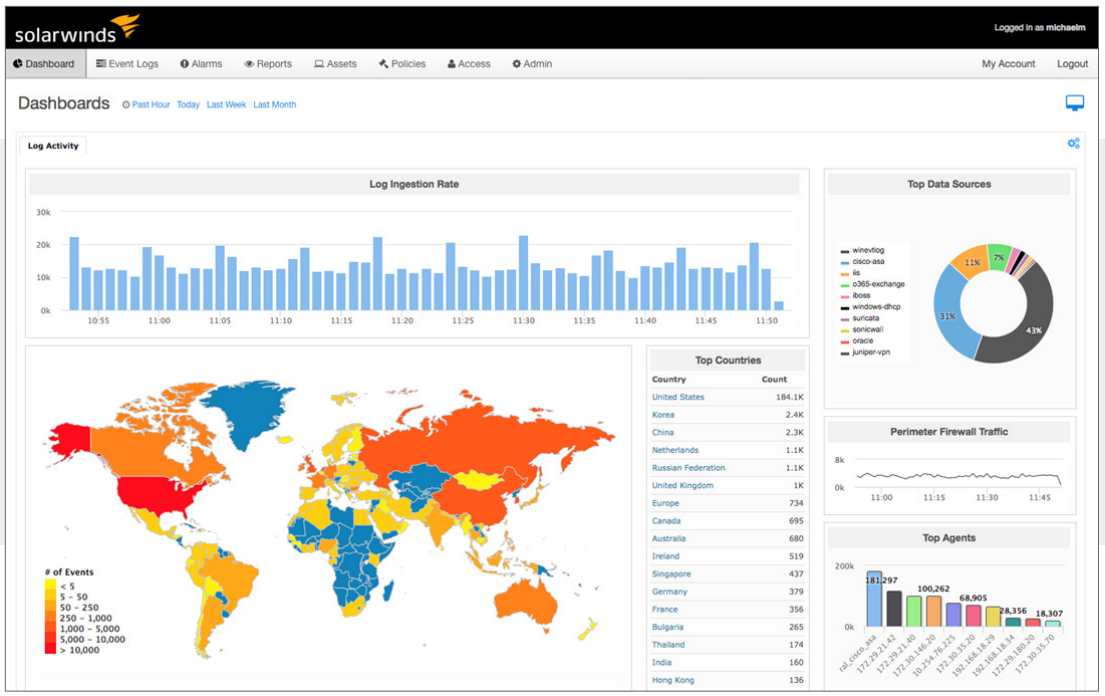
Threat Monitor — IT Ops Edition



Monitor, respond, and report security threats in real time.

SolarWinds® Threat Monitor™ – IT Ops Edition is designed to be the ideal tool to hunt for security threats and automatically correlate logs in real time from the devices and applications on your network, and analyze them against Situational Awareness sources like DHCP, Active Directory®, Vulnerability Reports, and IP Reputation Databases, to produce actionable notifications that IT professionals can deploy quickly and easily.

REQUEST A DEMO

THREAT MONITOR – IT OPS EDITION AT A GLANCE

- Centralized, cloud-based security monitoring
- Simple, scalable, rapid deployment
- Continuously updated thread intelligence data
- Security Information and Event Management (SIEM)
- Automated threat response
- Integrated compliance tools

FEATURES

REQUEST A DEMO

Continuously updated threat intelligence

Receive updated threat intelligence from multiple sources, including IP and Domain Reputation databases, to monitor for known and unknown security threats.

Security Informaiton and Event Management (SIEM)

Collect log-file information from disparate sources and hone in on the most critical threats by rapidly assessing intent and severity.

Automatic log correlation

Process and store logs from your ecosystem, and analyze them against incoming threat intelligence feeds.

Automated incident response

Fully automate intelligent responses to quickly remediate security incidents, removing the need for constant user interaction.

Integrated Network and Host Intrusion Detection

Automatically analyze the amount and types of attacks, and use this data to create and implement actionable incident responses.

Highly indexed log search capabilities

Rapidly normalize, search, and analyze thousands of logs to understand the nature of ecosystem threats and attacks.

Cutting edge alarm engine

Multi-conditional, cross-correlated alarms work in tandem with the Active Response engine to identify and summarize.

Integrated compliance tools

Demonstrate regulatory compliance by leveraging out-of-the-box report templates, or create custom reports to fit your business needs.

SYSTEM REQUIREMENTS – VIRTUAL MACHINE DATA COLLECTOR

REQUEST A DEMO

HARDWARE	MINIMUM REQUIREMENTS
CPU	4 vCPUs (processors, not cores)
Memory	8GB of RAM
Hard Drive	150GB HDD volume
NIC	»1 NIC for IP address management »1 NIC for Intrusion Detection (optional)

NETWORK CONNECTIVITY & ACCESS LISTS
• Static IP address - Connected to an accessible vSwitch instance
• TCP and UDP port 53 access to internal DNS servers
• Outbound TCP port 443 (HTTPS) to SolarWinds VPN Gateway (to be determined at deployment time)
• Local Network Inbound TCP and UDP port 514 - for local Syslog data sources
• Local Network bi-directional TCP and UDP port 1514 - for OSSEC Agent connectivity
• Inbound TCP port 9654 - for OSSEC Agent key negotiation
• Available Physical NIC on the HOST VMware/Hyper-V server - to connect to a SPAN/Monitor port within the core-switching environment to facilitate Intrusion Detection capabilities (optional). Specific configuration requirements will be provided prior to implementation
No inbound connectivity is required from the Internet.

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

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

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

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

For product information about SolarWinds products, vist 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 solarwinds.com/partners/reseller_locator.aspx