Symantec Enterprise Security Framework

Executive Overview
Symantec Enterprise Security Framework

Executive Overview

Contents

Today's computing environment ................................................................. 1
A comprehensive framework of security products and services ..................... 1
Megatrends affecting security ....................................................................... 5
Today’s computing environment

For IT security professionals today the pace of change has accelerated dramatically. The current Internet security threat landscape continues to evolve in both volume and complexity of attacks. At the same time, trends such as virtualization, cloud computing and the use of consumer mobile devices raise new issues for security. Meanwhile, slow business growth and tight budgets mean IT security must do more with less.

Security professionals agree: yesterday’s security tools and strategies are no longer enough to counter emerging threats. The level of sophistication of new attacks is unprecedented. The market for “black hat” selling of intellectual property and access to critical infrastructure, as well as personally identifiable information (PII) and payment card industry (PCI) credentials, is well established. New forms of security intelligence are required to combat the new strains of auto-mutating malware that are resistant to traditional signature-based antivirus techniques. Education programs that promote security awareness among employees are also needed to prevent breaches of both personal data and intellectual property.

New virtual, cloud and mobile technology platforms force IT to carefully balance enhanced agility, potential ROI, and risk. Senior management is demanding that IT enable a mobile workforce with consumer-oriented devices from smartphones to iPads®. Although these devices promise to boost productivity, they also introduce new risks to data and networks. And they make the perimeter defense of any enterprise more porous and vulnerable. Virtualization and cloud computing projects aimed at cutting IT costs bring with them additional security concerns. As virtual, cloud and mobile platforms expand, they sharply increase the available methods for creating, carrying and storing information, and the resulting information explosion brings further exposure. It is the task of IT Security to assess and mitigate these risks.

Current macroeconomic pressures add to the challenges of this volatile environment. Clearly IT professionals have their work cut out for them. Chief Information Security Officers (CISOs), Vice Presidents, and Directors of IT share three top priorities: stay on top of emerging threats, secure new computing models and manage the cost of security. Without security solutions designed to tackle all three of these priorities, IT Security can seem like a high-wire juggling act.

A comprehensive framework of security products and services

As a global leader in providing IT security solutions, Symantec delivers all of the essential ingredients to make IT Security professionals successful.

- Symantec provides the security intelligence and advanced technology you need to counter emerging threats.
- Symantec offers comprehensive protection that is content, identity and location aware and performance-optimized to support innovative new mobile, cloud and virtual computing models.
- Symantec delivers integrated security management that lets you identify trends, prioritize tasks and automate processes so you can achieve the lowest total cost of ownership.

The Symantec Enterprise Security Framework is a comprehensive platform of security products and services that enables security executives to successfully execute on all three of these top priorities. Symantec delivers the complete range of products, security automation and foundational security capabilities to meet all of today’s IT security requirements.
Symantec enables you to protect information wherever it is stored or used – on servers, desktops, laptops and mobile devices, as well as on virtual and cloud computing systems.

Symantec delivers security updates in a bandwidth-friendly way that allows users to prioritize resources, applications and infrastructure.

Symantec allows you to rapidly provision and patch mobile devices, laptops, desktops and servers in response to security vulnerabilities and knowledge of the threat landscape.

Symantec delivers its patent-pending Symantec Insight™ reputation-based threat detection services for faster, more robust defenses against malware and other targeted attacks.

Symantec products take feeds from the Symantec™ Global Intelligence Network on a daily basis, empowering Symantec customers with early warning data on evolving threats worldwide.

Symantec provides an identity database that allows you to engage in trusted online relationships, control access to sensitive data and use strong credentials to encrypt and sign transactions.

Symantec offers Symantec™ Managed Security Services to complement in-house staff, remotely delivering hosted security monitoring, advanced analysis and early warning intelligence supported by Insight anti-malware technology and fed by the Global Intelligence Network.

**Symantec product families**

The Enterprise Security Framework includes five product families that combine to protect information, identity and infrastructure, and manage security, compliance and IT resources throughout the enterprise. At the heart of the Enterprise Security Framework is a single console that allows for integrated security management, deep visibility and broad control across all security products. Finally, the Enterprise Security Framework is driven by five foundational capabilities that power all Symantec products and clearly differentiate Symantec in the security marketplace.

