# Table of Contents

See All. Know More. Respond Faster. 3

Security Analytics by Symantec 3

Security Analytics Overview 3

Symantec Value Proposition 3

Product and Solution Overview 4

Why Security Analytics from Symantec? 4

  - Application Identification with Advanced Deep Packet Inspection 4
  - Machine Learning and Anomaly Detection 5
  - Threat Intelligence with Security Analytics Indicator and Rules 5
  - Real-time File Brokering to Sandbox Technologies 5
  - Comprehensive Analysis with Security Analytics 5

Automated Deep Packet Analysis in Symantec Security Analytics 7

System Architecture and Performance 8

Wide-Area System Management 10

How the Solution Works 11
See All. Know More. Respond Faster.

Sophisticated, targeted attacks can take weeks, months, or longer to discover and resolve. Incident response teams need tools that quickly uncover the full source and scope of an attack to reduce time-to-resolution, mitigate ongoing risk and further fortify the network. Like a security camera for the network, Symantec Security Analytics delivers full network security visibility, advanced network forensics, and real-time content inspection for all network activity. This effectively arms security and incident response teams to identify and detect advanced malware crossing the network, and contain zero-day and advanced targeted attacks. A comprehensive record of all network activity lets you conduct swift forensic investigations, perform proactive incident response, and resolve breaches in a fraction of the time.

Security Analytics by Symantec

Symantec delivers a comprehensive and innovative network forensics and incident response solution to enable enterprises to quickly respond to any security event. Its award-winning Security Analytics levels the battlefield against advanced targeted attacks and zero-day malware. Security Analytics enables the security operations center to deliver clear and concise answers to the toughest security questions. It's powered by full-packet capture, next-generation deep-packet inspection and indexing technologies, file brokering, and advanced malware analysis, as well as real-time threat intelligence, anomaly detection and alerting capabilities.

Security operations centers at leading global 2000 enterprises, cloud service providers and government agencies rely on Symantec Security Analytics for comprehensive network forensics, swift incident response, and real-time situational awareness. It empowers security operation centers and Governance and Risk and Compliance Management to detect and respond quickly and intelligently to advanced threats and targeted attacks while also protecting critical information assets and minimizing exposure, loss, and business liabilities.

Security Analytics Overview

Organizations are losing the battle against advanced malware and targeted attacks. Sensitive data is being stolen and networks are successfully attacked every day. Security professionals have been blind to the activities of attackers on their networks and are realizing that their prevention-based technologies alone are unable to prevent security breaches, advanced malware, and zero-day attacks.

That is why advanced threat detection, prevention, and effective preparedness have become urgent priorities as organizations accept the inevitability of successful security breaches. Security operation centers need to rely on new security technologies that allow them to gain real-time situational awareness, context, intelligence, and visibility. Symantec Security Analytics is needed not only to detect advanced threats but also to respond to major security events and attacks in a comprehensive way.

Symantec has developed a network forensics solution that enables security operation centers to hasten this shift in the security paradigm. Symantec Security Analytics records and classifies every packet of network traffic — layers 2 through 7. It indexes and stores all network data to provide 20:20 visibility of network events — all with clear, actionable intelligence. As a security camera for the network, Security Analytics provides swift and targeted responses to any threat or breach by providing a complete copy of all the traffic going in and out of the network – complete with reconstruction of the activity related to an event or breach.

Symantec Value Proposition

The award-winning Security Analytics solution prepares organizations for advanced malware and targeted attacks by allowing security professionals to answer the most important post breach questions, including the Who?, What?, When?, Where?, Why? and How? of a successful security breach. Symantec Security Analytics delivers the advanced network forensics and incident response capabilities needed for next generation security operation centers. It is the only solution capable of meeting the demands for high-performance networks operating at wire speeds. Its core components include:

- Flexible deployment options as pre-configured appliances, virtual appliances, or software on your hardware to optimize TCO and minimize capital expenses
- Lossless packet capture performance on the fastest enterprise networks
- A patented database supporting 2M+ input/output operations per second (IOPS)
- Scalable direct-attached and SAN-based storage options for very large deployments, scaling to multiple petabytes of historical network traffic
• Application classification and discovery of more than 2800 applications
• Machine-learning-based anomaly detection that learns your organization’s unique behavior and can alert on threats that are specific to your network
• Direct integration with best-of-breed security technologies such as NGFW, IPS, SIEM and endpoint technologies to create a highly efficient security and incident response ecosystem
• Intelligence Services for Security Analytics to harness the Symantec Global Intelligence Network, threat intelligence from 175 million endpoints reporting on billions of web and URL threats

Global 2000 enterprises and government agencies use these military-grade solutions to save valuable time for incident response, provide clear forensics details of what and how information was exfiltrated, and protect intellectual property and the company’s reputation from modern malware-based attacks. Understanding whether data has been compromised is an increasingly important component to complying with information security mandates. Customers who rely on Symantec gain awareness of attacks and can respond swiftly and intelligently.

