

Symantec™ Security Information Manager

Comprehensive log management and real-time event monitoring

Data Sheet: IT Risk and Compliance

Overview

Symantec™ Security Information Manager combines comprehensive log management, analysis and retention with real-time event monitoring, providing security leaders with a composite view of security exposures and malicious activity across the enterprise.

Security Information Manager's log collection platform aggregates and normalizes diverse log data from a wide range of technologies. Our industry-leading correlation engine then combines these log-based security events with threat intelligence and contextual business information enabling security leaders to prioritize incident response activities based on relative business risk.

This comprehensive approach not only provides the enterprise-wide visibility needed to effectively defend your organization against threats; it also helps teams efficiently demonstrate compliance with industry regulations.

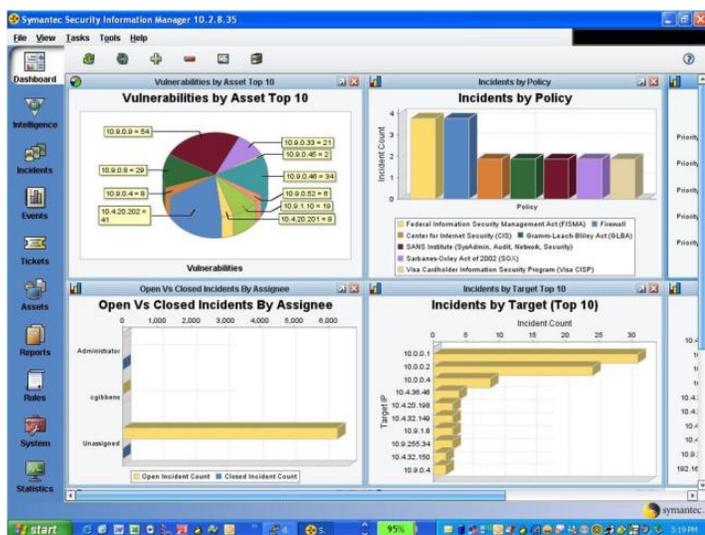
Identify Threats in Real-time

Security Information Manager helps security leaders leverage existing infrastructure investments to gain the enterprise-wide perspective necessary to identify and respond to malicious activities in real-time.

Leveraging our highly scalable architecture, Security Information Manager's event collectors aggregate and normalize log data from a wide range of diverse technologies throughout your IT infrastructure. While more than 200 predefined source collectors are currently available, custom collectors can easily be created to capture information from unique business applications and data sources.

Events flow from the collectors to the product's correlation engine for real-time threat monitoring. More than 80 predefined rules, covering a wide range of security signatures, are used to detect threats before they occur.

Symantec simplifies rule creation by eliminating the issue of third-party devices each having their own unique signatures. A first in the industry, Security Information Manager provides a common signature taxonomy, resulting in more than 40,000 signatures being available out of the box. In addition, because rules are written in an intuitive, English-like language, security teams can easily create additional rules, specific to their environment.



Security Information Manager Dashboard

Meet Compliance Requirements

Increasingly, organizations must comply with industry regulations, internal mandates, and best practice frameworks to demonstrate they are adequately protecting their information and infrastructure and that security policies are actively enforced.

Security Information Manager provides more than 400 out-of-the-box compliance rule sets, dashboards, reports, and queries specifically designed for demonstrating compliance. All content is available in easy to use templates, simplifying customization. In fact, many users implement our compliance report templates, adding only a logo.

Compliance requirements necessitate organizations archive event information for audit purposes, placing significant storage demands on your environment. Achieving up to 30:1 data compression, Security Information Manager captures and stores normalized data as well as raw event information. Users may query multiple separate archives on an ad-hoc basis for audit response, incident investigation or forensic-quality data analysis. Security leaders can also leverage predefined, compliance-specific queries to demonstrate compliance with regulations such as HIPAA, PCI, and SOX.

Accelerate Time to Value

Offered as a comprehensive, turn-key solution including out-of-the-box connectors and predefined rules, queries and compliance reports, Security Information Manager is designed for ease and speed of deployment.

Because Security Information Manager does not require time-consuming database setup or administration, most customers deploy out of the box, avoiding costly professional services.

Symantec Security Information Manager offers flexible 'check-box' options, allowing users to easily scale their implementation and tailor roles as organizational needs change. In addition, integrated monitoring of system health further lowers operational overhead.

To ensure your Security Information Manager deployment receives the latest collectors, reports, query templates and security correlation rules, Symantec delivers quarterly product updates via Symantec LiveUpdate, greatly simplifying on-going maintenance.

Gain an External Perspective

For organizations trying to keep pace with the accelerating threat landscape, aggregating event data from diverse sources and then identifying which threats are relevant is a time intensive task requiring highly specialized security expertise. Time spent on research and analysis diverts focus from integrating newly gained threat intelligence data into existing security systems, incident remediation – and implementing new solutions to enhance security.

Offered as an optional subscription, Symantec DeepSight Security Intelligence dynamically updates Security Information Manager, providing organizations with timely, relevant, and actionable global intelligence about emerging threats, threat sources and vulnerabilities.

Combining the power of Security Information Manager's correlation engine with DeepSight's real-time intelligence updates allows IT security teams to not only keep pace with the threat landscape; it enables teams to take proactive measures to defend their enterprise against malicious attacks.

More Information

Visit our website

<http://enterprise.symantec.com>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Symantec helps organizations secure and manage their information-driven world with IT Compliance, discovery and retention management, data loss prevention, and messaging security solutions.

21276568 10/12