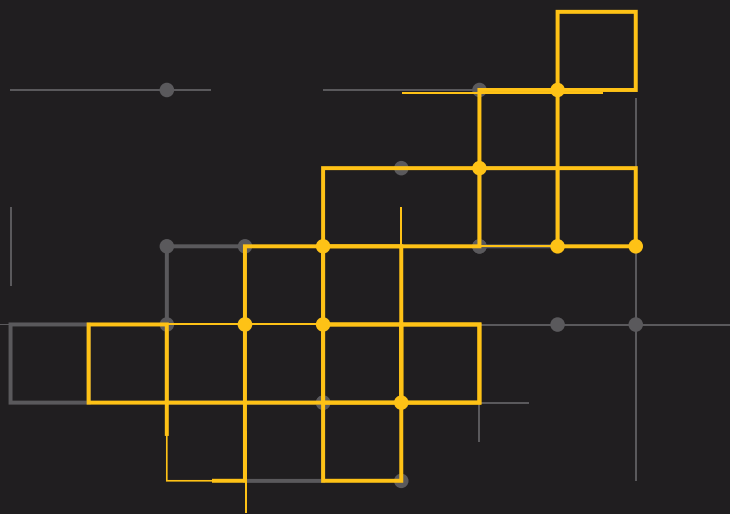
Moving Beyond Check-Box Compliance to Truly Effective Security



Compliance with information security regulations is a necessity for companies in virtually every industry. The question is, does compliance alone deliver effective protection against today's sophisticated and targeted security threats? The steady stream of media reports about companies that have been breached despite being in compliance provides a clear indication that the answer is no.

Effective security – the kind that keeps your workforce productive, your business initiatives moving forward, and your company out of the news – should naturally support compliance. However, it should also provide total visibility into all network data, so you can prevent attacks and swiftly and intelligently respond to incidents that do occur. Symantec Security Analytics is uniquely capable of meeting these demands.

Compliance ≠ Security

For companies in most industries, the list of information security compliance requirements is large and growing. From complying with annual FISMA (Federal Information Security Management Act) audits, to meeting the continuous monitoring requirements outlined by NIST (National Information Security & Technology) SP 800-137 and NIST SP 800-53, to satisfying the requirements of the Sarbanes-Oxley Act (SOX) and Payment Card Industry (PCI) regulations, compliance is increasingly complex and expensive.

Yet time and time again we are reminded that compliance alone does not ensure effective security. The Heartbleed bug, Shellshock vulnerability, and the Home Depot data breach are prominent reminders advanced threats still succeed, even among companies that are meeting all relevant compliance requirements.

While current security regulations do not explicitly require the capture and analysis of all available data, this is bound to be a requirement very soon – and for good reason. Today, many security-related mandates focus only on "retaining security information", "delivering evidence" or "enabling incident response." However, most regulations are vague about the level of detail that must be retained, or do not require a full record (every packet) of network activity. The result, all too often, is that organizations do not have full visibility into the true cause or severity level of attacks that succeed, or they misinterpret the data they do have, or they cannot resolve breaches in a timely way because they can't answer the "who, what, when, where, and how" of an attack.

> **"...Compliance to FISMA requirements does not accomplish the most important goal of improving overall security posture."**
>
> -SANS Institute Report

A typical phone bill provides a useful analogy. It may show that a call was placed on September 20 at 4:03 p.m. and lasted 14 minutes, or that a call was received on September 21 from 608-658-2675 and lasted 9 minutes. However, it provides no information about who actually placed or received the calls or what was said. That level of detail, from an information security perspective, can be critical in identifying, diagnosing, and quickly remediating an attack.

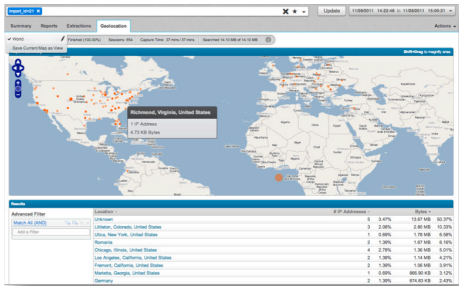
Security Analytics: Complete Visibility, Continuous Monitoring

It is ultimately up to enterprises and organizations to decide for themselves what level of intelligence gathering and monitoring is necessary; however, many organizations have insufficient expertise in this area to make an informed decision.

