CUSTOMERONE

Symantec

How Always-On SSL Protects Our Website—And Its Visitors

Dave Ott and Ted Garvey had just joined the Symantec team. And they were surprised and shocked.

They became Symantec employees when we acquired VeriSign's identity, authentication, and SSL certificate businesses. They were shocked because VeriSign content was folded nonsecurely into the Symantec corporate website, and served as http; only login and transaction pages were secured as https. (This sometimes-secure delivery is called *intermittent SSL*.) To Dave and Ted, that was a step backward; on the former VeriSign site, every page—from a visitor's first click to the last—was secured. This is *always-on SSL*, AOSSL for short.

Intermittent SSL was common practice when Symantec acquired VeriSign—but it wasn't *good* practice, because it potentially exposed visitors' information to cyber-sniffers using the right tools. "We had always had https at VeriSign," recalls Dave, a senior program manager in our Website Security group. "It was important for us, for our business, and for our customers throughout the world."

Dave and Ted advocated tirelessly for AOSSL at Symantec, and offered their help to make it happen. Meanwhile, big-name technology and social-media companies began boasting about their secure websites and chiding competitors (including us) whose sites weren't secure. SSL Labs, a respected site-security analysis tool, gave www.symantec.com a B grade—and that didn't sit well with anyone here. It became clear that Dave and Ted were right: AOSSL was no longer optional for Symantec. It was a must-have.

Moving www.symantec.com to AOSSL took concerted effort and clever work by Symantec's web development team. This paper describes what we did, why we did it, and why we think AOSSL is important. We explain some of the challenges we ran into and how we overcame them, and share some of the tools and tricks we used to find and fix problems. We've also included a primer on website security and SSL/TLS certificates.

Always-On SSL is becoming the standard for legitimate websites because it protects both a website itself and the people who visit it. Symantec has moved its main site, www.symantec.com, to AOSSL. This paper will help CIOs, CTOs, CISOs, and senior managers understand **best practices** for AOSSL, **who** needs to be involved, **what** to look out for, and **where** to go for help to succeed. You'll see what we did, why we did it, and what you can learn from our experience.

Checking Every Nook and Cranny

There are plenty of good reasons to make an enterprise website AOSSL: It **improves your visibility**, since Google's search engine favors secure sites over nonsecure ones.[1] It **guards your visitors** from "man in the middle" attacks where cybercriminals take advantage of intermittent SSL gaps to "sidejack" an online session. And AOSSL **protects your business** from exposing important data.

All of these reasons came to mind when we decided to make the move. "Beyond security considerations, AOSSL has benefits when it comes to getting noticed," says Alex Horovitz, senior director in Symantec's Global Security Office. "In the last two years Google's search engines have been increasingly taking into account sites' usage of secure, encrypted connections as a signal in their search ranking algorithms. Going forward, they are only likely to increase the weight of this particular signal."

Of all the good reasons to adopt AOSSL, the evolving nature of our website–and our business–really drove Symantec down that path.

Since its launch in December 1996, our website was mainly used for marketing: It explained our products and services, and provided a portal to data sheets, case studies, documentation, and other resources. A marketing-driven site made sense given our business model: software (for both enterprises and consumers) was sold with a perpetual license, delivered on physical media, and installed and managed on-premises.

Today, Symantec solutions are increasingly available as services. Customers can subscribe to them, consume them, and manage them online. Consequently, our website is becoming the front door to a growing transaction engine, rather than a marketing billboard. We want that door to be open wide to legitimate visitors, and we also want to showcase best practices for website security. That means having AOSSL.

AOSSL and Certificate Basics

Always-on SSL is not a product. The Online Trust Alliance (of which Symantec is a member) calls it "an approach to security that recognizes the need to protect the entirety of a user's session, not just the login screen."[2]

To make a website AOSSL, you must purchase one or more **SSL certificates** and install them on the environment that serves your website. SSL (Secure Sockets Layer) certificates are data files that connect a webserver, or some other part of a website environment, to the organization that owns it. Certificates also enable encrypted connections between a website and a browser. You know you're on a site with a properly installed certificate when its address begins with https, rather than http.

