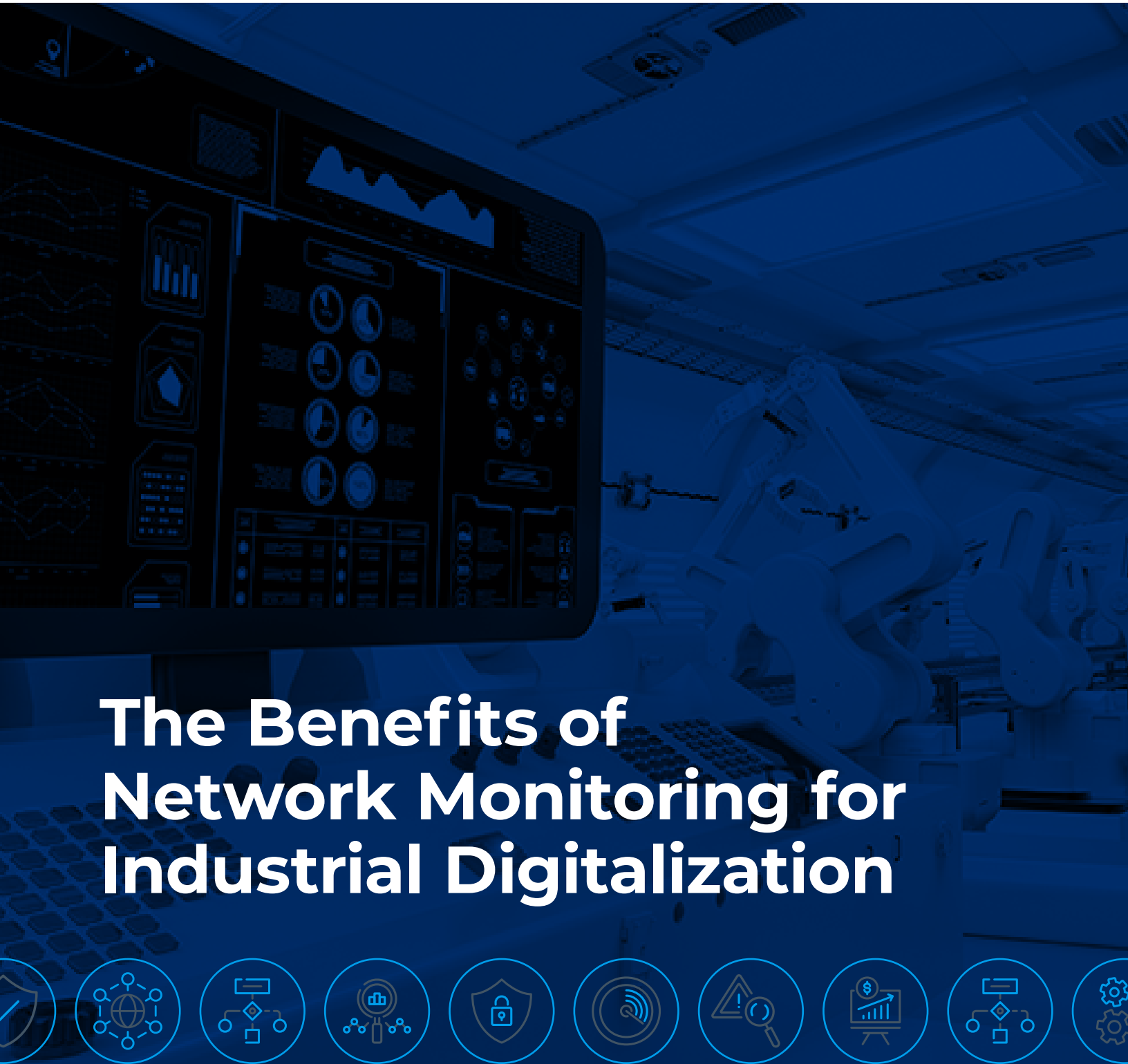
FORESCOUT

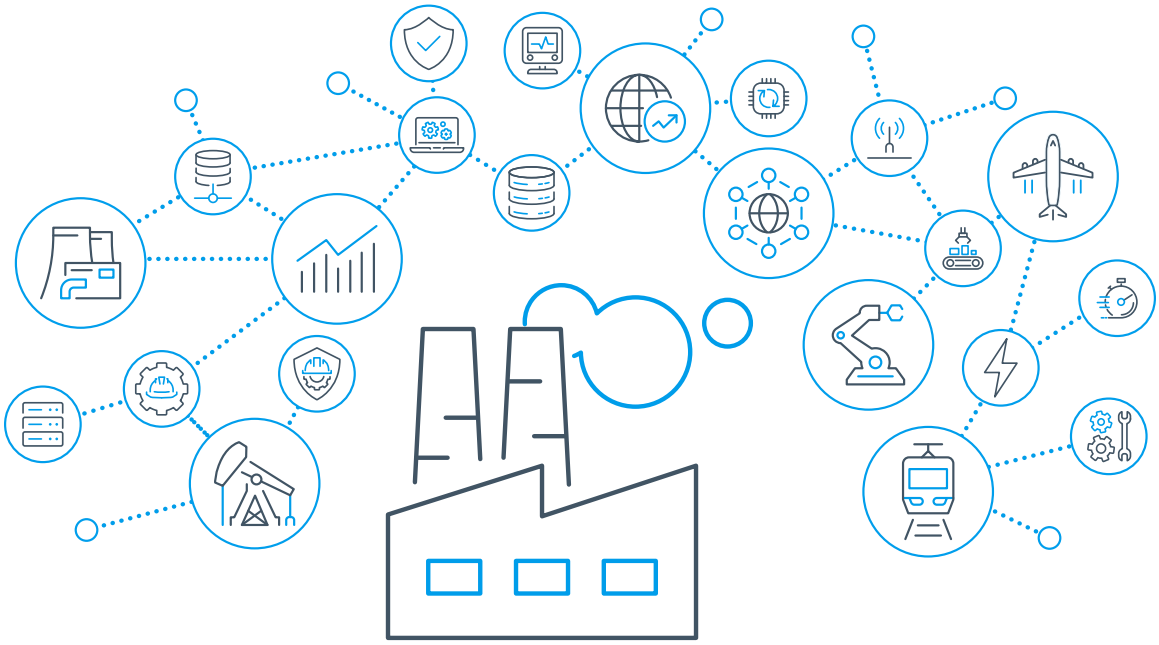


The Benefits of Network Monitoring for Industrial Digitalization

Industrial Digitalization

Today, manufacturing is powered by thousands of connected devices, massive computing power and artificial intelligence. These advances enable manufacturers to adopt flexible, built-to-order production methodologies that include automated workflows and real-time performance monitoring. Together they improve efficiency, reduce errors and cut costs, but with these benefits comes increased cyber risk.

Industrial digitalization is characterized by the integration of computation, networking and physical processes, which bring clear business advantages. It has also led to highly complex, heterogeneous manufacturing networks due to the convergence of enterprise and manufacturing assets and increased use of Internet of Things (IoT) devices. As a result, manufacturers are operating with increased cybersecurity and operational risk that can lead to downtime if they are not top-of-mind in a holistic cybersecurity and digital transformation strategy.



Today, industrial asset owners have little to no visibility into existing industrial threats and vulnerabilities, and therefore no way to anticipate, analyze and respond to incidents. Providing visibility into industrial networks is the first step to gain full control of the environment. This white paper shows how network monitoring and automating cybersecurity in manufacturing networks brings tremendous value to information technology (IT) and operational technology (OT) teams.

