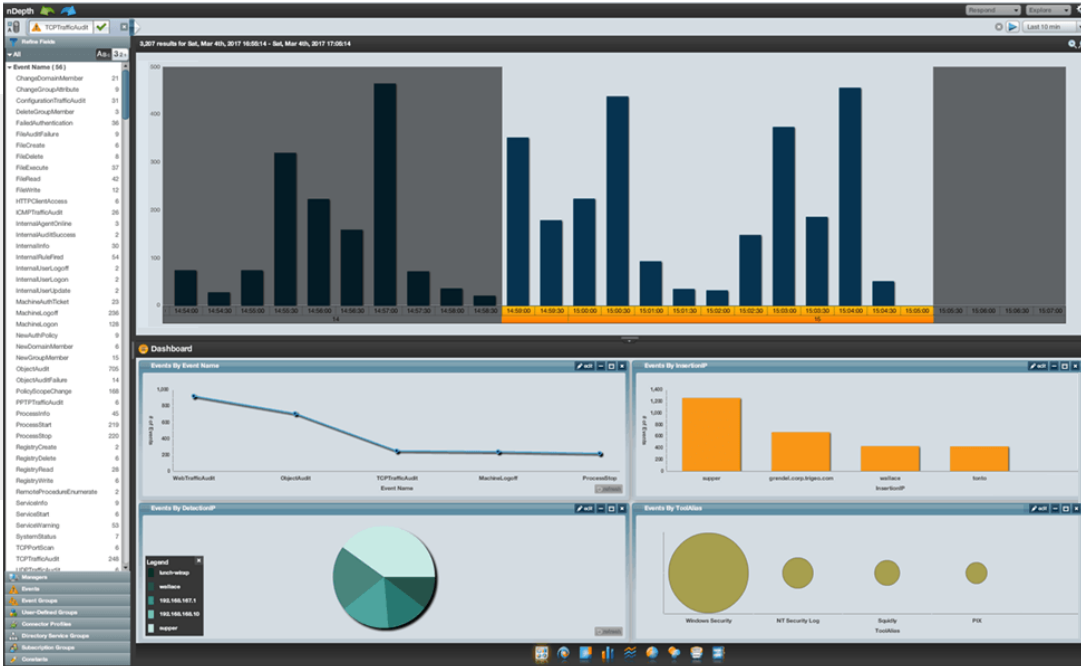


Log & Event Manager

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 3,500 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 and 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 most other enterprise SIEM solutions.

[DOWNLOAD FREE TRIAL](#)

Fully Functional for 30 Days

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, SOX, ISO, DISA STIGs, FIS-MA, FERPA, NERC CIP, GLBA, GPG13, and more

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.](#)

DOWNLOAD FREE TRIAL

Fully Functional for 30 Days

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.

[DOWNLOAD FREE TRIAL](#)

Fully Functional for 30 Days

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 24/7 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
- » User-friendly login process with single sign-on integration—use user ID and password, smart card, one-time password or biometric device

DOWNLOAD FREE TRIAL

Fully Functional for 30 Days

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 R2, 2012, 2012 R2, 2016
Database	Integrated with virtual appliance

TRY BEFORE YOU BUY. DOWNLOAD A FREE TRIAL!

Don't just take our word for it. At SolarWinds, we believe you should try our software before you buy. That's why we offer free trials that deliver full product functionality. Simply download Log & Event Manager, and you will be up and analyzing your log files in less than an hour. It's just that simple! Download your free, fully-functional trial today!

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable IT management software to customers worldwide, from Fortune 500® enterprises to small businesses, managed service providers (MSPs), government agencies, and educational institutions. We are committed to focusing exclusively on IT, MSP, and DevOps professionals, and strive to eliminate the complexity that our customers have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address key areas of the infrastructure from on-premises to the cloud. This focus and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as the worldwide leader in both network management software and MSP solutions, and is driving similar growth across the full spectrum of IT management software. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at www.solarwinds.com.

LEARN MORE

For product information about SolarWinds products, visit solarwinds.com, call, or email.

AMERICAS

Phone: 866.530.8100

Fax: 866.530.8040

Email: sales@solarwinds.com

EMEA

Phone: +353 21 5002900

Fax: +353 212 380 232

Email: emeasales@solarwinds.com

APAC

Tel : +61 2 8412 4900

Fax : +65 6593 7601

Email: apacsales@solarwinds.com

[DOWNLOAD FREE TRIAL](#)

Fully Functional for 30 Days

FEDERAL, FEDERAL RESELLER AND SYSTEM INTEGRATORS

Phone: 877.946.3751 or 512.682.9884

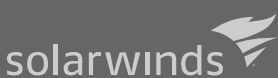
Email: federalsales@solarwinds.com

EUROPE NATIONAL/CENTRAL/FEDERAL GOVERNMENT

Phone: +353 21 233 0440

Email: nationalgovtsales@solarwinds.com

7171 Southwest Parkway | Building 400 | Austin, Texas 78735



For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

© 2017 SolarWinds Worldwide, LLC. All rights reserved.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.