Solution Brief

# ForeScout Extended Modules for SIEM

## Improve real-time visibility over managed and unmanaged devices while automating network access control and threat response

### Highlights

**See**

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor managed devices, including corporate, BYOD and IoT endpoints

**Control**

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints as determined by your SIEM product
- Improve compliance with industry mandates and regulations

**Orchestrate**

- Share contextual information with your SIEM product and proactively take appropriate action
- Automate common workflows, IT tasks and security processes across systems
- Leverage the integration between ForeScout and your SIEM product to provide real-time view of threats across the enterprise

### ForeScout Extended Modules for SIEM Systems

ForeScout CounterACT® is a network security appliance that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices and works with ForeScout ControlFabric® Architecture and ForeScout Extended Modules for SIEM to orchestrate information sharing and automate operation among disparate security and IT management tools, including Security Information and Event Management (SIEM) systems.

The combination of CounterACT and a SIEM can result in a significant increase in situational awareness and proactive risk reduction. Where most SIEM solutions offer situational awareness primarily through the collection of periodic log entries from many different products, they typically do not provide in-depth, real-time endpoint data visibility. What's more, SIEMs are only as good as the information that is fed into them, and if the SIEM is not aware of all network endpoints on a continuous basis, then it is not able to produce an accurate security snapshot of your network. This gap in endpoint visibility exists in SIEMs without CounterACT. However, by discovering network endpoints and feeding that data into the SIEM, CounterACT closes the endpoint visibility gap in your situational awareness.

The combination of CounterACT and some SIEM systems also provides enforcement capabilities that the SIEM alone lacks. For example, a compatible SIEM system can send commands to ForeScout CounterACT to automatically update an endpoint's operating system, disable a USB device, or quarantine an endpoint.

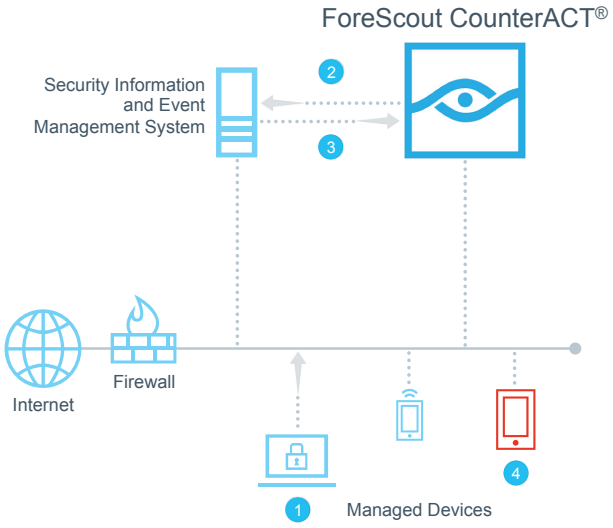
### The Challenges

**Visibility.** According to industry experts, the vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. However, most organizations are unaware of a significant percentage of the endpoints on their network because they are either not managed, Bring Your Own Device (BYOD), guest or Internet of Things (IoT) devices. Also, they may have disabled or broken agents, or are transient devices that aren't detected by periodic scans. As such, you are unaware of the attack surface on these devices.

**Threat Detection.** Today's cyberthreats are more sophisticated than ever before and can easily evade traditional security defenses. Multivectored, stealthy and targeted, these attacks are focused on acquiring sensitive personal information, intellectual property or insider information. Compromised endpoints and data breaches can often remain undetected for weeks or months. To detect these advanced threats, zero-day attacks and infected endpoints, you need next-generation security controls that do not rely on signatures.

**Response Automation.** The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating the perfect storm for IT security teams. Without an automated system to continuously monitor and mitigate endpoint security gaps, valuable time is lost performing these tasks manually. And without the ability to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyberthreats to propagate within your network and exfiltrate data.

1. An endpoint attempts to connect to the network. ForeScout CounterACT is immediately aware of it.
2. CounterACT informs the SIEM system of endpoint status.
3. CounterACT receives instruction from the SIEM system assessment of the endpoint based on events and logs collected.
4. CounterACT allows or denies access based on compliance assessment




## Supported SIEMs

SIEMs that are currently supported by ForeScout Extended Modules for SIEM are:

- HPE ArcSight
- IBM QRadar
- Splunk
- Any SIEM that supports configurable messages in CEF, LEEF or plain Syslog

Note that different SIEM products have different capabilities in terms of correlating the data provided by CounterACT with data provided from other sources. Also, SIEM products vary in their ability to send triggers to CounterACT. For example, some SIEM products provide both manual and automated ways to trigger CounterACT to take action on an endpoint. For a more complete description of the features available with each specific SIEM product, talk with your SIEM vendor.

For details on our licensing policy, see www.forescout.com/licensing.

Learn more at
**www.ForeScout.com**

## How Extended Modules for SIEM Work

The combination of ForeScout CounterACT and an Extended Module for SIEM provides a SIEM system with real-time information, including data about managed (company-owned) and unmanaged (BYOD, IoT and rogue) mobile devices as they connect to the network. The SIEM can correlate this information with real-time information provided from other sources. Through this correlation, your SIEM can identify the threats that pose the greatest risk.

With Extended Modules for SIEM, CounterACT can notify your SIEM of endpoint system changes, the presence and activity of endpoint security agents, and logging applications and services. The SIEM's correlation engine can elevate the priority of an identified threat based on the type of threat reported and the severity of the threat based on other issues that have been reported. The SIEM console provides continuous monitoring and support mitigation of enterprise-wide threats that can originate from non-compliant endpoints by department or organization. The SIEM can also generate compliance reports for the entire organization or by business unit in order to meet regulatory requirements.

Extended Modules for SIEM are optional plug-ins for ForeScout CounterACT and are sold separately. When used in conjunction with existing SIEMs, ForeScout CounterACT and these Extended Modules provide automation for daily tasks while providing a dynamic threat detection approach to security that assures compliance and reduces the attack surface of your network.

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
**Fax** 1-408-371-2284