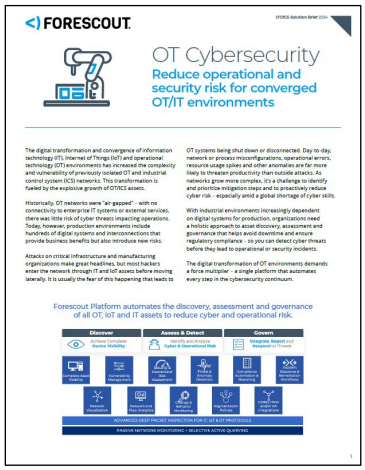
FORESCOUT

carahsoft


FORESCOUT

OT Cybersecurity
Reduce operational and security risk for converged OT/IT environments

OT/ICS Solution Brief

Reduce operational and security risk for converged OT/IT environments

Thank you for downloading this Forescout solution brief. Carahsoft is the dealer and distributor for Forescout cybersecurity solutions available via GSA Schedule 70, NASA SEWP V, ITES-SW, and other contract vehicles.

To learn how to take the next step toward acquiring Forescout's solutions, please check out the following resources and information:

For additional resources:
carah.io/ForescoutResources

For upcoming events:
carah.io/ForescoutEvents

For additional Forescout solutions:
carah.io/ForescoutProducts

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Forescout@carahsoft.com
833-FSCT-GOV

To purchase, check out the contract vehicles available for procurement:
carah.io/ForescoutContracts

For more information, contact Carahsoft or our reseller partners:
Forescout@carahsoft.com | 833-FSCT-GOV

OT Cybersecurity

Reduce operational and security risk for converged OT/IT environments

The digital transformation and convergence of information technology (IT), Internet of Things (IoT) and operational technology (OT) environments has increased the complexity and vulnerability of previously isolated OT and industrial control system (ICS) networks. This transformation is fueled by the explosive growth of OT/ICS assets.

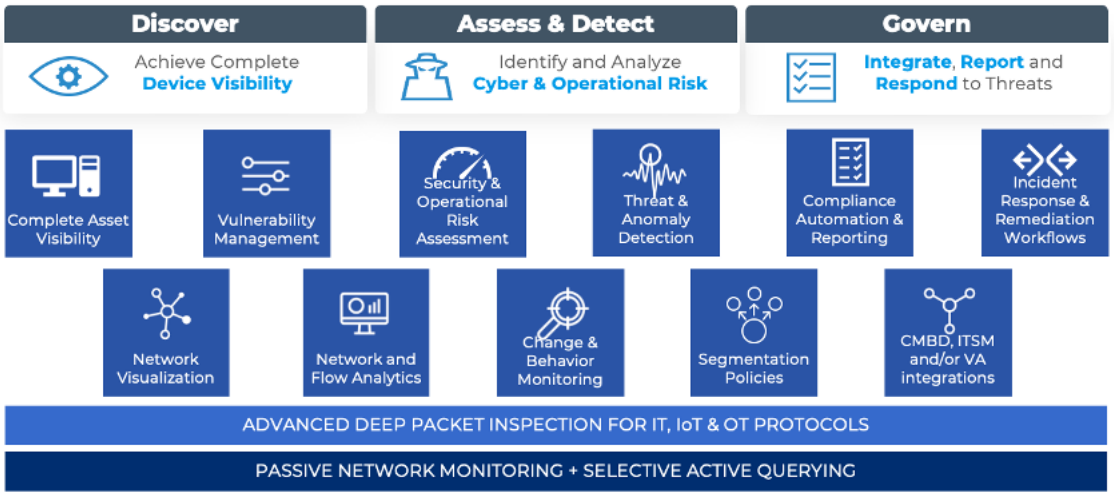
Historically, OT networks were "air-gapped" – with no connectivity to enterprise IT systems or external services, there was little risk of cyber threats impacting operations. Today, however, production environments include hundreds of digital systems and interconnections that provide business benefits but also introduce new risks.

Attacks on critical infrastructure and manufacturing organizations make great headlines, but most hackers enter the network through IT and IoT assets before moving laterally. It is usually the fear of this happening that leads to OT systems being shut down or disconnected. 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. As networks grow more complex, it's a challenge to identify and prioritize mitigation steps and to proactively reduce cyber risk – especially amid a global shortage of cyber skills.

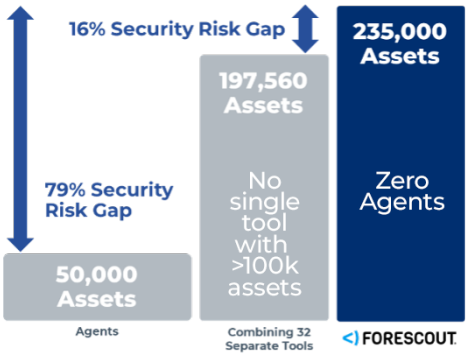
With industrial environments increasingly dependent on digital systems for production, organizations need a holistic approach to asset discovery, assessment and governance that helps avoid downtime and ensure regulatory compliance – so you can detect cyber threats before they lead to operational or security incidents.

The digital transformation of OT environments demands a force multiplier – a single platform that automates every step in the cybersecurity continuum.

Forescout Platform automates the discovery, assessment and governance of all OT, IoT and IT assets to reduce cyber and operational risk.



Energy Company



As a baseline, this large energy company only had visibility into its **50,000** agentable assets. Fragmented information from 32 separate security tools identified closer to 200,000. Using zero agents, Forescout identified **235,000 total assets** – revealing a **79% security risk gap** over agent solutions and creating a single source of truth.

- **$600,000+** saved in 3-year ROI benefits
- **1 wee**k to discover all assets
- **5+ months** saved on asset inventory

Discover and inventory all your OT/ICS assets, continuously.

