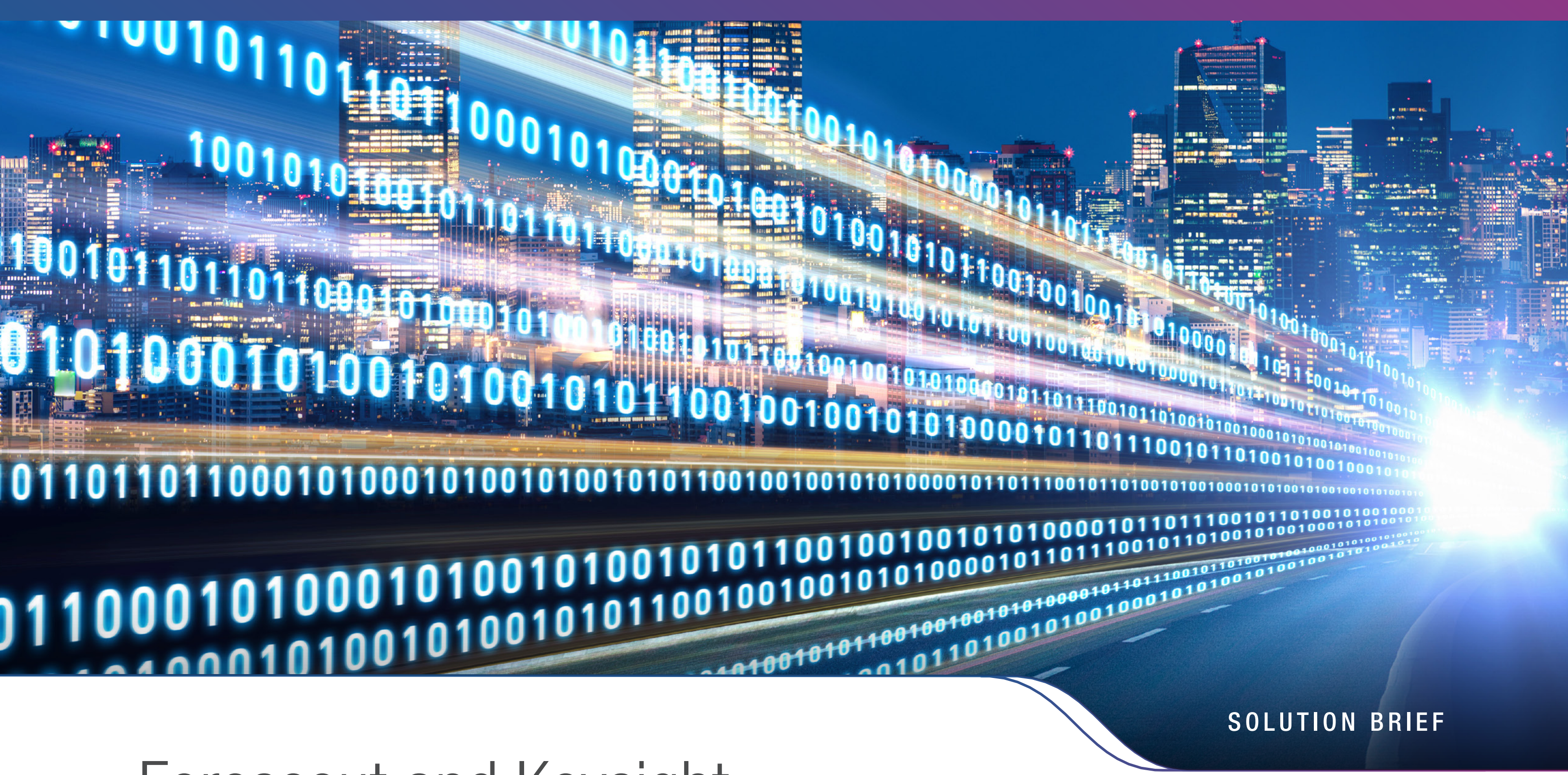


SOLUTION BRIEF

Forescout and Keysight: Securing OT and ICS Deployments

Information Technology (IT) has always been the nexus of change within enterprise networks, and enterprises themselves. While traditionally isolated from the outside world, increasingly Operational Technology (OT) and Industrial Control System (ICS) networks are now interconnected to the IT Enterprise and more and more typical IT devices are deployed inside OT networks. As a result the cyber security attack surface has now grown beyond the IT/OT boundary.

At the same time OT devices are often much older than IT devices and are not compatible with the latest security agents or other techniques deployable into IT infrastructure. As such agentless and non-intrusive passive network monitoring approaches that are agnostic to the OT devices and operating systems are ideal.

