Solution Brief

McAfee ePolicy Orchestrator Platform and CorreLog SIEM Deliver Enhanced Compliance

CorreLog SIEM security integrated with the McAfee® ePolicy Orchestrator® (McAfee ePO™) platform

Organizations using the McAfee ePO security management platform can now extract more value from their security investment by using CorreLog's advanced real-time log management, multiplatform security correlation, and z/OS mainframe connectivity.

McAfee Compatible Solution

Correlog Server 4.1 and McAfee ePO platform 4.5 after 4.6

"CorreLog is the only product I have found that can monitor and correlate IBM mainframe z/OS events with events from the rest of the enterprise and have bidirectional support for McAfee's ePO [McAfee ePolicy Orchestrator software]. CorreLog's compliance suite also provides us the tools to make our mainframe compliant to new security audit requirements."

—Major US Retailer

Log messages originating from every imaginable device and application can flood your monitoring environment. As a result, security events and notifications may appear harmless when viewed independently. With limited resources, how do you correlate everything and keep track of the threats? How do you respond to breaches, compliance violations, or failed audits when they occur?

Collecting log data and presenting that data in a single, consolidated view is not revolutionary. However, CorreLog not only allows the user to take raw log data from disparate sources and apply logical correlation rules to that data, it also sends alerts, opens tickets, or takes action based on security or regulatory compliance rules. This is what separates CorreLog from others.

CorreLog helps administrators visualize the activity of users, devices, and applications to proactively meet regulatory requirements and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior, and policy violations by collecting, indexing, and correlating user activity and event data to pinpoint security threats. CorreLog enables organizations to respond quickly to compliance violations, policy breaches, cyberattacks, and insider threats.

CorreLog provides a built-in user activity monitor that tracks user activity independent of system type and event log information. This monitor allows more sophisticated intrusion detection as well as user anomaly detection in a consistent manner across multiple UNIX, Microsoft Windows, and z/OS operating systems, without reliance on external event messages.

Meet SIEM Requirements Set Forth by Compliance Standards

Are you concerned with meeting security information and event management (SIEM) requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, NERC, and others? This may seem like an alphabet soup, but it contains requirements enforced by regulatory agencies like the US Department of Homeland Security with penalties for noncompliance. With CorreLog and McAfee, your enterprise can achieve compliance with standards while ensuring secure transactions, database use, and Internet access. Threats are intelligently correlated and displayed on a single screen allowing for instant defensive and forensic action. Agents for network products as well as protocols from different manufacturers can all be customized into one secure application.

Security Computing Magazine
—May 2011
★★★★★

"The SIEM product from CorreLog provides organizations with an easy-to-implement, affordable log management and correlation system. This product consists of the CorreLog Server as the central point of management and a series of agents that can be deployed to Windows- and Linux-based machines.

We find this product to be a solid value for the money. The CorreLog SIEM package provides a lot of easy-to-use functionality at a reasonable price."

—Peter Stephenson
Security Computing Magazine
May, 2011

Integrated with McAfee ePolicy Orchestrator Platform Dashboards

CorreLog aggregates large amounts of log message data from a variety of sources. This data is then correlated with existing data in the McAfee ePO platform, as well as data within external data stores including Microsoft Active Directory. The correlated results are sent to McAfee ePO software and reports, providing detailed visibility into the current state of users, devices, and applications and enabling administrators for the McAfee ePO platform to respond with the right context required for each incident.

Roll-Up of CorreLog Data to McAfee ePolicy Orchestrator Software

The joint solution includes the capability for a CorreLog Server to send ticket (or alert) information to McAfee ePO software, allowing it to monitor critical SIEM events from within its dashboards and furnishing a single security console. This information consists of CorreLog "ticket," not raw message information, which will reside in the CorreLog console and not the McAfee ePO platform.

A key capability of the CorreLog integration is its ability to make the McAfee ePO platform aware of non-virus events, such as distributed denial-of-service (DDoS) attacks and invalid login attempts.

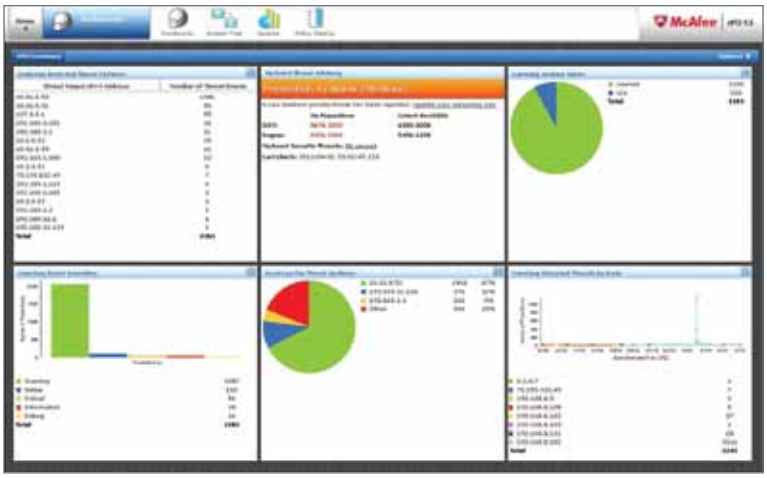

Figure 1. CorreLog SIEM events in McAfee ePO dashboards.

About CorreLog, Inc.

CorreLog, Inc. delivers SIEM combined with deep correlation functions. CorreLog is real-time SIEM software solution that automatically identifies and responds to network attacks, suspicious behavior, and policy violations. CorreLog collects, indexes, and correlates user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyberattacks, and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/ DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners worldwide. Visit www.CorreLog.com for more information.

About McAfee ePolicy Orchestrator Software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance. Visit www.mcafee.com for more information.

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

32300brf_correlog_0711_fnl_ASD