CONFIDENCE REDEFINED

Symantec™ Complete Website Security
No organization is safe from cyber attacks. Organized crime drives the rapid growth and sophisticated evolution of advanced threats that put your entire website ecosystem at risk. And the threat landscape will only grow more dangerous as attackers create more innovative and damaging ways to profit from their efforts.

To make matters worse, weeks and months can pass before you even realize your websites have been breached. The stealthy nature of today’s threats gives cybercriminals more time to pillage and plunder deeper and broader across your website environment.

The longer the time before detection and resolution, the more damage gets inflicted. The risk and size of fines, lawsuits, reparation costs, tarnished reputation, loss of sales, and loss of customers continue to pile up higher and higher. It doesn’t help that you never have enough resources or time to invest in your protection and compliance efforts. The complexity of website security management and lack of visibility across your website ecosystem further frustrate your efforts by making it near impossible to know how and where it’s best to allocate your resources.

That’s why you need Symantec™ Complete Website Security to harmonize and fortify your website security. Across the board, Symantec provides best-in-class solutions for securing your website environment. It helps you strengthen your overall website security posture, prevent or minimize damage from the escalation of sophisticated threats, free up resources for business strategic initiatives, simplify website security complexities, and run and grow your business with confidence.

In a single month in 2016, 96.1 million new malware variants appeared.¹

The number of zero-day vulnerabilities has doubled year-on-year.²

Protect your business, brand & customers

Symantec™ Complete Website Security gives you the visibility, agility, and security breadth and depth you need to protect your business, brand, and customers.

• Real-time visibility into your website ecosystem helps you quickly spot problems, block attacks, fix issues, and stay in compliance.
• Security agility speeds your ability to keep your business safe and growing, while keeping you in control.
• Comprehensive best-in-class solutions give you multi-point and multi-layer protection to keep your website ecosystem safe from the most sophisticated new and emerging threats.

Since Symantec™ Complete Website Security is backed by the global leader in cyber security, you can trust you’ll get the level of security, service, and support you need to protect your website environment, customers, and business.

The threat landscape in numbers

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>78%</td>
<td>Scanned websites with vulnerabilities in 2015</td>
</tr>
<tr>
<td>❌</td>
<td>11 million</td>
<td>Web attacks blocked each day</td>
</tr>
<tr>
<td>🦠</td>
<td>431 million</td>
<td>New malware variants emerged in 2015</td>
</tr>
<tr>
<td>!</td>
<td>125%</td>
<td>Increase in zero-day vulnerabilities from 2014 to 2015</td>
</tr>
</tbody>
</table>

24/7 real-time website security visibility

The complexity of managing security and compliance with finite resources and limited visibility creates a difficult game of resource allocation that you can't win on your own. Without visibility and an understanding of your true risk and compliance posture, it becomes near impossible to make the right decisions and take necessary actions to safeguard your website environment.

Symantec™ Complete Website Security gives you a broad variety of capabilities to harmonize visibility and insights into your overall website security. This includes real-time visibility of your website servers, apps, and data security. As a result, you can more easily spot vulnerabilities, block attacks, maintain integrity of applications and certificates, stay compliant, discover breaches quickly, and remediate faster.

• Automated discovery gives you visibility of all SSL/TLS certificates in your website environment, including who purchased which certificates, when they were issued, the CAs they were issued from, when they expire, and the security posture of those certificates.
• Automated reports verify whether SSL/TLS certificates are valid, conform to standards and determine if servers are properly configured.
• Real-time monitoring and profiling of website traffic combine with global security intelligence and behavioral analysis to proactively detect, block, and remediate threats before they cross your organization’s edge.
• Daily website scans and weekly assessments of website pages, website applications, server software, and network ports detect potential malware and vulnerabilities.
• Tracking, reports, and controls give you visibility and granular insight into all of your code signing activity, including how code signing keys are protected and stored, who can access them, when apps were signed, which keys were used to sign apps, who signed the apps, and when keys expire for signed apps.
Agility with control
You need agility and speed to combat the rapid growth of evolving, sophisticated threats. You also need security that can match business protection with business growth. Security solutions that can’t scale leave your business vulnerable to attack and hinder your ability to grow.

