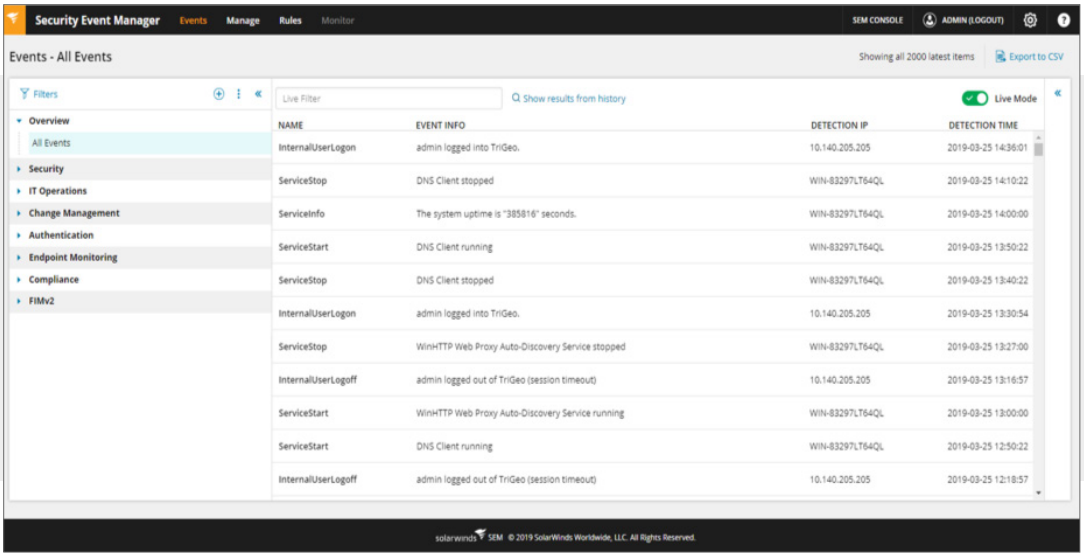
DATASHEET

solarwinds

Security Event Manager

(formerly Log & Event Manager)



An All-In-One Solution for Advanced Threat Detection, Automated Incident Response, and Compliance Reporting Designed for IT and Security Professionals

Thousands of resource-constrained IT and security pros rely on SolarWinds® Security Event Manager (formerly Log & Event Manager), a powerful on-premises tool for affordable and efficient threat detection, automated incident analysis and response, and compliance reporting for IT infrastructure. Our all-in-one SIEM combines log management, threat detection, normalization and 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

SECURITY 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 threats and attack patterns
- Supports the forwarding of raw log data to other solutions for further analysis
- Designed to detect known bad IPs and malicious activity with integrated threat intelligence
- Automatically respond to suspicious activity with Active Response actions, including blocking USB devices, killing running processes, logging off users, and more
- File integrity monitoring (FIM) to monitor files, folders, and Windows registry settings for unauthorized or suspicious changes
- Produces out-of-the-box compliance reports for HIPAA, PCI DSS, SOX, ISO, DISA STIGs, FISMA, FERPA, NERC CIP, GLBA, GPG13, and more

Scalable and Easy Collection of Network Device, and Machine Logs

Security Event Manager collects and catalogs log and event data in real time from anywhere data is generated across your network. Explore the supported data sources here.

Real-Time, In-Memory Event Correlation

By processing log data before it is written to the database, Security 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

Security Event Manager forwards raw log data with syslog protocols (RFC3164 and RFC 5244) to other applications for further analysis.

Log Export to CSV

Export event log data to CSV and perform operations like attaching important data to helpdesk tickets, share data with external vendors and contractors, upload event log data to other tools for further analysis, archive logs, and more.

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

Security 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

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

Enhanced, Real-Time File Integrity Monitoring

Embedded File Integrity Monitoring (FIM) is designed to deliver broader compliance support and deeper security intelligence for insider threats, zero-day malware, and other advanced attacks. Leverage enhanced filter capabilities for finer tuning and significantly reduce the noise associated with lower priority file changes, increasing productivity and efficiency.

Built-in Active Response

Security Event Manager can help you to immediately respond to security, operational, and policy-driven events using automated active responses that take action, such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory® settings.

USB Detection and Prevention

Security Event Manager can help prevent endpoint data loss, and protect sensitive data with real-time notifications 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

Security 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

Security 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 SECURITY EVENT MANAGER?

Designed for resource-constrained IT and 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 SECURITY EVENT MANAGER HELPS SUPPORT YOUR SECURITY PROGRAM

- Automation and embedded intelligence provide a Virtual Security Operations Center (SOC) 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
- **Expand visibility into your security posture** by deploying SEM in your Amazon Web Services (AWS) environment
- Monitors and blocks USB usage based on behavioral policy rules
- Export event log data to CSV and perform operations like attaching important data to helpdesk tickets, share data with external vendors and contractors, archive logs, and more
- **Reduce File Integrity Monitoring change noise by filtering out lower priority results, and streamline reporting** for regulatory standards like HIPAA, PCI-DSS, SOX, FISMA, and more
- User-friendly login process with single sign-on integration—use user ID and password, smart card, one-time password, or a biometric device

SIZING CRITERIA

Use the following table to determine if a small, medium, or large deployment is best suited to support your environment.

SIZING CRITERIA	SMALL	MEDIUM	LARGE
Number of nodes	Fewer than 500 nodes in the following combinations: • 5 – 10 security devices • 10 – 250 network devices, including workstations • 30 – 150 servers	Between 300 and 2,000 nodes in the following combinations: • 10 – 25 security devices • 200 – 1,000 network devices, including workstations • 50 – 500 servers	More than 1,000 nodes in the following combinations: • 25 – 50 security devices • 250 – 1,000 network devices, including workstations • 500 – 1,000 servers
Events received per day	5M – 35M events	30M – 100M events	Up to 215M events (2,500 EPS)
Rules fired per day	Up to 500	Up to 1,000	Up to 5,000

LOG & EVENT MANAGER VM REQUIREMENTS

See Allocate CPU and memory resources to the LEM VM in the LEM Administrator Guide for information about how to manage LEM system resources.

HARDWARE	SMALL	MEDIUM	LARGE
CPU	2 – 4 core processors at 2.0 GHz	6 – 10 core processors at 2.0 GHz	10 – 16 core processors at 2.0 GHz
Memory	8GB RAM	16 GB – 48 GB RAM	48 GB – 256 GB RAM
Hard Drive	250GB, 15K hard drives (RAID 1/ mirrored settings)	500GB, 15K hard drives (RAID 1/mirrored settings)	1TB, 15K hard drives (RAID 1/mirrored settings)
Input/output operations per second (IOPS)	40 – 200 IOPS	200 – 400 IOPS	400 or more IOPS
NIC	1 GBE NIC	1 GBE NIC	1 GBE NIC

SOFTWARE	MINIMUM REQUIREMENTS
OS/Virtual	VMware® vSphere ESX 5.5 or ESXi 5.5 and later
Environments	Microsoft Hyper-V® Server 2016, 2012 R2, or 2012
Database	Integrated with virtual appliance
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 Security 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: 512.682.9301
Email: sales@solarwinds.com

APAC

Tel : +61 2 8412 4900
Fax : +65 6593 7601
Email: apacsales@solarwinds.com

EMEA

Phone: +353 21 5002900
Fax: +353 212 380 232
Email: emeasales@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