



March 17, 2014

## Fortinet Extends Security Incident and Event Manager (SIEM) Ecosystem: Includes AccelOps, IBM and LogRhythm

### Broad Ecosystem Gives Customers Extensive Choices for Proactive Alerting, Log Analysis and New Levels of Security Intelligence and Rapid Response

SUNNYVALE, CA -- (Marketwired) -- 03/17/14 -- Fortinet® (NASDAQ: FTNT) -- a global leader in [high-performance network security](#) -- today announced an expansion of its Security Incident and Event Manager (SIEM) ecosystem with AccelOps, IBM and LogRhythm. This ecosystem gives Fortinet customers and resellers a broad choice of solutions providers for delivering broad visibility into data center service availability, performance, security, change management and compliance. Fortinet's SIEM ecosystem is designed to address the unique requirements of a wide range of customers, from large enterprises to managed security service providers (MSSPs) that manage thousands of individual customer environments.

"AccelOps, IBM and LogRhythm expand upon and complement Fortinet's existing hardware and software portfolio, which includes the high-performance, enterprise-grade [FortiGate](#) platform as well as supporting [FortiManager](#) and [FortiAnalyzer](#) platforms," said John Maddison, vice president of marketing for Fortinet. "Our customers have indicated they wish to use these partner products in their IT environments, and today's announcement illustrates our ability to fulfill these customer requirements with a high level of integration and compatibility."

#### ***AccelOps (key strength: Monitors SIEM, performance and IT infrastructure availability on a single platform)***

AccelOps provides analytics-driven IT Operations Management that integrates SIEM, performance and availability of IT infrastructure and applications on a single platform. The AccelOps monitoring platform is built for highly dynamic and scalable virtualized data centers. It works across private and public clouds as well as traditional data centers to provide comprehensive service health visibility.

AccelOps' monitoring approach is anchored on patent-pending distributed real-time analytics technology that is extremely efficient at detecting patterns in high-volume IT events and data. Unlike software suites built from disparate applications, AccelOps offer a scalable, high-performance solution that spans server, storage, network, security user, and application domains across an entire infrastructure -- both physical and virtual.

"AccelOps' and Fortinet's combined offering gives businesses the ability to increase service reliability while improving their operational efficiency with a fully integrated data center monitoring solution," said Flint Brenton, president and CEO of AccelOps. "MSSPs need a broad, unified way to monitor, manage and optimize their IT services. AccelOps offers a scalable, high-performance monitoring platform that helps MSSPs reduce costs and improve overall security both in traditional data centers and the cloud."

#### ***IBM (key strength: Combines the power of QRadar SIEM with IBM Security X-Force Threat Intelligence)***

IBM Security QRadar Security Intelligence Platform consolidates log source event data and network flows natively from thousands of devices, endpoints and applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives. As an option, the software incorporates IBM Security X-Force Threat Intelligence, which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. IBM Security QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

Key features include near real-time visibility for threat detection and prioritization, delivering visibility across the entire IT infrastructure. It reduces and prioritizes alerts to focus investigations on an actionable list of suspected incidents. And it enables more effective threat management while producing detailed data access and user activity reports.

"The IBM QRadar Security Intelligence Platform enables Fortinet customers to perform immediate normalization and correlation activities on raw data to distinguish real threats from false positives," said Michael Loria, Vice President, Business and Corporate Development, IBM. "QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to better prioritize security incidents."

#### ***LogRhythm (key strength: Integrates SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Host and Network Forensics)***

LogRhythm's Security Intelligence Platform uniquely combines next-generation SIEM, log management, file integrity monitoring, network forensics and host forensics in a fully integrated solution that empowers organizations worldwide to detect breaches and today's most sophisticated cyber threats faster and with greater accuracy than ever before. LogRhythm also provides

unparalleled compliance automation and assurance as well as IT predictive intelligence to Global 2000 organizations, government agencies and mid-size businesses.

Key features include next-generation SIEM, log management; independent host forensics and file integrity monitoring; network forensics with application ID and full packet capture; state-of-the art machine analytics; advanced correlation and pattern recognition; multi-dimensional user /host /network/application behavior anomaly detection; large data set analysis through rapid, intelligent search, pivot, and drill down; analytics-driven countermeasures via LogRhythm's SmartResponse™; integrated case management; and management-level dashboards.

"LogRhythm's Security Intelligence Platform enables Fortinet customers to get broad, actionable insight into their environments and respond rapidly to potential threats," said Matthew Winter, vice president of business development, LogRhythm. "By integrating with Fortinet's NGFW, LogRhythm dramatically reduces the time needed to investigate and respond to suspicious behavior and advanced threats."

For more information on Fortinet's partner program please visit: <http://www.fortinet.com/partners/index.html>

### **About Fortinet**

Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at [www.fortinet.com](http://www.fortinet.com).

Copyright © 2014 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiAP, FortiDB, FortiVoice and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties, and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions, including statements regarding product releases and functionality. Changes of circumstances, product release delays, changes in product plans and other risks as stated in our filings with the Securities and Exchange Commission, located at [www.sec.gov](http://www.sec.gov), may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

### **Media Contact:**

Rick Popko  
Fortinet, Inc.  
408-486-7853  
[rpopko@fortinet.com](mailto:rpopko@fortinet.com)

### **Investor Contact:**

Michelle Spolver  
Fortinet, Inc.  
408-486-7837  
[mspolver@fortinet.com](mailto:mspolver@fortinet.com)

Source: Fortinet

News Provided by Acquire Media