Symantec Security Analytics Virtual Appliance

Delivering Security Visibility and Intelligence for Any Virtual Environment

At A Glance

The Security Analytics Virtual Appliance enables you to:

Achieve Full Security Visibility

- Gives you visibility and retrospective analysis into all your network traffic, with full traffic capture and replay, classification, anomaly detection and deep inspection capabilities.

Provide Real-Time Visibility for Virtual Assets

- Delivers the context you need to understand what is happening in your virtual environments to support fast incident response and resolution.

Save Time and Money

- Provides a single, unified view of your infrastructure that makes it simple to conduct incident response and achieve real-time situational awareness.

Virtualizing your IT resources – from data centers and mission-critical systems to applications – can help you reduce capital expenses and increase utilization rates; securing these virtualized resources, however, often introduce new security challenges. Most organizations have very little visibility into what is happening within their virtualized environments, making it extremely difficult to protect their virtualized assets from the advanced malware and targeted attacks that threaten their operations and integrity. The Symantec Security Analytics Virtual Appliance, which is part of our Incident Response and Forensics solution, gives you the comprehensive visibility you need to effectively protect all your assets, physical and virtual alike. It provides you a unified view of all your network traffic and delivers valuable retrospective analysis, unified security analytics and threat intelligence, so you can better protect your virtual assets, wherever they reside, to maximize their benefits.

Achieve Full Security Visibility

You can't protect what you can't see or monitor; this is why you need visibility into your entire environment, including both your physical and virtualized assets, so you can effectively protect what is critical to your organization. The Security Analytics Virtual Appliance gives you full enterprise-wide visibility and retrospective analysis, so you can quickly understand what is happening within your varied environments and the threats you are facing. The Security Analytics Virtual Appliance provides:

- Complete Network Capture, Layers 2-7: Gives 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.

Symantec

- Real-time Threat Intelligence: Leverages the Symantec Global Intelligence Network to provide actionable intelligence on web, file, and email threats in real time.

- Application Classification: Uses 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 details. This feature efficiently provides descriptive information about a network session, including application, identity, geographic location and more.

- A Flexible Virtual Appliance that Supports All Environments: Ensures you can deliver consistent protection, regardless of where your assets are located – works within both physical and virtual networks, including cloud (private, hosted or hybrid), and can be easily deployed in remote/branch office environments. The solution provides the performance and scale needed to match the rapid growth of your data centers, servers, applications and network traffic.

Provide Real Visibility for Virtual Assets

The Security Analytics Virtual Appliance provides the monitoring and real-time situational awareness you need to take the appropriate action, facilitate swift incident response and protect your assets. With the Security Analytics Virtual Appliance you have:

- Comprehensive Network Forensics: Performs full network packet capture, indexing, classification, replay and reconstruction of all network traffic to enable retrospective analysis and speed network breach investigations.

- 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 analytics can also be used to support post-breach forensic activities.

- 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.

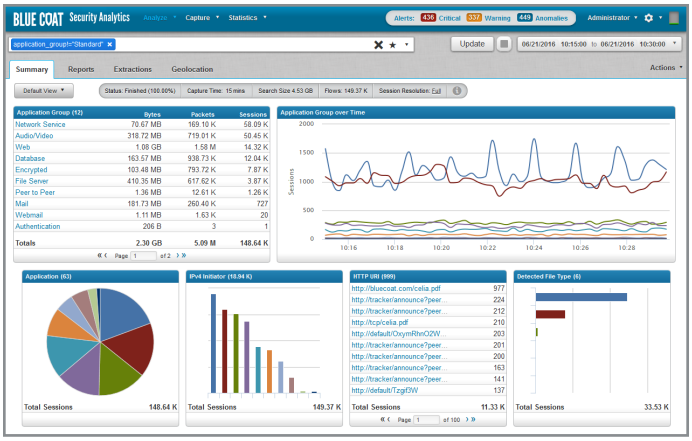
- Context-Aware Security: Delivers greater context by leveraging existing security processes and workflows, as well as available security alerts and threat intelligence. The solution can capture and port all virtual traffic to other best-of-breed network security technologies in your network to improve the overall effectiveness of your security infrastructure. It allows you to pivot directly from any alert or log and obtain full-payload details of the event, before, during and after the alert. You can leverage leading 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, this tool reconstructs a timeline of suspect web sessions, emails, and chat conversations. By automatically enumerating these events, Root Cause Explorer helps the analyst quickly identify the source of an infection or compromise and reduce time-to-resolution.

Save Time and Money

The Security Analytics Virtual Appliance enables you to make the most of your infrastructure investments, helping you record all activity and analyze threats, so you can ensure appropriate measures are in place to protect and optimize your environment. With the Security Analytics Virtual Appliance you can save time and money through:

- Virtualized Central Management: providing a single, unified view of your infrastructure to support effective incident response and forensics, real-time situational awareness and continuous monitoring.
- IT Footprint Reduction: saving you valuable resources with minimal capital expenditures; enabling easy deployment and management in stand-alone or distributed networks.
- On-demand Incident Response: enabling flexible remote deployment anywhere in the network to accelerate incident investigations and breach responses.



About Symantec

Symantec Corporation World Headquarters

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

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, 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 suite of products for protection at home and across all of 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 or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_ds_Security_Analytics_Virtual_Appliance_EN_v2a