Symantec™ Complete Website Security enables you to scale security at business speed. It gives you security agility that helps you quickly detect and respond to potential threats, while dramatically enhancing your ability to protect intellectual property, private data, customer loyalty, brand reputation, and profitability without negative impacts to the business.

• Increase reliability, prevent outages and free up staff with enterprise-grade SSL/TLS management tools that can discover potential certificate problems before they occur, as well as automate routine replacement tasks.
• Increase the ease, speed, and control of code signing efforts across multiple platforms.
• Speed up and simplify management, renewal, and revocation of application code signing keys on an individual and large-scale basis, including the ability to backdate revocation to minimize customer impact.

Seamless multi-layered security
Trying to secure your website ecosystem is a difficult and consuming balancing act. You try to invest the most protection and remediation in the highest risk areas and most valuable spaces in a way that minimizes risk exposure across your entire environment, and strengthens your overall risk posture. But the rapid evolving complexity and growth of threats and their methods of attack make that increasingly difficult to do.

Too many organizations try to tackle the problem by throwing together different solutions from different security vendors. Unfortunately, this creates a level of discontinuity that frustrates and complicates website security efforts. Additionally, variations in quality and capability from different vendors often lead to gaps and weak links in security postures. Not to mention that simply having to deal with more than one security vendor increases the overall complexity of an already complex effort to secure an organization’s website servers, apps, and data.

Symantec™ Complete Website Security brings together the best-in-class website security solutions you need from a single vendor you can trust. It harmonizes and fortifies your website security with multi-point and multi-layer protection that keeps your website servers, data, and apps safe from the most sophisticated evolving and targeted threats. As the global leader in cyber security, Symantec has the most complete security portfolio, along with the expertise, experience, and global support to give you the help you need, when you need it no matter where you’re located.

The following sections detail some of the solutions, services, and technologies that combine to deliver the best-in-class multi-layer security offered with Symantec™ Complete Website Security.
Discovery and Automation

When your team engages in routine manual tasks such as certificate management, you not only potentially waste valuable resources, but you risk introducing human error. For example, unknowingly allowing key certificates to expire exposes you to vulnerabilities and service disruption risks. As well as the risk to security and business continuity, research shows that over 75% of consumers will abandon a website transaction upon encountering an expired certificate.

Rogue certificates can also increase website vulnerabilities and risk. A Symantec survey indicated that four out of five companies with more than 2,000 certificates had rogue certificates in their systems.

Before taking advantage of certificate discovery and automation from Symantec, expired certificates would disrupt operations for LocalTapiola Group about once a quarter.

“Expired SSL certs created a lot of extra work and could cause internal service blackouts.”

Leo Niemelä
CISO of ICT Security and Risk Management
LocalTapiola Group, a Finnish financial services provider with over 5,000 active certificates.
Secure App Service (code signing)

Another major risk to customer loyalty is the threat of malicious code being unwittingly downloaded while masquerading as one of your legitimate software applications. Code signing all your software with a trusted key is the primary way to combat this threat. However, managing code signing processes across a large software development organization presents a number of challenges in terms of management and security.

Symantec Secure App Service gives you a comprehensive cloud-based code signing management solution. Instead of signing your apps locally, you upload them to our secure cloud service and we sign them for you. This allows us to securely store your certificate and keys in the cloud in our military-grade data centers.

And since we support all the major code signing models expected by most software and operating system vendors, we make it easy for you to choose the model that meets the requirements for your target platform and your own internal security policies. These include unique keys, on-demand/multiple signing keys, and rotating pool keys. As part of the solution we also include vetting and approval of software publishers, certificate revocation, administrative controls, reporting, and audit logs.

