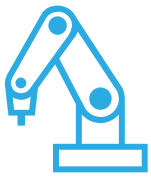
> **By partnering, we further strengthen our Industrial Cybersecurity Suite to expand our asset detection and system-hardening capabilities while introducing Forescout's industry-leading network access control and segmentation capabilities to our IT and OT customers."**
>
> — Dhrupad Trivedi, Executive Vice President and Chief Technology Officer of Belden and President of Tripwire.

Belden and Forescout Joint Solution for Operational Technology

Enhance Network Visibility, Access Control and Performance Assurance



The increasing interconnectivity between the worlds of information technology (IT) and operational technology (OT) introduces new networking challenges that can compromise the core value of every mission-critical network: Availability.

Previously hidden attack surfaces in OT networks emerge, forcing OT network operators to adopt new defensive postures. The "air gap"—the complete disconnection of the OT network from any other networked resource—is largely a thing of the past. To support the availability mandate, networking resources need to be guaranteed and performance assured to ensure maximum uptime for the operations.

Therefore, mission-critical network operators need to find cybersecurity and availability solutions that take into account the special considerations of OT networks, and work with established partners to protect their networks.

Forescout, an established security leader in visibility and control, has teamed up with Belden subsidiaries Hirschmann, the technology and market leader in industrial networking, and Tripwire, a leading provider of integrity assurance solutions that drive cybersecurity and availability. The goal of this partnership is to offer a best-of-breed solution stack for assessing and reducing enterprise risk across IT and OT environments.

The Challenge

Many organizations still have significant investments in OT equipment with lifespans of 15-20+ years. This legacy equipment predates current IT practices, but increasing interconnection between IT and OT continues unabated. Within devices themselves, and on the network level, finding the right balance between tightening security and ensuring the necessary availability is paramount in the convergence of IT and OT. Security personnel and OT equipment operators face challenges for securing their equipment, whether it is OT-, IT- or IoT-connected devices. These challenges include:

Necessity for Continual Uptime and Safety Considerations

OT equipment downtime can result in lost production, disgruntled customers and regulatory fines. Machines must reach a high OEE (overall equipment effectiveness) that doesn't allow time for IT-style updates and patches that can take equipment offline. Plus, safety and security for employees and customers have always been top priorities in industrial and utility companies, causing them to become highly regulated fields. Security mandates with compliance requirements and fines, in the case of noncompliance, exist across most industries and agreed-upon standards must be met to help institutionalize best practices.

Lack of OT Asset and Network Activity Visibility

Operations staff in industrial environments suffer from a lack of visibility regarding OT, IT and IoT equipment. This highly regulated equipment is often connected and disconnected from the network. For example, many maintenance processes are still performed manually or performed as part of a maintenance agreement through their equipment vendors. With hidden or temporarily connected transient devices, such as service laptops, and externally generated network activity taking place, a constant potential threat level is present in the network that needs to be controlled.

Limited Network Access Restrictions and Segmentation Controls

Security practices for legacy OT equipment tend to focus on physical access restrictions rather than network access controls. Plus, the air gap formerly served as the ultimate segmentation from the business network, where most of the threat activity took place. Without proper network access controls and more fine-tuned network segmentation, bad actors face few restrictions that prevent them from traversing the network and reaching critical operations. Yet conversely, without the right intelligence to build context, controls and segmentation could unknowingly disrupt operations and challenge the availability mandate.

Addressing the Challenges: Forescout Technologies and Hirschmann, a Belden Brand

Forescout and Hirschmann are working together to deliver a new approach for network visibility and control in industrial networks. As devices connect to the network, Forescout sees the devices, profiles them and classifies them using non-disruptive methods. The platform serves as an overarching network access engine, assessing in real time multiple variables, such as the device identity, ownership/user, integrity and security posture. Forescout continues to monitor these devices as they repeatedly join and leave the network. Network access decisions are translated to detailed access and authorization instructions, enforced by Hirschmann devices on the plant floor and the network ingress points. Hirschmann is uniquely positioned to effectively enforce security within the unique constraints of an industrial environment while making sure that system availability is not compromised.

The Forescout/Hirschmann Integration Provides the Following Benefits

Solution Capability	Benefit
Hirschmann and Forescout Interoperability	**Leverage a trusted partnership.** Multiple Hirschmann Layer 2 and Layer 3 switch models have been tested for interoperability and certified with the Forescout platform. Products that are designed for use in harsh environmental conditions, such as the OCTOPUS switch series or the MACH family of ruggedized switches and routers, can be auto-discovered, and device intelligence and context can be shared with the Forescout platform to build a comprehensive security foundation. This includes the latest HiOS operating system and the Classic Switch Software OS to ensure full compatibility throughout the entire Hirschmann device portfolio, ranging from the Classic Basic Rail Switch RSB to the HiOS Industrial Backbone Switch/Router Dragon MACH 4000.
Non-Disruptive Asset Discovery	**Discover and secure unknown devices** on the network that cannot be outfitted with software agents using non-disruptive methods to preserve maximum uptime. Forescout doesn't require endpoint agents to discover, classify and assess devices or to determine security compliance status. Appropriately apply network access control based on security policies to enforce controls and remediation on selected IT devices in OT environments.

