

BUSINESS CONTINUITY AND BREACH
PROTECTION: WHY SSL CERTIFICATE
MANAGEMENT IS CRITICAL TO
TODAY'S ENTERPRISE



White Paper

Business Continuity and Breach Protection: Why SSL Certificate Management Is Critical to Today's Enterprise



VeriSign
Authentication Services



Business Continuity and Breach Protection: Why SSL Certificate Management Is Critical to Today's Enterprise

Contents

Introduction	3
Challenges in SSL Certificate Management	3
The Dangers of Expired and Rogue SSL Certificates	4
Theft of customer data.	4
Losing customers to competitors.	6
Increased calls to customer support.	6
Increased strain on IT departments	6
Best Practices in SSL Certificate Management.	7
Conclusion	8
Symantec® Certificate Intelligence Center: Robust SSL Discovery and Management	8

Introduction

SSL Certificates have been in use for almost 15 years, and they continue to serve a vital role in protecting data as it travels across the Internet and other networks. From online financial transactions to e-commerce to product development, SSL Certificates make it possible for users around the world to communicate sensitive information with the confidence that it is safe from malicious hackers.

The Internet has evolved in innumerable ways over the past decade and a half; so why do SSL Certificates continue to instill trust? Simply put, SSL Certificates are very effective in protecting data in transit. In fact, according to some calculations, it would take about six thousand trillion years—or about a million times longer than Earth has existed—to crack a 128-bit encryption on SSL Certificates with a brute force attack.¹ Even so, the security industry is ever vigilant and many Certificate Authorities have started phasing in 2048-bit encryption on their SSL Certificates, further strengthening the protection for online data communications.

Yet, customers transacting on websites and systems that are protected by SSL security still face serious threats. One key reason for this danger: poor SSL Certificate management. Enterprises with hundreds of SSL Certificates from several different providers could lose track of certificates in their environment. When this happens, certificates could expire and go unnoticed for months, leaving website visitors vulnerable to hackers.

Sometimes, the first sign that there is a “lost” SSL Certificate is a call from a customer who has noticed an expired certificate and asks if it really is safe to make a purchase at the website. Other times it may be something more serious, like a phishing incident that allows cybercriminals to steal sensitive customer data. Or, a security breach that occurs at a Certificate Authority (CA) reverberates through an organization due to its inability to act quickly for lack of visibility into its SSL Certificate inventory.

Whatever the case may be, losing track of SSL Certificates can cause significant financial loss and reputation damage. Fortunately, discovering and managing SSL Certificates within the enterprise does not have to be complex or time-consuming.

This white paper will present the pitfalls associated with poor SSL Certificate management, why they are potentially dangerous to the enterprise, and how enterprises can keep track of SSL Certificates effectively.

Challenges in SSL Certificate Management

Today's enterprise is a complex environment that often encompasses multiple internal networks and public-facing websites. For this reason, a company can have dozens if not hundreds of different SSL Certificates deployed at any given time.

1. <http://www.inet2000.com/public/encryption.htm>

In addition to a large number of SSL Certificates, many enterprises employ a mix of various certificates from different CAs. As an example, an enterprise may install SSL Certificates from a well-known, trusted provider on its customer-facing website and value brand or self-signed certificates on its intranet.

Although some CAs offer online tools to manage their particular certificates, often these tools cannot provide visibility into all of the certificates from multiple CAs across an environment. Instead of making management easier, multiple management portals exacerbate the problem of tracking numerous SSL certificates in a multi-CA environment. Administrators need to constantly monitor their SSL Certificate inventory through multiple systems and put together their own reports to gain a comprehensive view of their SSL Certificate inventory.

To complicate matters, enterprises with distributed networks may have security policies that differ from group to group. In practice, this means that Group A may require Extended Validation SSL Certificates to protect the data that it manages, but Group B uses a different type of SSL Certificates from another Certificate Authority. Or in a scenario that may be more common, Group A might require 2048-bit SSL Certificates while Group B uses 1024-bit certificates. With different policies and no single way to gain a comprehensive view of SSL Certificates across an enterprise, these inconsistencies could lead to security risks and non-compliance with corporate and regulatory policies.

