Symantec™ Complete Website Security

A comprehensive solution for all your website security needs, with features ranging from Extended Validation SSL/TLS certificates and malware scanning, to DDoS mitigation and performance optimization.
There’s only one constant in website security: that the threats we face will continue to grow in both scale and sophistication. The reality of this situation can be seen in the on-going battle between those seeking illegal access to online information, and those attempting to protect it. It’s been a sobering experience, and one that’s forced us to wave goodbye to the notion that a secure boundary can be built to keep out all unwanted intruders. The reality is that criminals have tunneled under, made holes where no one was looking, or simply donned a disguise and walked through the front door.

Understanding the threat
Until now, the role of website security has been predominantly reactive – rapid firefighting whenever a new threat arises to build up defenses and mitigate the potential impact. A solution is needed that proactively and effectively protects your website from increasing danger. As a function, we’re no longer facing the single threat of lone hackers working out of their bedrooms. Rather, this danger now comes from criminal networks, government-sponsored threats, and hacktivists. Ensuring the right resources are deployed at the right place and the right time is no longer just important, it’s essential.

Generating a response
Building and maintaining a secure corporate infrastructure, alongside customer trust, is a continuous exercise that can be undone in seconds, and this rapidly changing threat landscape has meant that constant innovation is required to evolve website security solutions at the same pace. Although we know that sitting still is simply not an option, it’s also impractical to expect a response to each new emerging threat given the twin constraints of time and money. Instead, you should be looking to your security partner for support, and for education in spotting vulnerabilities and mitigating any risks.

Enter Symantec™ Complete Website Security.

The threat landscape in numbers
(from Symantec’s Website Security Threat Report 2015)

- **29,927** New unique malicious web domains in 2014
- **317,256,956** New malware variants emerged in 2014
- **496,657** Web attacks blocked each day
- **183%** Increase in DNS amplification attacks between January and August 2014
A focus on security

The challenge of resourcing your security
As we all know, website security is ultimately about confidence – and building a sense of trust with each visitor. Generating this trust requires a realistic understanding of the dangers faced by your organization and an accurate assessment of the capabilities needed to counter them. It could be argued that the biggest threat is actually the limited resources typically dedicated to website security – and a reliance on manual processes that, combined with time pressures, make even the simplest security task difficult to achieve.

Extended Validation SSL/TLS Certificates
Instilling confidence and trust in your website is vital; visitors need to feel assured that your business’s site is safe to transact on. Research from Econsultancy showed that 50% of customers who abandon an online purchase do so because of a lack of trust. A recent YouGov online survey in the UK, US, France and Germany gave clear and encouraging results: the majority of people know what to look for when deciding whether or not to put their trust in a website. Not displaying clear visual signs of a secure website can damage your end consumers’ trust in your business, and might lose you valuable 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>DV</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>OV</td>
<td>Yes</td>
<td>Yes</td>
<td>Good</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EV</td>
<td>Yes</td>
<td>Yes</td>
<td>Strong</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*And/or a green padlock or green treatment within the address bar
A denial of service
It’s also an established fact that many organizations fall victim to hacks and malware infections because they don’t carry out basic website health checks. In 2014 for example, 75% 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 6 weeks before they’re restored. Then there are the high profile breaches and, in particular, Distributed Denial of Service (DDoS) attacks that range from simple HTTP404 error pages to complete blackout, and are constantly increasing in intensity. Symantec™ Complete Website Security now includes Imperva Incapsula DDoS Protection - capable of mitigating all types of DDoS attacks targeting any type of online service - alongside our established armory of tools to help keep your website at full health.

Malicious bots at the application layer
In addition to the above, there are application level DDoS attacks, which target vulnerabilities in your OS or web applications, and are immune to generic filtering. These are attacks performed by malicious bots designed to impersonate legitimate human visitors and hijack browsers in a bid to take down an organization’s servers. In 2014 we identified a 240% increase in Bot traffic, numbers that confirm what many security experts already know: hacker tools are now being designed first and foremost for stealth. Our response has been to further enhance the protection our solution offers, with the addition of Imperva Incapsula Website Application Firewall (WAF) – redefining and extending the WAF beyond traditional concepts.