Product and Solution Overview

The patented architecture of Symantec Security Analytics delivers enterprise-class network forensics and enables open interoperability, extensible storage, and portability to any network, giving security operation centers flexible deployment options while leveraging their existing investments. Key components include:

Security Analytics Appliances – Turnkey appliances with full network capture, classification, and indexing at peaks up to 10Gbps with onboard storage up to 42TB and the ability to expand capture through attached storage

Security Analytics Software – Flexible software-only option to achieve high-performance at a lower TCO and capital expense

Security Analytics Virtual Appliance (Deployed on a VMware ESX server) – the perfect option for remote or branch office locations to deliver the full capabilities of dedicated appliances and provides complete visibility into all network traffic – even traffic within the virtual host

Security Analytics Central Manager – A centralized platform that provides aggregated views from over 200 different security analytics sensors in a single pane of glass

Security Analytics Storage Modules – Modular storage capacity modules, available as direct-attached or SAN-based storage, to attain highly scalable retention of data – up to petabytes for days, weeks or months of historical network data to facilitate complete forensics investigations and rapid incident response

Why Symantec Security Analytics from Symantec?

Symantec Security Analytics differentiates itself from other security solutions in the following ways:

Application Identification with Advanced Deep Packet Inspection

Most enterprises have hundreds or thousands of applications running through their network. Security operation centers in most of these enterprises are not fully aware of all the applications that are traversing the network. Security Analytics from Symantec has the unique capability of not just classifying and identifying over 2800 applications, but also extracting detailed attributes from them to assist in clear discovery. The identification is based on stateful inspection of protocol conversations that yield precise classification of specific application activity. Furthermore, the advanced DPI engine extracts and indexes thousands of session-flow attributes enabling efficient reports of all activity associated with any indicator. This ability empowers IT organizations with information on all applications running on their network, and which hosts, users and artifacts are associated with them to reveal the complete context for any investigation.
Application security should be a top priority for any IT organization. A variety of applications—most commonly web applications—are used to penetrate network defenses and carry out advanced targeted attacks. The basic step of knowing all the applications in a network is critically important in preventing and protecting all the assets and vital information in an enterprise network. Security Analytics delivers unrivaled and comprehensive application and protocol intelligence, enabling IT organizations to regain application control and security in their networks.

Machine Learning and Anomaly Detection

Security Analytics includes a powerful machine learning engine to automate the process of establishing what a normal baseline of activity is within the organization’s network. It then uses sophisticated statistical modeling to identify and report on abnormal activity. This capability leverages the captured packet and metadata within Security Analytics to significantly reduce the manual, human effort of trying to identify malicious activity and eliminate many false positives when it comes to identifying threats. It can combine single viewed behaviors and indicators and correlate them with others to expose threats that otherwise might go undetected. Anomaly detection in Security Analytics can uncover suspicious behavior in a number of areas, including abnormal activity to restricted countries; suspicious account, endpoint, server, or network behavior; and suspicious volumes of traffic, botnet, or command and control activity.

Threat Intelligence with Security Analytics Indicators and Rules

The Security Analytics Indicators and Rules engine allows security professionals to automate the notification of targeted events in real time. Indicators can be created for suspicious, malicious, or prohibited behavior, and then rules associated with those observed packet and network behavior can automatically notify analysts of suspicious activity and violations. The Security Analytics Indicators and Rules engine enables analysts to automate common tasks such as checking for traffic against a list of known bad websites, receiving notification of unknown applications on the network, or alerting on the presence of encrypted traffic on non-standard ports.

All traffic that is captured on a Symantec Security Analytics appliance is analyzed for any known malicious web, mail and file-based threats. Security Analytics uses Intelligence Services for Security Analytics to harness the Symantec Global Intelligence Network, threat intelligence from 175 million endpoints reporting on billions of web and URL threats.

