ForeScout

splunk>

Smart Transportation

Driving innovation and security through collaboration

Organizational Challenges

- Improve transportation safety and efficiency
- Securely embrace IoT and smart vehicle innovations
- Leverage existing network security investments
- Maintain resiliency and availability of critical services
- Comply with current regulatory mandates and anticipate future requirements
- Protect sensitive systems and data

Technical Challenges

- Discover unknown devices such as IoT sensors that do not include security software
- Ensure security software is up to date on endpoints
- Classify endpoints and determine their owners
- Scale to address rapid growth, distributed networks and smart transportation operations centers
- Assess and continuously monitor endpoints
- Correlate and analyze data to detect anomalous behavior
- Prevent infected or non-compliant endpoints from spreading malware across networks

Transportation systems worldwide are ripe for a major overhaul. Increasing populations, congestion and pollution must be countered with efficient, environmentally friendly modes of transport and transportation hubs, and security must be part of the solution. Together, ForeScout Technologies and Splunk Inc. are offering intelligent security solutions today that are the foundation for tomorrow's smart—and secure—transportation systems.

Challenge: IoT and Cybersecurity

Smart transportation proponents envision efficient and sustainable intermodal transport systems and infrastructure that can deliver levels of intelligence and performance that make gridlock on roads and at airports and seaports a thing of the past. However, tomorrow's smart transportation systems will be made possible through the integration of countless devices, networks and other key infrastructure, *all of which must be secured*. Otherwise, one rogue device or errant application can wreak havoc.

In fact, *every* device or sensor that connects to the network broadens the attack surface, creating a potential entry point for cybercriminals to hack to or hack through. Without advanced cybersecurity, unauthorized access to critical systems, information theft and malicious cyberactivity will thrive in the future's ultra-connected, highly automated and data-driven environment.

Smart devices and sensors, collectively known as Internet of Things (IoT) devices, are manufactured by multitudes of vendors who haven't put a premium on security. As a result, their products often feature few if any built-in management or security capabilities. And these highly vulnerable "Things" are already being exploited:

- On November 25th, 2016, the San Francisco Municipal Transportation Agency (MUNI) was hacked, shutting down ticketing systems and compromising more than 2,100 of the agency's computers as cybercriminals demanded payment of $70,000 in ransom, forcing the agency to operate free service for two days.[1]
- In 2014, a University of Michigan team accessed a traffic light network using readily available hardware. Once inside the system, the team quickly gained the ability to change traffic signals, alter logic commands and disable signal devices.[2]
- IoT devices can be hacked in as little as three minutes, but can take days or weeks to remediate.[3]

Moving forward, the big question for smart transportation system planners will be, Who is responsible when a device, network or infrastructure component is compromised? Sophisticated tools and wide-ranging expertise will be required in order to ensure that responses to attacks are appropriate, immediate and effective.

> 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."
>
> **— Splunk President and CEO Doug Merritt**

Challenge: Rapid Incident Analysis and Response

The digital transformation required for smart transportation will result in vast amounts of data being generated by new devices—data that must be correlated, analyzed and acted upon in near real time. New levels of system orchestration and automation will be needed to bridge data silos and allow analysts and interconnected systems to quickly respond to security incidents, accidents, weather events, changing traffic flows and other unanticipated factors that impact smart transportation systems. Traffic operations teams will need this data to understand both short- and long-term trends, event relationships and consequences. In addition, they will need to continuously monitor and analyze security events and device behavior. This can help prevent cybercriminals from hacking through video cameras, printers or other IoT devices to steal data or wage distributed denial of service attacks on the network.

The ForeScout-Splunk Solution

Transportation system administrators and planners face constant threats as new types and higher volumes of devices increase the complexity and expand the attack surface of their networks.

To address these formidable challenges, ForeScout CounterACT® offers agentless visibility, continuous monitoring, access control and automated response over wired *and* wireless networks. Furthermore, the ForeScout Extended Module for Splunk enables bi-directional integration of CounterACT with Splunk Enterprise and Splunk ES—adding Splunk's powerful correlation, analysis and search features to the mix. This can help security teams correlate data and events in transportation operations centers, improve security, better-manage traffic flow and optimize smart vehicle management and maintenance.