To add another dimension to the problem, consider what happens when the employees who are responsible for managing SSL security change roles or leave the company. If they do not rigorously document which certificates they manage—and communicate that information to other team members—those particular SSL Certificates may go unnoticed when a new team member takes over. Since enterprise IT teams are busy and frequently pressed for resources, manual tracking of SSL Certificates is not only a burden, but prone to human error as well.

All of these factors contribute to an environment where SSL Certificates can be lost or overlooked. Such an environment could lead to business disruptions for an enterprise and create security risks for its customers.

The Dangers of Expired and Rogue SSL Certificates

An expired or rogue SSL Certificate in a network environment could have severe repercussions. It takes just one out-of-date or rogue certificate to expose the enterprise—and perhaps more importantly, its customers—to malicious cybercrime. The following are just a few potential consequences of expired and rogue SSL Certificates.

Theft of customer data

Thanks to years of news headlines about data breaches and education efforts led by consumer advocacy groups and businesses, the public is more concerned about identity theft than ever before. A recent study found that 64 percent of Americans

are very or extremely concerned about someone stealing their identity, with 31 percent describing their level of worry as extremely concerned.²

In this context, the risk of phishing is a major concern. In a phishing attack, a hacker will assume the identity of a legitimate business—taking advantage of the business's lack of authentication from non-existent or expired SSL Certificates—and create a fake website that looks similar if not identical to the real site. Unsuspecting customers will then enter confidential information, such as credit card or social security numbers, on the site. The phished site feeds data directly to the hacker, who may in turn sell it to other criminals.

Even if a phishing incident or data breach is relatively minor, it can exacerbate these fears and seriously threaten the enterprise.

Beyond these immediate losses, phishing and data breaches can also affect the reputation of an enterprise and lead both current customers and prospects to question whether a particular business can be trusted. Industry experts say that it takes about six months to stabilize sales and confidence in a company's network after a breach³—and even then a company's reputation may not be completely restored.

The Increasing Cost of Data Breaches

While damage to a company's reputation can be hard to measure, understanding the economic impact of a data breach is easier to pin down. According to a recent US study, the average cost of a data breach was \$7.2 million per event, or roughly \$214 per compromised record,⁴ numbers that are predicted to continue rising.



Consequences of Unexpected SSL Expirations and Browser Warnings

2. "Identity theft fears weigh on Americans," by Tim Greene, Network World, 4/12/2010

3. "Sony Data Breach Exposes Users to Years of Identity-Theft Risk," by Cliff Edwards and Michael Riley, BusinessWeek.com, 5/3/11

4. "Cost of a data breach climbs higher," Ponemon Institute, ponemon.org, 3/8/11

Losing customers to competitors

Another factor that concerns business is expired SSL Certificates. An expired SSL Certificate can lead to lost business in other ways. Chief among them is simply losing traffic when customers see warnings of SSL Certificate expiration and leave your site to purchase products and services on sites that are secured with SSL Certificates.

Customers may not know exactly how public key encryption works, but visible signs of SSL security—such as an SSL trust seal or the green Extended Validation bar—will make them more likely to transact on a particular site.⁵ If SSL Certificates on e-commerce or other types of public-facing sites expire, they will lose customers' trust resulting in loss of business.

Increased calls to customer support

Today, many companies offer web tools, automated phone menus, and other self-service options to make it easier for customers who have questions to find the information they need. However, if customers visit a website and have any concerns about whether their private data is secure, they will either abandon their transaction (as discussed above) or they may call customer support.

The average cost per support call varies widely across industries, but one fact is certain: the costs of numerous support calls add up over time. Not only do extra support calls drain a company's financial resources, they place an additional burden on the contact center and divert support staff from handling other high-value customer calls.

The extra cost and inconvenience associated with customer inquiries can be easily avoided by maintaining up-to-date security, including valid SSL Certificates.

Increased strain on IT departments

Just like customers who call customer support when they're uncertain about a website's security, employees who see warnings that stem from expired SSL Certificates on intranets or other internal sites will often contact IT staff to resolve the issue. This can add a significant burden to IT departments that are already overwhelmed.