Threats and Needs

In February of 2021, Toyota halted production in all 14 of its Japanese plants after a significant parts supplier fell victim to a cyberattack. The attack also led to work stoppages at Toyota affiliates like Hino Motors, which makes buses and trucks, and Daihatsu Motor Co. Toyota saw production drop 5% that month, a large amount considering Toyota is the world's largest automaker. Supply chain cyberattacks are no longer rare, and manufacturers must take heed of the downstream impacts. Hackers have discovered that by compromising production of key suppliers they can also shut down operations for their customers, including industry leaders like Toyota.

However, cyberattacks are by far not the most imminent threat to the manufacturing industry. Despite the noise from the media, the likelihood of a successful attack against industrial control systems (ICS) is relatively low. On the contrary, cyber incidents happen daily. They include small to major network or process disruptions due to misconfigurations, erroneous commands and operations, software errors and device failures – none of them intentional, but nevertheless all impacting the asset owner's bottom line.

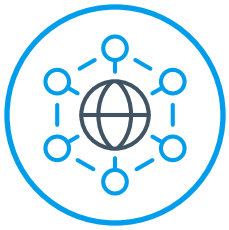
To effectively protect the network and avoid downtime, asset owners must be able to detect all these threats in a timely manner. When choosing a strategy to implement, guidelines such as the NIST Cybersecurity Framework and IEC 62443 can provide valuable advice on how to improve the overall cybersecurity of industrial networks.

