SOLUTION BRIEF

Symantec Security Analytics

See, understand, and swiftly respond to advanced threats

Symantec

Choose a modern security strategy

Because advanced malware and zero-day attacks fly under the radar of traditional security defenses, many organizations expect that attackers will at some point breach their networks. It doesn't have to be that way. The right intelligence and real-time analysis enables you to see, understand, respond to, and fortify the network and cloud against advanced threats and targeted attacks.

Symantec Security Analytics closes security gaps by combining security visibility, security analytics, and real-time intelligence for advanced network and cloud forensics that ensure you immediately detect and effectively respond to incidents. Simply put, Security Analytics moves your security team past anxiety about each new security threat—and towards better defending your business.

Adapt to a dynamic threat landscape

The number, variety, and sources of security attacks always increases. Thousands of new malware samples appear every day—advanced zero-day threats, sophisticated malware, and targeted attacks—from outside sources and even employees.

Traditional blocking strategies simply aren't effective. To close the gaps in today's signature-based tools, security and incident response teams need an adaptable and customizable defense that sees everything going in and out of the network, no matter how huge the traffic volume. Organizations also require security that's simple, flexible, and cost-effective.

Security Analytics, an integral part of the Symantec Integrated Cyber Defense platform, prepares you for the unknown and protects against ongoing attacks. Security Analytics:

- Works across complex ecosystems, processes, and workflows
- Draws on the broadest sources of real-time threat intelligence while delivering a full record of all activity before, during, and after an attack
- Scales to meet organization growth, the need for centralized security management, and increasing performance demands
- Is available in preconfigured appliances, virtual appliances, or cloud-based virtual appliances

Actionable intelligence, stat

Symantec Security Analytics clearly and concisely answers critical post-breach security questions including:

- Who did this?
- When?
- How?
- What was accessed?

This award-winning solution records and classifies every packet of traffic—from Layer 2 through Layer 7—while indexing, classifying, enriching, and storing the data. Complete threat intelligence and post-breach analytics give you actionable evidence as the basis for:

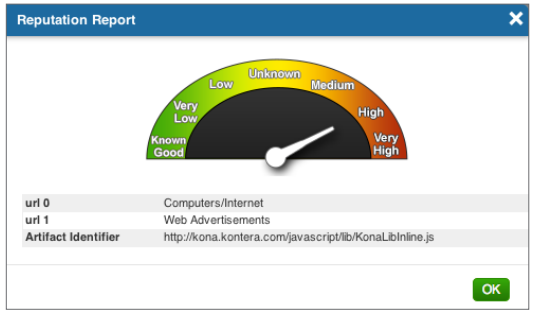
- Swift incident response and forensics
- Real-time situational awareness
- Continuous monitoring
- IT governance
- Risk management and compliance
- Security assurance

Costs*

$3.9M
Total average cost of a breach

$148M
Average cost per record breached

48%
of breaches are malicious attacks



Real-Time Threat Analysis

*Source: Ponemon Institute, 2018

Key capabilities and benefits

Flexible, cost-effective Security Analytics is the only solution that integrates with multiple highly reputable threat intelligence sources and advanced sandboxing technology to provide complete, real-time visibility and retrospective forensics analysis.

Key capabilities and benefits include:

Application classification

Security Analytics uncovers the true identity of any application hiding in your network. Deep packet inspection (DPI) classifies over 2,800 applications and thousands of descriptive metadata details. In addition, DPI describes network session information including:

- Applications
- User personas
- Intended actions
- Content types
- Filenames

Real-time threat intelligence

Security Analytics integrates with Symantec Intelligence Services, creating unparalleled visibility. Intelligence Services taps the Symantec Global Intelligence Network—the world's largest civilian threat intelligence database—and data from more than 15,000 customers and millions of users, generating instant, actionable intelligence on web-, email-, and file-based threats. Security Analytics uses automatic, real-time file extraction to inspect files, immediately identifying known threats and optimizing malware sandboxing by removing known threats from unnecessary detonation.

Layer 2 to 7 security analytics

Security Analytics strengthens incident response with the most complete and conclusive analyses available. Key capabilities include:

- Full-session reconstruction
- Real-time reputation lookup
- Instant messaging reconstruction
- Email and image reconstruction
- Root Cause Explorer
- Complete artifact (not just packets) delivery

Context-aware security

Security Analytics integrates with a range of leading network and endpoint security technologies, allowing escalation from any alert or log to full-payload event details before, during, and after the alert. The open, web services REST API adds complete context to any security tool.

Full security visibility

Gain insight into thousands of applications, dozens of file transports, and all flows and all packets—including encrypted traffic (through tight integration with the Symantec SSL Visibility Appliance).

Root Cause Explorer

The Root Cause Explorer feature simplifies incident response. The tool uses extracted network objects to automatically reconstruct a timeline of suspect web sessions, emails, and chat, enabling analysts to quickly identify an incident's source and dramatically speed its resolution.

Anomaly detection

Anomaly detection analyzes all captured data, then alerts you on anomalous behavior. Pivot from the alert to the Anomaly Investigation view to see when the anomaly occurred, how often, and which other endpoints were involved.

Central Manager

Central Manager supports simple management of Security Analytics appliances, VMs, cloud sensors, and high-density storage from a single point. Get central access to all Security Analytics sensors for directed, aggregate searches and management—no need for heavy data replication. Central Manager supports over 200 sensors, adding efficiency and ease for global, enterprisewide IR investigations.

Flexible deployment

Minimize capital expenditures and optimize total cost of ownership through implementation flexibility unmatched by any other solution. Whether you choose preconfigured or virtual appliances, on premises or inside public and private clouds, you're assured of complete security that scales from branch offices to the data center to your cloud workloads.

Managed Network Forensics

With the Symantec Managed Network Forensics service, even organizations with limited security resources benefit from Security Analytics' advanced capabilities. Managed Network Forensics extends your team's capabilities with our security experts available around the clock across six global security operation centers (United States, United Kingdom, India, Singapore, Australia, and Japan).

Visualize | Analyze | Remediate

The industry's most complete incident response and advanced network forensics gives you swift, complete visibility into network traffic, revealing the full scope and source of security threats. Quickly close the window on exposure, mitigate ongoing risk, and restore your organization to fully normal operations.

Take the next step

Contact your local Symantec representative now to arrange a Security Analytics demonstration or find out more.

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

19D227483_SB_SECURITY_ANALYTICS_EN