The Forescout Platform combines passive and active discovery techniques to identify and assess any device and its network activity across all environments and all technologies – IT, IoT, and OT. This enables organizations to build a complete asset inventory, to perform security audits of all device types including legacy OT devices, and to continuously assets the risks to operational continuity.

Keysight taps and network packet brokers feed the Forescout Platform, allowing monitoring where the (legacy) network infrastructure can't enable traffic mirroring or where dedicated monitoring sensors cannot be deployed. Furthermore, Keysight visibility helps avoid blind spots, and monitoring bottlenecks.

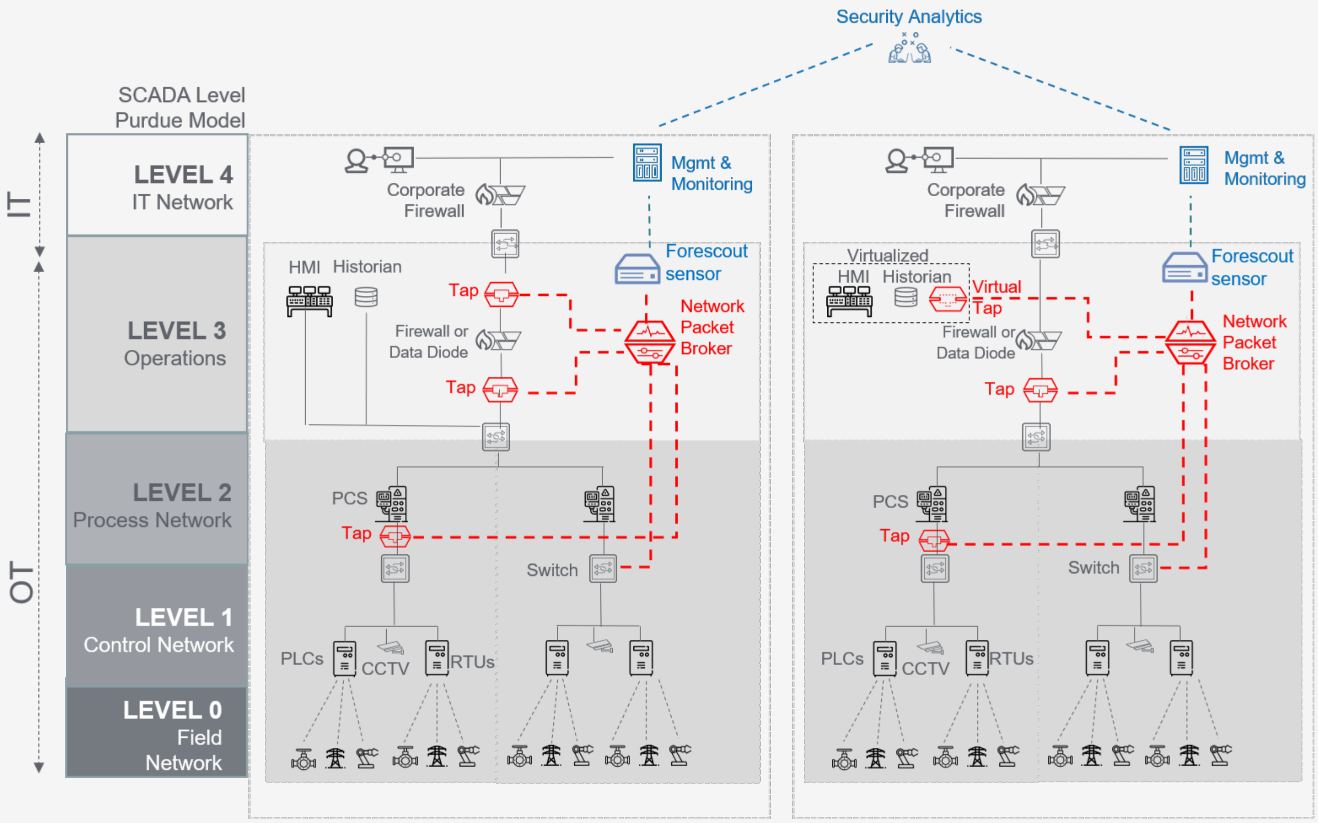
- Discovery, inventory, and secure audit of legacy OT assets
- Identification of rogue devices connected to the OT network
- Regulatory compliance to avoid fines
- Agentless deployment suitable for OT devices incapable of running agents
- Avoid physical and virtual blinds spots
- Filter out traffic not needed for security analysis (e.g. CCTV)
- Industrial Grade solution for harshest environments and compliance requirements.