The figure below provides a good overview of the industrial automation threat landscape, including the frequency and impact of threats and problems. These operational and networking threats are detected daily at most of our manufacturing customers.

CYBERSECURITY

- Ransomware
- Targeted, zero-day attacks and malware
- Industrial espionage
- Insider threats (employees, vendors, and contractors)
- Firewall misconfiguration
- Use of insecure devices, protocols, and services

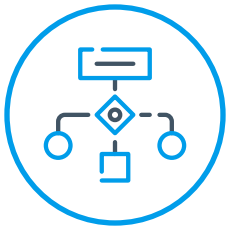
Frequency: Yearly
Impact: $$$$$



NETWORKING

- Unstable & broken links
- Commands that do not reach the destination
- Misconfiguration of network services (including NTP, DHCP etc.)
- "Noisy" devices causing traffic floods
- IP misconfiguration

Frequency: Weekly-Monthly
Impact: $$$

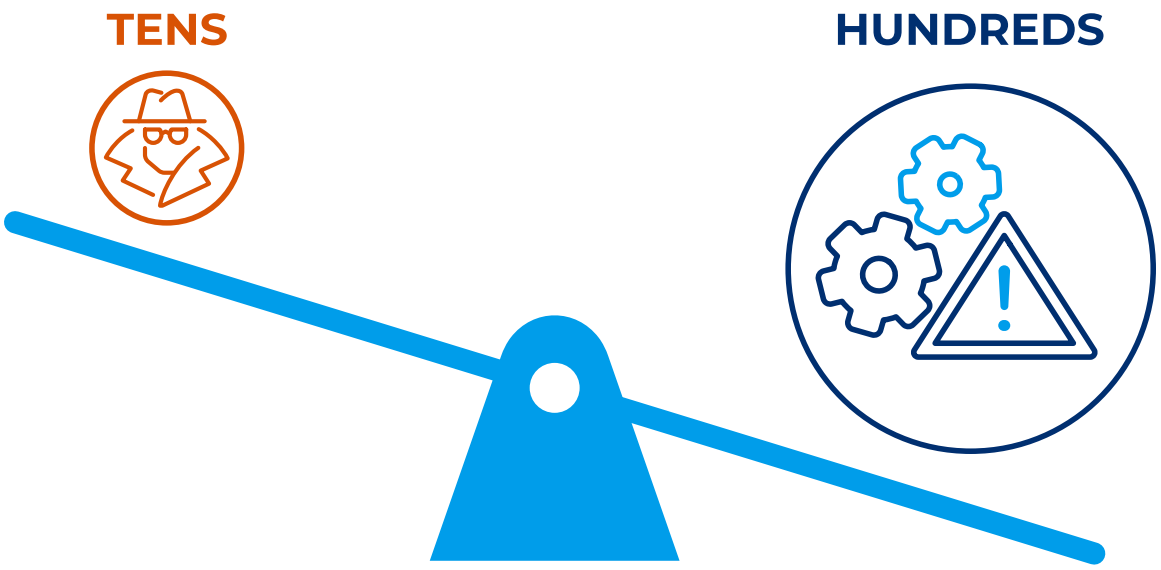


OPERATIONS

- Misconfigured and malfunctioning devices
- Device failure and downtime
- Non-compliant data exchange
- Undesired maintenance activity
- Process instability and anomalies

Frequency: Daily-Weekly
Impact: $$$$

The following visual represents the actual proportion of cybersecurity vs. networking and operational threats experienced by our global customer base in the last 12 years.



Network and operational threats outweigh attacks and intrusion attempts ten to one.

Note that the cybersecurity incidents referenced above are limited to intrusion attempts and attacks and do not include weak security implementations such as firewall misconfiguration and insecure devices, protocols and services, which are extremely common across all industrial sectors. As these statistics show, the most imminent threats to manufacturing processes stem from the lack of infrastructural resilience – in other words, the lack of network cyber resilience, of which security is only a part.

