solarwinds®

SolarWinds Log & Event Manager

BASED ON TECHNOLOGY FROM TRIGEO®

Your Log Files Have Never Looked So Good... or Delivered So Much Information!

Meet the newest member of our family: SolarWinds Log & Event Manager, a new product based on technology from TriGeo®. This powerful product combines real-time log analysis, event correlation, and ad hoc search to deliver the visibility, security, and control you need.

Finally, you can declare victory over IT operations, compliance, and security challenges with a product that is so easy to use and deploy that you'll be jumping for joy. Forget about expensive, complex solutions and get the rich log collection, log analysis, and event management functionality you need – at an amazingly affordable price!

SolarWinds Log & Event Manager Highlights:

- Troubleshoot performance and availability issues and immediately spot abnormalities with visibility into data from millions of files and events

- Ensure compliance with PCI, HIPAA, NCUA, GLBA, NERC-CIP, FISMA, SOX, or your own corporate policies with an "audit-proven" compliance solution that meets the security monitoring and log management requirements imposed by every auditing authority

- Generate compliance reports quickly and easily with 300+ reports and out-of-the-box compliance packs

- Perform proactive log analysis and real-time event correlation across your infrastructure to quickly identify attacks, highlight threats, and uncover policy violations

- Correlate millions of events from your network, systems, apps, virtual machines, and storage infrastructure with an unprecedented correlation engine that is real-time, in-memory, non-linear, and multi-dimensional

- Visualize search data and understand how to take action on it with an intuitive search interface that employs a Word Cloud, treemaps, bubble charts, and histograms

- Mitigate threats with Active Reponses by automatically taking action to protect your infrastructure by quarantining, blocking, routing, and controlling services, processes, accounts, and privileges

- Protect sensitive data with real-time detection and ejection of USB drives

- Store terabytes of log data without purchasing additional storage using a high performance, high compression data model that stores data at a 60:1 ratio

- Deploy SolarWinds Log & Event Manager in a matter of hours — without the aid of consultants

- Enjoy support for dozens of manufacturers, hundreds of products, and thousands of models


SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

SC MAGAZINE BEST BUY BEST BUY 2011 2010
Best Buy Group Test: SIEM

SC MAGAZINE AWARDS 2007 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2008 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2009 WINNER Honored in the U.S.
SC MAGAZINE INNOVATOR 2010

SolarWinds Log & Event Manager Features

Proactive Log Analysis

In today's IT environments, you can drown in log data if you're not careful. The multitude of distributed systems, applications, and networks in your infrastructure all have associated log files – but this information is useless if you can't effectively collect and analyze it.

SolarWinds Log & Event Manager not only provides real-time log analysis, it also delivers interactive data visualization and built-in knowledge that automates collecting, normalizing, and interpreting logs from a variety of devices and applications. That means you can immediately spot events that are of interest and take action. Say goodbye to mounds of useless data and hello to simplified log analysis!
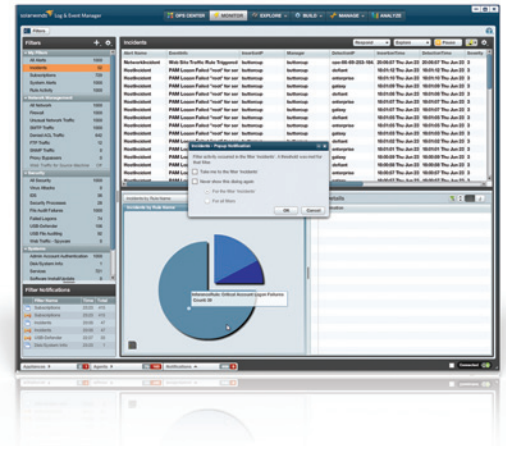
Real-time Event Correlation

Correlating millions of events from your network, systems, applications, virtual machines, and storage infrastructure can be daunting… unless you have SolarWinds Log & Event Manager at your fingertips. An unprecedented correlation engine fires on all cylinders; it is real-time, in-memory, non-linear, and multi-dimensional. No other solution at this price point can promise you that kind of power and flexibility!

With nearly 700 built-in correlation rules, SolarWinds Log & Event Manager starts delivering visibility right out of the box, eliminating hours of work for you. But we know you also need rules tuned to your specific environment. That's why we created an unbelievably simple correlation rule builder that employs a graphical interface to make it easy for IT administrators to quickly build custom rules. Finally, you can get powerful correlation without the headaches!