**Infrastructure Protection.** Symantec delivers unrivalled security and proven superior performance for endpoints, networks and servers in both physical and virtual environments. Led by its flagship product Symantec™ Endpoint Protection, the Symantec family of infrastructure protection products includes anti-virus, anti-spyware, firewall, intrusion prevention, network access control, device management and application management.

**Endpoint and Server Management.** Symantec™ Client Management Suite, powered by Altiris™ technology and Symantec™ Server Management Suite, powered by Altiris™ technology mitigate the administrative complexities and costs of layered security solutions, so you can reduce operating costs, increase operational effectiveness, improve security and sustain compliance. The solutions also allow companies to provision and patch mobile devices, laptops, desktops and servers to remediate security vulnerabilities.

**Information Protection.** Now you can measurably reduce the risk of a data breach, educate users and stop emerging threats to your customers, brand and information with Symantec™ Data Loss Prevention and Symantec™ Endpoint Encryption, the most popular and highly-rated data loss prevention and encryption products in the industry.
Identity Protection. VeriSign™ Trust Services, now from Symantec, and Symantec User Authentication help organizations engage in trusted online transactions. SSL certificates and trust services help businesses demonstrate the legitimacy of their websites and encrypt private information. Symantec User Authentication controls access to sensitive data and uses strong credentials to encrypt and sign transactions.

Security and Compliance Management. Symantec products enable organizations to centrally view, assess and automate security and compliance operations throughout the enterprise. Symantec Protection Center is a management console that allows organizations to identify emerging threats, prioritize tasks and accelerate time to protection based on relevant, actionable intelligence. Symantec Security Information and Event Management enables a documented, repeatable process for security threat response and IT policy compliance via integrated log management and incident response solutions. Symantec™ Control Compliance Suite enables users to manage all aspects of IT risk and demonstrate compliance with multiple mandates at reduced levels of cost and complexity.

Foundational Symantec Capabilities

Symantec Security Solutions enable enterprise organizations to protect information proactively, respond rapidly to threats, educate employees, enable new computing models and simplify security management to improve both efficiency and effectiveness. Symantec delivers industry-leading products in nearly every category of security, along with the deep security domain expertise and real-world security intelligence. The following five capabilities are exclusive to Symantec and serve as a foundation for the entire breadth and depth of Symantec Security products.

Threat Intelligence. The strategic value of the Symantec security community is multiplied by the network effect of its constituent parties including thousands of Symantec analysts, partners and customers worldwide. The Global Intelligence Network provides Symantec with an unparalleled, data-driven view of the entire security landscape.

The Intelligence Network utilizes more than 240,000 sensors in more than 200 countries and territories to monitor attack activity through a combination of Symantec products and services. Symantec gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec’s distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks that provide valuable insight into attacker methods. Symantec security products take feeds from the Intelligence Network on a daily basis, empowering Symantec customers with early warning data on evolving threats worldwide.

Reputation-based Malware Detection. The Symantec Enterprise Security Framework is powered by Symantec’s patent-pending Insight™ detection technology. Insight tracks usage across more than 100 million systems and correlates tens of billions of linkages to accurately assess user, file and website reputations and identify new threats as they are created. Based on advanced data mining techniques, Insight can’t be fooled by changing encryption or mutating code. Insight separates files at risk from those that are safe, for faster and more accurate malware detection and improved scan performance of up to 70 percent.

### Regulatory Intelligence

In addition to the evolving threat landscape, today’s IT organizations are constantly faced with new platforms and technologies as well as changes in security standards and regulatory requirements. Symantec simplifies the process of adjusting to this dynamic environment by providing deep regulatory and security expertise that is refreshed and expanded regularly to keep you up to date and informed. Symantec’s content team combines deep technical security knowledge with real world audit and regulatory experience to provide you with out-of-the-box security and regulatory advice you can trust to both secure your environment as well as prepare for your audits.

The Symantec Regulatory Intelligence team provides security best practices standards for new versions of operating systems, databases, and applications; technical checks and remediation guidance to meet new or changing regulations; configuration, patch and vulnerability updates to address new attacks; and policy content and procedural attestations to meet new or changing regulations.

### Location awareness

Symantec’s location-aware technologies assist in making security decisions and enforcing policy based on device type, network and user location. For example, Symantec information protection can, by policy, encrypt sensitive information on mobile phones to prevent a data breach in the event of a lost device. Similarly, location awareness may come into play when restricted data is copied from a laptop to a USB drive or mobile device, enforcing encryption based on the relocation of the data.

