Symantec | Website Security Solutions

Symantec™ Complete Website Security

Symantec is the world's leading provider of Internet trust, authentication and security solutions. Symantec™ Complete Website Security offers you SSL management plus exclusive trust features that extend a secure experience beyond just encrypting online transactions.

Make website security complete with Symantec

The threat landscape never stands still. So Symantec continually evolves solutions to keep your organization one step ahead. What was once a lone hacker and random attacks has now become ‘big business’ for Organized Crime syndicates, now malicious actors target individual companies as Advanced Persistent Threats. Where selective use of security solutions could once keep a company safe, today’s dangers demand the many features of Symantec™ Complete Website Security.

The Norton Secured Seal

The most trusted mark on the Internet, it assures customers that your website is safe and transactions will be secure.

Viewed over a billion times a day in 170 countries.[1]

Recognized by 77% of consumers.[1]

85% of respondents more likely to continue transaction if they see the Norton Seal.[1]

“ We’re constantly trying to equip our merchants with the best security tools possible. We chose Symantec because it gives them the clout they require to gain customers’ trust, wherever their customers might reside.”

Alvin Chan, Senior Sales and Marketing Manager, AsiaPay Limited.[5]

DISPLAYED ALMOST A BILLION TIMES A DAY[1]

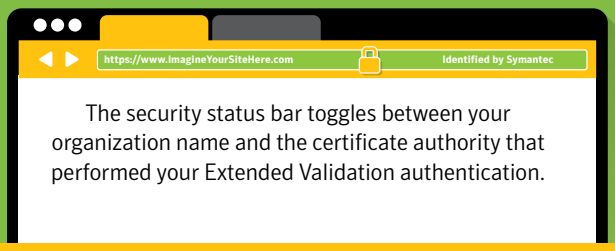
The Norton Secured Seal

Extended Validation

An EV SSL Certificate triggers browsers to display the green address bar which shows your organization's name and the name of the Certificate Authority that issued it.

Giving customers a visual cue that they are interacting with a trusted website and that their information is secure.

Get the Green bar



Proven to increase conversion rates and lowers site abandonment:

- Papercheck – 87% increase in online registrations go.symantec.com/papercheck.[2]
- Keespeek – 20% year-over-year enrolment increase go.symantec.com/keespeek.[3]
- Roseversand – 60% conversions increase using Symantec EV SSL go.symantec.com/roseversand.[4]

Vulnerability Assessment

An automatic weekly scan for vulnerabilities on your public-facing web pages, web-based applications, server software and network ports.

- Identifies the most critical vulnerabilities on your website that hackers most commonly exploit.
- Provides an actionable report that identifies critical vulnerabilities that should be investigated immediately, and items that pose a lower risk.

IDENTIFIES THE MOST CRITICAL
VULNERABILITIES
ON YOUR WEBSITE THAT HACKERS MOST COMMONLY EXPLOIT

Vulnerability Assessment

Malware Scanning

Helps protect you from getting blacklisted by search engines and reduces the risk of propagating viruses to your customers' systems.

Because of the potential damage caused by malware, Google, Yahoo, Bing, and other search engines scan and then blacklist or exclude any site found with malware. Google blacklists 10,000 sites a day, with up to 6 weeks' recovery time.

- Scan detects and reports malware to site owner.
- Highlights malicious code so time taken to resolve is minimized.

GOOGLE BLACKLISTS
10,000
SITES PER DAY

Malware Scanning

Discovery and Automation

With Symantec's discovery and automation tools, you can simplify and centralize the management of your organization's SSL certificates enterprise-wide.

Discovery Tool

Expired, high-risk, rogue or unknown certificates could adversely affect your organization and brand. Discovery helps by enabling administrators to gain detailed information via a central, easy-to-use dashboard.

- Discover and monitor all SSL certificates - no matter which Certificate Authority issued them - to help avoid unexpected expiration.
- Discovery will also identify and catalog self-signed and internal SSL Certificates.
- Get security ratings on all SSL certificates to mitigate non-compliance and security risks.

Automation Tool

By automating manual and routine actions, the automation tool helps ensure efficiency, consistency and accuracy. This capability allows IT teams the time to focus on other mission-critical tasks while providing auditable records for accountability.

- Automate renewal of Symantec certificates to save time and reduce the risk of human error.
- Increase operational efficiency with automated SSL certificate.

GET SECURITY RATINGS ON ALL

SSL CERTIFICATES

TO MITIGATE NON-COMPLIANCE AND SECURITY RISKS

Discovery Tool

01001
00101
00111

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is the future of SSL. Symantec are the first CA to adopt the ECC Algorithm, taking SSL to all-new levels of security and performance.

Stronger encryption

- Elliptic Curve Cryptography offers 10,000 times stronger encryption than RSA in all situations.
- 256 bit ECC key provides the same level of security as 3,072 RSA key.

ELLIPTIC CURVE CRYPTOGRAPHY OFFERS

10,000

TIMES STRONGER

ENCRYPTION THAN RSA IN ALL SITUATIONS

Faster performance

For public-facing servers:

- 30% reduction in server resources - less compute capacity for the same task.[6]
- 15% payload reduction- faster response times for site visitors. [6]

In private server-to-server applications:

- 30-60% reduction in server resources. [6]
- Up to 60% reduction in server resources - less compute capacity for same task. [6]

" In our testing, the Symantec ECC-based SSL certificate reduced the CPU burden on the web server by 46% compared with an RSA-based SSL certificate, and shortened response time by 7%.[7] "

Kel Kato, President, Directorz Co. Limited

Private CA

In line with the CA/Browser Forum's Baseline Requirements, from the 1st November 2015, the issuance of certificates with an internal server name is prohibited. From October 1, 2016, all publicly trusted SSL certificates with an internal name address will be revoked and/or blocked by browser software. Symantec Private CA Solution provides alternative SSL certificates chained to private roots to allow organizations to continue using non-fully qualified domain name certificates.

- Symantec Private CA removes risk while lowering costs.
- Create a private SSL hierarchy for your internal servers.
- Enables the continued use of internal server names and the ability to ignore migrations associated with public roots.
- Create a customized hierarchy based on your needs.
- Reduce the risks, errors, and costs associated with Self-Signed CAs.

Secure App Service

Enables you to sign apps and files in the cloud, protect signing keys and provides reporting of signing activity.

- Easy-to-use dashboard for code signing and management of keys and signing requests.
- Enables you to maintain integrity of files and apps by eliminating issues from lost and stolen signing keys by leveraging Symantec's secure cloud-based service.
- Drive business agility with support for all major file types and integration with third-party test houses.
- Help you to minimize non-compliance and enforce accountability with detailed reports and audit logs.
- Prevent fraud with authentication by IP address(es).

EASY-TO-USE DASHBOARD FOR

CODE SIGNING

AND MANAGEMENT OF KEYS AND SIGNING REQUESTS

Secure App Service

Take control, reduce risks, cut costs

Visit www.cheapSSLsecurity.com
or email support@cheapSSLsecurity.com

[1] Symantec internal customer data [2] Source: Symantec Customer Case Study from papercheck.com, Customer conducted A/B test for approximately three weeks to obtain results.
[3] Source: Symantec Customer Case Study from keespeak.com [4] Source: Symantec Customer Case Study from Roseversand [5] Source: Symantec Customer Case Study from AsiaPay Ltd.
[6] Huang, Lin-Shung, Adhikarla, Shrikant, Boneh, Dan, and Jackson, Collin. An Experimental Study of TLS Forward [7] Source: Symantec Customer Case Study from Directorz Co Ltd