



WHITE PAPER

# CHOOSING THE RIGHT SECURITY SOLUTION: MOVING BEYOND SSL TO ESTABLISH TRUST



## **CONTENTS**

- 1 INTRODUCTION
- 1 THE INEVITABLE EVOLUTION OF TECHNOLOGY PLATFORMS
- 1 EXTENDED VALIDATION (EV) SSL:  
THE GOLD STANDARD FOR AUTHENTICATION
- 2 SSL: THE FOUNDATION OF TRUST
- 2 VERISIGN: THE LEADER IN SSL, AND BEYOND
- 3 THE VERISIGN TRUST SERVICES PLATFORM
- 4 CONCLUSION
- 4 ABOUT VERISIGN





# CHOOSING THE RIGHT SECURITY SOLUTION: MOVING BEYOND SSL TO ESTABLISH TRUST

## 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—73% of U.S. Internet users are extremely threatened by identity theft.<sup>1</sup> 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 web sites, 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.

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.

1. VeriSign Trust Index Report, March 2010. [https://www.trustthecheck.com/assets/VeriSign\\_Internet\\_Trust\\_Index\\_March\\_2010.pdf](https://www.trustthecheck.com/assets/VeriSign_Internet_Trust_Index_March_2010.pdf)



## SSL: THE FOUNDATION OF TRUST

Since its first commercial introduction in 1995 by VeriSign, 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 web sites 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% of users have not concluded an online purchase due to security concerns over credit card data.<sup>2</sup>

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, web site security and consumer safety. The use of highly-visible trust marks helps convey this message. 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.<sup>3</sup>

A trust mark is a form of advertising that communicates to online consumers that a web site meets the requirements of a trusted third-party. For example, the VeriSign® seal communicates, among other things, that the web site and its owner or operator have been authenticated by VeriSign, and that the web site 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 web site 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 web sites 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. The phishing threat remains real, and continues to grow. The fourth quarter of 2009 saw a rise in the number of hijacked brands to a record 356 in October, up nearly 4.4 percent from the previous record of 341 in August 2009.<sup>4</sup>



To be successful, online businesses need to employ security solutions that provide assurances at all consumer interaction decision points. The solutions should also holistically address both actual and perceived threats, as both are e-commerce inhibitors. Point solutions that only address a narrow set of issues should be avoided.

2. [www.antiphishing.org](http://www.antiphishing.org)

3. Netcraft Report, April 2010

4. VeriSign Trust Index Report, March 2010. Available at: [https://www.trustthecheck.com/assets/VeriSign\\_Internet\\_Trust\\_Index\\_March\\_2010.pdf](https://www.trustthecheck.com/assets/VeriSign_Internet_Trust_Index_March_2010.pdf)





## VERISIGN: THE LEADER IN SSL, AND BEYOND

VeriSign is the leading provider of trust enablement solutions for the online world. The VeriSign SSL customer list includes the biggest names in e-commerce and banking, 97 of the world's top 100 banks that use SSL as well as 93% of the Fortune 500 that employ SSL use SSL Certificates sold by VeriSign.<sup>5</sup> Viewed up to 250 million times a day, the VeriSign seal is the most recognized trust mark worldwide, with 86 percent online consumer recognition in the U.S.<sup>6</sup> Over 90,000 domains in 160 countries display the VeriSign seal. Web users are accustomed to seeing e-commerce sites display the VeriSign seal—prominently featured to assure users that their online business is authentic and that their web site is capable of securing their confidential information with SSL data encryption.



## THE VERISIGN TRUST SERVICES PLATFORM

By nature of being first-to-market with an SSL solution, and its stature as the industry leader, VeriSign has been associated with trust from the beginning. The ultimate transformation into a broad security platform designed to address today's complex Internet threat environment has been a natural evolution. VeriSign provides SSL, and more, 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.

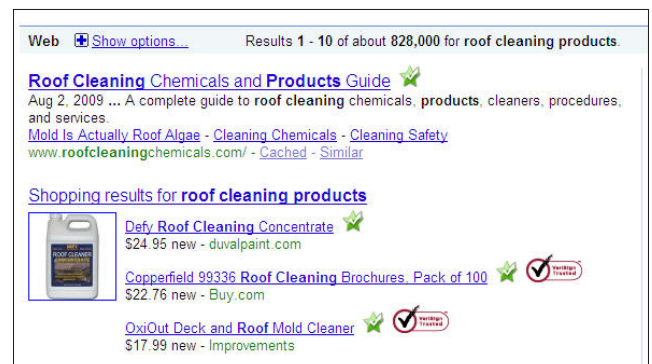
VeriSign has a long successful history of providing its customers with more value as it evolves its SSL-based Trust Services Platform. In addition to the peace-of-mind that comes with selecting a proven SSL Certificate, VeriSign has continued to address its customers' needs by constantly augmenting its SSL technology through support for new standards and integration with complementary technologies and solutions. Integration with third-party technologies, like Qualys (vulnerability assessment) and RatePoint (customer review management) are examples of incremental value-

add through partnerships. The VeriSign Trust™ Seal and VeriSign® EV SSL Certificates are examples of “home grown” functionality that have been added to the SSL core in the recent past.

VeriSign's commitment to address customer needs in a changing threat environment continues with the introduction of web site malware scanning and the related display of the VeriSign Trust Seal in conjunction with search results. Both are included with VeriSign® 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, VeriSign 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 web sites for malware. For owners of a VeriSign SSL Certificate, VeriSign 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 VeriSign Trust Seal, which can be displayed prominently on the site's home page and with search results.



*Display of trust marks can help businesses demonstrate their trustworthiness in search results and encourage traffic to their web site.*

VeriSign® Seal-in-Search™ functionality allows enabled browsers and VeriSign partnered sites to instantly recognize VeriSign trusted sites and display the VeriSign seal next to links in search results.

5. Includes VeriSign subsidiaries, affiliates, and resellers.

6. VeriSign Brand Tracker Study, 2009





This capability enables online businesses to convey a sense of trust to customers prior to navigation to their web site. It also helps links stand out and visually signifies that the online business is a VeriSign 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 VeriSign SSL Certificates and adjacent services.

When combined with the use of the VeriSign seal on the web site 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 VeriSign continuing to evolve the value proposition of its SSL-based solutions to meet the needs of online businesses and consumers.

---

### **Avoid Blacklisting of Your Web Site**

Regular scanning for malware helps you to find and fix malicious code on your web site before search engines block your traffic—a.k.a. “blacklisting.” The blacklisting of your web site 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 as it can be a very painful and long process to get your site reinstated. VeriSign SSL Certificates, with daily malware scanning, help you avoid blacklisting and ensure availability of your web site to 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 VeriSign, 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 web site is free from malicious code that could lead to unwanted malware infections for web site 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, VeriSign has been synonymous with trust from the beginning. VeriSign's Trust Services Platform represents the state-of-the-art in technology, brand, and long-term vision. Web site malware scanning and Seal-in-Search are the most recent innovations that VeriSign has incorporated into its SSL-based solutions to protect online businesses and consumers from emerging threats. VeriSign 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.

### **ABOUT VERISIGN**

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at [www.VeriSign.com](http://www.VeriSign.com) for more information.