Symantec™ Complete Website Security

Security features spotlight:
- Vulnerability Assessment
- Malware Scanning
- Extended Validation SSL/TLS Certificates
- Imperva Incapsula DDoS Protection
- Imperva Incapsula Web Application Firewall
- Secure App Service

At Symantec we thrive on providing solutions to the challenges you face, to support you today and for the future.
A focus on management

The quest for greater simplicity
There’s a growing appreciation that managing website security has become far harder than it should be. This is particularly the case when it comes to licensing SSL/TLS certificates, and many PKI administrators and website security managers still face the daunting task of searching out hidden certificates to avoid unexpected expiration dates.

The problem of tracking certificates
At Symantec we understand that tracking SSL/TLS certificates isn’t easy, especially if multiple people in your organization have the ability to implement them in isolation. Expired certificates can hurt you even more – our research found that over 75% of consumers would abandon their transaction if they encountered an expired SSL/TLS certificate. On top of that, 45% of surveyed businesses experienced security breaches that were due to SSL/TLS certificate issues. That’s why you need tools that simplify and centralise this process, which is exactly what’s on offer with Symantec™ Complete Website Security.

SSL/TLS certificate management made easy
Of course there’s more to life – or at least website security – than just focusing on the buying and renewing of certificates. There is also the need to search out rogue certificates, monitor expiration dates, and maintain standards – all of which can prove difficult in large, geographically dispersed organizations. In a recent Symantec survey, four out of five companies with 2,000+ certificates found rogue certificates in their systems. However, with Symantec’s discovery and automation tools you can centralize SSL/TLS management – and discover all certificates across the enterprise regardless of which certificate authority issued them.
A focus on performance

Website management
Let’s face it, the key metric when measuring website performance is traffic – which also involves considerations such as conversion levels, alongside more technical aspects including latency, availability, and bandwidth. Symantec™ Complete Website Security solution can support your website in each of these areas.

Optimised content delivery
According to Forrester, 40% of shoppers will wait no longer than three seconds for a web page to load before abandoning a retail site.¹ Today there are number of sophisticated tools available to help your website load and run faster. For example, a Content Delivery Network (CDN) is a global system of strategically positioned servers that brings your web content closer to your consumers. Symantec™ Complete Website Security now includes Imperva Incapsula CDN that offers caching, content and network optimization tools, and research has shown that websites using it are typically 50% faster and consume up to 70% less bandwidth. In addition, CDN supports load balancing, ensuring workloads are efficiently distributed to help maintain high website availability.

Strength and speed through encryption
As we know, SSL/TLS certificates enable encryption all the data that passes between a user’s browser when they consult a protected website and the company server hosting this website. So, obviously, stronger encryption is more desirable. Elliptic Curve Cryptography (ECC) 256-bit is a more advanced encryption algorithm that is 64,000 times more secure than RSA 2048-bit. What makes it even better is that it requires much less server capacity to encrypt information, reducing costs and improving your website’s performance. Just for example, Directorz Co. Ltd., a Japanese firm, saw a 46% lower CPU burden and a 7% improvement in response time when they implemented ECC. Today, you can also combine the ubiquitous RSA root with the stronger security and server performance offered by ECC in our hybrid SSL/TLS certificates.

Building on trust
We’ve already demonstrated how important it is for consumers to feel confident when providing data or making an online purchase, and trust marks are a well-recognized indicator of website security. Of these, the Norton Secured Seal is one of the most trusted on the internet, and is viewed over a billion times a day in 170 countries. It makes a big difference: 90% of respondents in an international consumer study said they are more likely to continue online transactions if they see the Norton Secured Seal.² Displaying the seal beside your link in search engine results is also proven to significantly increase traffic to your website.

Symantec™ Complete Website Security

Performance features spotlight:

- Imperva Incapsula CDN & Optimization
- Elliptic Curve Cryptography
- Norton Secured Seal
- Seal in Search

Symantec™ Complete Website Security
Advanced threats, enhanced solution

Complete Website Security goes far beyond encryption to deliver protection for websites, data and applications—with 24/7 control that helps to mitigate risk and helps to ensure uninterrupted performance for every website. Multi-layered security and controls make our certificate issuance and authentication processes one of the most rigorous in the industry. Automated management pinpoints certificate and website weaknesses due to unexpected expirations, flawed installations, depreciation and critical vulnerabilities in the event of attacks. Meanwhile, Symantec’s unified security identifies worldwide security vulnerabilities, delivers real-time analytics and helps our customers to protect against damage, 24/7. It’s why we’ve become the name people trust.

