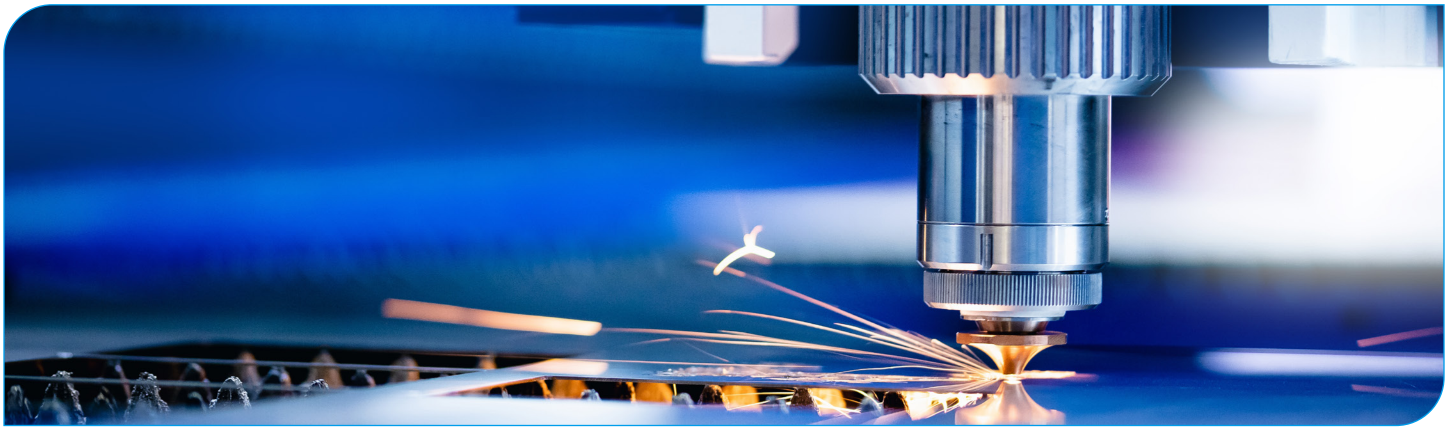
> “Forescout is invaluable for identifying, consolidating and segmenting assets as we continue to grow by acquisition.”
>
> — *CISO, Fortune 500 Manufacturing Company*

Today, manufacturers rely on flexible, built-to-order production methodologies that improve efficiency, reduce errors and cut costs – but also introduce greater cyber risk through the convergence of OT, IT and IoT networks. Unwanted communication links often go unchecked and vulnerabilities hide in plain sight based on the assumption that OT and IT are separated when they are not. Ransomware attacks make headlines, but day-to-day network or process misconfigurations, operational errors, resource usage spikes and other anomalies are far more likely to threaten productivity than outside attacks.

Managing exponential OT/IoT asset growth amid a shortage of specialized cybersecurity talent presents many challenges for OT asset owners and security teams. Two of the most difficult are:

- Visibility into assets, their connectivity within and beyond the OT networks and what cybersecurity and operational risk this creates
- Ability to detect any threat to operational continuity and prioritize response across geographically dispersed plants to reduce downtime

With industrial environments increasingly dependent on digital systems for production, automated cybersecurity is essential. Organizations need a continuous, automated approach to asset discovery, assessment and governance to ensure proactive risk management and security compliance – so you can detect cyber threats before they lead to operational or security incidents.



Forescout excels in ICS asset visibility

Forescout has “the broadest ICS protocol support of the vendors evaluated” according to the Forrester Wave™: Industrial Control Systems (ICS) Security Solutions, Q4 2021. This extensive protocol knowledge, coupled with ICS-specific threat intelligence and 12+ years of experience deploying our OT solutions to various manufacturing verticals, enables industrial organizations around the globe to secure their digital transformation and lay the foundation for a zero trust architecture across their entire digital terrain, including critical OT and IoT devices and networks.

