FORESCOUT BELDEN HIRSCHMANN A BELDEN BRAND tripwire

Solution Brief

The Secure Factory: Belden and Forescout Strengthen Industrial Network Security

Increase asset intelligence, network access control and cyber resilience

> Over 40% of organizations are moving toward centralized OT security, either with increasing reliance on their IT infrastructure or an industrial SOC." [1]
>
> – SANS State of OT/ICS Cybersecurity Survey, 2019

The increasing interconnectivity between the worlds of information technology (IT) and Industrial Control Systems (ICS) or operational technology (OT) poses new operational risks to industrial process integrity and human safety.

The Challenge

More and more industrial devices are connecting to networks for innovations that capitalize on machine data and help with process optimization. Industrial networks are also under pressure to expand capacity, providing additional bandwidth to new machines and field I/O devices, used by both employees and contractors, frequently allowing multiple applications to share the same network to keep costs down. This vast increase in connectivity opens previously air-gapped or physically isolated control networks to the world of cyberthreats, potentially damaging impacts to brand reputation, human safety, operational productivity and product quality.

This evolution of expanding interconnectivity accelerates the need for cybersecurity controls that extend to the network-enabled machines and field I/O devices while meeting the high availability requirements. Such controls need to include dynamic network access restrictions and segmentation that utilizes existing network infrastructure to rapidly reduce the attack surface without requiring a costly network redesign project. Industrial organizations also need to proactively address both cybersecurity and operational risk without compromising the integrity of the network, connected devices or the processes they support.

Detect and respond to known and unknown cyber and operational threats such as:

- Connectivity or network performance issues
- Unauthorized network communications
- WannaCry-like malware propagation
- Vulnerable devices
- Widespread use of default passwords
- Use of insecure protocols
- Critical equipment failures
- Misconfigured device or network infrastructure
- PLC configuration changes
- Regulatory compliance violations

Organizations face challenges to rapidly adopt innovations while securing existing heterogeneous network environments across OT, IT and IoT connected devices. Primary challenges to address are:

- Incomplete visibility of connected devices and network communications to prevent cyber attacks, noncompliance and operational failures
- Limited network access and segmentation controls to reduce the attack surface and prevent malware propagation
- Lack of continuous monitoring and rapid response capabilities for threats, misconfigurations, vulnerabilities and operational effectiveness issues while preserving operational uptime

The Solution

Industrial organizations need to find solutions that close cybersecurity gaps by providing cohesive contextual insight for all connected assets, proactively detecting both cybersecurity and operational threats plus intelligently automating threat mitigation and remediation workflows as much as possible. Forescout and Belden provide integrated solutions that close cybersecurity gaps by increasing context-aware network and asset intelligence and streamlining policy-driven workflows. Forescout, an established security leader with enterprise-wide device visibility and control and OT risk management, joins Belden across the solution brands, Hirschmann, the technology and market leader in industrial networking, and Tripwire, a leading provider of integrity assurance solutions that drive cybersecurity and availability. The result is a best-of-breed solution stack for assessing and reducing enterprise risk across both IT and OT environments for industrial customers.

Gain continuous non-disruptive IT and OT asset and threat visibility

The Forescout and Belden solution provides continuously connected device intelligence, identifying cybersecurity threats and pinpointing operational issues that would otherwise go unnoticed, potentially disrupting safety, productivity and quality over time. This enables organizations to streamline asset inventorying and immediately identify threats. This intelligence also allows automation of context-aware policy-driven network or system actions to confidently protect assets while maintaining operational uptime.

- Continuously monitor and profile all devices as they connect, classify them and detect changes in real time using non-disruptive methods. Assess multiple variables, such as device identity, ownership/user, configuration compliance, network behavior and security posture and detect rogue assets with the Forescout platform. Plus capitalize on Forescout data by analyzing trends and log diagnostic events in Tripwire Log Center.
- Gain additional OT asset information such as firmware version, indicators of compromise and Purdue network layer context with Forescout eyeInspect (formerly SilentDefense).
- Gain industrial network operations, performance and availability context via Hirschmann Industrial HiVision. See a network topology diagram down to the switch port, showing where links go up/down or not operating correctly.

"The amount of information we get back from the Forescout platform is incredible. While many other tools will find the IP address of endpoints, it is by far the best tool I have ever used to properly find, identify and control systems. It has been beyond valuable to us."

