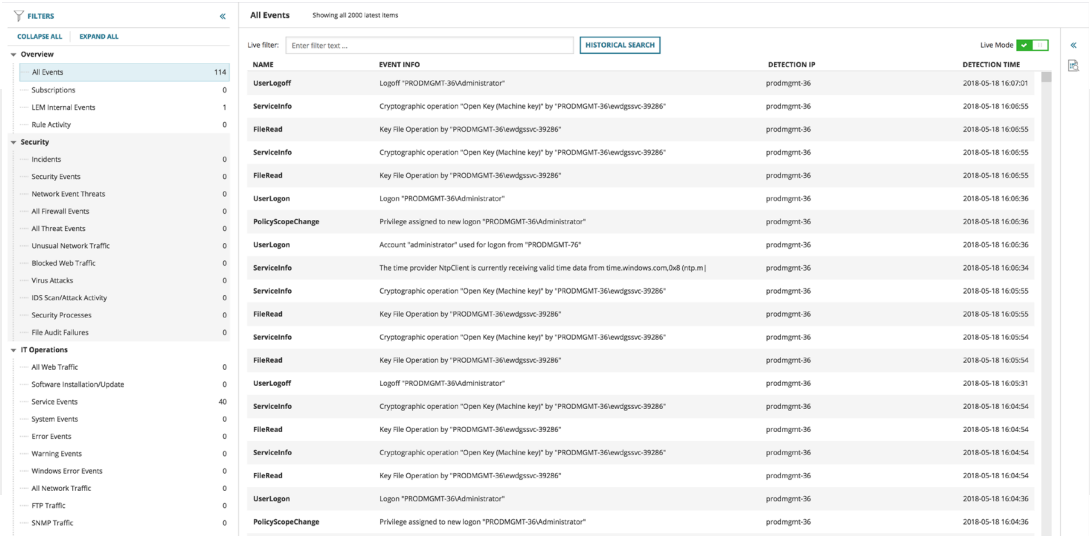
DATASHEET

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.

Thousands of 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, forwarding, 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

- Designed to collect, consolidate, and analyze 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
- Supports the forwarding of correlated and normalized log data to other solutions for further analysis
- Designed to detect breaches with threat intelligence
- Supports root cause analysis with built-in intelligence that applies to networks, applications, and security management
- Can block and quarantine malicious and suspicious activity, including inappropriate USB usage
- Can deliver 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, FISMA, 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.

Real-Time, In-Memory Event Correlation

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

Log Forwarding

Once Log & Event Manager has correlated and normalized log data, it can be forwarded to other solutions for further analysis. Forward entire logs or identify specific nodes and log events to forward.

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 is designed to deliver broader compliance support and deeper security intelligence for insider threats, zero-day malware, and other advanced attacks.

Built-in Active Response

Log & Event Manager can help 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 can help 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 report templates and a console that lets you customize reports for your organization's specific compliance needs.

Ease-of-Use and Deployment

Log & Event Manager was built to be 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?

Designed for 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 HELPS SUPPORT 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 reliable detection of suspicious and malicious activity—including zero-day malware, insider, and advanced threats
- Helps eliminate 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
- Expanded security tool integration by providing the capability to forward logs or log data to other tools
- 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 a biometric device

SYSTEM REQUIREMENTS

HARDWARE	MINIMUM REQUIREMENTS
CPU	Dual Processor, 2.0GHz
Memory	8GB RAM
Hard Drive	250GB
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 can 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 is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premise, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals – IT operations professionals, DevOps professionals and managed service providers (MSPs) – to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.

DOWNLOAD FREE TRIAL

Fully Functional for 30 Days

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

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