Symantec Security Analytics

See, Understand, And Swiftly Respond To Advanced Threats

Today's advanced malware and zero-day attacks fly under the radar of traditional security technologies. As a result, organizations are accepting the fact that at some point their networks will be breached. That is why a shift is now underway toward a more modern strategy – a comprehensive approach that provides the intelligence and real-time analysis needed to see, understand, respond to, and fortify the network against advanced threats and targeted attacks. Symantec Security Analytics closes the security gap by combining security visibility, security analytics, and real-time intelligence for immediate detection and effective incident response. Simply put, it enables advanced network forensics and swift incident response and empowers your security teams to get beyond fear and anxiety about each new security threat – and start seeing new possibilities for your business.

Adapt to the Evolving Threat Landscape

The number, variety, and sources of security attacks are all in an upward spiral. Thousands of new malware samples appear every day and advanced zero-day threats, sophisticated malware, and targeted attacks from outside sources or even employees are constantly increasing in size and scale.

Traditional blocking strategies simply aren't effective against advanced attacks. As security landscapes continue to evolve, security and incident response teams will need adaptable and customized solutions that overcome the gaps in today's signature-based tools and deliver complete visibility of everything going in and out of the network – even in the face of rapid growth and huge volumes of network traffic. And to efficiently address the growing void in their security frameworks, organizations will also require simple, flexible and cost effective security solutions.

Security Analytics, an integral part of the Symantec Incident Response solution, closes the security gap and overcomes the major challenges of preparing for the unknown and protecting against ongoing attack, including:

- Complex ecosystems, processes and workflows
- The ability to leverage the most comprehensive sources of real-time threat intelligence while delivering a full record of all activity before, during and after an attack
- Scaling to meet organization growth, the need for centralized security management, and increasing network performance demands

$4M
Total average cost of a breach

$158
Average cost per record breached

48%
of breaches are malicious attacks

Source: Ponemon Institute, 2016

Clear Intelligence, Right Now

Symantec Security Analytics gives security professionals clear and concise answers to the critical post-breach security questions, including: Who did this? How? When? What was accessed? This award-winning platform can be deployed on your own industry-standard hardware, as pre-configured appliances or as a virtual appliance that records and classifies every packet of network traffic – from Layer 2 through Layer 7 – while indexing, classifying, enriching, and storing the data to provide comprehensive threat intelligence and post-breach analytics on any security event.

The result is actionable evidence for swift incident response and forensics; real-time situational awareness; continuous monitoring; IT governance, risk management and compliance; and security assurance.

Key Capabilities and Benefits

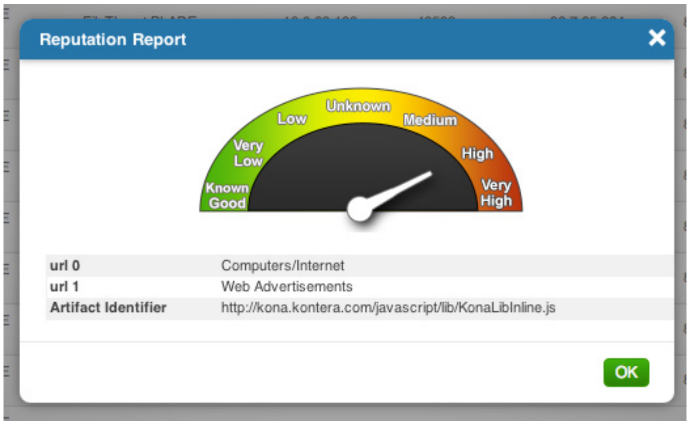
Security Analytics is the only solution that is flexible, cost-effective and integrates with multiple highly-reputable threat intelligence sources and next-generation sandboxing technology for comprehensive real-time visibility and retrospective forensics analysis. This solution provides:

Application classification

Security Analytics uncovers the true identity of any application trying to hide within your network. Comprehensive deep packet inspection (DPI) classifies over 2,500 applications and thousands of descriptive metadata details. This feature not only efficiently identifies applications, but also provides descriptive information about a network session including applications, user personas, intended actions, content types, file names and more.

Real-time threat intelligence

The platform integrates directly with Symantec Intelligence Services to deliver a real security game changer. Leveraging the Symantec Global Intelligence Network and the "network effect" from more than 15,000 customers and millions of users, Intelligence Services provides instant, actionable intelligence on web, email, or file-based threats. The Security Analytics real-time file extraction also automatically extracts and inspects files to enable immediate, automatic identification of known threats and optimizes malware sandboxing by eliminating known threats from unnecessary detonation.



url 0	Computers/Internet
url 1	Web Advertisements
Artifact Identifier	http://kona.kontera.com/javascript/lib/KonaLibInline.js

Real-Time Threat Analysis

Layer 2 to 7 security analytics

Security Analytics provides a variety of advanced analytics capabilities to strengthen security incident response with comprehensive and conclusive analysis. Key capabilities include full session reconstruction; real-time reputation look up; instant messaging (IM), email and image reconstruction; Root Cause Explorer; and delivery of complete artifacts, not just packets.

Context-aware security

The solution integrates with best-of-breed network and endpoint security technologies to pivot directly from any alert or log and obtain full-payload detail of the event before, during, and after the alert. The open, web services REST API adds complete context to any security tool and lets you leverage leading technologies such as Carbon Black, Cisco, Countertack, Dell SonicWALL, FireEye, Guidance Software, HP ArcSight, Sourcefire, Splunk, Tripwire, and many other security applications.

Full security visibility

With Security Analytics you gain insight across thousands of applications, dozens of file-transports, all flows and all packets, including encrypted traffic through tight integration with the Symantec SSL Visibility solution.

Root Cause Explorer

Root Cause Explorer simplifies incident response. Using extracted network objects, the tool reconstructs a timeline of suspect web sessions, emails, and chat conversations. By automatically creating a timeline of these events, Root Cause Explorer helps the analyst quickly identify the source of an infection or compromise and dramatically reduce time-to-resolution.

Flexible deployment

Security Analytics provides multiple deployment options to optimize total cost of ownership (TCO) and minimize capital expenditures (CapEx) – a level of flexibility that no other solution can deliver. It is easily deployed on industry-standard hardware, as pre-configured appliances, or as a virtual appliance for comprehensive security that scales from branch offices to the enterprise data center.

Visualize. Analyze. Remediate.

Symantec Security Analytics delivers the industry's most comprehensive solution for swift incident response and advanced network forensics. It provides complete visibility into network traffic with actionable intelligence to uncover the full source and scope of security threats so you can quickly close the window of exposure, mitigate ongoing risk and bring your organization to whole again.

Contact your local Symantec representative today for more information – or to arrange a demonstration. Take your security defenses and incident response to a new level of sophistication and enable new opportunities for business empowerment.

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.