



Secure IT, OT, and ICS Environments with Keysight and Forescout

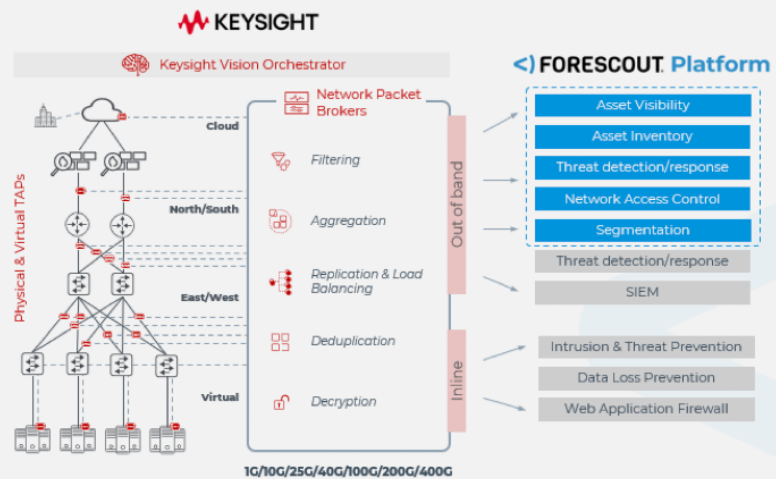
Joint Solution Highlights

- ▶ **Complete real time visibility** across IT, OT, IIoT and virtual/ cloud environments
- ▶ **Discovery, inventory, and secure audit** of all OT assets, including legacy ones
- ▶ **Identification of rogue devices** connected to IT/OT networks
- ▶ **Industrial-grade solution** for harsh environments and compliance requirements

IT and security operations (SecOps) teams need complete visibility and control to maintain uptime and streamline operations across interconnected technologies, remote access, and security operations. Deploying a Keysight network visibility platform with Forescout delivers:

- ▶ 100% visibility and complete access to traffic across enterprise IT, operational technology, industrial control system (ICS), and virtual/cloud environments
- ▶ Flexible scalability with matching network speeds and traffic relevance
- ▶ Optimal monitoring tool efficiency
- ▶ Resilience to ensure operational continuity

Deploying Keysight and Forescout Together



Keysight Delivers Analysis-ready Data

Keysight’s intelligent network visibility feeds the Forescout Platform a steady stream of reliable data, enabling efficient monitoring and analysis of traffic, even where legacy networks won’t support traffic mirroring or agent-based monitoring. Keysight physical (copper, fiber, industrial) and virtual taps capture traffic anywhere in the extended network and forward it to Keysight’s purpose-built network packet brokers (NPBs) for advanced processing and efficient delivery to Forescout.

Keysight NPBs aggregate and process traffic from multiple taps and switched port analyzer (SPAN) ports to eliminate 1:1 tool connections that fail to scale. Operating out of band, Keysight physical and virtual solutions reduce the strain on monitoring infrastructures by decrypting and pre-processing aggregated network traffic for analysis. Keysight NPBs:

- ▶ Capture all packet data for monitoring
- ▶ Aggregate tapped traffic needed for monitoring
- ▶ Filter out data and remove duplicates ensuring valuable packets are not dropped
- ▶ Replicate, load balance and deliver data required for analysis to the right tools
- ▶ Prevent failures to ensure business continuity

Keysight’s Vision Orchestrator (KVO) acts as the central point of management, automation, and orchestration of all Keysight visibility solutions to enable scale and industry-best ease of use.

Forescout Protects Every Connected Asset

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. Organizations can build complete asset inventories and perform security audits of all device types including legacy OT devices to continuously assess risk.

In addition to Forescout's governing capabilities, the platform automates security response and workflows along with the sharing of contextual data between systems. Real-time insight into devices, protocols, and risks equip organizations to respond to potential threats with advanced segmentation, new network access controls, and faster, more targeted incident response. Automation reduces the number of tools and analysts cycles needed to resolve incidents and issues before they turn into problems.

Joint Solution Benefits: End-to-End Visibility and Control

Combining Keysight visibility with the Forescout security platform lets analysts leverage network packets – the single source of truth – to investigate and document issues for routine reporting, compliance audits, detailed investigations, and cyber insurance requirements. Deploy Keysight and Forescout together to achieve:



100% visibility across IT, OT, and cloud environments

- ▶ Discovery, inventory, and control of all IP connected assets
- ▶ Identification of rogue devices connected to the network



Faster analysis, automated response

- ▶ Real-time insight into the precise network data needed to assess operational and cyber risk
- ▶ Automated mitigating actions



Streamline operations to improve tool performance and reduce cost

- ▶ Deduplicate and filter traffic not needed for analysis
- ▶ Optimize utilization of monitoring resources



Analytics to strengthen security and compliance

- ▶ Eliminate network and security blind spots
- ▶ Ensure continuity of services and operations

About Forescout

Forescout Technologies, Inc., a global cybersecurity leader, continuously identifies, protects and helps ensure the compliance of all managed and unmanaged connected cyber assets – IT, IoT, IoMT and OT. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide vendor-agnostic, automated cybersecurity at scale. The Forescout® Platform delivers comprehensive capabilities for network security, risk and exposure management, and extended detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats to critical infrastructure. Forescout products directly leverage this research, which is also shared openly with vendors, agencies, and other researchers.



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](https://www.forescout.com)

©2024 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc.

is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trade-marks>. Other brands, products, or service names may be trademarks or service marks of their respective owners. 01_01