Forescout Continuum Platform for Manufacturers

Forescout Continuum provides the continuous, automated asset management, risk compliance and remediation, non-intrusive OT/ ICS network monitoring, network access control, segmentation and security orchestration you need to protect your digital terrain from a wide range of threats. The platform combines patented deep packet inspection (DPI) and anomaly detection technology specifically designed for OT/ICS and IoT environments with a library of thousands of ICS-specific threat checks and indicators of compromise (IOCs) for advanced cyberattacks, network misconfigurations and operational errors so you can detect both known and unknown threats.

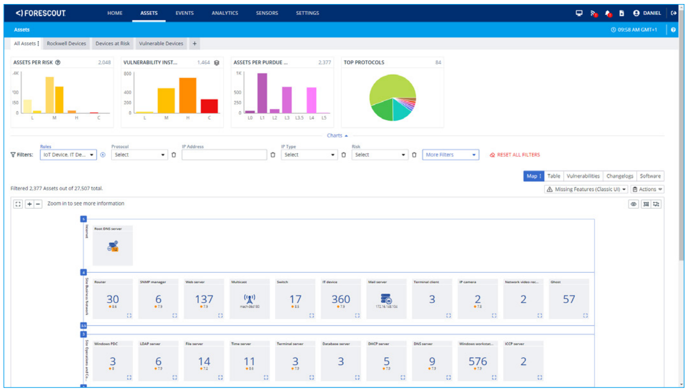
Real-time network maps, visualizations and in-depth traffic analysis offer complete visibility into asset configurations, communication behavior and the changing threat landscape, so any cybersecurity and operational risks are known and any threat to operational continuity is detected, prioritized and remediated. The cybersecurity platform enables manufacturers to act on identified risks and automate responses actions, from modest to stringent, to protect vulnerable, high-risk and compromised devices while keeping mission critical assets online.

Achieve real-time network visibility

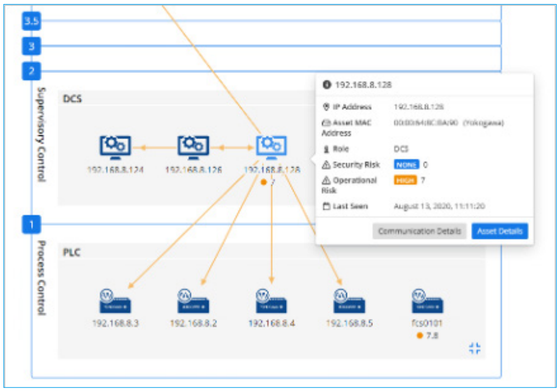
Forescout Continuum provides a real-time asset inventory for the entire ICS network and beyond using passive, active or hybrid asset discovery options for identifying and assessing any type of device connected to the network – from decade-old process controllers to dormant IT systems and new IoT devices – driving compliance automation and efficiency. DPI passively discovers details including network address, host name, vendor and model, serial number, OS or firmware version, hardware version and backplane module information, while non-intrusively identifying OT/ICS vulnerabilities.

The platform provides visibility down to serial devices, such as I/O modules at Purdue level 0, logging configuration and behavioral changes for security analysis and operational forensics. It automatically builds a detailed and interactive network map with extensive device information, baselines for each asset, communication visualizations and groupings by network, role, Purdue level and communication relationship.

Integration with the security ecosystem and bi-directional workflow automation allows any asset to be identified upon connect, while our optional active discovery technology for OT/ICS networks securely and selectively queries specific endpoints on the network, including industrial controllers, to get a complete inventory of all connected assets quickly and effectively. For Windows, Linux and Mac endpoints, patch levels and compliance status can be verified automatically against common or customer-specific security policies and best practices.



Filtered 2,377 Assets out of 27,507 total.



192.168.8.128

IP Address: 192.168.8.128
Asset MAC Address: 00:00:64:8C:8A:90 (Yokogawa)
Role: DCS
Security Risk: NONE 0
Operational Risk: HIGH 7
Last Seen: August 13, 2020, 11:11:20

Identify cybersecurity and operational risks to reduce downtime

Forescout provides a unique Asset Risk Framework that continuously calculates an impact-based risk score for each asset, considering both a **cybersecurity** risk score (for SOC teams) and an **operational** risk score (for OT operators). The scores are continuously evaluated using detected events associated with the asset, proximity to other potentially infected assets, communication links and behavior, known vulnerabilities and other details. This provides the most relevant and up-to-date risk assessment that can be used to make more informed decisions when mitigating risks and other activities. Typical security risks identified include:

- Use of default credentials and insecure authentications and protocols
- New and non-responsive assets
- Poor segmentation exposing vulnerable devices to the internet
- Suspicious user behavior/policy changes
- Malformed messages including those used in exploit attempts
- Unauthorized network connections and communications
- Malware infections and malware spread
- Cyberattacks (DDoS, data exfiltration, MITM & scanning, etc.)

Occasional networking and operational issues are inevitable, but they needn't result in significant downtime. The operational risk analysis enables OT engineers to quickly spot urgent issues including:

- Failure of critical devices
- Unstable process values
- Incorrect process measurements
- Devices exhibiting signs of misconfiguration or malfunction that could cause unexpected downtime
- Unauthorized PLC logic and firmware changes

Forescout Continuum combines signatures with behavioral and patented anomaly detection techniques to detect known and unknown security and operational threats from the earliest stage (discovery) through the actual exploit. An interactive map identifies the source and spread of an incident, and the data provided in its packet captures (PCAPs) supports root cause analysis to expedite response efforts.

Actionable Research from Vedere Labs

Staying ahead of bad actors requires relentless diligence. The Forescout Device Cloud is the world's largest cyber asset repository, with anonymized data collected and monitored from millions of deployed IT, IoT, IoMT and OT devices. This intelligence is plowed into our platform to supply the most accurate asset auto-classification and threat detection available.

Vedere Labs, Forescout's threat intelligence and research team also leverages the Device Cloud for advanced intelligence to alert customers and the broader security community about emerging risks and supply mitigation steps through threat briefings, vulnerability disclosures and demonstrations including Project Memoria, R4IoT and OT:ICEFALL.

Manage the exponential growth of connected assets and changing threat landscape

The threat landscape is evolving fast, so security teams need to be able to quickly identify new assets, assess their risks and manage any threats with pro-active mitigation and automated remediation. With Forescout Continuum you can:

- Visualize communications and automatically optimize segmentation so vulnerable devices continue operating securely as interconnectivity increases or changes.
- Automatically verify the security and compliance posture of every asset, including third-party or contractor devices, before granting them access to the network and specific assets to perfom maintenance operations
- Optimize threat analysis and remediation with ICS-specific threat intelligence, multi-dimensional alert aggregation and MITRE ATT&CK for ICS classification to enable efficient incident response.

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. Further integrations with the security ecosystem to exchange insights, automate workflows and initiate response to emerging cyber threats are available.

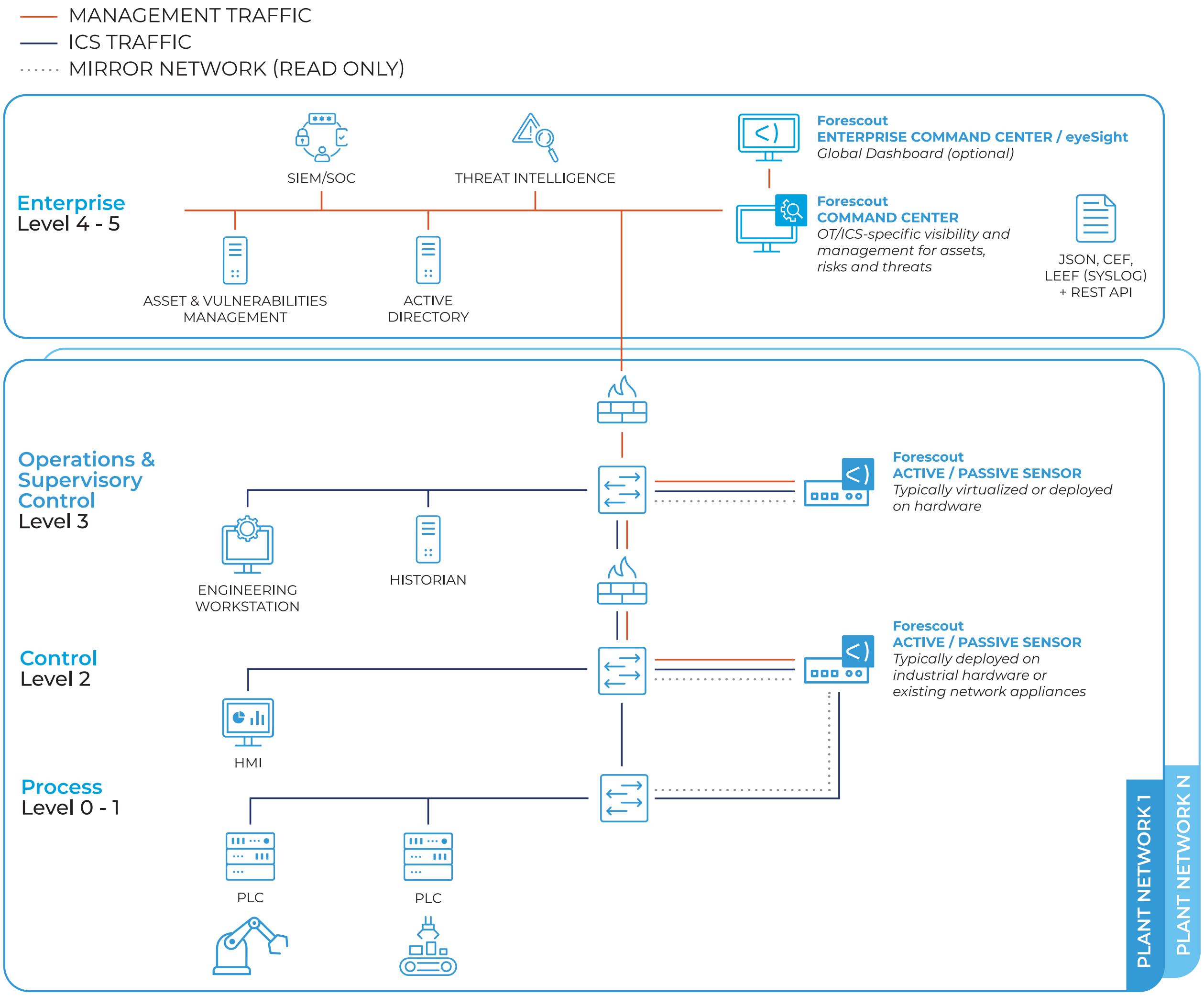

MANAGEMENT TRAFFIC
ICS TRAFFIC
MIRROR NETWORK (READ ONLY)
Enterprise
Level 4 - 5
SIEM/SOC
THREAT INTELLIGENCE
Forescout
ENTERPRISE COMMAND CENTER / eyeSight
Global Dashboard (optional)
Forescout
COMMAND CENTER
OT/ICS-specific visibility and management for assets, risks and threats
JSON, CEF, LEEF (SYSLOG) + REST API
ASSET & VULNERABILITIES MANAGEMENT
ACTIVE DIRECTORY
Operations & Supervisory Control
Level 3
Forescout
ACTIVE / PASSIVE SENSOR
Typically virtualized or deployed on hardware
ENGINEERING WORKSTATION
HISTORIAN
Control
Level 2
Forescout
ACTIVE / PASSIVE SENSOR
Typically deployed on industrial hardware or existing network appliances
HMI
Process
Level 0 - 1
PLC
PLC
PLANT NETWORK 1
PLANT NETWORK N

Figure 1: Typical deployment architecture for manufacturing environments combines passive network monitoring with active discovery and integrations to automate cyber security across the OT/ICS environment and beyond.

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