Symantec automatically updates its intelligence on millions of malicious files and URL threat indicators every day. From endpoints to servers, and at the network traffic level, we share telemetry amassed from Symantec customers across the globe, creating a deeper level of protection that no other company matches.

- Servicing 8 billion requests per day
- Protecting 80 million web proxy users
- Securing 175 million endpoints
- Protecting 63 million email users

Real-time File Brokering to Sandbox Technologies

Security Analytics extracts files in real time, and if the file is not in the local or cloud-based known-good or known-bad databases, it is immediately delivered to Symantec Malware Analysis for sandboxing detonation, analysis and risk scoring. Symantec Malware Analysis then updates the Symantec Global Intelligence Network with the verdict from the Sandbox. Security Analytics directly integrates with Symantec Malware Analysis and acts as an intelligent broker to deliver only “unknown” URLs and files for further analysis, optimizing malware inspection and analysis, while eliminating multiple false positives. Security Analytics can also leverage other third-party sandboxing technologies and provide much needed context of what happened before, during and after malware is identified.

Comprehensive Analysis with Security Analytics

Security Analytics provides a variety of analytics across the network layer—from packets, ports/protocols, and applications to user sessions and files—to strengthen security incident response with comprehensive and conclusive analysis. Security Analytics includes many powerful features for effective incident response.

Always-on Classification and Extraction – With over 2800 protocols and applications classified, Security Analytics provides complete visibility and context of network activity, exposing session-level details from layers 2 through 7.

Session reconstruction – Security Analytics reconstructs the full session from packet data, including web, email, and chat sessions, along with associated files so analysts can easily investigate security incidents without the need for packet expertise.
Media Panel – In addition to displaying all the images, video, and voice sessions traversing the network during a given time, the media panel also includes details such as Initiator and Responder IP addresses.

Artifacts and Timeline – Reconstructs numerous artifacts such as File Transfers, PDF, Word, Excel, and many more, making it easy to track the file exploit distribution and file-type activity over time for a single user or all users.

Root Cause Explorer – The explorer quickly identifies the source of an exploit or compromise and reduces time-to-resolution by correlating relevant email, IM and HTTP information and creating a chain of all HTTP referrers.

Built-In Packet Analyzer – Security Analytics includes a full-featured packet analyzer integrated into the interface, eliminating the need to transfer huge PCAP files over the network and speeding investigations.

Extended Metadata Retention – Optimize the storage available on your Symantec Security Analytics appliance and extend the window of your forensics data. Create independent allocations of storage for metadata and full packets. This enables retention and analysis of longer periods of metadata and packets—weeks, months, or more. This allows for a long-term window for trend analysis and optimizes the limited amount of storage.

PCAP Import – Security Analytics allows analysts to import data, making it easy to analyze historical data and compare captured data to a “known-good” baseline. It also allows playback of captures to verify the effectiveness of remediation measures and security enforcement tools and can use a PCAP taken from anywhere in your network and analyze it with the full power of the Security Analytics toolset.

Complex Rules Alerting – Analysts can build granular, stateful alerts, based on sequences of activity exposed by the advanced DPI engine and then delivered via email, CEF Syslog, and SNMP.

Alerts Management – To provide a comprehensive view of your network activity and highest priority alerts at first glance, the Security Analytics web interface defaults to the Alerts Management Dashboard. This new view presents a histogram of alert activity plus new “alert cards” that pivot to filtered lists of alerts and their threat scores. From this page, you can filter your alerts by IP, by indicator, or by threat level.

FIPS 140-2 Level 2 Functional Testing Validation – With FIPS (Federal Information Processing Standards) certification, Security Analytics is recognized by US government agencies as meeting very stringent standards for data processing and use of encryption. FIPS certification shows that Security Analytics can provide stronger security for your sensitive data.

Role Based Access Control (RBAC) – Sensitive information collected in the Security Analytics Platform can be masked, limiting views to specific areas of responsibility.

Strong Authentication – Security Analytics supports LDAP/AD and RADIUS authentication for access control, PKI x509 certificates, and two-factor authentication using time-based one-time password (TOTP) tokens.

SCADA analysis – Industrial Control Systems (ICS) are attractive targets for cyber attack and like the rest of the network, require complete visibility. Security Analytics supports SCADA protocol analysis and delivers the power of comprehensive forensics to industrial control environments.

Threat Analysis Report – Capture network traffic for a few days or more and then push a button to get a full report on what’s happening on your network. A full report generates with an executive summary of alerts, malicious files, SSL traffic, risky applications, anomalies and more.