Complete security starts with an accurate inventory of all assets, where they are located and their compliance status. With rapid digitalization of critical infrastructure and manufacturing environments – often geographically dispersed across large sites – accurately identifying and managing all OT, IoT and IT assets is increasingly challenging. Moreover, industrial assets use proprietary protocols and are more fragile than most, which makes them and the processes they support tricky to identify.

Discovery approaches that work for IT and IoT might not work for sensitive OT devices given safety rules, vendor interoperability issues, industrial process requirements and other considerations. Especially when OT devices control critical infrastructure, there can be no downtime or service disruption. Therefore, they require non-intrusive passive monitoring or agentless techniques.

Forescout offers continuous discovery of all cyber assets across all networks, with full visibility into OT/ICS networks to detect cyber threats before they lead to operational or security incidents. In-depth asset management and monitoring of OT networks and device types employs more than 30 passive and active discovery techniques to identify assets, their location and their cyber posture, and to detect anomalies. They include deep packet inspection (DPI) of 300+ IT, OT and IoT protocols as well as carefully selected active queries for OT/ICS to query selected endpoints, including industrial controllers, and network infrastructure for complete device visibility, well beyond SPAN.

Features

Complete and real-time asset discovery with 30+ passive, active and hybrid techniques for complete coverage across all OT/ICS networks and all device types, well beyond SPAN:

- **Passive monitoring** – DPI of 300+ OT, IoT and IT protocols for in-depth behavioral monitoring of all assets and non-intrusive OT/ICS vulnerability identification.
- **Active endpoint discovery** – 30+ OT/ICS-specific active queries to identify common OT, IoT and IT devices and extract critical information for improved asset inventory data acquisition and fewer manual audits. Extensible with in-depth security compliance queries for Windows, Linux and Mac endpoints.
- **Network integration** – Integration with network infrastructure to identify assets the moment they connect to the network and determine where they are connected for efficient asset management.

Cut through the noise with security and operational risk scores

Forescout provides a unique Asset Risk Framework that calculates two risk scores for each asset, evaluating both cybersecurity and operational risk. Based on impact, they are continuously refreshed using detected events associated with the asset, proximity to other potentially infected or misbehaving assets, communication links, known vulnerabilities and other details. These multi-factor risk scores enable OT engineers and security teams to make informed decisions and prioritize the right actions.

Assess cyber and operational risks, continuously.

Given the broad range of asset types in every organization, assessing risks and compliance requires various techniques and integrations. Security teams typically rely on dozens of risk assessment products to accommodate every need. But who is watching the watchers and consolidating all details into a single source of truth?

Forescout is the only platform that continuously identifies and mitigates risk across all cyber assets in your digital terrain, including sensitive OT/ICS. The platform enhances your investment in security tools by helping to ensure they are deployed, configured and working correctly, and orchestrating communication among them.

Forescout offers a continuously expanding Industrial Threat Library and ICS-specific Indicator of Compromise (IOC) & Vulnerabilities (CVE) database to passively identify any threat to operational continuity and assess every connected asset's risk. Updated regularly, it contains thousands of behavioral checks and threat indicators to protect asset owners from advanced cyberattacks, network misconfigurations and operational errors.

Unless you can validate your security posture, you're still subject to unplanned downtime whether there's a viable threat or not. Lacking proof of compliance in the face of a lateral cyber attack, cautious OT operators will take systems offline pre-emptively. With Forescout, staying operational during a cyber incident is a byproduct of continuously assessing and remediating your digital terrain.

Features

Asset configuration management – Automatic collection of OT asset information and logging of configuration changes for security analysis, regulations reporting and operational forensics, avoiding operational disruption

Real-time threat detection and incidence response – ICS-specific threat indicators built on more than 14 years of OT/ICS threat research and aligned with MITRE ATT&CK® for ICS to detect any threat from misconfigurations and operational errors to advanced cyberattacks

Streamlined compliance – Powerful dashboards, analytics and reporting tools to simplify compliance with key standards including NERC CIP, EU NIS Directive, NIST CSF and IEC 62443.

Zero downtime? Zero downtime.

Operational downtime or business disruption are the quickest ways to impact safety and revenue. Forescout enforces flexible mitigation actions, from modest to stringent, so even vulnerable OT/ICS systems can continue to operate securely.

Govern OT/ICS assets proactively to minimize the attack surface and breach impact, continuously.

Governance requires an array of options for swift mitigation or remediation, as well as knowing which option to use based on all available intelligence. Modest options include automating workflows to open a ticket or notify an OT engineer to check a misconfiguration. More stringent options include automated remediation, network access control, dynamic segmentation and cross-product orchestration.

Patching is typically the first form of remediation when a vulnerability is discovered. But patching OT devices is notoriously difficult, due to their mission-critical nature. Systems need to be stopped and restarted to load patches, which means downtime, and some processes and equipment, such as a blast furnace, need to be shut down slowly for safety reasons. Instead of patching, vulnerable devices must often be segmented from other parts of the network and monitored to detect any unwanted changes in behavior.

Forescout automates response workflows, including SIEM/SOC incident response and dynamic segmentation, to protect high-risk networks and keep mission critical assets online. This is achieved natively and via other security tools using pre-built bi-directional integrations. By connecting the existing security ecosystem, Forescout multiplies the effect of each solution operating in isolation.

Features

Product integrations – Information-sharing and automated workflows across IT and security products, including ITSMs, SIEMs, telemetry systems, firewalls and authentication servers, for better situational awareness across your digital terrain.

Network access control – Upon-connect verification of third-party technician and remote employee security posture before granting access to critical assets.

Scalability – Flexible deployment options and seamless integration with existing network infrastructure, SIEM/SOC, asset management and other security tools.

FORESCOUT

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