— Joseph Cardamone, Sr. Information Security Analyst and NA Privacy Officer, Haworth Center

- Manage all of your Hirschmann switches from a single interface across their entire lifecycle.
- Assess configuration state and changes against industry standards (IEC 62443 and NIST SP 800-82) with Tripwire Enterprise
- Detect vulnerabilities that introduce the most significant risk to your operation from field I/O to the enterprise datacenter and cloud environments. Forescout eyeInspect provides deep risk context for industrial devices such as PLCs, Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs), while Tripwire IP360 provides rich context for enterprise IT environments in the data center or cloud

Dynamically control network access and enforce segmentation based on rich context

The Forescout-Belden integrated solution combines best-of-breed Hirschmann industrial networking infrastructure with the Forescout platform's real-time heterogeneous network access and segmentation control capabilities across both IT and OT heterogeneous networks, with or without 802.1X. This makes network access control and segmentation an immediate, viable defense mechanism against cyberthreats to protect the availability, operation and safety of mission-critical industrial control environments.

- Automate policy-driven, context-aware network control actions applied to Hirschmann infrastructure at scale, from the aggregation layer or zone level down to the machine or cell level, without network upgrades. Apply more granular controls at the switch port, access or distribution layers as needed.
- Easily detect any unauthorized or unnecessary network communications by leveraging both SNMP and sFlow data sent from Hirschmann to the Forescout platform and using Forescout eyeSegment to visualize communication patterns among logical zones across both IT and OT networks.
- Simulate new policies using Forescout eyeSegment to see what impact they could have prior to implementation to confidently deploy granular segmentation without impacting operational performance.

Automated threat response and compliance enforcement while maintaining uptime

The Forescout platform provides a unified cybersecurity policy engine that immediately responds to Forescout and Tripwire detected threats, as well as other integrated sources, with orchestrated context-aware workflows that mitigate and can proactively remediate threats. Automating threat response with context-aware actions drastically reduces MTTR (mean time to resolve) without affecting critical operations.

- Detect both known and unknown threats across IT and OT with: Forescout eyeInspect's ICS/OT threat intelligence through deep packet inspection and anomaly detection technology, library of over 3,500 IoCs for advanced cyberattacks and network misconfigurations and operational errors; Tripwire IP360's high-risk IT vulnerability detection information for managed assets; Tripwire Enterprise's detection of unauthorized configuration changes; and Tripwire Log Center's operational diagnostic log events

- Automatically mitigate threats detected by Forescout, Tripwire and other threat intelligence sources with Forescout context-aware policy-driven actions that preserve operational integrity. Targeted threat response actions span from simple notification to isolation of a threat on the network to blocking an unauthorized or compromised device from network access and more.
- Automate relevant remediation workflows on managed devices such as patch installs or running a Tripwire IP360 vulnerability scan on a noncompliant IT devices that will not impact operations.