Flexible Deployment Options – Symantec’s integrated appliances, software, and virtual appliances enable flexible, easy deployment – with enterprise-wide visibility and awareness. Security Analytics sensors are deployed throughout the network with the capability of monitoring thousands of networks segments – from data centers to virtual networks.
to remote offices. A central management system provides a single pane-of-glass view across multiple sensors. In addition to the ability to span across the network, Security Analytics sensors offer multiple optimized storage options. On-board storage, direct attached storage or SAN-based storage allows organizations to accommodate remote or branch offices to the largest of data centers. This gives IT organizations the ability to maintain back-in-time visibility to fully analyze an attack or breach from its inception, regardless of the size of the organization or their desired window of capture.

Augment Traditional Security with Integration – Security Analytics integrates with best-of-breed network security products to pivot directly from an alert to obtain full-payload details of the event, before, during, and after the alert. The open web services RESTful API enables integration with network and endpoint security solutions such as Symantec, HP ArcSight, IBM QRadar, FireEye, Splunk, Cisco Sourcefire, Guidance Software, CounterTack, Carbon Black, Reversing Labs, Tripwire, Ziften, and many others. This integration with next-generation firewall (NGFW), intrusion prevention system (IPS), security information event management (SIEM), sandboxing and endpoint security solutions leverages a security operations center’s existing technology while providing context to alerts and logs and expediting incident response.

Symantec Security Analytics delivers unprecedented visibility and control over packet, application, session, protocol, and user data traversing the network, while enhancing and providing added value to existing security investments.

Automated Deep Packet Analysis in Symantec Security Analytics

Next-generation threats ignore standards of communication and take advantage of systems that look for existing signatures and expect to see the status quo. We can’t just assume, for example, that any traffic on TCP port 80 is HTTP because next-generation threats will try to hide themselves in all types of traffic. Today’s security and incident response teams must be able to classify network traffic by protocol and application – and by the attributes within them – in order to have the visibility needed to discover and remediate next generation threats. Security operation centers need solutions that can provide advanced deep packet inspection (DPI), application and attribute classification of all network traffic, in real time. The ability to extract data from network traffic at this depth provides a richness and accuracy that paints a vivid picture for analysts and investigators to help them find anomalies and threats. The Security Analytics Platform implements DPI using protocol parsers that track state transitions to precisely classify flows and extract rich metadata to present a complete context of flows for advanced threat detection.

Symantec Security Analytics helps you visualize and analyze network data and uncover specific network activity – without requiring specific knowledge of networking protocols and packet analysis methods. Its powerful features let you locate system compromised, or did your active defenses block the attack? Now you can pivot directly to a view of that endpoint within Symantec ATP to see what happened once the malicious file reached the endpoint.

Security Analytics also includes pivot integration from Security Analytics to Symantec DeepSight as well. Incident Responders now can get the deep and detailed adversary threat intelligence DeepSight Provides including vulnerabilities, malware, indicators of compromise, adversary campaigns, their tactics/techniques and procedures and profiles of tracked adversaries. They have a full view of relevant threats and exposures and most importantly, this is based on managed research, leveraging Symantec’s industry leading threat research professionals.

Symantec Security Analytics delivers unprecedented visibility and control over packet, application, session, protocol, and user data traversing the network, while enhancing and providing added value to existing security investments.
and reconstruct specific communication flows, as well as network and user activities, within seconds. The platform does this by classifying captured network packets and identifying meaningful data flows. A flow is the collection of packets that comprises a single communication between two specific network entities. Within a particular data flow, you can then identify and examine network artifacts such as image files, Word documents, emails, and video, as well as executable files, HTML files, and more. Security Analytics also allows you to reconstruct HTML pages, emails, and instant messaging conversations.

Security Analytics provides the ability to do real-time, policy-based artifact extraction, and is not limited to any specific operating system (OS) environment. Extracted artifacts can be automatically placed in centralized network repositories for analysis by forensics tools within Security Analytics as well as other security tools in your toolset. These artifacts are hashed and stored for “future retrospective analysis” on newly discovered malware variants and provide a method to understand relatedness to preexisting hashes.

**System Architecture and Performance**

The Security Analytics appliances, virtual appliances, and software meet the requirements of small to large enterprises. Security Analytics sensors are able to achieve this based on the underlying file and system architecture that were designed with efficient capture and query performance from its genesis. This architecture has proven scalability in demanding environments with many deployments across Global 2000 companies.

