

# Symantec™ Security Information Manager

Enabling organizations to apply a documented, repeatable process for responding to security threats and addressing IT policy compliance

---

## Overview

Symantec Security Information Manager enables organizations to collect, store, and analyze log data as well as monitor and respond to security events to meet IT risk and compliance requirements. It can collect and normalize a broad scope of event data and correlate the impact of incidents based on the criticality to business operations or level of compliance to various mandates. Incidents are prioritized using its built-in asset management function, which is populated using scanning tools and allows confidentiality, integrity, and response ratings and policies to be assigned to help prioritize incidents.

In addition to establishing priority to events, Symantec Security Information Manager can provide recommended best practices for response and remediation efforts. Automated updates from Symantec's Global Intelligence Network provide real time information to the correlation process on the latest vulnerabilities and threats that are occurring across the rest of the world.

Symantec Security Information Manager can enable organizations to produce executive, technical, and audit-level reports that are highly effective at communicating risk levels and the security posture of the organization. Over 300 out-of-the-box queries can create custom reports via Symantec Security Information Manager. Real-time correlation of network and host security breaches with Symantec's trusted

global security intelligence makes it the vehicle for a world-class incident response system promoting the integrity of business-critical information assets. Security Information Manager can deliver a framework that automates the real-time collection, monitoring and assessment of audit mechanisms and security controls and can dramatically lower costs and improve the effectiveness of managing activities related to IT security and compliance risks.

---

**Key Challenges of security and compliance executives include:**

### ***Understanding Security Posture and Meeting Audit Standards***

Symantec Security Information Manager is a real-time security information management solution that collects, correlates, and stores event, vulnerability and compliance logs and documents the actions that your security staff takes to help keep your information systems secure. It provides compliance reporting that lets you and your auditors see, firsthand, the state of your security environment. These are crucial to helping your organization provide the accountability and transparency required to comply with stringent mandates and regulations.

### ***Assessing threats and security issues***

Symantec Security Information Manager allows you to identify the threats you are most vulnerable to and provides remediation steps to address those threats in

### **Assessing threats and security issues - continued**

real-time. It will also classify threats and security issues as they occur based on the effect those events will have on your business environment.

### **Identity and access management**

Symantec Security Information Manager can leverage information from existing security and compliance products to assist in monitoring identity and access activities. It can help organizations gain visibility into user access of systems and produce audit trails showing access and changes to critical applications and assets.

---

### **Key features:**

- Compliance and audit reporting
- Log retention and retrieval
- Real-time threat analysis
- Automated incident prioritization
- Incident remediation workflow

### **Benefits:**

- Align security and compliance requirements with IT operations
- Meet compliance reporting requirements quickly and effectively
- Gain accurate and timely visibility into your security risk posture
- Increase IT staff productivity by prioritizing the most critical of security issues

- Reduce IT security operational costs and improve response time
  - Provide appropriate security service levels to different business units and geographies
- 

### **Log management and data retention**

Mandates and regulations require organizations to collect, store, and analyze various types of logs to demonstrate that they are adequately protecting information and infrastructure.

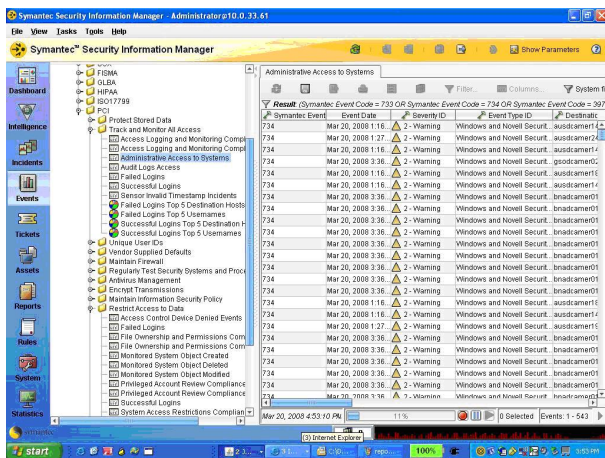
Symantec Security Information Manager enables organizations to collect, store, and analyze log data as well as monitor and respond to security events to meet IT compliance requirements. Flexible archiving, querying and reporting provide organizations the means to manage logs from every source. Symantec Security Information Manager stores events in a collection of archive files within a specified location. The archive is implemented as a self-maintained module where it monitors disk usage and the age of individual archive files. Based on policy, when a specified maximum disk space is reached or files approach their expiration date, the system deletes old archives to make room for new ones. These files can be stored on the appliance, direct attached storage (DAS), network attached storage (NAS), or on a storage area network (SAN).

Symantec Security Information Manager can archive data faster than traditional databases because it is optimized for one function - to save a high volume of events. General database applications are built for

## Log management and data retention - continued

hundreds of different functions limiting their ability to accommodate such a specialized requirement. Symantec Security Information Manager can achieve up to 30:1 data compression and captures and stores normalized data as well as raw event information for forensic-quality log data analysis.