ForeScout and Splunk customers can also leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation. The result is enhanced threat insight, analytics-driven decisions and greater operational efficiency.

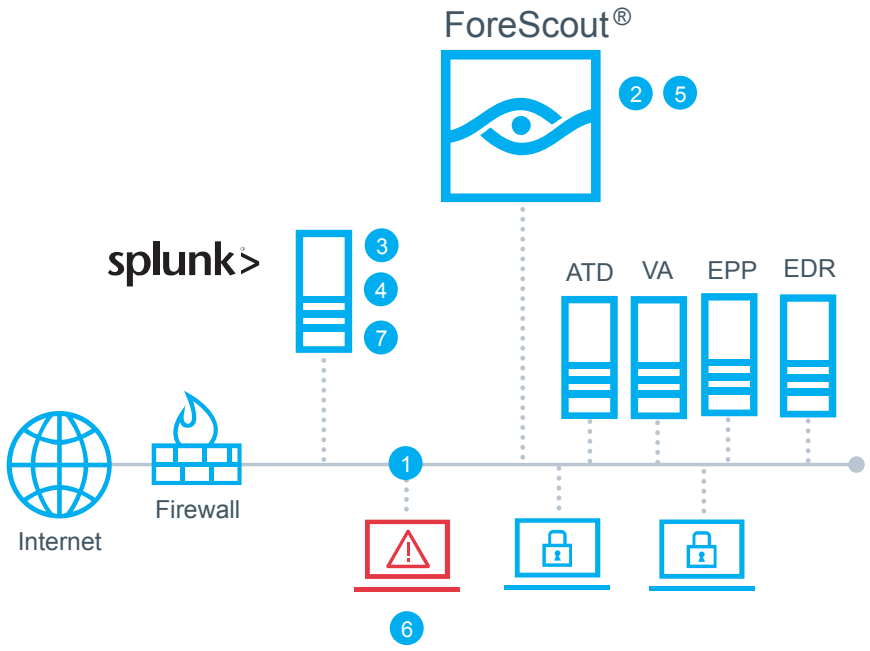
Joint ForeScout-Splunk solutions can protect sensitive systems and data while preventing infected or non-compliant devices from spreading malware. What's more, they deploy quickly with minimal disruption to users, work with new and existing infrastructure and enhance the effectiveness of tools that public- and private-sector IT teams already use. Equally important, they scale, as proven by ForeScout CounterACT deployments in networks exceeding 1,000,000 endpoints.

> 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 President and CEO Michael DeCesare**

Benefits

With ForeScout and Splunk, security teams can:

- Store CounterACT data in Splunk solutions for long-term trend analysis, visualization and incident investigation
- Identify anomalous behavior and events based on CounterACT data
- Correlate high-value endpoint context from CounterACT with other data sources to identify and prioritize incidents
- Initiate CounterACT network and host actions from Splunk to automate incident response, remediation and threat mitigation
- Comply with log retention mandates and other regulatory requirements
- Optimize the management and maintenance of vehicles, fleets and myriad digital assets



1. CounterACT discovers, classifies and assesses devices as they connect to the network
2. CounterACT sends up-to-date device context to Splunk for long-term storage and correlation, including device connection, classification and compliance information
3. ForeScout App for Splunk visualizes CounterACT data for trend analysis, monitoring and reporting
4. Splunk leverages device context from CounterACT and correlates with other data sources to identify and prioritize incidents
5. Using Splunk, automate or manually initiate adaptive response actions using CounterACT based on the severity and nature of the alert
6. CounterACT triggers policy-based mitigation and remediation actions on non-compliant, vulnerable or suspicious endpoints and reports action status back to Splunk
7. Splunk Enterprise operators can review response action status and results using the ForeScout App. Splunk ES customers can see the complete alert and response action lifecycle in the Alert Mitigation Center.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] *Forbes*, November 28, 2016 https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/#5ebc65947061
[2] "The Future of Smart Cities: Cyber-Physical Infrastructure Risk," U.S. Dept. of Homeland Security, August 2015
[3] How Hackable Is Your Smart Enterprise, https://www.forescout.com/wp-content/uploads/2016/10/iot-enterprise-risk-report.pdf

*As of March 31, 2017