The built-in network access control in Symantec infrastructure protection can also block or quarantine non-compliant devices or networks from accessing resources on the corporate network based on their location. Symantec identity protection uses sophisticated fraud detection algorithms to evaluate user location and login behavior and allow or disallow access to networks and applications. And Symantec’s hosted security offering, Web Security.cloud, utilizes geo-location awareness to connect users to optimal infrastructure access points within the Symantec.cloud global infrastructure.

### Trust Services and User Authentication

Trust Services and User Authentication are critical to maintaining trusted-only business interactions and the security of today’s mobile workforce. Symantec’s certified identity infrastructure maintains digital certificates that can authenticate the identity of any application, person, process or organization in an enterprise network or extranet, or on the Internet.

Now from Symantec, VeriSign Trust Services, including VeriSign™ SSL Certificates and the VeriSign Trust Seal, provide users with assurance that the websites they are interacting with are legitimate, secure and safe for information sharing. VeriSign SSL certificates are used on more than one million web servers, with two billion certificate checks daily. The VeriSign seal is the most recognized trust mark on the Internet.\(^3\) It is seen by Internet users more than 500 million times a day.\(^3\)

The cloud-based Symantec User Authentication solutions help organizations doing business online confirm the identities of their customers, employees and partners through digital certificates, two-factor authentication credentials or risk-based authentication, ensuring that only legitimate users can access information. Strong authentication credentials from Symantec User Authentication have been issued to more than five million individuals and 200 million devices.

---

\(^3\) “VeriSign Seal Sets Staggering New Record with More than Half a Billion Views in a Single Day.” Symantec, November 18, 2010
Megatrends affecting security
IT security priorities in 2011 are being driven in part by large-scale industry trends, including the need for data breach defense, mobile security, secure virtualization and security in the cloud. Here we will examine each of these trends and describe some of the ways in which Symantec Enterprise Security solutions address the security issues these trends create.

Advanced threats
In a world where data is everywhere, it has become harder than ever for organizations to protect their confidential information. The recent WikiLeaks breach not only shook the confidence of world governments in their ability to maintain state secrets, but also put every organization on notice that its sensitive data is at risk. Advanced threats, such as auto-mutating malware and hacker techniques like cross-site scripting, search engine optimization (SEO) attacks and vulnerability loading, have changed security requirements forever. In this environment, signature-based AV black-listing is no longer enough.

To identify and defeat new cybercrime techniques, you need a security network that includes both systems and people. You need an early warning system that automates data collection and analysis on a global basis to accurately anticipate and respond to emerging threats. And you need a network of experienced experts dedicated to tracking and countering threats every day. Only a global community of security experts with up-to-the-moment intelligence on threats to reputations, websites and users worldwide can provide sufficient knowledge to combat advanced threats.

To satisfy the demands of senior management, IT Security must be prepared to answer the following questions:

- How do we enforce IT policies and remediate deficiencies?
- Do we know where our confidential data is and how to protect it?
- Can we control who has access to our information?
- Have we protected our systems against incursion?
- And can we easily manage the lifecycle of our IT assets?

As described above, the Symantec Security Framework is designed to help IT Security answer each of these questions with confidence. Symantec solutions for information, identity and infrastructure protection, and security, compliance and IT resource management combine to deliver a comprehensive, proven defense against data breaches.

Protecting against the advanced persistent threat
Advanced persistent threats (APT) often use targeted techniques that involve social engineering and unique malware that is designed specifically for key individuals within the victim organization. Once in, the persistent malware stays as quiet as possible to avoid detection while the attackers have time to map out the network. This stage often involves multiple
parallel attacks to prevent removal by the victim organization. These attacks are designed to steal highly valuable confidential information. Symantec offers a full complement of products designed to combat APT.

**Symantec™ Endpoint Protection 12** is fast, powerful security for endpoints. It offers advanced defense against all types of attacks for both physical and virtual systems. Seamlessly integrating the essential security tools you need into a single, high-performance agent with a single management console, Endpoint Protection provides leading protection without slowing systems down.

**Symantec Global Intelligence Network**, is one of the world’s largest commercial cyber-intelligence communities, has established a leadership role in identifying malware aimed at client and server platforms.