Ad Hoc IT Search

We know you don't have time to sift through a mountain of log events and data sources… and we know that lots of tools just give you disappointing search toolbars that don't really help you identify the important data. SolarWinds Log & Event Manager raises the bar (no pun intended) by giving you advanced search functionality that enables you to effectively perform forensic analysis on events.

With an intuitive search interface, you can get immediate insight into activities that would normally go unnoticed. Using a unique Word Cloud, along with treemaps, bubble charts, and histograms, SolarWinds Log & Event Manager offers a fully interactive search environment that makes it easy to visualize search data and understand how to take action on it. Plus, you'll be amazed at how quickly (and securely) you can search terabytes of data, thanks to our innovative approach to data aggregation, archiving, and encryption.

Compliance Reporting

We know that compliance reporting is one of your least favorite activities, so we built in more than 300 "audit-proven" compliance reports that will turn your frown upside down. Regardless of which acronym you need to comply with – PCI DSS, GLBA, SOX, NERC CIP, or HIPAA, to name a few – the built-in reporting console makes it easy to generate reports and provide graphical summaries. You can even schedule the reports to run on a regular basis and export them to a wide variety of formats to make your life easier. And you can rest assured that SolarWinds Log & Event Manager also meets the security monitoring and log management requirements imposed by every major auditing authority.
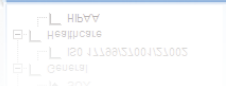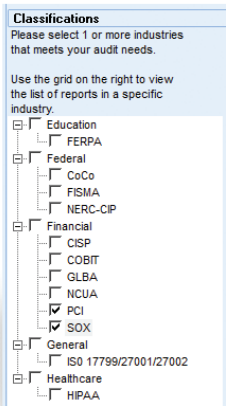
Active Response & Threat Mitigation

When threats are detected, you need to respond immediately to prevent disaster. With the arrival of SolarWinds Log & Event Manager, it's a dark day for malware, zero-day attacks, and worms that would love to wreak havoc on your infrastructure. With a library of built-in Active Responses, you get the automated response you need to mitigate threats and take actions like quarantining infected machines, blocking IP addresses, disabling user accounts, killing unauthorized processes, restarting services, and more.

USB Detection & Prevention

USB devices are a nightmare for IT administrators; gigabytes of sensitive data can walk out the door on a device the size of a subway token. To defend against data loss, we built technology into SolarWinds Log & Event Manager that can track USB activity and identify unauthorized use or copying of sensitive files. In fact, the product can notify you in real time, disable the user account, quarantine the workstation, or even automatically eject the USB drive. It's like a silent defender for your most valuable data!
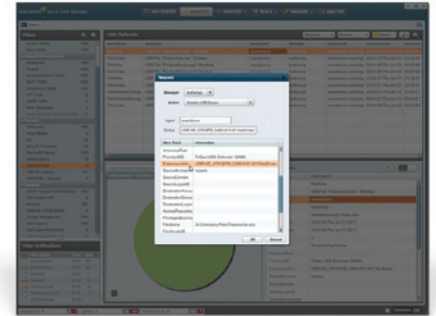
Log Storage for the Long Term

How to store terabytes of log data is a conundrum for most IT departments. And it's no fun to spend more money on more storage devices. SolarWinds Log & Event Manager uses a high performance, high compression data model, storing data at a 60:1 ratio at breakneck speeds. That means you can store the massive amounts of data required for regulatory compliance while eliminating the need for external storage. Plus, you can enjoy years of online data access!

Fast & Easy Implementation

We pride ourselves on providing products that are easy and fast to deploy; SolarWinds Log & Event Manager is no exception. You won't need a team of consultants or a weekend to read through a dry manual to get this product up and running. Oftentimes described as "live by lunch," SolarWinds Log & Event Manager can start delivering the visibility and protection you need in a matter of hours – not days.

"This is by far the
best SEIM system I've ever seen
let alone owned. It's everything it
was represented to be and more.
Everything about my experience
including purchase, installation,
support and training has been
positive"

- Lou Porreco,
Technology Director at
Windsor Management Group

Intuitive Interface

An intuitive interface is the key to making a product easy to use. SolarWinds Log & Event Manager offers the superior usability and simplicity you crave. The console is designed to help you visualize log and event data so that you can take action instead of spending hours sifting through the data. It also offers the drag-and-drop, point-and-click features that make it easy to sort through all this data without having to learn a complex query language.

Comprehensive Support for a Plethora of Data Sources

SolarWinds Log & Event Manager was built to support the diversity that is the rule (and not the exception) in today's IT environments. It supports dozens of manufacturers, hundreds of products, and thousands of models. SolarWinds Log & Event Manager integrates with best-of-breed products in every major category, with more being added each week.

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