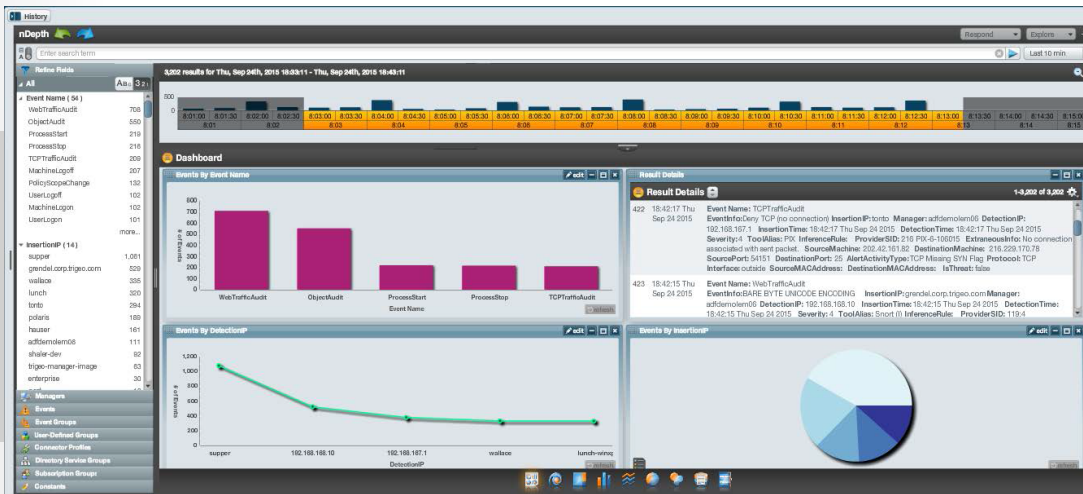




SOLARWINDS LOG & EVENT MANAGER DEMONSTRATE COMPLIANCE AND IMPROVE SECURITY



"Intuitive, easy to use interface that pulls all of the network enterprise data into meaningful and understandable information."

– Marie Karaffa, IT Director,
John Roberts Co.

Over 3500 resource-constrained security pros rely on SolarWinds Log & Event Manager for powerful, affordable, and efficient security information and event management (SIEM). Our all-in-one SIEM combines log management, correlation, reporting, file integrity monitoring, user activity monitoring, USB detection & prevention, threat intelligence and active response in a virtual appliance that's easy to deploy, manage, and use. We've designed our SIEM to provide the functionality you need without the complexity and cost of other enterprise SIEM solutions.

LOG & EVENT MANAGER AT A GLANCE

- » Collects, consolidates, and analyzes logs and events from firewalls, IDS/IPS devices and applications, switches, routers, servers, operating system logs, and other applications
- » Real-time correlation to identify attacks
- » Detect breaches with threat intelligence
- » Supports root cause analysis with built-in intelligence that applies to networks, applications, and security management
- » Blocks and quarantines malicious and suspicious activity, including inappropriate USB usage
- » Delivers deeper intelligence and broader compliance support through embedded File Integrity Monitoring (FIM)
- » Produces out-of-the-box compliance reports for HIPAA, PCI DSS, GPG 13, SOX, and more quickly and easily

FEATURE HIGHLIGHTS

Scalable and Easy Collection of Network Device, Machine, and Cloud Logs

Log & Event Manager collects and catalogs log and event data in real-time from anywhere data is generated within your IT infrastructure. Explore the supported data sources

Real-time, In-memory Event Correlation

By processing log data before it is written to the database, Log & Event Manager delivers true real-time log and event correlation, enabling you to immediately troubleshoot and investigate security breaches and other critical issues.

Threat Intelligence Feed

Leverage an out-of-the-box feed of known bad IPs to identify malicious activity. The feed regularly updates from a collection of research sources and automatically tags events as they enter the appliance. From there, you can quickly run searches or reports to view the suspect activity or create rules to perform automatic actions.

