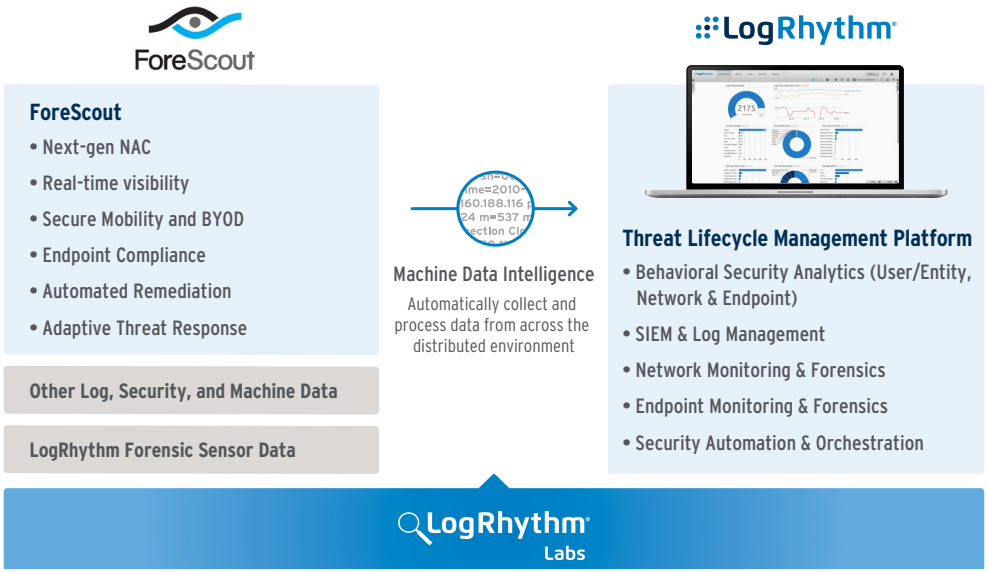
LogRhythm and ForeScout CounterACT™: Integrated Enterprise Security

LogRhythm and ForeScout offer an integrated solution for comprehensive enterprise security intelligence and threat management. With the rapid expansion of the mobile workforce, organizations are increasingly at risk from a multitude of attacks that specifically target the endpoint. ForeScout CounterACT™ detects, monitors and controls devices, operating systems, applications and users connecting to an enterprise network, including unauthorized devices and BYOD endpoints owned by employees, guests and contractors. LogRhythm's award winning Threat Lifecycle Management Platform combines this enhanced real-time endpoint visibility with extensive, real-time forensic data to perform host, user, network and endpoint behavior analytics, providing real-time cyber threat protection and continuous compliance enforcement.

LogRhythm and ForeScout allow users to monitor and secure systems and applications across their organizations.

The integration delivers:

- Deep visibility into the activities of an extensive array of mobile and BYOD endpoints by integrating LogRhythm machine analytics and search analytics with ForeScout CounterACT's continuous endpoint monitoring and mitigation.
- The ability to investigate suspicious events by drilling down into rich endpoint logs and pivot into other sets of logs that might unmask a wider attack.
- Dynamic enforcement and risk mitigation via LogRhythm's out-of-the-box compliance automation modules and ForeScout CounterACT's endpoint remediation and quarantine capabilities to automatically detect and respond to security threats, compliance risks and policy violations.



About LogRhythm

- Empowers organizations to rapidly detect, respond to and neutralize cyber-threats
- Provides a holistic platform for end-to-end Threat Lifecycle Management, uniquely unifying next-gen SIEM, log management, network & endpoint forensics, advanced behavior analytics & machine learning, and security automation and orchestration
- Delivers rapid compliance automation and assurance, and enhanced IT intelligence
- Consistent market leadership including recognition as a Leader in Gartner's Magic Quadrant since 2012

About ForeScout

- Enables organizations to continuously monitor and mitigate security exposures and cyber-attacks
- CounterACT™ appliances dynamically identify and evaluate network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security problems
- Open ControlFabric™ architecture allows a broad range of IT security products and management systems to share information and automate remediation actions
- Chosen by the world's most secure enterprises and government agencies due to solutions that are easy to deploy, unobtrusive, extensible and scalable

LogRhythm and ForeScout are tightly integrated, combining the value of ForeScout's next-generation network access control and endpoint compliance with the capabilities of LogRhythm's Threat Lifecycle Management Platform. The combined offering empowers customers to detect and mitigate internal and external threats, identify behavioral anomalies, enhance security, and enforce compliance.

LogRhythm for Integrated Enterprise Security Intelligence

- Dynamic defense for detecting and stopping unauthorized network threats
- Multi-dimensional behavioral analytics to deliver real-time security intelligence
- Deep visibility into all aspects of user, network and endpoint behavior activity throughout the IT environment
- Tight integration for consolidated threat management

Quarantine Host in Suspected APT

Challenge:
Many advanced attacks take advantage of trusting users by embedding malicious code in attachments that otherwise seem legitimate. BYOD systems are particularly vulnerable, as they frequently fall outside of the protection of many corporate security platforms.

Solution:
LogRhythm receives detailed endpoint intelligence from ForeScout and correlates it against other environmental log and event data to create baselines for what should be considered normal behavior. This enables highly focused alerts to identify suspicious activity occurring at the endpoints for immediate detection and response.

Additional Benefit:
Organizations can build a LogRhythm SmartResponse™ plug-in to initiate an automated response to any suspicious activity or behavior pattern by instructing ForeScout to quarantine the endpoint until the account can be validated. The quarantine action can be fully automated or subject to multiple levels of approval.

Control Unauthorized Access

Challenge:
The lack of good information about what constitutes normal behavior for a mobile workforce can make it difficult to detect when a user is logging in from a suspicious location or device. This makes it particularly difficult to detect threats such as a stolen user credentials being used to penetrate a network's traditional defenses.

Solution:
ForeScout can detect information, such as device type and operating system, for any device attempting to access the network. LogRhythm, using AI Engine's behavioral profiling, can then detect when a user's account doesn't match a hardware or OS profile, potentially identifying when an attack using stolen credentials is occurring.

Additional Benefit:
Organizations can develop a LogRhythm SmartResponse plug-in to automatically initiate a device quarantine with ForeScout through an integrated process in response to any alarm. SmartResponse could also take additional actions, such as adding a specific user or device to a watch list for higher priority alerts.