Symantec Security Information Manager provides compliance specific queries (HIPAA, PCI, SOX, etc..), offers flexible data access across multiple separate archives and can distribute reports on a scheduled basis. It can easily support log collection and management from every source with predefined queries, reports and flexible archive options.



Log Management and Data Retention

## Incident management

Symantec Security Information Manager helps organizations to collect, store and analyze log and intelligence data in order to identify and respond to critical malicious activities after, during or even before they occur. By combining existing protection and prevention device and application data with external intelligence on malicious activities occurring globally, it can deliver comprehensive insight into what incidents are occurring or are most likely to occur.

Most organizations already have significant investments in applications and devices designed to achieve objectives such as protecting their perimeter, managing access rights, and securing against challenging end point vulnerabilities. Unfortunately, these collective efforts are often mutually exclusive in terms of their effectiveness and offer no centralized oversight to the critical threats that can pose the greatest risks to the business. Symantec Security Information Manager can help these organizations to gain centralized visibility, leverage the value of existing investments and prepare for potential threats that could compromise business-critical information assets.

## Data collection

The first critical step in this process is to enable the broad collection of diverse data that is generated by existing security devices and applications. The inherent value of these investments is in the resulting intelligence that they can provide. Symantec Security Information Manager uses over 150 predefined source collectors and provides flexible options for customizing the additional

### **Data collection - continued**

collection of unique source logs. This enhanced collection process, combined with Symantec Security Information Manager's optimized archiving and event processing capabilities provide a highly scalable ability to centralize large amounts of diverse log data.

### **Correlation based on priorities**

Data aggregation enables many organizations to fulfill on basic compliance requirements around data archiving and even sets the stage for rudimentary analysis of events occurring across their environment. There is not, however, any ability to set priorities based upon the criticality of these events. As such, there is no relative difference in this schema between events that include one single desktop computer that might impact a single user versus a critical email gateway that could impact an entire organization. Symantec Security Information Manager allows organizations to prioritize such events automatically by employing a framework of rules based correlation.

Symantec Security Information Manager uses a proposed standard to identify security threats through an open standards process within what is called the Distributed Management Task Force (DMTF). This method classifies threats and security issues based on the effect the event could have on the environment, the method used to carry out the attack, and what information assets might be affected. This classification is referred as Effects Mechanisms and Resources (EMR) and is the heart of the Symantec Security Information Manager correlation engine.

Symantec Security Information Manager collects events and analyzes them in real time using rules-based correlation on the normalized event stream.

Pattern-based intelligent rules are highly leveraged, allowing a single rule to take the place of more specific rules used with more conventional approaches. This provides much simpler maintenance and authoring of rules and allows the system rules to cover a multitude of conditions. In addition to condition action rules, Security Information Manager supports plug-in rules that can fire based on arbitrary conditions as well as statistical anomalies. An example of one of these types of rules is a negative condition rule, where the absence of an event over a period of time fires the rule such as a back up process that misses a scheduled routine. Rules based correlation allows greater flexibility in how organizations establish priority ranking incidents.

### **Intelligence to respond and take preemptive action**

Security monitoring should not rely solely on events that have already occurred. In many cases, being aware of vulnerabilities that have not yet been exploited can provide an organization the ability to take action prior to an event occurring. Symantec Security Information Manager helps customers to establish such an early warning system to take helpful preventive actions.

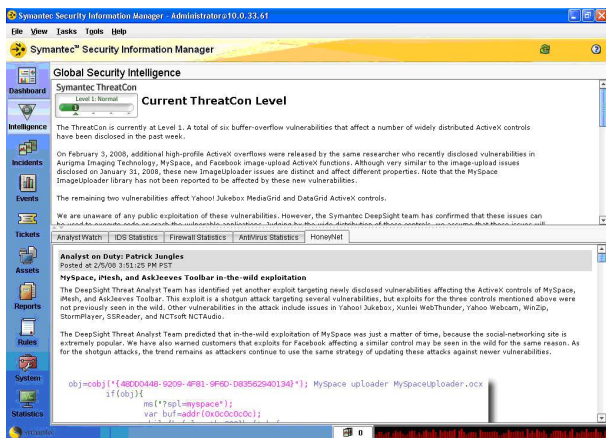
An effective early warning system detects threats based on a global perspective and provides in-depth information about them. It also recommends measures a company can take to protect itself. Symantec Security Information Manager provides automated updates from Symantec's Global Intelligence Network to provide

### Intelligence to respond - continued

real-time information to the correlation process on the latest vulnerabilities and threats that are occurring across the rest of the world.

Fast and effective response to security incidents requires an automated way to assess real time data. Security Information Manager can automatically generate an incident based on a conclusion or conclusions drawn during the detection phase of a security threat. When an incident is created, it can be assigned to an individual or a team. The incident creates a workflow to facilitate the containment, eradication, and recovery process. This workflow can be created as a ticket, which can be sent to a third-party ticketing help-desk solution to be worked on and tracked back into the system using a bidirectional feed.