Solution

Being cyber resilient means being able to identify and quickly recover from any threat to operational continuity. Manufacturing operators can save considerable time, effort and money by detecting and fixing existing and emerging problems and threats before they cause disruptions, thereby creating a healthier and more robust infrastructure. Cyber resilience starts with the effective and continuous application of four activities, which align with the five functions of the NIST Cybersecurity Framework (CSF):

Assess

Gather all asset details to determine the current security and operational risks of each connected asset and develop a complete network map, including asset zones and communication flows, to determine the security perimeter and interconnectivity. (NIST CSF Identify function)

Secure

Deploy security controls and dynamic network segmentation to limit unnecessary connectivity, protect vulnerable assets that cannot be patched or upgraded and respond to a changing threat landscape. (NIST CSF Protect function)

Monitor

Use a variety of passive techniques compatible with sensitive OT/ICS environments to continuously monitor the infrastructure to ensure assets remain in compliance, catch early symptoms of problems and threats, and avoid downtime. (NIST CSF Detect function)

Respond

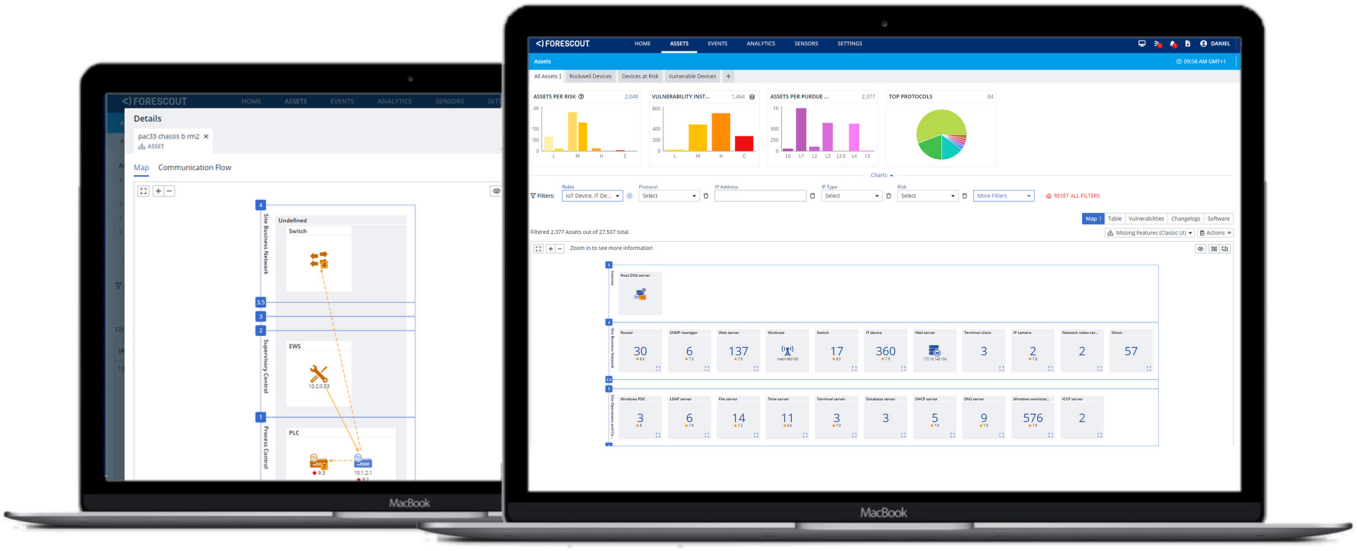
When a threat is detected, apply the appropriate measures to restore the desired system operation and the network's cyber resilience. (NIST CSF Respond and Recover functions)

The Forescout Continuum platform incorporates OT/ICS-specific network monitoring and threat detection capabilities, specifically designed to continuously monitor, assess and govern industrial assets and networks and enhance the cyber resilience of industrial sites. It's ideal for a manufacturing environment as it delivers value and protection for every "ingredient": network infrastructure, process automation, and cybersecurity.

Forescout performs all four key cyber resilience activities as follows:

Assess

- Automatically creates a complete asset inventory and network baseline with 30+ passive and carefully selected endpoint and network-active techniques covering every connected asset – from legacy process controllers to dormant IT systems and modern IoT assets
- Provides accurate asset fingerprinting with the broadest ICS protocol coverage and easy extensibility, including asset function, installed firmware and device modules, and allows for all collected information to be exported or automatically synchronized with other IT security tools, such as a CMDB
- Delivers automated, impact-based security and operational risk scoring to effectively guide the prioritization of mitigation activities, such as patching and segmentation
- Offers non-intrusive OT/ICS vulnerability assessment and identifies existing networking and operational issues, pinpointing weak spots and current inefficiencies
- Presents all information in an intuitive, interactive network map that visualizes asset relationships



