# Symantec Security Analytics:

## A Cornerstone of Effective Security Incident Response

WHITE PAPER

# Table of Contents

# Integrated Cyber Defense

Today's threat landscape is populated by increasingly sophisticated intrusions that take the form of advanced persistent threats, advanced targeted attacks, advanced malware, unknown malware, and zero-day threats. Enterprises are experiencing material security breaches as a result of these attacks because advanced security operations teams – as well as the defenses they deploy – operate in silos with limited ability to share information across the entire security organization or environment.

Symantec's Integrated Cyber Defense (ICD) platform unifies products, services, and partners to drive down the cost and complexity of cyber security while protecting enterprises against sophisticated threats. ICD combines information protection, threat protection, identity management, compliance, and other advanced services, powered by shared intelligence and automation across endpoints, networks, applications, and clouds.

# Security Analytics by Symantec

Symantec delivers a comprehensive and innovative network forensics solution to enable enterprises to detect and respond to security events quickly. 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 to enable threat detection, 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 inevitably 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, enriches and stores all network data to provide complete visibility of network events – all with clear, actionable intelligence. Like 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 a reconstruction of the activity related to an event or breach.

## Security Analytics

### Complete Answers for Focused Resolution

Security Analytics
System of Record

> "At a minimum, organizations should capture 30 days' of packet data. 60 days' worth is even better."

SANS

**Records all traffic** – 24/7 lossless packet capture (header and payload) – days/weeks/months

**Massive intelligence** – Enriches with Symantec and 3rd party threat and reputation data

**Reconstructs all evidence** – Artifacts, flows, files, and activity in human-readable form

**Security Analytics** – Doesn't disrupt the Networking / IT department

*Figure 1*

# 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
- Scalable storage options for very large deployments, scaling to multiple petabytes of historical network traffic
- Application classification and discovery of more than 2,800 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 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, data enrichment and indexing at peaks up to 10Gbps with onboard storage up to 42TB and the ability to expand capture through attached storage to support up to 1.5PB of storage per appliance

**Security Analytics Virtual Appliance** – 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 in the Cloud** – Security Analytics supports deployment in cloud environments – This means the same forensics and visibility you have for on-premises protection can now provide the same visibility and incident response capabilities for your cloud workloads.

**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 high-density storage arrays, 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

**Context-aware Integration** – A powerful API enables Security Analytics to integrate with leading security solutions to facilitate incident response and remediation workflow

## Security Analytics

### Components

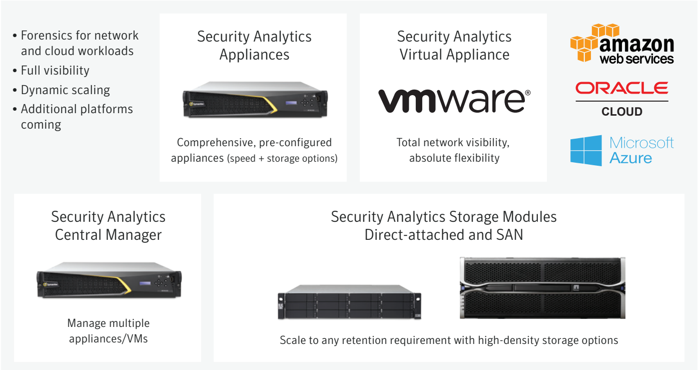

• Forensics for network and cloud workloads
• Full visibility
• Dynamic scaling
• Additional platforms coming
Security Analytics Appliances
Comprehensive, pre-configured appliances (speed + storage options)
Security Analytics Virtual Appliance
vmware®
Total network visibility, absolute flexibility
amazon web services
ORACLE CLOUD
Microsoft Azure
Security Analytics Central Manager
Manage multiple appliances/VMs
Security Analytics Storage Modules Direct-attached and SAN
Scale to any retention requirement with high-density storage options

*Figure 2: Symantec Security Analytics Product Portfolio*

# Why Security Analytics from Symantec?

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

## Application Identification with 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 2,800 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 a 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.

## Threat Intelligence with Security Analytics Alerts and Services

The Security Analytics Indicators and Rules engine allows security professionals to automate the notification of targeted events in real time. The engine can create indicators for suspicious, malicious, or prohibited behavior, and the rules associated with that 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.

The Symantec Security Analytics appliance analyzes all the traffic that it captures 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 10 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 Content Analysis for sandboxing detonation, analysis and risk scoring. Symantec Content Analysis then updates the Symantec Global Intelligence Network with the verdict from the Sandbox. Security Analytics directly integrates with Symantec Content 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 a 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 2,800 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 reconstructing all packet data and 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, together with additional media-related metadata.

**Geolocation** - With Security Analytics Geolocation you see the origin and destination of all network traffic. Identify patterns and concentrations of traffic traveling to and from non-traditional locations. See hot spots of activity, zoom-in on specific paths and flag IP addresses, locations or even countries as suspicious. Abnormal traffic patterns may be your starting point of an investigation and reduce your time to resolution. Export any network traffic as a .klm file and import into Google Earth. "Traffic to a restricted country – that's not right!"

**Artifacts and Timeline** – Reconstructs numerous artifacts such as File Transfers, PDF, .EXE, 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.

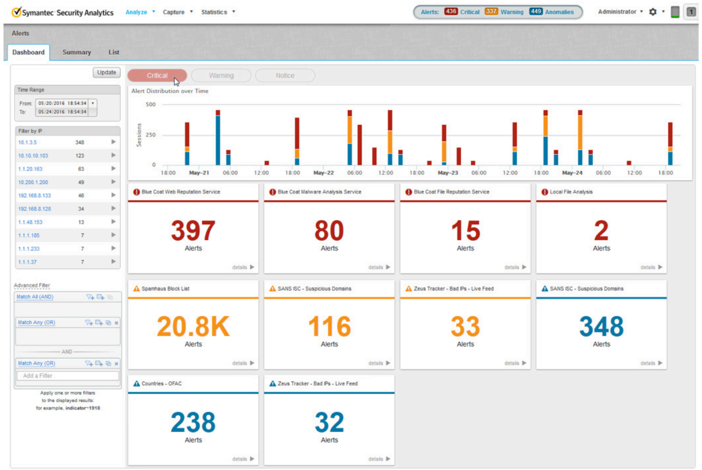
**Built-In Packet Analyzer** – Security Analytics includes a full-featured packet analyzer integrated into the interface, eliminating the need to transfer huge PCAP files over the network and speeding investigations.

**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, enabling retention and analysis of longer periods of metadata and packets—weeks, months, or more. The extended retention allows for a long-term window for trend analysis and optimizes your 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.



Time Range
From: 05/20/2016 18:54:34
To: 05/24/2016 18:54:34

| Filter by IP | |
|---|---|
| 10.1.3.5 | 348 |
| 10.10.10.103 | 123 |
| 1.1.20.163 | 63 |
| 10.200.1.200 | 49 |
| 192.168.8.133 | 46 |
| 192.168.8.128 | 34 |
| 1.1.48.153 | 13 |
| 1.1.1.185 | 7 |
| 1.1.1.233 | 7 |
| 1.1.1.37 | 7 |

Apply one or more filters to the displayed results: for example, indicator~1918

Blue Coat Web Reputation Service: 397 Alerts
Blue Coat Malware Analysis Service: 80 Alerts
Blue Coat File Reputation Service: 15 Alerts
Local File Analysis: 2 Alerts
Spamhaus Block List: 20.8K Alerts
SANS ISC - Suspicious Domains: 116 Alerts
Zeus Tracker - Bad IPs - Live Feed: 33 Alerts
SANS ISC - Suspicious Domains: 348 Alerts
Countries - OFAC: 238 Alerts
Zeus Tracker - Bad IPs - Live Feed: 32 Alerts

*Figure 3: Alerts Management Dashboard*

**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.

**Risk and Visibility 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, virtual appliances, and cloud offerings 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 and virtual networks to remote offices and your cloud workloads. 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. Onboard storage, direct attached storage, or high-density storage arrays 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. This integration with next-generation firewall (NGFW), intrusion prevention system (IPS), security information event management (SIEM), sandboxing and endpoint security solutions leverage a security operations center's existing technology while providing context to alerts and logs and expediting incident response.

## Security Analytics

### Incident – Response – Forensics

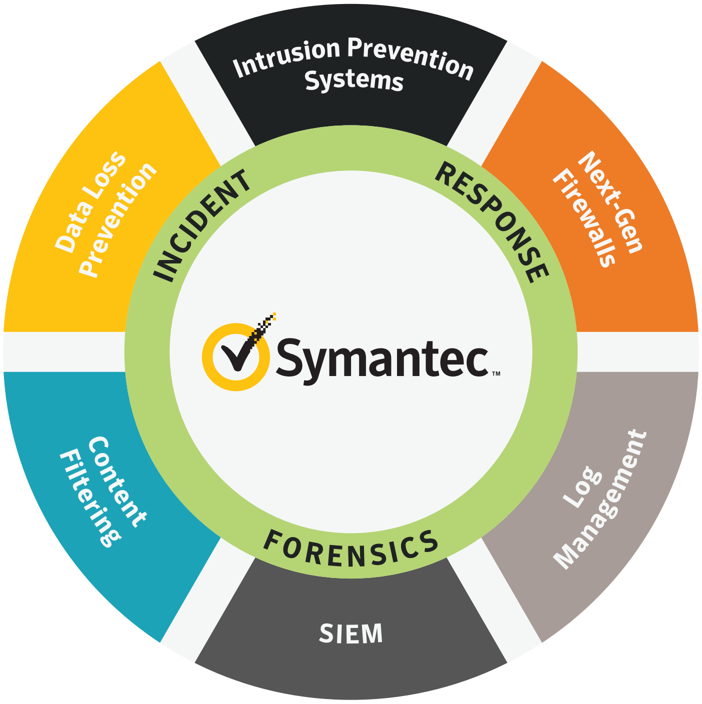


*Figure 4: Comprehensive Integrated Partner Ecosystem*

Sometimes, even network visibility and forensics are not enough. Utilizing the API, you can leverage the power of endpoint technologies like Symantec Endpoint Protection (SEP) to correlate your network forensic findings with endpoint forensics. For example, in Security Analytics, you may observe that a malicious file was transferred to a particular endpoint. However, what happened after that? Was the system compromised, or did your active defenses block the attack? Now you can pivot directly to a view of that endpoint within SEP Manager 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.

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 try to hide 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 – 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. Security Analytics 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.

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 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 forensic 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 can achieve this based on the underlying file and system architecture that was 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 sessions, 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 which packets are retained using Intelligent Capture (IC). With IC, all packets for a particular session are indexed, but the determination of whether or not to retain those packets is based on the application of user-defined rules to the meta data extracted from that session. This provides fine-grained control for packet retention policies while gathering all essential meta data. Fine-grained control over packet retention 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 estimated 3,200 attributes include data related to the packet, application, user, and session, as an example. These metadata elements provide full context surrounding the network traffic when evaluated in context. Other detailed attributes include items such as IP and MAC address, protocols, ports, application names, user identities, actions, email attributes, and thousands of other metadata.

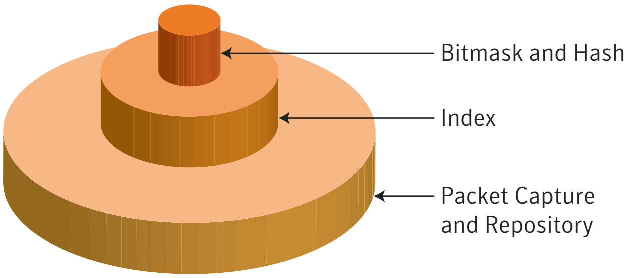


*Figure 5: Security Analytics Layered Data Model*

The Security Analytics File System contains all network packets, both header, and payload. It is based on a “Slot Architecture” of variable-length slots which correspond directly to associated ring buffers in memory. As shown in the graphic above, the Security Analytics DB Bitmask & Hash layer (top) maps metadata, and other search attributes to every 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 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 over 3,200 types 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, structured around the associated metadata. 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, and more) 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 can 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 are 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 packet 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.

- Packet 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 unique combination of the 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** – Security Analytics provides a RESTful API, allowing packet capture data to be described and retrieved through a simple HTTPS request. The API 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.

## Security Analytics

### Scalable Architecture

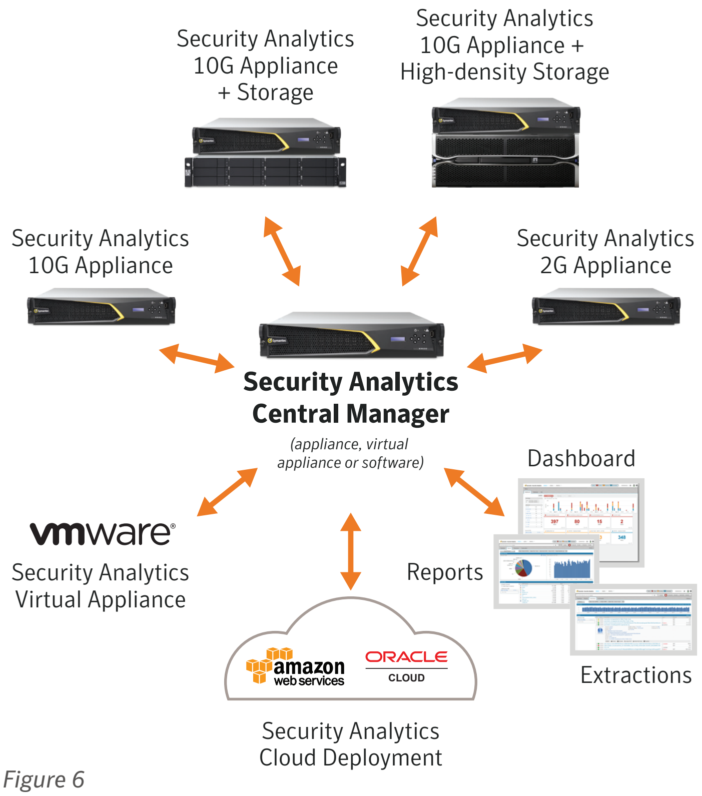


*Figure 6*

# Wide-Area System Management

The Security Analytics Central Manager is a dedicated instance of Security Analytics (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 the user, RBAC, and authentication
- Central software upgrade host for all managed sensors

All communications between the managed sensors and Central Manager occur over a dedicated Virtual Private Network (VPN), with each link between a managed sensor and the Central Manager having its 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. 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.

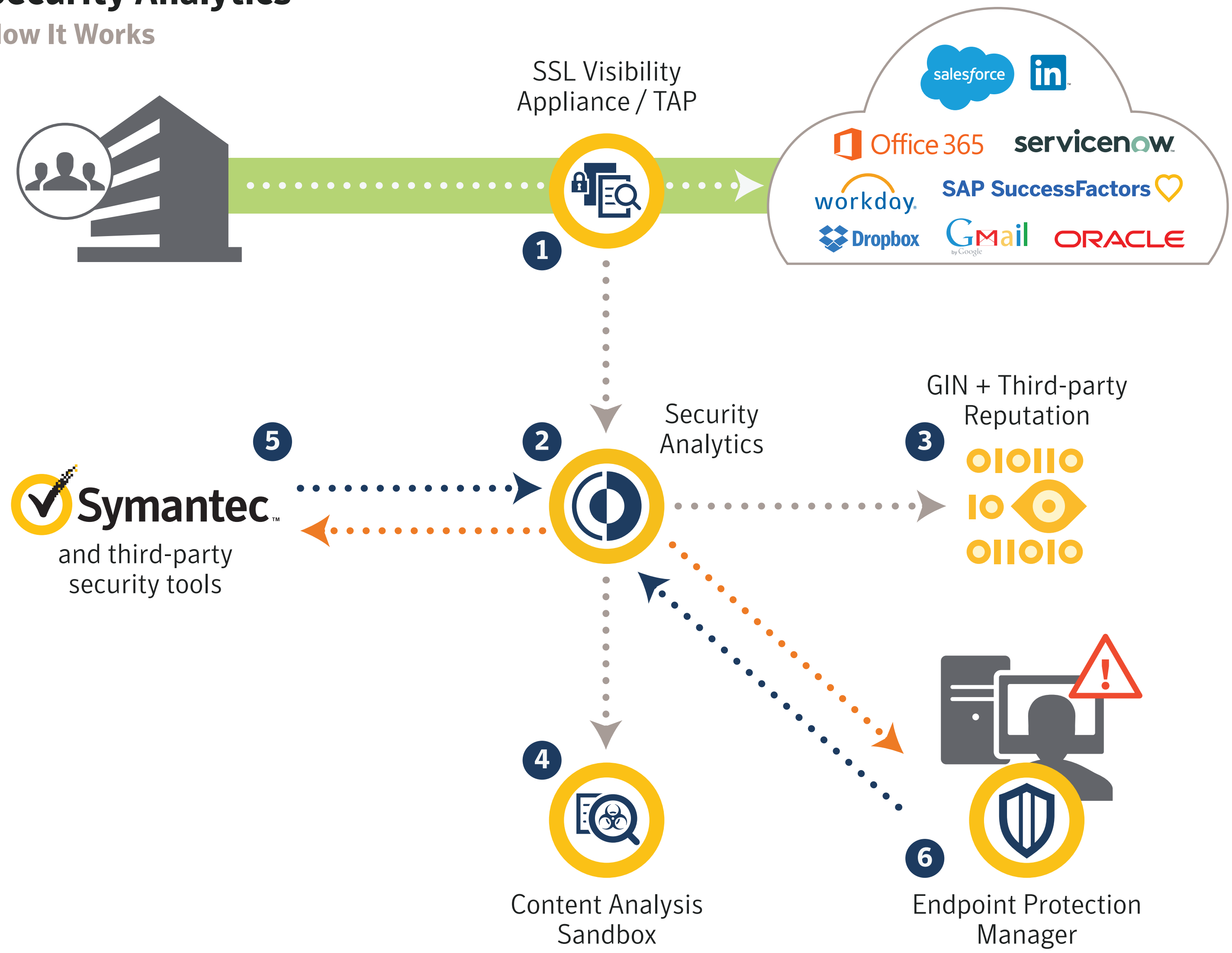
The Security Analytics Central Manager supports over 200 Security Analytics managed sensors. The Central Manager is capable of operating in an Active/Active clustered and decentralized configuration, providing Continuity of Operations (COOP), with each Central Manager maintaining a full state of the other, in case of a failure condition. A heartbeat method is implemented to verify the 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.

## Security Analytics

### How It Works



1 Security Analytics sits passively off the network (SSLV or TAP)

2 Captures all network traffic (packet header/payload)

3 Taps GIN and outside threat intelligence to enrich packet data

4 Unknown files sent to Content Analysis/3rd party to Sandbox

5 Alerts from SA or other tools may trigger an investigation

6 Incident response team finds source/scope of attack, resolves

*Figure 6: Typical Deployment of Security Analytics Solution*

Given the expense of staffing a skilled incident response team, the ability of Security Analytics to reduce 'time-to-insight' by orders of magnitude makes 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 device 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.

# More Information

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.

## About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec.

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

Copyright ©2019 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.