Features and benefits - Security

VULNERABILITY ASSESSMENT
- A weekly scan helps identify and act against exploitable website vulnerabilities
- Delivers actionable reports that identify critical vulnerabilities requiring immediate investigation and lower risk items
- Provides an option to then rescan website to help confirm that vulnerabilities have been rectified

MALWARE SCANNING
- A daily scan detects and reports malware to site owner
- Highlights the malicious code, meaning time taken to resolve the issue is minimized
- Mitigates the risk of being blacklisted by search engines
  (Google blacklists 10K sites a day – with up to 6 weeks' recovery time)

EXTENDED VALIDATION SSL/TLS CERTIFICATES
- EV SSL/TLS certificates deliver the highest level of consumer trust through the strictest authentication standards
- Sites with EV display well-recognized visual trust indicators for added assurance
- The most secure and best performing choice for website security; EV is known to increase conversion rates and lower site abandonment

IMP ERAVA INCAPSULA DDOS PROTECTION
- Market-leading protection against one of the most common website attacks
- Automatic always-on detection and triggering of ‘under-attack’ mode
- Zero business disruption based on transparent mitigation with minimum false positives
- End-to-end protection against the largest and smartest DDoS attacks
IMPERVA INCAPSULA WEB APPLICATION FIREWALL

- Innovative cloud based firewall to protect against Layer 7 attacks, powered by Imperva Incapsula
- Defends against OWASP Top 10 threats including: SQL injection, cross-site scripting, illegal resource access and remote file inclusion
- Proactive remediation from constant monitoring and application of dedicated security rules
- Activated by a simple DNS change

SECURE APP SERVICE

- Enables enterprises to:
  - Sign apps and files in the cloud
  - Protect signing keys
  - Provide reporting of signing activity
  - Keep track of engineering output through use of an integrated web-based portal or via API

Features and benefits - Management

DISCOVERY

- Allows you to discover all SSL/TLS certificates in your environment regardless of CA
- Eliminates the chance of certificates expiring unexpectedly

AUTOMATION

- Allows you to automate the renewal of Symantec certificates to save time and reduce the risk of human error

PRIVATE CA

- Improves security and enables consolidation with Public and Private Certificates in one console
- Reduces the risks, errors, and hidden costs associated with Self-Signed CAs
- Allows the continued use of internal server names, and the ability to ignore migrations associated with public roots
- Allows you to create a customized hierarchy based on your precise needs

24 HOUR SUPPORT

- Includes access to a dedicated technical account manager* 7 days a week who:
  - Monitors and drives prioritization for your support cases
  - Tracks product enhancement requests (if applicable)
  - Communicates any service-impacting maintenance
  - Acts as a service/support escalation point

*Does not include Imperva Incapsula products
Features and benefits - Performance

IMPERVA INCAPSULA CDN & OPTIMIZATION
- Application-aware, global CDN for full site acceleration
- Layer 7 Load Balancing solution for optimal utilization
- Static and dynamic content caching for maximum website performance

ELLiptic CURVE CRYPTOGRAPHY
- Elliptic Curve Cryptography (ECC) Algorithm
  - 64,000 more secure than RSA – compared to an industry-standard 2048-bit RSA key
  - ECC-256-bit keys are 64,000 times harder to crack
  - 7-10% faster using less CPU power
- ECC/RSA Hybrid Algorithm
  - Improves browser compatibility; better root ubiquity
  - Improved performance
  - More secure than pure RSA

NORTON SECURED SEAL
- The Norton™ Secured Seal is the most recognised trust mark on the Internet
- In a U.S. online consumer study, 90% of consumers recognized the Norton™ Secured Seal, more than our competitors’ trust seals
- 90% of respondents more likely to continue online transactions if they see the Norton Seal

SEAL IN SEARCH
- Establish trust and credibility with visitors by displaying the Norton Secured Seal
- Demonstrate that your site is both a legitimate and safe environment to perform transactions
- Convert more visitors into customers

---

1 International Online Study (U.S, Germany, UK, France, Australia and Singapore only) October 2015
2 Study conducted October 2015
3 International Online Consumer Study: US, Germany, UK, July 2013

---

9 | Symantec Corporation

Symantec Complete Website Security
Greater security, simplified management, enhanced performance

To find out more about how Symantec™ Complete Website Security can deliver an efficient, effective and comprehensive solution for all your website security needs, contact us today:

Call 1-866-893-6565 or email SSL_EnterpriseSales_NA@symantec.com