At its most basic level, the solution takes network data packets from a network interface card (NIC), classifies the network flows, and then moves that data to storage in a specialized format that has been optimized for extremely high throughput, accuracy, manageability, and security. In addition to enabling organizations to capture 100% of network traffic, Security Analytics also provides complete control over the type of traffic captured using Berkeley Packet Filters (BPFs), providing the ability to filter network traffic, either during capture or when replaying captured traffic at a later time, inclusively or exclusively. Filtering traffic at the point of ingestion can be useful to you if you have a regulatory or compliance concern that prevents you from capturing certain network traffic.

As a Security Analytics sensor captures and stores each packet, reference and metadata is extracted and stored, providing highly efficient query, response and reconstruction of captured packet data. These attributes include data related to the packet, applications, users, and session flow, providing full context surrounding the network traffic. Detailed attributes include items such as IP and MAC address, protocols, ports, application names, user identities, actions, email attributes, and thousands of other metadata.

![Figure 4](image-url)

The Security Analytics File System is a custom-built file system that contains all network packets, both header and payload. It is based on a “Slot Architecture” of N*64MB slots, which corresponds directly to associated ring buffers in memory. Captured data is formatted and moved to disk using direct memory access (DMA). As shown in the graphic above, the Security Analytics DB Bitmask & Hash layer (top) maps metadata and other search attributes to each and every 64MB memory or storage slot that contains relevant data.

The Security Analytics DB Index layer (middle) contains the data necessary to find and reconstruct packets, flows, and entire network sessions in perfect fidelity (lossless). Search queries are processed using a proprietary algorithm that generates hash values used by the top layer of the search engine (bitmask & hash) to quickly determine which 64MB slots the data are in. When a Security Analytics sensor has captured a network traffic stream, the stream becomes immediately available for replay and analysis.

Security Analytics not only performs full packet capture, but also provides a tremendous amount of metadata derived from DPI and other methods of packet and flow analysis. Simultaneously with full packet capture, Security Analytics indexes thousands of elements of metadata into a highly optimized custom database. This performance enhancement
provides for highly accelerated and efficient queries. These queries drive much of the Security Analytics user interface, an intuitive, operating system and browser-agnostic Web UI that provides a contextual view to the security analyst. User-defined dashboards provide instant situational awareness of network activity and events, and a front-end to the system’s ability to deep-dive into network flows.

As packets are captured, attributes such as protocol, source/destination MAC/IP, port, VLAN, are stored and serve as the data source to the GaugeFS virtual file system. This allows near instantaneous access to any captured data navigable through a familiar folder hierarchy. Unlike files on a conventional file system, the data available through GaugeFS does not occupy any space; instead, it dynamically retrieves packets by querying the Security Analytics DB for the location of the requested packets directly from the capture file system.

The virtual file system also provides the capability to instantiate “any to any” relationships between all metadata (applications, filenames, etc.) and quickly presents the full context of all activity surrounding a given set of search criteria. Metadata and indices are always stored on a separate disk array for performance reasons, and metadata can generally be stored longer than packet data. By using the available metadata, analysts are able to efficiently narrow their search criteria and minimize the amount of packet data needed to perform detailed incident response or artifact extraction.

Other unique characteristics of GaugeFS are the inclusion of timespans, Boolean query logic, and ranges. Timespans are an optional top-level path within the GaugeFS hierarchy. If a timespan is not used, then all packets within the capture file system matching the attributes described by the GaugeFS path will be presented in the result data. In many cases, it is desirable to constrain the data retrieval to a specific time-domain. Descending into a timespan path provides this sort of constraint so that the resulting PCAP matches not only packet attributes but also time attributes.

Although each model of a Security Analytics sensor is slightly different, they all have a common overall structure. There is a collection of hard drives, which are separated into three distinct functional areas. The largest is the storage array. This collection of disks is where all the incoming raw data is stored. The next largest is the indexing array, which contains the custom database which stores all the metadata about the packets (where they came from, where they were going to, their time, and so on). The smallest is the system array, which contains the operating system and related storage. This is also where any artifacts and reports are created and stored.

- Storage Array – Raw network data, stored as received across multiple HDs
- Indexing Array – Metadata stored and indexed using multiple HDs
- System Array – Linux operating system on multiple HDs
- As packet capture data is collected, Security Analytics performs the following functions:
  - Stores the full contents of the packet capture data
  - Records the data reference and the metadata about each packet (size, IP addresses, ports, etc.)
  - Builds an index of the data and metadata in each conversation (time, ports, URLs, login information, application ID, etc.)