Solution Capability	Benefit
Continuous Asset Monitoring	**Stay continuously apprised of device status and compliance.** Forescout continuously discovers and monitors device behavior and compliance status of industrial assets as reported through Hirschmann switches and routers as devices come and go from your network. This real-time activity monitoring helps to maintain a continuous security posture and accurate asset inventory.
Network Access Control with or without 802.1X to Drive Secure Remote Access Adoption	**Manage the secure access** to corporate, employee-owned and IoT devices, as well as those belonging to contractors, vendors and service providers. Control access to confidential data by making network access and dynamic authorization decisions based on device and user profiles, location of connectivity, device integrity and security posture.
Orchestrate Information Sharing and Workflows as Designed by Policy	**Make existing security investments work better.** Forescout orchestrates information sharing and policy-based security enforcement operations with leading IT security and management products, including Tripwire IP360, to accelerate threat response. Correlate Forescout's industrial device intelligence with Hirschmann's network intelligence to better understand the potential impact of a given event.
Heterogeneous Device Interoperability	**No problem with vendor lock-in.** Forescout and Hirschmann work in environments with a mix of networking platforms, including wired, wireless and virtualized networks—all with consistent coverage and a single management console.

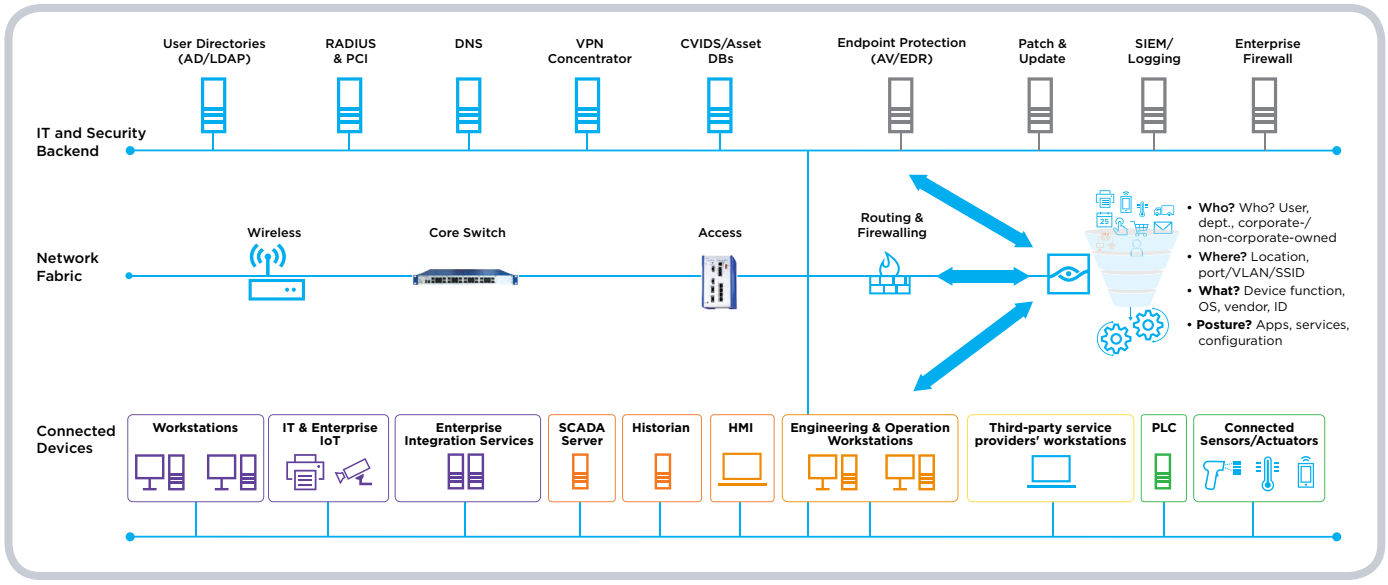


Figure 1. Application of Hirschmann switches and routers with Forescout

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

Addressing Best-in-Class Configuration Baselining: Forescout and Tripwire

Tripwire

Tripwire IP360 is an enterprise-class vulnerability management solution designed for large, complex network environments. New challenges for vulnerability management programs, such as achieving full network visibility and meaningful scoring, are met with this powerful, highly scalable solution.

https://www.tripwire.com/products/tripwire-ip360/

Forescout Platform

Forescout is the visibility platform that provides insight into virtually any connected device across your extended enterprise, and gives you a single-pane-of-glass perspective.

https://www.forescout.com/wp-content/uploads/2018/09/Forescout-CounterACT-DataSheet.pdf

Summary

This joint effort by Belden and Forescout illustrates how current security principles can enable network security in mission-critical installations without compromising either security or availability. Through a meaningful and efficient combination of technical features on different levels, such as the integration of Hirschmann-branded Industrial Ethernet switches and IP routers with the industry-leading Forescout network access control software, advanced security mechanisms are enabled throughout the entire network infrastructure.

Next Steps

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 or follow us on Twitter @BeldenInc.

About Forescout

Forescout Technologies is transforming security through visibility, providing continuous, agentless visibility and control of traditional and IoT/OT devices the instant they connect to the network. Forescout technology works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. See devices. Control them. Orchestrate system-wide threat response. Learn how at www.forescout.com.

Learn more at
www.Forescout.com

FORESCOUT

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