Automating Log Management, Compliance and Incident Response Processes

Joint Solution Brief

ForeScout + LogLogic

ForeScout and LogLogic have partnered to alleviate log management deployment and maintenance complexity while at the same time deliver greater network access and log management assurance. With this joint solution, you can lower SIEM / log management administrative costs, respond to preempt access threats, and maintain access and endpoint compliance audit records for compliance and forensic processes. The result increases actionable security intelligence and operational efficiency.

Challenge: SIEM / Log Management Assurance

The foundation of any security and compliance program is Security Information Event Management or Log Management. You can only measure and respond to what you can see and know. As a best practice and to meet numerous compliance mandates, all business critical and compliance-relevant endpoints must have log software or services installed, initiated, configured and continually monitored. This requirement is challenging.

Challenge: Access Control and End Compliance

Do you have visibility, control and intelligence over all users and endpoints accessing your enterprise? Can you enforce policy for employees and guests using mobile devices? Can you enforce endpoint compliance on all virtual machines? How are you preempting access threats and enforcing endpoint compliance policy? Do you have all the necessary information to easily assess, validate and support control effectiveness?

Highlights

Simplify Logging Deployment and Maintenance

Dynamically check, install, reactivate and configure log application or services, by policy, on thousands of known and new endpoints.

Expedite Incident Response

Capture, centralize, retain and analyze network access violations, endpoint configuration issues and remediation events with ease and high performance.

Cost Savings

Save time and money through ForeScout automated SIEM / log management agent and application deployment capabilities. Streamline investigation and compliance processes with LogLogic’s flexible search and reporting capabilities.

Joint Solution Benefits

• Simplify deployment and reduce administrative effort to assure active log data collection
• Centrally aggregate, retain and analyze network access control and endpoint compliance information for incident response, compliance reporting and forensics processes
• Cost savings with regards to the deploy and operation of log collection applications / agent / services and the efficient retention and investigation of NAC event logs

Complexity. The multitude of access, configuration changes and threats can trigger a variety of controls and actions. Capturing and assessing the impact of related events is critical to support incident response and forensics, identify security gap and exceptions, and enable improvements.

Retention. Network and security infrastructure generate a tremendous amount of event log data. To support auditing and compliance mandates, this big data must be efficiently aggregated and stored in a manner that meets retention requirements while enabling effective analysis.

Simplifying Log Management Deployment and Operations

ForeScout’s automated security platform, ForeScout CounterACT™, lets you see and control everything connected to your network no matter the device or user. The solution simplifies deployment and on-going use of security information event management (SIEM) systems by facilitating activation and vigilant monitoring of all logging sources. ForeScout’s real-time endpoint classification, policy assessment and threat remediation capabilities offer the means for organizations to find and fix security issues associated with log management with little to no IT intervention. (see Figure 1) ForeScout’s multi-factor application fingerprinting identifies software installation, running services and processes, open ports and other criteria. ForeScout CounterACT can identify thousands of known and new endpoint devices, such as business critical servers and
virtual machines, as they connect to the network, and can dynamically:

- Check for the presence and activity of the LogLogic Lasso Enterprise ™ application or service
- Install or reactivate Lasso Enterprise with settings as per device type, configuration and location
- Enforce or change Lasso Enterprise settings according to pre-defined configuration policies (see Figure 2)

In addition to LogLogic Lasso Enterprise support, ForeScout now offers rich support for the popular SNARE (System Intrusion Analysis and Reporting Environment) open-source agents for Windows, UNIX, Solaris and other operating systems and applications that are employed by hundreds of thousands of organizations and leading SIEM vendors worldwide.

Managing Big Data and Enhancing Security Responsiveness

With Big Data, security and compliance issues proliferating, LogLogic continues to help companies with the most comprehensive solution for log and security intelligence. LogLogic’s architecture enables users to collect and analyze terabytes of big data generated by IT assets.

LogLogic’s Log and Security Intelligence platform offers enterprise-class log management infrastructure and analysis that enables customers to instantly collect (leveraging the industry leading Lasso Enterprise and Universal Collector), centralize, contextualize and consume their IT data in an easy-to-use and cost-effective manner.

LogLogic can capture, retain and analyze events generated from ForeScout CounterACT including real-time network access violations, endpoint compliance problems and mobile security issues, as well as ForeScout CounterACT’s policy-based threat mitigation.
Automating Log Management, Compliance and Incident Response Processes

ForeScout ControlFabric™
The integration between ForeScout CounterACT and LogLogic is just one of many IT system integrations that leverage the ForeScout ControlFabric architecture. ControlFabric is an open technology enabling ForeScout CounterACT and other solutions to exchange information and more efficiently mitigate a wide variety of security issues. Learn more at www.forescout.com/controlfabric.

Take the ForeScout Challenge
Let us know which ForeScout solution is right for you, and we’ll arrange a free on-site evaluation.

About ForeScout
ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyber attacks. The company’s CounterACT appliance dynamically identifies and assesses all network users, endpoints and applications to provide complete visibility, intelligence and policy-based mitigation of security issues. ForeScout’s open ControlFabric technology allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout’s solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.

LogLogic’s support for ForeScout CounterACT includes:
- ForeScout CounterACT CEF-formatted event logs are can be collected via Syslog directly from LMI appliances
- LogLogic can automatically identify ForeScout CounterACT event logs and apply available parsing rules
- LogLogic users can conduct RegEx search logs, use prebuilt message signatures and generate reports against retained CounterACT event logs
- LogLogic can retain all the event logs generated by ForeScout CounterACT for subsequent analysis (see Figure 5)

Learn more at www.forescout.com.