WHITE PAPER:
CHOOSING THE RIGHT
SECURITY SOLUTION

White Paper

Choosing the Right Security Solution

Moving Beyond SSL to Establish Trust

Symantec™

Norton™ SECURED
powered by VeriSign

Choosing the Right Security Solution

Moving Beyond SSL to Establish Trust

CONTENTS

Introduction

The online world can be a scary place as the integration of the Internet into everyone's lives has also brought with it an ever-increasing trend towards malicious activity. Consumers are understandably concerned. This angst leads to diminished trust in e-commerce and sub-optimal results for online businesses. Consumers and businesses, alike, need protection from online security threats in order to thrive on the Internet and take full advantage of the many benefits of e-commerce.

Secure Sockets Layer (SSL) was invented at the dawn of e-commerce to address security challenges with data encryption. It was a key ingredient in the rapid growth of online business in its early years. However, as with all technologies, the original SSL (aka "traditional SSL") needed to evolve to meet the ever-changing Internet threat environment. To remain effective, measures have been taken to enhance SSL's capabilities – both by expanding upon SSL's functionality and combining it with complementary technologies. As new threats emerge, SSL-based security solutions must also continue to evolve.

This paper discusses how online businesses can instill trust and confidence in their websites, protect valuable brands, and safeguard customers' sensitive information. It is critical to choose e-commerce security solutions that continually evolve and extend to address a range of ever-changing needs. SSL-based security platforms with solid track records of meeting new challenges are the best way to defend, and future proof, e-commerce environments against a growing and dynamic Internet threat environment.

The Inevitable Evolution of Technology Platforms

The evolution of e-commerce security technologies follows a familiar pattern. As technologies mature, point solutions coalesce into multi-function technology platforms that can address an ever-increasing range of needs.

An example that illustrates this pattern is the maturation of office productivity suites. In the early days of "personal computing" text editors were sold separately from spell checkers. Eventually, they merged into a common solution – a word. processing "platform" comprised of a range of functionality. Ultimately, word processors were combined with spreadsheets and other tools to form "productivity suites" – Microsoft Office is the most noteworthy example of an office productivity platform. The coalescence of multiple hardware technologies (e.g., graphic cards) onto computer motherboards is another example of point solution technologies evolving into multi-function platforms. This evolution toward technology platforms is the natural course of things, and it is critical to identify and align with the vendors that have the vision and capability to survive and thrive past point solution "adolescence" into comprehensive business solution "adulthood," and beyond.

A "technology platform" can be thought of as a collection of complementary point solutions that are unified by a common foundation and provide a one-stop-shop to address the needs of consumers and business. Viable platforms are also ecosystem foundations where synergistic third-party vendors can integrate their technology point solutions

SSL: The Foundation of Trust

From an e-commerce perspective, online businesses should look for a security platform that has a proactive evolutionary history of introducing new functionality to address the ever-changing needs of online business. The solution should have a range of capabilities that deliver confidence and peace-of-mind to business and consumers, alike.

Since its first commercial introduction in 1995, SSL has become the de facto security standard for e-commerce. The data encryption and authentication that come with an SSL certificate purchased from a reputable Certificate Authority (CA) have been essential ingredients for e-commerce websites to build trust with their customers.

However, the online threat environment continues to mutate and evolve. The encryption and authentication provided by traditional SSL certificates is no longer enough to deliver sufficient threat protection required for successful online businesses. As consumers have become more e-commerce savvy, they have also grown more skeptical of the ability to keep their confidential information secure – they expect to be protected. Their awareness of the growing threat landscape has influenced their online behavior, often to the detriment of e-commerce – for instance, 21 percent of users have not concluded an online purchase due to security concerns over credit card data.[1]

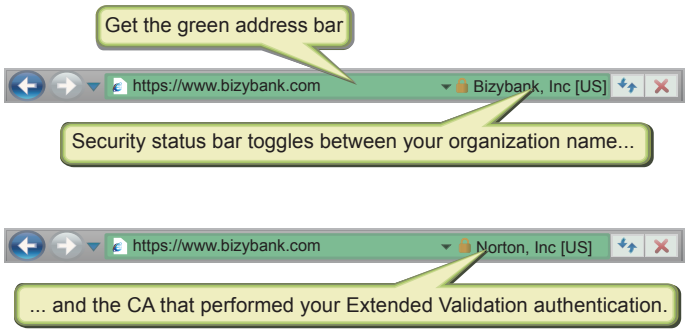
To meet the challenges of emerging e-commerce security threats, leading security solutions need to continually add capabilities to their SSL offerings. Some past examples of innovations include:

- **Trust Marks:** Consumers are beleaguered by the wide array of security threats that face them in the online world. To prevent user trepidation, online merchants need to communicate their investments in, and commitment to, website security and consumer safety. The use of highly visible trust marks helps convey this message. The Online Trust Alliance (OTA) 2011 Online Safety Honor Roll and Scorecard reported a 68 percent year-to-year increase of EV SSL adoption. EV SSL turns part of the browser address bar green, showing that the website (and, by extension, the organization behind it) are legitimate. This visual cue provides immediate verification and increases consumer confidence. According to a recent study, trust levels increase by more than 60 percent when users check for security seals, the SSL padlock, a green address bar, or "https" when making online purchases or sharing personal information.[2]

[1] www.antiphishing.org
[2] http://www.businessinsider.com/5-ways-to-frustrate-hackers-attacking-your-web-site-this-holiday-season-and-beyond-2011

A trust mark is a form of advertising that communicates to online consumers that a website meets the requirements of a trusted third-party. For example, the Norton™ Secured Seal communicates, among other things, that the website and its owner or operator have been authenticated by Symantec, and that the website uses SSL and/or another service to enhance security.

- **Extended Validation SSL:** Extended Validation, or "EV," SSL provides the highest level of authentication available with an SSL certificate and assures visitors that a website is safe with the display of the green address bar. EV SSL was developed as a response to the growing threat of phishing schemes, which use emails and websites that appear legitimate to trick visitors into sharing personal information. These "man-in-the-middle" attacks were developed in an attempt to capitalize on inconsistent issuance and authentication methodologies of CAs. Counter measures were conceived by leading vendors to address this evolving threat – EV SSL was the result.



Symantec: The #1 Provider of Online Security

Symantec secures more than one million Web servers worldwide, more than any other CA. 100 percent of the Fortune 500, 97 of the 100 largest SSL-using banks in the world, and 81 percent of the 500 largest e-commerce sites in North America use SSL certificates sold by Symantec.[3] Symantec also maintains more SSL certificates with EV than any other CA. And Symantec follows rigorous authentication practices that are audited annually by KPMG, and widely regarded as leading the industry in reputation qualification measures to establish online credibility for businesses of all sizes.

[3]Includes all Symantec affiliates and subsidiaries

The Symantec Trust Services Platform

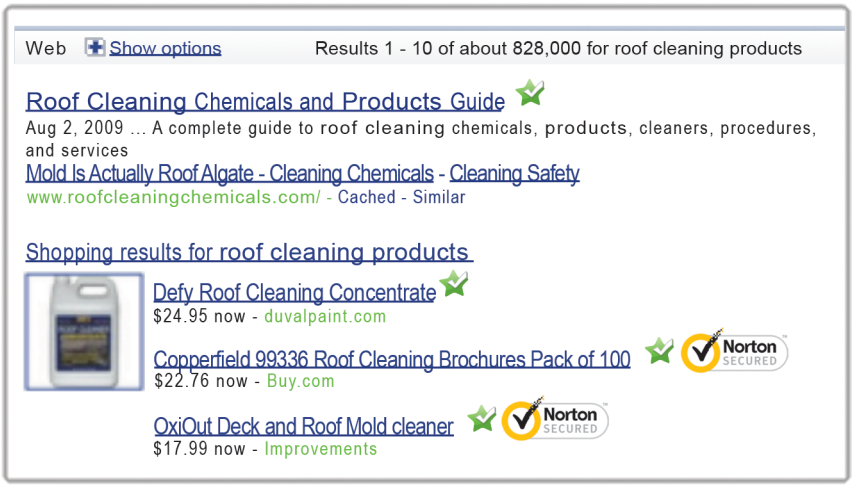
Symantec provides SSL certificates, website malware scanning, and Web vulnerability assessment services in a single solution, and continues to invest in its technology, partnerships, and leading Internet trust brand to ensure that its business customers and consumers can continue to reap the full benefits of e-commerce in spite of any new security threats that may emerge.