Sometimes the letters TLS (Transport Layer Security) are used when discussing SSL; TLS is, in essence, an updated, more secure, version of SSL. While TLS and SSL are technically different, SSL remains the common term.

To be considered AOSSL, a website with a certificate must redirect every http visitor to connect via https. The way you redirect visitors, the number of certificates you need, where you install them, and how those certificates connect and communicate with each other (called **chaining**) varies from website to website. In the Symantec environment we have certificates on content management systems, several load balancers, and the central content delivery network (Akamai, in our case). Some of our content-vendor partners also have certificates on their services.

SSL certificates are available from a **Certificate Authority** (CA) such as Symantec. The certificate you need depends on your circumstances; certificates can be created to secure a single domain name, multiple domain names, or multiple subdomains.

There are also several levels of validation, the most robust of which is called an **Extended Validation SSL Certificate**, or **EV SSL**. To purchase an EV SSL, a website owner goes through an extensive authentication process in compliance with the CA/Browser Forum, a group of CAs and browser developers that defines industry best practices.[3]

Although Symantec is a CA, we too are subject to those rules when we issue certificates for our own web properties. "You would think if we needed a certificate that there would be some sort of fast-track process," Ted says. "There's not. We have to go through the same process as everyone else."

AOSSL does not require an EV SSL Certificate. Sites secured with a standard SSL certificate typically show a lock in the browser's address bar; visitors to EV SSL–secured sites get additional visual cues about the extra validation, such as a green lock or green address bar on their browser.

AOSSL is becoming a web standard and a best practice, even for companies not in the security business. Only 3 percent of the 1 billion websites worldwide today are secure or have basic encryption, and Symantec wants to change that. Through an initiative called **Encryption Everywhere**, we're working with leading web-hosting partners to secure 100 percent of legitimate websites by 2018.[4]

"It's a question of user perception and confidence," says Michael Matsui, our senior manager of Web development. "Whether or not a transaction happens on www.symantec.com, it's the starting point for our customers. If we want customers to click a 'Buy' button, they need to feel secure from start to finish."

"If we want customers to click a 'Buy' button, they need to feel secure from start to finish."

— Michael Matsui, Senior Manager of Web Development, Symantec

But there were challenges. We needed to account for our site's complex structure, its thousands of pages of content (some of it years old—still valid, but not built to be secured), and the aging content management system that hosted it all. "We couldn't just slap an SSL certificate on it and be done with it," Michael continues. "That would be guaranteed to break things."

"Problems appear when you have a secure site that serves up nonsecure assets," explains Ted, a web development manager and SSL expert in our Website Security group. "It becomes a terrible experience. Users get popups about nonsecure content, or the green bar goes away. People know right away that something's not right." These problems are called *mixed active content* issues.

"It's not a small undertaking to switch a site that's been around for a very long time and that has legacy content in lots of little nooks and crannies," agrees online marketing specialist Elizabeth Medford, our site search expert. "You have to make sure all of those resources will chain up to a certificate." That can be difficult when all elements of a site aren't directly under your control.

Weighing the Options and Benefits

That was the case at Symantec—and we're not alone. Very few enterprise websites are freestanding operations; instead, they're a collection of services—some of which the website owns and hosts, and others it doesn't.

"To run the website of a big business, you need third-party vendors to handle some specific technical requirements," Ted explains. "Some of those vendors don't deliver their services securely, and that can create mixed active content errors. It can be a lot of work if you want to continue to use a particular service in AOSSL."

So the first step toward AOSSL was to locate every nonsecure service used by our site. Using the developer toolkit built into the Chrome browser, Mike and his team crawled thousands of pages, looking for things that wouldn't work with https. They identified two site-wide problems; here's what they were and how we fixed them:

Embedded video. More than a thousand videos are hosted on our site using a popular third-party platform for corporate media. The specific player we embedded in our pages wasn't made to support https. (We're not alone; marketing manager Jim Presley, our video guru, says the same nonsecure player is "used all over the Web.") When the player was embedded in a secure page, the problems varied by browser; the page wouldn't load at all, or blank boxes would appear in place of videos, or the page would load but the secure connection would break when the video played.