“One of the distinguishing features that we found with Symantec Secure App Service is that people never get access to the keys themselves. We have 4,000-plus committers - our term for developers authorized to write code - on six continents. Trying to secure all the keys that they need would be a nightmare. With Symantec Secure App Service, the keys remain in the cloud, and access is provided to sign with them, but not to get the actual keys themselves. That is a huge win for us.”

David Nalley
Vice President of Infrastructure
The Apache Software Foundation
Extended Validation SSL/TLS Certificates

Instilling confidence and trust in your website is vital. Visitors need to feel assured that your site is a safe place to do business. The safest way to secure your customers’ web sessions is through public key encryption between browser and webserver, and the most widely accepted way to achieve this is Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

Of the three levels of SSL/TLS certificate validation shown in the table, EV SSL/TLS certificates employ the strictest authentication standards and deliver the highest level of consumer trust. Sites using EV display well-recognized visual trust indicators such as the green address bar for added assurance. EV provides the most secure and best performing choice for website security, and is known to increase conversion rates as well as lowering site abandonment.

Research from Econsultancy showed that 50% of customers who abandon an online purchase do so due to lack of trust. The good news is that according to a recent online survey in the UK, US, France, and Germany by YouGov, the majority of people know what to look for when deciding whether or not to put their trust in a website. Clear visual signs of augmented website security can enhance consumers’ trust in your business, winning you increased click-throughs and conversions.

### Finding your right level of SSL/TLS certificate

**Level 1: Domain validation (DV)**
The lowest level of authentication – for situations where trust and credibility are less important

**Level 2: Organization Validation (OV)**
A more secure step – for public-facing websites dealing with less sensitive transactions

**Level 3: Extended Validation (EV)**
The gold standard in SSL/TLS certificates – for websites handling credit card and other sensitive data

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Domain validated?</th>
<th>https encrypted?</th>
<th>Identity validation</th>
<th>Address validation?</th>
<th>Padlock displayed in browser user interface</th>
<th>Green address bar*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DV</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>OV</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Good</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>EV</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Strong</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*And/or green padlock or green treatment within the address bar
Malware Scanning

It’s an unfortunate fact that many organizations fall victim to avoidable hacks and malware infections simply because they don’t carry out basic website health checks. In 2015 for example, 78% of scanned websites had vulnerabilities – a fifth of which were critical. These infections can be crippling – Google blacklists 10,000 websites every single day, and it takes an average of six weeks before such domains are restored to search results. Lack of basic website health checks also open the door to severely damaging high profile breaches, such as Distributed Denial of Service (DDoS) attacks that range from simple HTTP404 error pages to complete blackouts.

That’s why Symantec™ Complete Website Security performs weekly vulnerability assessments and daily malware scanning of your website pages, applications, server software, and network ports. Weekly assessments can alert you to vulnerabilities that need to be fixed in order to keep them from being exploited by cyber criminals. They provide you actionable reports that identify all known vulnerabilities whether critical and requiring immediate action, or lower risk items that can wait for the next scheduled update. Upon patching, there is an option to rescan the website to help confirm the vulnerabilities have indeed been rectified.

Daily malware scans help you make sure your websites are free of malware. Additionally, once you install the Norton Secured Seal, it will continue to automatically display on your sites as long as the scans report your websites to be free of malware.

The Norton Secured Seal gives your customers another clear sign that you’ve gone the extra mile to protect their privacy and online security. The Norton Secured Seal is viewed over half a billion times per day on websites in 170 countries, in search results on enabled browsers, and on partner shopping sites and product review pages. The Norton Secured Seal is one of the trust marks most readily recognized by consumers.

90% of respondents indicated they would be more likely to continue online transactions after seeing the Norton seal.
Elliptic Curve Cryptography

A more recent alternative to the standard RSA encryption used in traditional SSL, is Elliptic Curve Cryptography (ECC). ECC 256-bit not only makes use of a more advanced encryption algorithm that is 64,000 times harder to crack than the standard RSA 2048-bit, but its use of a smaller key (only 256 bits long) means that it requires far fewer CPU cycles to encrypt the data. That can help you reduce costs and improve website performance. If desired, you can also combine the ubiquitous RSA root with the stronger security and server performance offered by ECC in our hybrid SSL/TLS certificates.