The combination of internal incident data with external global intelligence provides the response team with optimized capabilities to effectively and efficiently respond to security incidents.



Global Security Intelligence

### User access monitoring

Many enterprises are facing the challenges of monitoring various data activities associated with user access. Privileged access policy violations and information access control are increasingly important areas for gaining visibility to improper behavior that can lead to compromised information. Symantec Security Information Manager can help keep track of user behaviors relative to sensitive data, changes in access privileges, failed login attempts and other events that can collectively indicate disruptive incidents.

The rules and correlation capabilities available with Symantec Security Information Manager can become a crucial element in access management. Organizations can create file watch lists or asset policies and roles to help prioritize incident identification. Symantec Security Information Manager can ensure real time alerting to inappropriate accesses or attempts to change permissions on restricted data. When an event requires further investigation subsequent events that match tracking rules can automatically be included in the assessment process. All this is supported with flexible querying and reporting capabilities to provide auditors and other related stakeholders the information they need.

User access monitoring through Symantec Security Information Manager also enables documented and repeatable responses to events. Symantec Security Information Manager can provide reports on account profiles and activities, including elevation of privileges for groups or individual accounts. It can monitor

### **User access monitoring - continued**

password restriction requirements across the enterprise and generate alerts if the same passwords are being used on multiple systems. Symantec Security Information Manager takes advantage of existing applications and data sources to provide a comprehensive view of which users are accessing what information, when and how often.

---

### **Security services provisioning**

Many midsized organizations and divisions of larger enterprises have requirements for managing security related events and activities. Unfortunately, many of these customers do not have the ability to secure the budget, resources and relative skills to establish their own on-premise solution. As such, many are looking to third party organizations to help them fulfill on these requirements. Symantec Security Information Manager enables these third parties to be able to deliver these capabilities on an as needed basis.

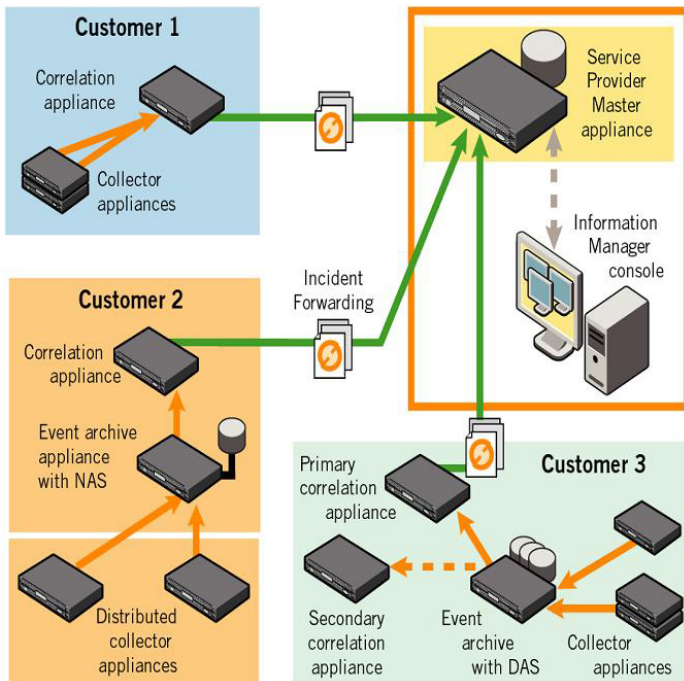
Midsized organizations look increasingly to third party partners for establishing service level agreements around monitoring their security data. Symantec Security Information Manager provides an effective, scalable architecture that enables these third parties to securely provide these services. Customers can independently aggregate and establish policies around the prioritization of security incidents within their environment.

In a similar manner, larger multi-national organizations require service provider-like capabilities to service divisional and geographical stakeholder needs. Security Information Manager can allow centralized IT resources to provide independent monitoring to each of these respective internal customers due to the ability to create central console views across multiple deployments. Not only is this of benefit to the independent stakeholder groups, but the overall organization can also benefit from the centralized cross correlation of event activity that can feed flexible reporting and query requirements from a central oversight perspective.

In a common information manager service provider scenario, the service provider installs at least one device at each site that provides a centralized view of all of the incidents that are generated by each customer. If the service provider uses more than one device to manage customers, each service provider-enabled device operates independently from any other service provider appliances. This creates a distributed services framework that can be centrally monitored and managed by one provider.

Symantec Security Information Manager can enable security incident management services to multiple business clients, including clients with multiple physical locations. The services that are offered by remote security management services typically include collection and correlation of security events, monitoring and resolving security incidents in real-time, creating and working with tickets, and generating and delivering custom reports.

**Security services provisioning - continued**



Security Services Provisioning

**More information**

Visit our Web site

<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 Web site.

**About Symantec**

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

**Symantec World Headquarters**

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

[www.symantec.com](http://www.symantec.com)

Confidence in a connected world.