**Symantec Insight Reputation-based malware detection** technology puts files in context, using their age, frequency, location and more to expose threats otherwise missed. Built on contributions from over 100 million systems in over 200 countries, Symantec Insight has the power to examine and track the context of files. Insight detects new and unknown threats that are missed by other approaches.

**Stopping the Malicious Insider**

Security professionals are increasingly concerned with stopping malicious insiders from unauthorized extraction or sharing of sensitive information. Symantec addresses this threat with a combination of user authentication, encryption and data loss prevention.

Symantec™ Data Loss Prevention can monitor flows of sensitive information out of an organization via email or copied in large quantities to a laptop or USB drive, and can block the flow of information depending on the user and the information. Symantec Encryption can be used to protect sensitive documents on internal file shares to provide stronger protection than basic access control lists. Symantec User Authentication can enforce strong two-factor authentication to prevent unauthorized users from gaining access to sensitive applications or data stores.

**Secure virtualization**

With the advent of virtualization, organizations are able to realize significant savings on hardware, support and facilities, including power and air conditioning for large data centers. By achieving higher density, virtual machines help operations scale, from a sales engineer running five demo applications on one laptop to large data-center servers running thousands of virtual machines.

While the advantages of virtualization are clear, its implementation raises several questions that security executives will be expected to answer.

- How do we protect our virtual machines without sacrificing higher density?
- How can we identify those virtual machines that are vulnerable to attack?
- And how do we know if there are rogue virtual machines in our environment?

**Ensuring protection without sacrificing density.** To protect virtual machines, most IT organizations do one of two things: install basic protection at the hardware level and hope for the best (not a good idea) or install protection on each
virtual instance. The problem with the second approach is that regularly scheduled security scans can degrade performance and compromise the level of density the virtual environment was designed to achieve in the first place.

Symantec solves this problem by factoring out repeated functions and sharing the protection load across multiple instances. In effect, Symantec has virtualized security itself. This capability is new with Symantec Endpoint Protection 12.

**Identifying vulnerabilities.** The proliferation of virtual machines creates a new problem for IT – how to ensure that every instance is in compliance with security policies, controls and regulations. Virtualization adds a whole new layer of infrastructure for the assignment of software patches and updates, security configuration standards, technical controls, user permissions, exceptions and audit requirements.

Symantec Control Compliance Suite automates the assessment of vulnerabilities and technical controls in virtual machines. In addition, Symantec Data Loss Prevention, the worldwide market share leader in Data Loss Prevention, can be configured to discover, monitor and protect confidential data on virtual machines.

**Discovering rogue instances.** In environments where virtualization tools are readily available, it is not uncommon for employees to create new business processes using homegrown virtual machines. Ad hoc reports, wikis and databases spring up on new virtual machines often unbeknownst to IT. Since they are under the radar, these virtual machines are not included in normal patch and protection updates and are therefore vulnerable to attack.

Symantec combines discovery and automated remediation of rogue virtual machines. Client Management Suite and Server Management Suite have the ability to discover rogue virtual machines anywhere on the network and identify those at risk. In such a case, Symantec™ Workflow can trigger actions such as vulnerability scanning or identification of the owner of the target domain.

**Security in the cloud**

Cloud computing is a way to provide scalable, elastic IT capabilities as services using Internet technologies. The cloud computing model enables organizations to consume software, platform and infrastructure resources as services, pay only for the resources they use and avoid the licensing, consulting and administrative costs associated with software deployments. A further advantage for the business is that IT spending can be accounted for as operational rather than capital expenditure.

Most IT professionals agree that cloud computing will play a big part in the future of IT. But questions remain as to whether cloud solutions can deliver the same quality of service as traditional software implementations. Among the top concerns slowing the adoption of cloud computing today are security, privacy and compliance. There are concerns that the move to cloud computing may jeopardize the security of proprietary information and processes, concerns that PII on customers and employees may be compromised, and concerns about the ability to demonstrate compliance with regulations and standards in the cloud environment.

Cloud computing is a complex subject comprising a wide range of technologies and processes. Software as a Service (SaaS) solutions from providers such as salesforce.com™ enable organizations to access packaged applications in the cloud. Platform as a Service (PaaS) solutions provide tools for custom application development using vendor-supplied technology such as the Force.com™ platform from salesforce.com. Infrastructure as a Platform (IaaS) solutions, available...
from vendors such as Amazon Web Services™, enable you to build an entire IT infrastructure in the cloud, including virtual machines, databases, applications and web servers.

