Forescout® and Keysight: Securing the Internet of Things (IoT) the Moment Devices Connect

The Internet of Things (IoT) has ushered in a relentless flurry of devices connecting to public and private networks: Patient monitors in healthcare facilities. Connected cars in major cities. Tablets, smartphones, and laptops as patrons visit office buildings, hospitals, airports, coffee shops, and a host of other business locations.

Verizon’s State of the IoT Market 2017 Report proclaimed 8.4 billion connected devices—a 31 percent increase over 2016—and that $2 trillion would have been spent on IoT technologies by the end of 2017. This exploding number of connected devices makes it more challenging than ever to thwart ransomware, viruses, phishing, and “insider” attacks before they can compromise networks and data.

Forescout helps promote better security and faster response times by allowing information technology (IT) teams to see and respond to devices the instant they connect to the network, and continually as the devices stay connected. Keysight’s deep network traffic and visibility data solutions combine with Forescout’s rich device visibility to ensure real time insight into the precise network data needed to assess risk and take action. Together, the two solutions deliver intelligent visibility that enables a new caliber of network security.

“Forescout provides JPMorgan Chase with enhanced visibility and control across the hundreds of thousands of devices connected to our corporate network. Forescout’s technology also helps us automate and dynamically enforce security policies across our environment.”

Robert Amin, Global Chief Information Security Officer, JPMorgan Chase & Co.
Stronger Together: Complete Visibility into Security

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

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 data centers. The joint solution delivers real-time visibility and automated control over users, devices, systems, applications, and virtual machines (VMs) accessing network resources and sensitive data.

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

- Extend or migrate services to new locations or the cloud
- Ensure continuous delivery of services
- Safeguard sensitive data
- Improve and demonstrate regulatory compliance
• Deliver secure guest access
• Manage assets
• Prevent operational impact due to ransomware, DDoS, or insider attacks

How It Works

Forescout equips security experts to automatically discover, classify, and assess devices as they connect to the network; and to continually monitor devices for as long as they stay connected. The Forescout solution allows users to automate a broad range of access controls and responses—such as: segment, quarantine, block, remediate—based on company-designed and/or pre-built security policies. Forescout’s agentless approach to orchestrated, system-wide visibility and responses greatly enhances security and return on investment (ROI) compared with more siloed approaches to security management.

Customers credit Forescout solutions with:

• Providing endpoint visibility of network and control over who can access resources
• Preventing malicious scanning, the spread of malware, misuse of corporate assets, and time-consuming reconnaissance
• Preventing computers that may have an exploit from obtaining IP addresses and connecting to the company network

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

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>More known devices</td>
<td>24%</td>
</tr>
<tr>
<td>More devices in compliance</td>
<td>18%</td>
</tr>
<tr>
<td>Reduction in network-related breaches</td>
<td>42%</td>
</tr>
<tr>
<td>Reduction in device-related breaches</td>
<td>38%</td>
</tr>
<tr>
<td>More known devices</td>
<td>11%</td>
</tr>
</tbody>
</table>

*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 or cloud. Keysight’s network and cloud visibility solutions add the physical and virtual taps for capturing near real time traffic; and intelligent network packet brokers (NPBs) that aggregate, filter, and groom traffic for fast analysis by Forescout.
Using Keysight Flex Taps to access network data overcomes limitations that occur when switched port analyzer (SPAN) ports on network switches are used. As data centers scale, there are rarely enough SPAN ports to go around which translates into dangerous visibility blind spots.

Feeding network data gathered by taps (and SPAN) to Keysight’s Vision series of NPBs before sending it to Forescout for analysis provides automatic removal of duplicate packets, masking of sensitive data, SSL decryption, header-stripping, and other advanced functions that ensure exactly the right data gets delivered to exactly the right tools in real time, every time.

Keysight packet brokers are renowned for industry-best ease of use, true application intelligence, and ultra-reliable performance while performing advanced functions (such as deduplication) at high speeds. Together with CounterACT, Keysight taps and NPBs deliver:

- World-class network access control
- Flexible mobile security
- Automated endpoint compliance
- Advanced threat protection
- Best-of-breed operational efficiency

**About Forescout**

Forescout Technologies is transforming security through visibility, providing agentless visibility and control of traditional and IoT/OT devices the instant they connect to the network. Our 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 systemwide threat response.


---

**Learn more at: [www.keysight.com](http://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](http://www.keysight.com/find/contactus)