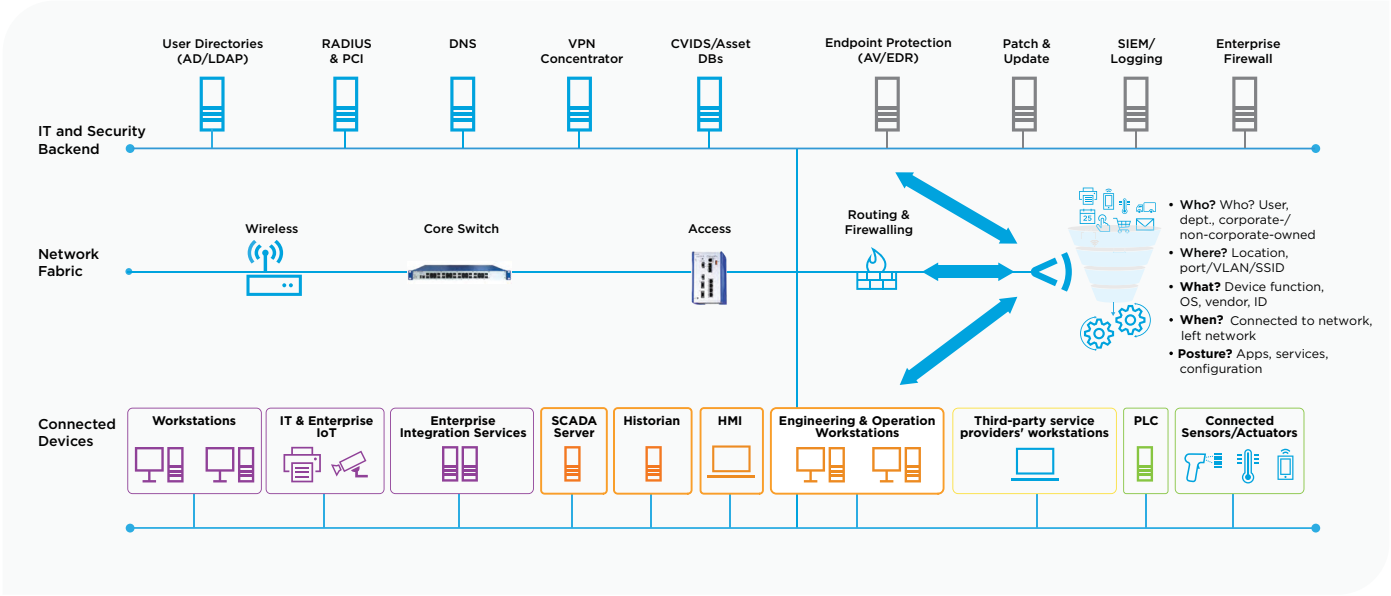

Figure 1. Application of Hirschmann switches and routers with Forescout

"By 2021, 80% of industrial IoT (IIoT) projects will have OT-specific security requirements, up from 40%" [2]

– Gartner

Belden Products Supported by Forescout

- Hirschmann Industrial Switches These hardened, compact, managed industrial DIN Rail Ethernet switches provide an optimum degree of flexibility with several thousand variants.

- Hirschmann Software HiOS and Classic The HiOS software from Hirschmann increases the power and performance of its Industrial Ethernet switches.

- Belden Industrial Networking With this powerful Layer 3 switch, you can build flexible, redundant and secure backbone networks with a high bandwidth (up to 10 Gigabit).

List of Hirschmann and Belden industrial networking equipment supported

- BRS
- EAGLE 30
- EES Series
- Greyhound 1020
- Greyhound 1030
- Greyhound 1040
- MACH 100
- MACH 1000
- MACH 1040
- MACH 104
- MACH 4000
- MACH 4500
- MS 20
- MS 30
- MSP 30
- MSP 40
- Octopus
- Octopus II
- PowerMICE
- RED
- RS 20
- RS 30
- RS 40
- RSB 20
- RSP
- RSPE
- RSPL
- RSPS
- RSR

Summary

The Hirschmann family of Layer 2 and Layer 3 ruggedized switches and routers have been tested for interoperability and certified with the Forescout platform. This includes the latest HiOS operating system and the Classic Switch Software OS to ensure full compatibility throughout the entire Hirschmann device portfolio. The Forescout platform can auto-discover Hirschmann infrastructure, allowing the consumption of connected device intelligence to build comprehensive asset accountability and security control foundation for Hirschmann as well as heterogeneous network environments, without requiring costly network upgrades. Adding the layer of threat intelligence Forescout eyeInspect and Tripwire solutions provide, enables organizations to achieve advanced threat defense enterprise-wide, dramatically reducing the risk of cyberattack.

Why Forescout and Belden

- Comprehensive device and risk visibility across IT and OT networks
- Logical zone-to-zone communication pattern insight and policy simulation to validate and deploy segmentation with confidence
- Dynamic access control and segmentation enforcement based on rich context
- Robust enterprise-wide policy engine that automates incident response workflows with context-aware actions that maintain operational integrity
- Apply advanced security measures while capitalizing on the long life of Hirschmann infrastructure – no networking upgrades required
- Avoid 802.1X complexity and operational costs
- Rapid time to value and ROI

About Forescout

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment. Learn how at www.forescout.com.

About Belden

Belden Inc. delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial and enterprise markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis and has manufacturing capabilities in North and South America, Europe and Asia. For more information, visit us at www.belden.com.

***Notes**

1. SANS State of OT/ICS Cybersecurity Survey, 2019 https://www.forescout.com/platform/operational-technology/2019-SANS-state-of-OT-ICS-cybersecurity-survey/
2. 7 Questions SRM Leaders Aren't Asking OT Security Providers During Technology Selection, Saniye Alaybeyi https://www.forescout.com/platform/operational-technology/gartn12er-report-7-questions-for-ot-security-providers

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591