Advanced IT Search for Event Forensic Analysis

Log & Event Manager's advanced ad-hoc IT search capability makes it easy to discover issues using a drag-and-drop interface that tracks events instantly. You can even save common searches for easy future reference.

Log Data Compression and Retention

Log & Event Manager stores terabytes of log data at a high compression rate for compliance reporting, compiling, and off-loading—reducing external storage requirements.

Embedded, Real-Time File Integrity Monitoring

Embedded File Integrity Monitoring delivers broader compliance support and deeper security intelligence for insider threats, zero-day malware, and other advanced attacks.

Built-in Active Responses

Log & Event Manager enables you to immediately respond to security, operational, and policy-driven events using built-in active responses that take actions such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory® settings.

USB Detection and Prevention

Log & Event Manager helps prevent endpoint data loss and protects sensitive data with real-time notification when USB devices connect, the ability to automatically block their usage and built-in reporting to audit USB usage.

User Activity Monitoring

Improve situational awareness by gaining insight into critical user activities. Learn when privileged accounts are being used, how they are being used, and from where.

Out-of-the-Box Security and Compliance Reporting Templates

Log & Event Manager makes it easy to generate and schedule compliance reports quickly using over 300 audit-proven templates and a console that lets you customize reports for your organization's specific compliance needs.

Ease-of-Use and Deployment

Log & Event Manager is quick and simple to deploy. You can be up and auditing logs in no time using our virtual appliance deployment model, Web-based console, and intuitive interface.

WHO SHOULD USE LOG & EVENT MANAGER?

Resource-constrained security pros challenged with:

- » Lack of visibility into attacks as well as limited time for staffed monitoring
- » Compliance demands requiring automation and/or file integrity monitoring
- » Inability to prioritize, manage, and respond to security incidents
- » Slow incident response time
- » Inability to determine the root cause of suspicious activity
- » The need to monitor internal users for acceptable use and insider threats
- » The need to share log and activity data across security, network, applications, and systems
- » Inefficient, inoperable, or costly existing SIEM implementations

HOW LOG & EVENT MANAGER SUPPORTS YOUR SECURITY PROGRAM

- » Automation and embedded intelligence provide a Virtual Security Operations Center for 24x7 monitoring
- » Faster event detection and alerting on threat intelligence matches based on IPs
- » More intelligent and accurate detection of suspicious and malicious activity— including zero-day malware, insider, and advanced threats
- » Eliminates time-intensive manual reporting processes
- » Shortens time-to-respond duration through powerful forensics capabilities
- » Automatically blocks abuse and misuse through active response for network, system, and access policy violations
- » Monitors and blocks USB usage based on behavioral policy rules

SYSTEM REQUIREMENTS

Hardware	Minimum Requirements
CPU	Dual Processor, 2.0 GHz
Memory	8 GB RAM
Hard Drive	250 GB
Software	Minimum Requirements
OS/Virtual	VMWare® ESX®/ESXi™ 4.0 and above
Environments	Hyper-V® Server 2008, 2008 R2, 2012, 2012 R2
Database	Integrated with virtual appliance

ABOUT SOLARWINDS®

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, *thwack*®, to solve problems, share technology and best practices, and directly participate in our product development process.

LEARN MORE

DIMENSION SYSTEMS creating solutions with *technology*

To find out more:

Visit: www.DimensionSystems.com

Guam Office

643 Chalan San Antonio STE 107
DFS Pacific Plaza,
Tamuning, Guam 96913-3644
Phone: (671) 646-2007 | Fax: (671) 646-2006
Email us at: sales@DimensionSystems.com

Philippine Office

Suite 3004, 30/F Antel Global Corporate Center
Julia Vargas Ave., Ortigas Center
Pasig City, Philippines 1603
Phone: (632) 900-0198
Email us at: salesph@DimensionSystems.com