In addition to the peace-of-mind that comes with selecting a proven SSL certificate, Symantec has continued to address its customers' needs by constantly augmenting its SSL technology through support for new standards and integration with complementary technologies and solutions. Integration with third-party technologies from Qualys (vulnerability assessment) and RatePoint (customer review management) are examples of incremental value-add through partnerships. The Norton Secured Seal and Symantec SSL Certificates with Extended Validation (EV) are examples of "home grown" functionality that have been added to the SSL core in the recent past.

Symantec's commitment to address customer needs in a changing threat environment continues with the introduction of website malware scanning and the related display of the Norton Secured Seal in conjunction with search results. Both are included with Symantec SSL Certificates at no additional cost.

Early Communication of Trust

To combat the changing Internet threat environment, engender trust, and convey safety to consumers as early as possible, Symantec continues its legacy of bundling value-added trust functionality with its SSL certificates. The most recent innovations start with a regular scan of public-facing websites for malware. For owners of a Symantec SSL Certificate, Symantec performs a daily, non-invasive scan of an e-commerce site so consumers can be assured that there is regular monitoring for their safety. Visual assurance takes the form of the Norton Secured Seal, which can be displayed prominently on the site's home page and with search results.



Display of trust marks can help business demonstrate their trustworthiness in search results and encourage traffic to their website.

Symantec Seal-in-Search™ functionality allows enabled browsers and authorized Symantec partner sites to instantly recognize sites that are trusted by Symantec, and display the Norton Secured Seal next to links in search results.

This capability enables online businesses to convey a sense of trust to customers prior to navigation to their website. It also helps links stand out and visually signifies that the online business is a Symantec trusted site. The ability of an online business to reach a consumer with a positive trust message so early in their process, provides valuable differentiation from competitors that don't use Symantec SSL Certificates and adjacent services.

When combined with the use of the Norton Secured Seal on the website home page, Seal-in-Search gives online businesses a powerful set of tools to communicate to consumers that it is alright to conduct transactions and trust that their confidential information will remain secure. This is another example of Symantec continuing to evolve the value proposition of its SSL-based solutions to meet the needs of online businesses and consumers.

Conclusion

Choosing the right security solution is critical to the success of an online business. Look for trust-based security solutions from established vendors, like Symantec, that deliver protection and consumer peace-of-mind through cutting edge technology and integration with complementary third-party solutions.

E-commerce security platforms should be evaluated based on their ability to protect sensitive transactional information, provide a means to identify legitimate businesses (and disqualify those with malicious intent), and ensure that an e-commerce website is free from malicious code that could lead to unwanted malware infections for website visitors and blacklisting by search engines. Last, but not least, a viable e-commerce security platform should have a powerful brand so that investments in e-commerce security can be effectively communicated to consumers and partners.

As the first commercial vendor of SSL solutions, Symantec has been synonymous with trust from the beginning. The Trust Services Platform represents the state-of-the-art in technology, brand, and long-term vision. Website malware scanning and Seal-in-Search are the most recent innovations that Symantec has incorporated into its SSL-based solutions to protect online businesses and consumers from emerging threats. Symantec will continue this tradition of enabling trust, despite the shifting threat landscape, so online business and consumers can continue to take full advantage of the many benefits of e-commerce.

Avoid Blacklisting of Your Website

Regular scanning for malware helps you to find and fix malicious code on your website before search engines block your traffic – a.k.a. "blacklisting." The blacklisting of your website by search engines often occurs before you even realize that you have a malware infection. Once blacklisted, your online business can experience significant lost opportunities, and it can be a very painful and long process to get your site reinstated. Symantec SSL Certificates, with daily website malware scanning, help you avoid blacklisting and ensure availability of your website to consumers.

More Information

Visit our website

http://go.symantec.com.ssl-certificates

To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

To speak with a Product Specialist outside the U.S.

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

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.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com

Symantec

Norton SECURED
powered by VeriSign