In other cases, employees may ignore these expiration warnings altogether, a situation that continues to leave the affected resources vulnerable to attack. It also sets a negative precedent for security compliance by creating the impression that staff may disregard internal security measures.

Either scenario is preventable with up-to-date SSL Certificate security across the enterprise.

5. <http://www.verisign.ch/ssl/ssl-information-center/ecommerce-trust-ssl/>

Best Practices in SSL Certificate Management

Fortunately, there are services that make it easy to discover and manage SSL Certificates across the enterprise. Some solutions may claim to reduce the burden of SSL management even if they do not allow you to discover certificates from multiple Certificate Authorities. Other solutions might offer multi-CA scanning ability, but lack an intuitive, easy-to-navigate user interface.

To help ensure that you find the best solution to fit your needs, here are some key features to look for in any solution you consider:

- **Ability to scan your environment automatically:** While it is possible to audit networks manually, this approach would simply take too long and require too many staff resources to be feasible in a large, complex enterprise environment. Be sure to select a service that enables your team to conduct automatic scans that will detect SSL Certificates from any provider.
- **An easy-to-use interface:** Information that is hard to access or read will not be useful, so look for a tool that offers a dashboard that is easy to navigate and presents data in a way that is easy to understand at a glance.
- **Delegation capabilities:** In the typical enterprise environment, multiple employees are tasked with security management. For this reason, finding a certificate discovery solution that allows administrators to grant different levels of access and delegate tasks to various employees across the network is critical.
- **Alerts and reporting:** An expired SSL Certificate puts data at risk, so finding a service that will send alerts before a certificate needs renewal is critical. In addition, the ability to generate reports that are easy to read and comprehend is critical. Advanced reporting capabilities will not only provide a deep, comprehensive view of certificates in the network, but will also allow your team to communicate critical information to other staff—such as executives—more effectively.
- **Flexibility and scalability:** Enterprise networks are dynamic, ever-changing environments, which means a certificate discovery service should have configurable parameters, such as the duration of the scan, which IP addresses to scan, etc. In addition, the service must be scalable to allow for future growth.
- **Timeliness:** In order to be effective, network scans must be completed quickly. If a network-wide scan takes too long, the status of some SSL Certificates may change before the full scan is complete. This will result in an inaccurate view of the SSL Certificate inventory.

Conclusion

SSL Certificates are essential to protecting data in transit. Despite its strength and reliability, however, SSL security can still be vulnerable to attack for one simple reason: poor SSL Certificate management.

In a multi-certificate, multi-CA enterprise environment, getting a comprehensive view of SSL security is essential. Knowing the status of every certificate across sites and networks can not only help control customer service costs, but also lower the burden of SSL administration, giving busy IT teams more time to concentrate on other business-critical projects.

Rigorous SSL management can also prevent much more serious consequences, including a major phishing incident or other type of data breach that will not only be expensive to remediate, but may also cause long-term damage to your reputation with customers.

Symantec® Certificate Intelligence Center: Robust SSL Discovery and Management

Symantec Certificate Intelligence Center helps administrators discover and manage SSL Certificates more effectively. With deep visibility and management capabilities, Symantec Certificate Intelligence Center makes keeping track of SSL Certificates easy.

Symantec Certificate Intelligence Center features an intuitive interface that allows administrators to set up automatic scans that quickly discover certificates from any CA. Users can also set up alerts to proactively warn SSL managers when certificates are about to expire.



The easy-to-navigate dashboard offered by Symantec Certificate Intelligence Center

An easily scalable solution, Symantec Certificate Intelligence Center accommodates rapid network changes as business needs shift and grow. Advanced reporting capabilities also give managers a comprehensive view of SSL security that is easy to understand and communicate across the company.

To learn more about how Symantec Certificate Intelligence Center can help you simplify SSL Certificate discovery and management, please visit:

<http://www.verisign.ch/ssl/symantec-certificate-intelligence-center/index.html>

More information

Visit our website

<http://www.verisign.ch>

To speak with a Product Specialist

0800 56 29 24 or

+41 22 54 50 288

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.

Symantec Switzerland AG

Andreasstrasse 15,
8050 Zurich,
Switzerland