Secure

- Continuously assesses the security posture of every connected asset to protect OT assets and network segments in real time and as the threat landscape changes
- Validates and automates network segmentation efforts and firewall policy changes
- Enables predictive maintenance by providing early indicators of device misconfiguration, malfunction, or failure
- Automates appropriate response actions to maintain operational continuity if an asset fails specified policy conditions
- Drives effective, low-risk segmentation strategies to monitor or limit network access to critical or vulnerable assets and mitigate threats crossing IT/OT network boundaries

Monitor

- Provides real-time network visibility through visual network analytics widgets and dashboards to quickly spot trends and anomalies
- Features deep packet inspection for hundreds of industrial protocols and vendors, with patented technology to detect hidden threats
- Automatically creates a baseline of current network communications that operators can use for additional anomaly detection
- Monitors down to the process values so any issues with operational continuity are detected before they result in unexpected downtime
- Combines patented anomaly detection with a continuously growing Industrial Threat Library (ITL) containing thousands of ICS-specific checks, to detect network misconfigurations, operational errors and advanced cyberattacks
- Integrates with SIEM solutions and other logs collectors in a matter of minutes and applies MITRE ATT&CK for ICS classification to provide the operator with a unified security view for effective incident response

Respond

- Real-time alerting of any threat to operational continuity to enable immediate mitigation
- Includes rich contextual alert information, such as source and target asset details, associated risk levels and remediation suggestions for immediate response and a PCAP of the suspicious event for effective root cause analysis
- Provides quick diagnostics and troubleshooting support, saving operators from the tedious task of going through system and network logs
- Guides the incident prioritization and response process by indicating alert severity, operator profile best suited to follow up, and suggested next steps
- Supports visual forensic analysis with configurable widgets for in-depth search, filter and analysis of historical data and logs
- Visualizes incident details on the interactive network map, providing enhanced situational awareness and a bird's eye view of its spread
- Shares insights and coordinates workflows across the existing security ecosystem, such as asset management, vulnerability management, endpoint protection, ITSM and SIEM/SOC, to multiply the effect of each solution operating in isolation and automating cybersecurity across the entire digital terrain

Forescout Continuum can be deployed in a matter of hours and provides immediate value with its out-of-the-box assessment capabilities, delivering immediate return on investment (ROI). Its scalable and flexible deployment architecture lets operators monitor distributed and remote production environments from a single screen.

Continuum can be used in multi-vendor environments, as it natively supports all major ICS vendors and protocols, including proprietary protocols. Better yet, Continuum's Device Visibility and Threat Detection capabilities are continuously improved and expanded upon to keep up with the latest technology and emerging threats and you can even leverage a flexible framework to build custom use cases and integrations that fit your unique needs.

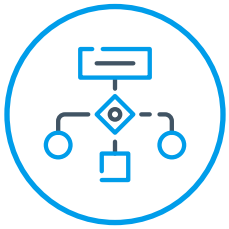
Optionally, Forescout's cloud-based data lake with advanced machine learning delivers actionable insights and crowd immunity based on real-time knowledge and activity from Forescout's millions of devices under management. Forescout's threat research team, Vedere Labs, leverages the Forescout Cloud data lake for advanced intelligence to alert customers and the broader security community about emerging risks, such as Ripple20, AMNESIA:33 and INFRA:HALT.

Benefits

Forescout Continuum benefits everyone from C-level management to engineers, and spans across multiple departments, from IT to OT. The platform provides IT teams with guidance for an informed risk management process, real-time visibility behind the OT firewall and a continuous overview of the network's security status. OT teams are supported in their daily activities with early detection of operational issues and threats, as well as guidance on mitigation and resolution. The result is more effective risk management of the manufacturing environment and less downtime.

FINANCIAL

- Increased productivity
- Averted loss of revenue due to unplanned downtime
- Reduced costs for problem mitigation
- Easier compliance with standards and guidelines
- Minimized corporate liability Immediate ROI



STRATEGIC

- Ability to anticipate cyber incidents
- Reduced exposure to cyber threats
- Reduced resource allocation for problem identification and resolution
- Ability to perform predictive maintenance
- Evidence of good operation and accountability
- Extends segmentation to ICS environments to build a strong foundation for zero trust implementations

TECHNICAL

- Complete network visibility and real-time situational awareness
- Early indicators of issues and threats
- Minimized troubleshooting effort and resolution time
- Validation of network changes and maintenance operations conducted by employees and third parties
- Enhanced reliability and availability of control systems

See Forescout Continuum in action!

Your organization is unique. Get a customized demo and let us show how you can benefit from improved cyber resilience.

Get my Demo

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