ForeScout Delivers New Splunk Integration for Faster Incident Response

- *New integration helps customers improve security posture while optimizing existing investments to minimize impact of malware and data breaches*
- *Bi-directional communication between ForeScout and Splunk solutions enhances real-time visibility, improves incident prioritization and automates response*

SAN JOSE, Calif., January 5, 2017 - ForeScout Technologies, Inc., a leading Internet of Things (IoT) security company, today announced a new Splunk integration to enable improved network visibility and the ability to take automated, policy-based actions on correlated data for a stronger security posture. The ForeScout Extended Module for Splunk enables bi-directional communication between ForeScout CounterACT® and Splunk® Enterprise or Splunk Enterprise Security (Splunk ES) to help organizations accelerate incident response and minimize the impact of data breaches.

"CISOs are deploying new security solutions at lightning speed to stay ahead of emerging threats resulting in a greater need for orchestration and information sharing among these technologies," said Michael DeCesare, president and CEO, ForeScout. "Through our collaboration with Splunk and agentless approach to visibility, ForeScout streamlines security operations and reduces the window of exposure to limit malware proliferation and data exfiltration from devices on the network."

ForeScout's integration with Splunk Enterprise and Splunk ES enables customers to leverage high-value, up-to-date context for all IP-connected devices from ForeScout for incident correlation and prioritization. The increasing volume of IoT devices connecting to the network has created new windows of opportunity for today's cybercriminals to enter an organization. ForeScout scans these connected devices in real time, sends the detailed device context to Splunk solutions for analysis and correlation, and quickly isolates non-compliant, infected and suspicious devices. Splunk ES users can then automate actions via ForeScout to respond to attacks for threat mitigation. This integration was developed in conjunction with Splunk's Adaptive Response Initiative, a best-of-breed security collective that leverages end-to-end context and automated response to help organizations better combat advanced attacks through a unified defense.

"To help stay ahead of advanced threats, Splunk customers rely on technology that enables an analytics-driven approach to security and automates the incident response process. The Adaptive Response Initiative, and collaboration with partners like ForeScout, helps break down the silos between what are typically disparate security systems to provide our customers with faster threat investigation and remediation," said Doug Merritt, president and CEO, Splunk.

Customers gain improved correlation and incident prioritization based on ForeScout data such as:

- Real-time and continuous inventory of IP-connected devices on the network—from traditional PCs, servers and mobile devices to Bring Your Own Devices (BYOD) and IoT;

- Device profiling and classification information;
- Device security posture and compliance gaps, and
- Network authentication, access and location information.

Customers can initiate closed loop remediation and threat mitigation leveraging Adaptive Response in Splunk ES and ForeScout actions to:

- Enable Splunk software to delegate alert mitigation actions in real-time;
- Take network actions to quarantine, isolate or limit access of IP-connected devices;
- Initiate remediation and threat mitigation actions on a broader range of devices, and
- Orchestrate a set of actions across multiple products in response to alerts from Splunk solutions.

Supporting Quotes:

"As a current ForeScout and Splunk customer, we look forward to the integration as it will mean bi-directional communication between both solutions and accelerated incident response for our business. The threat landscape continues to become more sophisticated and there is an extreme amount of value to be gained with a combined security solution and a strategic partnership between ForeScout and Splunk."

- Tim Callahan, SVP and Global Chief Security Officer, AFLAC

"The integration between ForeScout and Splunk adds tremendous value by illuminating blind spots in a network security posture. ForeScout assesses devices for policy-based compliance, and Splunk mitigates cybersecurity risk through operational intelligence. The combination of these two powerful technologies will offer enterprises comprehensive threat detection and mitigation paired with an automated and appropriate incident response."

- **Christopher Kissel, senior industry analyst, Information and Network Security, Frost & Sullivan**

About ForeScout Technologies, Inc.

ForeScout Technologies, Inc. helps make the invisible visible. Our company provides Global 2000 enterprises and government entities with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology integrates with disparate security tools to help organizations accelerate incident response, break down silos, automate workflows and optimize existing investments. Learn more at www.forescout.com.

© 2016. ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, ControlFabric, CounterACT Edge, ActiveResponse and CounterACT are trademarks or registered trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners.

Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Media Contact
Katie Beck
ForeScout Technologies, Inc.
Katie.beck@forescout.com
650-314-8705