FORESCOUT

KEYSIGHT TECHNOLOGIES

Forescout® enables better security and faster response times by allowing IT and OT security analysts to see and respond to devices the instant they connect to the network, and to continuously assess their behavior and risks. Forescout also provides OT process engineers more insights into the lower Purdue levels to detect network misconfigurations, operational errors as well as cyberattacks, so downtime can be avoided.

Keysight's deep network traffic and data visibility solutions combined with Forescout's rich device visibility helps ensure real time insight into the precise network data needed to assess operational and cyber risk and to take immediate mitigating actions. Together, the two solutions deliver intelligent visibility that enables a new caliber of network security.



Stronger Together: Complete Visibility into Security

Forescout and Keysight share a common belief that you cannot secure what you cannot see and that, as the number of devices connecting to your network grows, your attack surface grows right along with it. Together, Forescout and Keysight solutions provide security tools and teams with the complete visibility needed to make the right decisions as devices come online or are incompliant with security policies.

Forescout and Keysight have partnered to deliver reliable, automated network visibility and security controls that scale to meet the needs of the world's largest networks. The joint solution delivers real time visibility and automated control over users, devices, systems, applications, and virtual machines (VMs) accessing OT network resources and sensitive data.

This visibility into OT security operations makes it safer and easier to:

- Discovery and inventory known and unknown assets, including legacy OT devices
- Ensure continuous delivery of services and operations
- Safeguard sensitive data and systems
- Improve and demonstrate regulatory compliance
- Control access to critical networks and assets
- Manage assets including Rogue devices
- Detect network misconfiguration and operational errors
- Prevent operational impact due to ransomware, DDoS, or insider attacks

How It Works

Forescout equips security experts to automatically discover and assess devices as they connect or communicate on the network, and to continually monitor devices and their activity for as long as they stay connected. Forescout not only provides the required insights into devices, protocols, and risks, but also uniquely enables organizations to act upon these findings with advanced segmentation, network access control and incident response, leveraging built-in enforcement capabilities and a broad set of bi-directional integrations with existing security tools. The in-depth device visibility of IT, IoT and OT networks and devices offered by the Forescout Platform is key to enabling effective, real-time management of a full range of operational and cyber risks. The solution greatly enhances security and return on investment (ROI) compared with more siloed approaches to security management.

Customers credit Forescout solutions with:

- Providing complete device visibility and control over who can access resources
- Preventing malicious scanning, the spread of malware, misuse of assets, and time-consuming reconnaissance as well as downtime due to network misconfigurations or operational errors
- Enabling simple and non-disruptive Zero Trust across heterogeneous IT, OT and IoT networks

Forescout customers, on average, realize the following security benefits*:

24%
more known devices

18%
more devices in compliance

42%
reduction in network-related breaches

38%
reduction in device-related breaches

11%
more known devices

*According to an IDC report created after interviewing Forescout customers

The enhanced security and value achieved using Forescout begins with and relies upon accessing and analyzing data from the network. Keysight's network visibility solutions add the physical and virtual taps for capturing real-time traffic, and intelligent network packet brokers (NPBs) that aggregate, filter, and groom traffic for fast analysis by Forescout.

Using Keysight Taps and virtualization taps to access network data overcomes limitations that occur when switched port analyzer (SPAN) ports on network switches are used. As OT monitoring needs scale, there are rarely enough SPAN ports to go around, especially on legacy OT switches that lack SPAN support, which translates into dangerous visibility blind spots.

Providing complete, reliable access to network data, Keysight Taps prove vastly more scalable and reliable than using switched port analyzer (SPAN) ports on switches to gather traffic. Keysight offers a wide variety of taps to accommodate network speeds, interfaces, and security requirements; Industrial Grade taps suitable for deployment in the harshest environments, and virtual taps or vTaps for monitoring "east-west" traffic moving between VMs.

Together with Forescout, Keysight taps and NPBs deliver:

- World-class next generation network access control
- Complete asset discovery and inventory of OT, IoT and IT devices
- Automated compliance
- Advanced threat protection
- Best-of-breed operational efficiency

More About Forescout

Forescout Technologies, Inc. actively defends the Enterprise of Things by identifying, segmenting, and enforcing compliance of every connected thing. Fortune 1000 companies trust Forescout as it provides one of the most widely deployed, enterprise-class platforms at scale across IT, IoT and OT managed and unmanaged devices. Forescout arms customers with extensive device intelligence, data, and policies to allow organizations across every industry to accurately classify risk, detect anomalies and quickly remediate cyberthreats without disruption of critical business assets. Don’t just see it. Secure it.

Learn how at www.Forescout.com.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus