Symantec Security Analytics Software

See, Understand, and Resolve Advanced Attacks

Advanced targeted attacks, customized malware, and zero-day attacks are infiltrating networks at record speeds. Traditional security solutions are simply not keeping pace. In fact, recent reports indicate that the vast majority of attacks compromised their target in a matter of hours, minutes, even seconds, while 75% of attacks take days, months, even years before they are discovered and resolved. Symantec has a solution. Symantec Security Analytics Software, delivers the full visibility, security analytics, real-time threat intelligence and "system of record" you need to successfully uncover advanced threats and further protect your infrastructure and your workforce.

Simple Solution, Sophisticated Results

Symantec Security Analytics Software is an integral part of the Blue Coat Security Platform's Incident Response and Forensics solution, providing the intelligence and real-time analysis you need to protect against today's advanced security threats. Security Analytics Software enables you to see, understand, contain, and prevent the emerging, targeted attacks facing your organization. It offers a simple solution that provides:

- **Cost Reductions:** Uses cost-effective, industry-standard, server-class hardware platforms that enable you to lower capital expenditures and reduce your overall footprint.
- **Comprehensive Coverage:** Seamlessly fits into all corners of your organization, from the data center to remote/ branch offices, with the performance and scalability needed to support large-scale, multi-location deployments.
- **Investment Protection:** Leverages your existing security processes, workflows and technology investments and enhancing them with valuable insights into the traffic and threats in your environment. The solution can also easily expand as your coverage and storage needs grow.
- **Central Management:** Gives you enterprise-wide visibility across software, appliance and virtual appliance deployments.

Gain Visibility into Advanced Threats

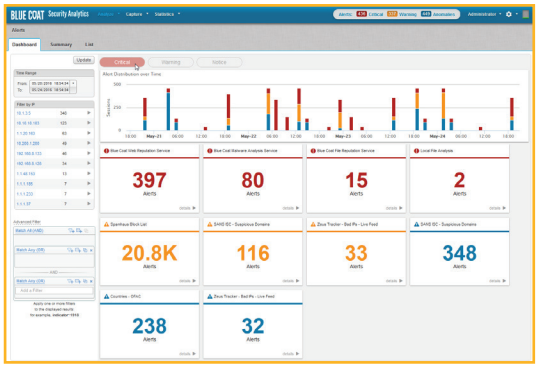
- **Complete Network Capture (Layers 2-7):** Provides you insights into all your network traffic, including communications between the applications running in your virtual networks; providing the indexing, classification, anomaly detection, storage and replay capabilities you need to gain a full understanding of what is happening in your network.

At-a-Glance

The Security Analytics Software enables you to:

- Accelerate Incident Response and Forensics to Contain and Remediate Attacks – Provides context around what is happening in your network to support fast incident response and resolution and streamlined post-breach forensics.
- Reduce Costs – Uses cost-effective, industry-standard, server-class hardware platforms to lower capital expenditures and reduce your overall footprint; centralized management enables you to streamline security response.
- Gain Visibility into Advanced Threats – Provides 100% situational awareness of your network traffic, with full traffic capture, classification and deep packet inspection capabilities.

- **Visibility into Encrypted Data:** With Symantec SSL Visibility, Security Analytics Software provides complete visibility into threats that hide within encrypted traffic.
- **Application Classification:** Offers comprehensive deep-packet inspection (DPI) to provide you a deep understanding of the types of applications running in your environment. It can classify more than 2,500 applications, with thousands of descriptive metadata attributes, including content types, file names, and user personas that are classified for easy analysis and recall.
- **Real-time Threat Intelligence:** Leverages the security alerts and threat intelligence of the Symantec Global Intelligence Network and numerous 3rd-party intelligence providers to deliver actionable intelligence on web, file, and email threats in real time.
- **Anomaly Detection:** Performs advanced statistical analysis on your captured data and baseline of your organization's network traffic and user activity. Security Analytics alerts you to anomalous behavior where you can pivot to the Anomaly Investigation view to see when the anomaly occurred, how often, and which parts of the network were involved.



Accelerate Incident Response and Forensics to Contain and Remediate Attacks

Symantec Security Analytics Software gives you the insight and evidence you need to get the answers to your most difficult post-breech questions, including: How did they do it? Which data/systems were affected? Do we know the full scope of the attack? Is it over? How do we prepare for subsequent attacks? With this information, you can quickly contain and remediate the full extent of a breach and support post-breach forensics activities. The Software provides:

- **Unified Security Analytics:** Provides comprehensive analysis of advanced threats, targeting both your physical and virtualized assets, with actionable intelligence that supports the quick containment and remediation of breaches in your environment. The complete session, file and object reconstruction, data visualization, timeline analysis, IP geolocation, and trend analysis help you quickly identify and shut down attack activity; the analytics can also be used to support post-breach forensic activities.
- **Context-Aware Security:** Enriches the information your security infrastructure uses to protect your environment, by providing needed context to alerts so you know what happened before, during and after any alert from your existing security solutions. It allows you to pivot directly from any alert or log and obtain full-payload details of the event. You can leverage leading network and endpoint technologies such as Carbon Black, Cisco, CounterTack, FireEye, Guidance Software, HP ArcSight, Splunk, Tripwire, and many other security applications.
- **Root Cause Explorer:** Uses extracted network objects to reconstruct a timeline of suspicious web sessions, emails, and chat conversations. By automatically enumerating these events, Root Cause Explorer helps security analysts quickly identify the source of an infection or compromise and reduce time-to-resolution.
- **On-demand Incident Response:** Enables flexible remote deployment anywhere in the network to accelerate incident response and breach investigations.

Symantec Corporation **World Headquarters** 350 Ellis Street, Mountain View, CA 94043 USA
1.800.721.393 www.symantec.com