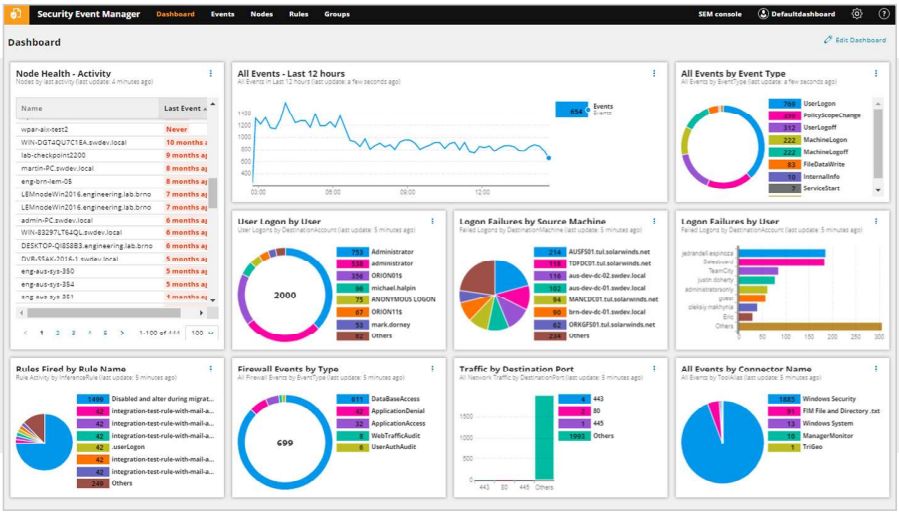
DATASHEET

solarwinds

Security Event Manager

(formerly Log & Event Manager)



An all-in-one SIEM solution for log collection, storage, analysis, and reporting designed to help IT pros identify and respond to cyberthreats as well as demonstrate compliance.

Thousands of resource-constrained IT and security pros rely on SolarWinds® Security Event Manager for affordable and efficient threat detection, automated incident analysis and response, and compliance reporting for their 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

- Collects, consolidates, normalizes, and visualizes logs and events from firewalls, IDS/IPS devices and applications, switches, routers, servers, OS, and other applications
- Performs real-time correlation of machine data to identify threats and attack patterns
- Responds to suspicious activity automatically with Active Response, including blocking USB devices, killing malicious processes, logging off users, and more
- Eases compliance reporting and audits with out-of-the-box reports and filters for HIPAA, PCI DSS, SOX, ISO, DISA STIGs, FISMA, FERPA, NERC CIP, GLBA, and more
- Intuitive interface and ample selection of out-of-the-box content means you don't need to be a security or compliance expert to get value from our SIEM solution
- Affordable, scalable licensing based on log-emitting sources, not log volume

Easy Collection and Normalization of Network Device and Machine Logs

Security Event Manager comes with hundreds of out-of-the-box connectors to simplify the process of collecting, standardizing, and cataloging log and event data generated across your network. Our industry leading log compression rate allows more data to be store with less resources required.

Customizable Visualizations and Dashboard

Quickly identify important or suspicious patterns in machine data with a wide variety of customizable visualizations and a flexible dashboard. Drill into interesting patterns with a click of a button and see the full list of related logs and their details.

Powerful and Simple Searching for Forensic Analysis and Troubleshooting

Security Event Manager is designed to allow users to quickly find important log data using simple keyword search in both real-time event data as well as historical data at predefined or custom time periods. Out-of-the-box and user-defined filters also provides fast data refinement.

Real-Time, In-Memory Event Correlation

By processing and normalizing log data before it's written to the database, Security Event Manager can deliver true real-time log and event correlation. Predefine and custom correlation rules allow Security Event Manager to automatically alert on possible security breaches and other critical issues.

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 allowing for customizable reports to meet your organization's specific needs.

Threat Intelligence Feed and Groups

Correlation rules are enhanced with a fully-integrated, regularly updating threat intelligence feed that automatically identifies and tags malicious activity from known bad IPs. Easily build groups containing values relevant to your environment, such as user and computer names, sensitive file locations, and approved USB devices. These groups can be auto-populated via correlation rules and simplify searching and reporting.

Built-in Active Response

Security Event Manager can do much more than trigger email alerts. SEM is designed to immediately respond to security, operational, and policy-driven events using predefined responses, such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory® settings.

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.

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.

Log Forwarding and Exporting

Security Event Manager forwards raw log data with syslog protocols (RFC3164 and RFC 5244) to other applications for further use. Additionally, users can export logs to a CSV file so the data can be shared with other teams and external vendors, uploaded to other tools, or attached to helpdesk tickets.

SECURITY EVENT MANAGER VM REQUIREMENTS

To see all systems requirements and to determine deployment size, see SEM system requirements in the SEM Install or Upgrade Guide.

HARDWARE	SMALL	MEDIUM	LARGE
CPU	2 – 4 core processors at 2.0 GHz	2 – 4 core processors at 2.0 GHz	2 – 4 core processors at 2.0 GHz
Memory	8 GB	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 moreIOPS
NIC	1GBENIC	1GBENIC	1GBENIC

SOFTWARE	MINIMUM REQUIREMENTS
OS/Virtual	VMware® vSphere ESX 5.5 or ESXi 5.5 and later Public cloud option available for Amazon Web Services and Microsoft Azure
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!

DOWNLOAD FREE TRIAL

Fully Functional for 30 days

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) 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-premises, 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.

LEARN MORE

AMERICAS
Phone: 866.530.8100
Fax: 512.682.9301
Email: sales@solarwinds.com

ASIA
Tel : +65 6422 4123
Fax : +65 6593 7601
Email: apacsales@solarwinds.com

EMEA
Phone: +353 21 5002900
Fax: +353 212 380 232
Email: emeasales@solarwinds.com

PACIFIC
Phone: +61 2 8412 4910
Email: apacsales@solarwinds.com

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