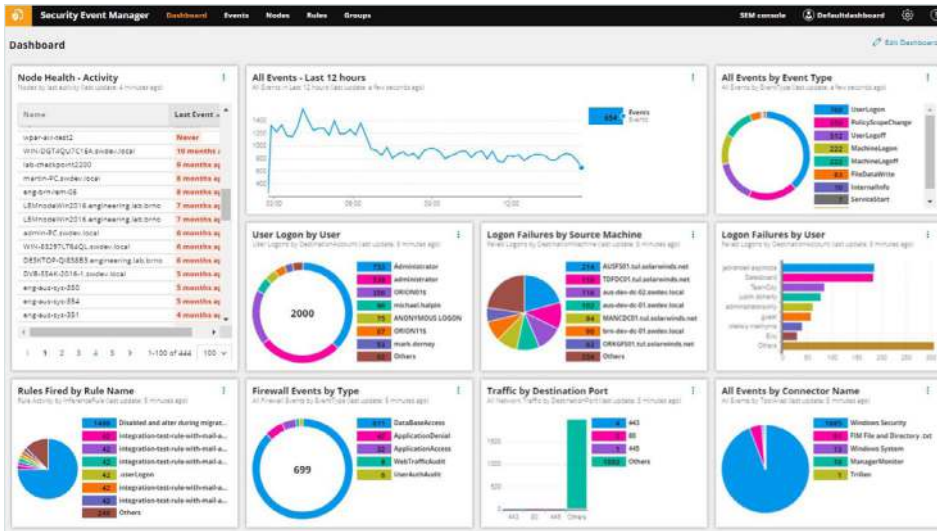


Security Event Manager



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

Thousands of resource-constrained IT and security pros rely on **SolarWinds® Security Event Manager (SEM)** for affordable and efficient threat detection, automated incident analysis and response, and compliance reporting for their IT infrastructure. Our SIEM solution 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.

[Try It Free →](#)

30 days, full version

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.
- Offers an intuitive interface and ample selection of out-of-the-box content, meaning you don't need to be a security or compliance expert to get value from SolarWinds SEM.
- 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 stored with fewer resources required.

Customizable Visualizations and Dashboard

Quickly identify important or suspicious patterns in machine data with various customizable visualizations and a flexible dashboard. Drill into interesting patterns with a click of a button and see the complete 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 searches in real time event data and historical data at predefined or custom periods. Out-of-the-box and user-defined filters also provide fast data refinement.

Real-Time, In-Memory Event Correlation

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

Web-based Regulatory and Compliance Reporting

Generate web-based reports from historical searches and convert these historical search queries into pie charts and tables to help you identify potential issues and make informed decisions about your network activity. You can also schedule the reports to be sent automatically (in CSV/PDF format) to all stakeholders as an email attachment or an external server using a secure file transfer protocol connection. You can also create and view tags for queries, allowing you to identify specific user activity quickly.

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 can help 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 block their usage automatically, and built-in reporting to audit USB usage.

Log Forwarding and Exporting

Security Event Manager forwards raw log data with syslog protocols (RFC 3164 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.

LIVE AND HISTORICAL EVENTS

See events stream in near real-time on the Live Events tab. You can also see critical trends by analyzing historical data via simplified network event searches in the Historical Events tab. The intuitive query builder presents tips and suggestions as you enter query parameters; then, the event histogram and custom time picker allow you to zero in on specific results in a designated period. In the historical events tab, you can save, load, browse, or schedule common searches.

SECURITY EVENT MANAGER SYSTEMS REQUIREMENTS

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

TRY BEFORE YOU BUY

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 that simple. [Download your free, fully functional trial today](#).

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of simple, powerful, and secure IT management software built to enable customers to accelerate their digital transformation. Our solutions provide organizations worldwide—regardless of type, size, or complexity—with a comprehensive and unified view of today's modern, distributed, and hybrid network environments. We continuously engage with technology professionals—IT service and operations professionals, DevOps and SecOps professionals, and database administrators (DBAs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures, applications, and environments. The insights we gain from them, in places like our [THWACK®](#) community, allow us to address customers' needs now, and in the future. Our focus on the user and our commitment to excellence in end-to-end hybrid IT management have established SolarWinds as a worldwide leader in solutions for observability, IT service management, application performance, and database management. Learn more today at www.solarwinds.com.

Try It Free →

30 days, full version



*For additional information, please contact SolarWinds at [866.530.8100](tel:866.530.8100) or email sales@solarwinds.com.
To locate an international reseller near you, visit [SolarWinds Partner Page](#).*

© 2024 SolarWinds Worldwide, LLC. All rights reserved. | 2403-EN

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.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NON-INFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.