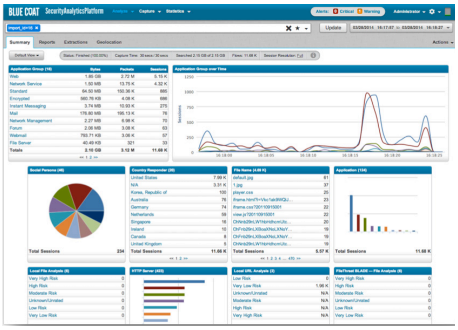
[1] "Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It," by Eugene Schultz, Ph.D., CISM, CISSP, published in the SANS Institute InfoSec Reading Room.

Symantec™

Media Panel: View all images files and all associated metadata



See where all your traffic and threats are coming from



Customized dashboard view for quick analysis

Symantec Security Analytics offers a rich set of dashboards that provide content, context, and analysis to ensure compliance and effective security.

Symantec, a security leader for more than 30 years and a trusted brand to more than 15,000 customers worldwide, has built its Security Analytics Solution to deliver a deeper understanding of everything that's happening on your networks – all the activities, applications, communications, files and personas – based on a thorough and ongoing recording and analysis of your data.

Essentially, Symantec Security Analytics acts as a security camera on the network, providing total visibility and clear, actionable intelligence about security threats to applications, files, email and web content. This makes it possible to quickly identify the advanced and targeted attacks that could still compromise your network even if you are in compliance with all information security regulations.

By providing a full record of all network activity, Security Analytics delivers the needed evidence to support compliance audits, prove adherence to regulations, and minimize costs and fines. The full record enables security professionals to validate that other security tools (blocking, data leakage protection, etc.) are actually doing their job and that adjustments or upgrades to defenses work as intended. Specifically, Security Analytics delivers:

Incident Response and Resolution

Security Analytics allows you to go back in time to identify the root cause of an infection or compromise and reduce time-to-resolution by automatically reconstructing a timeline of suspect web sessions, emails, chat conversations, and more.

Situational Awareness

You can protect against – and respond to – advanced persistent threats and attacks that fly under the radar of traditional security tools with a complete and forensically sound record of network activity that provides context, inferential analysis, and event correlation/trending.

Automated Alerts and Workflows:

You can instantly respond to security events with trigger-based notifications of targeted events, unknown applications on the network, encrypted traffic on non-standard ports or any other anomalous event. You can also save time with automated tasks, such as checking for traffic against a list of known bad sites.

Continuous Advanced Malware Detection

Security Analytics makes it possible to mitigate risks before they can be exploited and/or cause harm by delivering unknown files to sandboxing solutions for optimized detonation and by replaying network traffic against updated firewall, SIEM, or IPS signatures to catch prior intrusions. Continuously monitor the network to verify that previously eradicated malware is no longer present.

Symantec Security Analytics addresses a full range of compliance-related requirements and capabilities: Continuous monitoring, testing, surveillance, logging, auditing, data retention, and overall network security. It is easily deployed anywhere within the network – either as a pre-configured appliance, a virtual appliance, or software on your own hardware.

Moreover, Security Analytics is designed to meet the grueling demands of the largest government and enterprise networks. Its patented architecture captures network data at speeds up to 10 Gbps with full fidelity, and it integrates with best-of-breed network security technologies, so your security tools can work in concert – sharing data, creating insights, and empowering the team to identify and address security issues quickly and thoroughly.

Looking back at the phone bill analogy: Security Analytics provides not only the basic information about calls placed and received, but actually allows you to recreate the actual conversation so you can determine the true contents of the activity. In network security terms, it makes it possible to recreate the actual malicious file, email, web page, phone conversation, instant message, and so on that crossed the wire – rather than simply providing a record that such activity occurred.

Compliance is Just the First Step

Forward-looking organizations recognize that compliance should be the starting point for comprehensive, effective security, not the end goal. Security Analytics serves as a catalyst for deepening your security defenses because it supports a broad range of compliance requirements as a first step toward a more comprehensive approach. Below are just a few examples of regulations addressed by Security Analytics, along with brief descriptions of how Symantec solutions facilitate compliance efforts.