The combination of the patented packet capture file systems, multiple indexes, application classification, metadata extraction, and the underlying hardware components enable superior performance and scalability.

**Integration using the RESTful API for Security Analytics Platform:** The Security Analytics Platform provides a RESTful API, allowing packet capture data to be described and retrieved though a simple HTTPS request. This allows for the easy integration into other software platforms, such as an IDS/IPS, firewall, SIEM sandboxing and endpoint technologies. Security Analytics also provides JSON data sources to start or stop captures, retrieve interface statistics, artifact extraction, capture status, capture filters and reporting. These capabilities provide the freedom to integrate current and future tools/equipment with an open architecture utilizing industry standard protocols.
Wide-Area System Management

The Security Analytics Central Manager is a dedicated instance of Security Analytics (Software, Appliance or Virtual Appliance) running the Central Manager Software. This Central Manager provides a centralized query, reporting and management interface for all Security Analytics managed sensors connected to the Central Manager. The Central Manager provides:

- Single view of query, result and report data for all managed sensors
- Parallel query execution for all managed sensors
- Centralized configuration and management for all managed sensors
- Centralized provisioning of user, RBAC, and authentication
- Central software upgrade host for all managed sensors

All communications between the managed sensors and Central Manager are conducted over a dedicated Virtual Private Network (VPN), with each link between a managed sensor and the Central Manager having its own separate VPN connection operating within a common VPN subnet. Communications over the VPN subnet are protected by industry-standard SSL/TLS encryption using strong encryption keys. In order to complete the connection between the Central Manager and managed sensors, the managed sensor must be able to connect to the Central Manager via HTTPS.

The Security Analytics Central Manager will support over 200 Security Analytics managed sensors. The Central Manager is capable of operating in an Active/Active clustered and decentralized configuration, providing Continuity of Operations (COOP), with each Central Manager maintaining full state of the other, in case of a failure condition. A heartbeat method is implemented to verify health and state of the Central Manager. Managed sensors also utilize the cluster failover capability based on heartbeat and response from the primary Central Manager. A Central Manager failover occurs within a five second window.
How the Solution Works

This solution allows end users to achieve full situational awareness and investigate security incidents in real-time using Security Analytics. Symantec’s unique architecture allows the Security Analytics sensors to query all network data, utilizing parallel query architecture.

Given the expense of staffing a skilled incident response team, the ability of Security Analytics to reduce ‘time-to-insight’ by orders of magnitude will make the incident responders much more productive. The Symantec Security Analytics architecture scales better than any comparable architecture, primarily because it requires only a single device for all operations while the nearest competitor requires multiple devices such as a packet capture devices and a separate device for metadata and analysis.

In summary, Symantec Security Analytics offers the most efficient packet capture appliances and the most advanced enterprise architecture in the industry. The ability to handle data rates with peaks up to 10Gbps with only a single appliance and a high-performance storage subsystem, makes Symantec Security Analytics the clear technology solution to meet the increasingly demanding requirements of proactive incident response and advanced network forensics.

Learn more about Symantec Security Analytics. Visit our website go.symantec.com/security-analytics
Contact your Symantec Product Specialist or partner representative for a demo or trial of Security Analytics.

Figure 6: Typical Deployment Of Security Analytics Solution

Learn more about Symantec Security Analytics. Visit our website go.symantec.com/security-analytics
Contact your Symantec Product Specialist or partner representative for a demo or trial of Security Analytics.

Learn more about Symantec Security Analytics. Visit our website go.symantec.com/security-analytics
Contact your Symantec Product Specialist or partner representative for a demo or trial of Security Analytics.

Learn more about Symantec Security Analytics. Visit our website go.symantec.com/security-analytics
Contact your Symantec Product Specialist or partner representative for a demo or trial of Security Analytics.

Learn more about Symantec Security Analytics. Visit our website go.symantec.com/security-analytics
Contact your Symantec Product Specialist or partner representative for a demo or trial of Security Analytics.

Learn more about Symantec Security Analytics. Visit our website go.symantec.com/security-analytics
Contact your Symantec Product Specialist or partner representative for a demo or trial of Security Analytics.

Learn more about Symantec Security Analytics. Visit our website go.symantec.com/security-analytics
Contact your Symantec Product Specialist or partner representative for a demo or trial of Security Analytics.