DDoS Protection*

Symantec™ Complete Website Security also includes DDoS Protection, giving you the ability to mitigate all the most common DDoS attacks against any type of online service. Included in this defense is protection against application level DDoS attacks, which target vulnerabilities in your OS or web applications that are usually immune to generic filtering. With automatic, always-on detection and triggering of ‘under-attack’ mode, you are assured the fastest possible response and recovery with minimum business disruption. *Powered by Imperva Incapsula.

Directorz Co. Ltd., a Symantec customer in Japan, measured a 46% lower CPU load as well as a 7% faster web response time following its deployment of ECC.

Private CA

To help reduce the risks, errors, and hidden costs associated with self signed certificates, Symantec™ Complete Website Security offers a Private CA solution. Consolidating management of Public and Private Certificates within a single console improves both security and visibility. You can continue to use internal server names. Plus, you can ignore migrations associated with public roots, which allows you to create a customized hierarchy based on your unique needs.

Optimized content delivery through CDN

In addition to its seamless multi-level security, Symantec™ Complete Website Security now includes an application-aware, global Content Delivery Network (CDN) for full site acceleration. This global system of strategically positioned servers brings your website content closer to your customers, helping it to load and run faster. Including both static and dynamic caching as well as content and network optimization tools, research has shown that websites using it typically run 50% faster and consume up to 70% less bandwidth.
24-Hour Support
Symantec 24/7/365 global support and services give you confidence that you can always get the help you need when you need it, no matter where you’re located.

Our services include access to a dedicated technical account manager seven days a week who will:

- Monitor and drive prioritization for each of your support cases.
- Track product enhancement requests (if applicable).
- Communicate any service-impacting maintenance.
- Act as a service/support escalation point.

Simple, Flexible, and Predictable Subscription Service
Symantec™ Complete Website Security is a supportive and flexible website security partnership designed to let you focus on your business without having to worry about service cost and administration issues throughout the year.

Available through annual and multi-year subscription contracts with no additional charges – guaranteed – you can accurately anticipate your total annual spend. For a simple fixed price and fixed term, you get flexible access to all the services you need, whenever and wherever you need them, across your entire organization. And it’s covered all under a single PO.
Symantec™ Complete Website Security

Symantec Complete Website Security gives you the visibility, agility, and security breadth and depth you need to protect your business, brand, and customers. It harmonizes and fortifies your website security with comprehensive best-in-class solutions. Multi-point and multi-layer protection keeps your website ecosystem safe from the most sophisticated new and emerging threats. Real-time visibility into your website ecosystem helps you quickly spot problems, block attacks, fix issues, and stay in compliance. It delivers the tools and services you need to safeguard the integrity and performance of your website servers, certificates and apps. Its security agility speeds your ability to keep your business safe and growing, while keeping you in control. Since it’s backed by the global leader in cyber security, with the most recognized trust mark on the web and one of the world’s largest cyber intelligence networks, you can trust you’ll get the level of security, service, and support you need to protect your website environment, customers, and business.

The SSL Store™

The SSL Store™ is the world’s premier SSL service, combining strong industry partnerships with over a decade of experience in the cyber security sector. Based out of beautiful downtown St. Petersburg, FL, The SSL Store™ boasts clients in over 100 countries, has an office presence on three continents and offers the best prices and margins anywhere on the internet. Founded on an underlying ethos of integrity and hard work, customers rave about The SSL Store’s world class 24/7 customer service and powerful industry insights. And while the company cut its teeth on its retail and reseller programs, its Enterprise program is second-to-none—offering dynamic, scalable security solutions and a streamlined interface for enterprises of all sizes. Whether you’re a small business owner, a reseller or a large enterprise client—you can trust The SSL Store™ to secure your web presence.

Schedule a quick call for a detailed savings assessment
Call +1 (727) 565-4251 or email enterprise@theSSLstore.com