The Federal Information Security Act (FISMA)

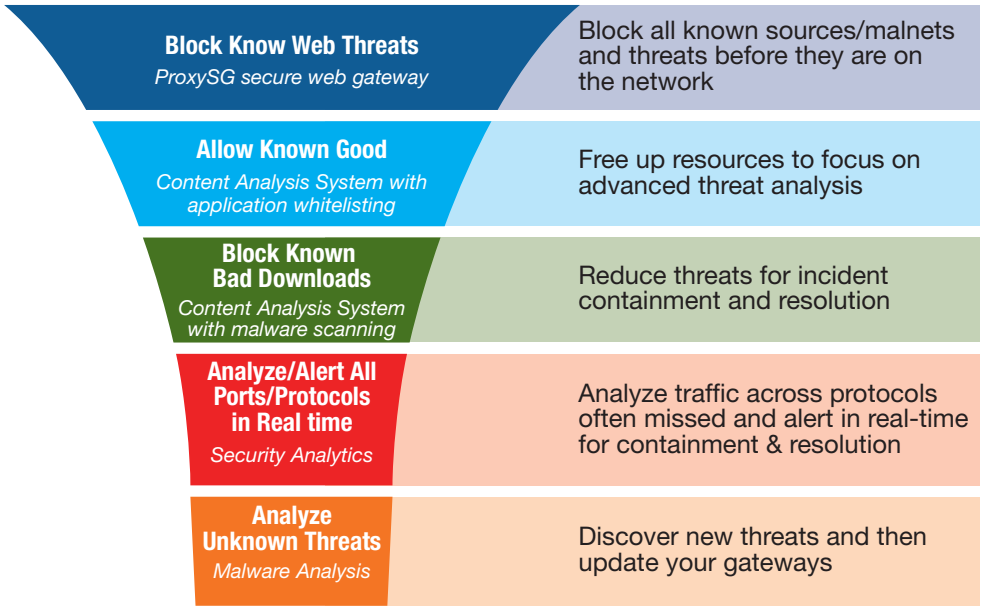
Requires that federal organizations generate and retain audit records that are sufficient to support after-the-fact investigations of security incidents. The Network Information Security & Technology (NIST) 800-37 publication provides guidance for complying with the FISMA Risk Management Framework that addresses security control selection for federal information systems in accordance with the security requirements in the Federal Information Processing Standard (FIPS) 200. Security Analytics supports FISMA mandates by replacing point-in-time audits and compliance checks with continuous monitoring that provides the level of visibility into network actions and security threats needed to help prioritize security initiatives.

Payment Card Industry (PCI)

Requires organizations that process credit cards to maintain high levels of network security to protect cardholder information and privacy. Symantec solutions create a secure IT infrastructure by completely monitoring and enabling comprehensive audits of all network activity to minimize vulnerabilities and protect cardholder data from data theft and cyber-attacks.

Health Insurance Portability and Accountability Act (HIPAA)

To ensure privacy and confidentiality, all patient healthcare information must be protected when stored, maintained, or transmitted. Symantec Security Analytics keeps a record of all network traffic and utilizes its forensics capabilities to verify whether sensitive data has been accessed.



Symantec offers a comprehensive approach to respond to both known and unknown advanced threats.

Sarbanes-Oxley Act (SOX)

Requires public companies to validate the accuracy and integrity of their financial management processes as well as document and assess internal controls. Security Analytics provides comprehensive visibility into all network traffic, confirming the integrity and security of confidential information.

Gramm-Leach Bliley

Mandates privacy and the protection of customer records maintained by financial institutions including strong access controls and encryption of electronic customer information to ensure system modifications do not affect security. Security Analytics stores, indexes, classifies and replays every action that occurs on the network, providing surveillance of every aspect of the network and detection of system attacks or intrusions.

Control Objectives for Information and Related Technology (CobiT)

Developed as a generally accepted standard for good information technology security and control practices for management, auditors, and security practitioners. The active network forensics provided by Security Analytics strengthens internal network security and the ability to monitor and evaluate internal data security, improving the standard for IT security.

EU General Data Protection Regulation (GDPR)

Regulates the complete lifecycle of personal data processing, from collection to deletion. It applies whether the data is stored on premises or in the cloud. It also requires organizations to deploy enhanced protection against security intrusions and establish a formal procedure for notifying authorities and affected individuals should a breach occur. Security Analytics enables organizations to provide fast and thorough notifications to authorities when a breach occurs by providing a detailed picture of what happened before, during, and after the breach – including what files and data records may have been compromised.

Learn More

We urge you to discuss with a Symantec account representative how Security Analytics can help you not only achieve compliance, but also improve your security posture and incident response readiness. Learn more about Security Analytics by visiting www.symantec.com, and contact your local Symantec account team to schedule an appointment.

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_sb_Security_Analytics_and_Compliance_EN_v1a