Cloud deployment models include hosted services provided by vendors on a SaaS model, public cloud services provided by cloud computing vendors on a multi-tenancy basis, and private cloud services provided by and for a single entity.

The shift to cloud computing raises questions about security on a number of levels. The important thing for most security teams is to focus on a few specific projects that can quickly reduce risk. IT and security executives should ask:

- How do we secure corporate IP stored and used in public clouds?
- How do we build a secure, cost-efficient, high-performance private cloud?
- And which of our current security capabilities should we consider moving to the cloud?

Protecting confidential data in the public cloud. For most organizations, the first step into cloud computing is the use of hosted SaaS applications to automate basic processes from word processing to customer relationship management (CRM). Information in Salesforce™ or Google Docs™, for instance, may be at risk when employees download it to desktops or laptops. A salesperson planning a jump to the competition may easily download then send or copy such data in violation of policy. Data uploads to SaaS applications like Google can also cause inadvertent exposure if password protection is weak, as happened recently at a leading social networking provider. Symantec Data Loss Prevention prevents SaaS data breaches by periodically indexing SaaS content and accurately detecting incidents whenever confidential data is copied, sent or stored in violation of policy.

Information protection is also a concern for organizations moving to public cloud infrastructure such as Amazon Web Services. In some cases, such projects are shelved due to fears that sensitive data may be exposed. Such fears can be tested and allayed with the use of Data Loss Prevention to discover whether confidential data will in fact be exposed through exchanges with public cloud servers.

Securing the private cloud. Private cloud implementations run on the premise by and for one entity require security at every level. Here the entire Enterprise Security Framework is applicable, including Endpoint Protection, Symantec™ Critical Systems Protectionand the rest of the Symantec security portfolio.

Security solutions in the cloud. Organizations looking to leverage the cost advantages of cloud computing may also want to consider running Symantec security products as hosted services. Symantec.cloud delivers email security, Web security, instant messaging security and endpoint protection as hosted services.

Mobile Security

IT departments are under pressure to embrace new technologies that support business innovation, including the mandate to provision and secure mobile devices such as smartphones and tablets. The increasing use of such devices for business purposes has led to demand for IT support in what has been termed “the consumerization of IT.”

Symantec Mobile Security and Management is a broad portfolio of enterprise security and management solutions designed to ensure the enablement, security and efficiency of mobile platforms. It allows organizations to enable the
mobile workforce with comprehensive protection of data, people and infrastructure and integrated management of endpoints and mobile devices.

Mobile Security and Management solutions should help you answer the following questions:

- How do I allow personal devices?

- How do I enable business applications on mobile devices?

- How do I secure sensitive data on mobile devices?

- How do I protect against increasing threats on devices?

- How can I simplify mobile deployments?

- How do I train my teams on managing the new endpoints?

**Unparalleled enterprise mobility.** A world leader in both enterprise and consumer security as well as IT operations management, Symantec is uniquely qualified to help customers embrace mobility with confidence. Symantec enables the business use of corporate and personal mobile devices with market-leading endpoint security and management products.

**Most comprehensive mobile security.** A world leader in information protection and strong authentication solutions, Symantec provides comprehensive protection that is content- and identity-aware.

- Data Loss Prevention, Web security, encryption and anti-threat solutions safeguard corporate data on servers, desktops, laptops and mobile devices.

- VeriSign Trust Services, now from Symantec, and Symantec User Authentication help organizations engage in trusted online transactions, including mobile transactions.

- Symantec Global Intelligence Network, one of the world’s largest commercial cyber-intelligence communities, has established a leadership role in identifying malware aimed at mobile platforms.

- Symantec Next Generation Network Protection (NGNP), a network-based policy control and enforcement solution, allows communication service providers to protect their subscribers against malware, phishing and other network threats.

**First Integrated Endpoint Management.** Symantec Client Management and Mobile Management solutions are tightly integrated to enable you to provide a common framework to standardize management of multiple mobile platforms, initiatives and applications. These solutions mitigate the administrative complexities of layered security solutions, increase operational effectiveness, improve security and sustain compliance across desktops, laptops, tablets and smartphones.
About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com