Fixing this required changing a few parameters in the page code—a relatively easy fix, once Mike and Jim figured out what those changes were and where they needed to make them on thousands of pages. But that initial fix exposed two additional video-related problems.

One was with a plug-in for delivering captioning and subtitles generated by a different third-party vendor. Mike and his team made a few more parameter changes to secure the connection to the captioning service.

The second problem was the result of an open-source, third-party plug-in that collected metrics on video use for our marketing analytics system. Michael's team ended up developing a custom solution to this problem that provides visitors with a baseline level of functionality. It's not the perfect solution Michael wanted, but the issue will be completely resolved soon—we'll explain how later.

Site-wide search. Symantec's homepage has a search function to help visitors find information on the site. Two load-balanced search appliances, separate from the webserver, do the searching. Because these appliances were not https devices, search results appeared on a nonsecure page with incorrect formatting.

This was more than an inconvenience; to serve our users, we really needed search to work perfectly. "The search bar is one of the few places where customers directly tell us what they need," Elizabeth says.

Applying certificates to the appliances, and chaining them up to the main certificate on the homepage, didn't fix the problem. However, applying a certificate to the appliances' load balancer—coupled with some code changes on the webserver—appeared in the lab to eliminate the errors.

To be certain the fix would work in production, Elizabeth wanted to perform a real-world test. She drafted a handful of U.S.-based colleagues for a guerilla project. "I'd say to them, 'Do you want to spend five minutes in Denmark?'" she recalls with a grin.

With her recruits lined up, Elizabeth switched the production environment for our Danish regional site to AOSSL, and her recruits quickly loaded the site using a variety of browsers and ran some searches. After a few minutes, she switched the site back and analyzed her testers' results–all of which were, thankfully, successful.

"We chose the Danish site–a smaller regional site in Europe–because of the low traffic volume and because when we did the testing, it was the middle of the night there," Elizabeth explains. "I don't recommend this normally, but in this case it was the most accurate and expedient test–and the risks were far outweighed by the benefits."

Taking AOSSL to the World

Tackling these site-wide problems–including finding the best approaches to resolving issues and the right places to make changes–took a few months for Michael and his team. This wasn't the only big thing they were doing at the time, by the way; they were implementing both a redesign and a platform change. More on that in a bit.

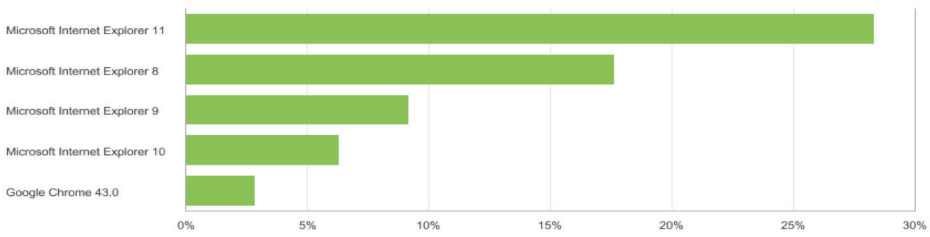
A few smaller issues also slowed our adoption of AOSSL. One concerned the customers and prospects who visited our site–the very people we most needed to impress with AOSSL. Our website metrics showed that they often used older technology; indeed, the second most commonly used browser used on our site in 2015 was more than six years old, as shown in the chart below.

"I think this is a function of enterprise companies and the PC images that their IT departments issue," Michael says. We adjusted the strength of our ciphers to work with a broad range of browsers. The browser issue is abating as more customers adopt modern platforms, but it's a good reminder: Make sure AOSSL doesn't get between you and your important visitors.

Cipher strength–which measures how secure a connection is–affected more than browsers. We discovered that one of our own software products had an embedded routine that pinged www.symantec.com to test its Internet connection; when we first turned on AOSSL, the product team immediately called Michael to complain that the test was suddenly failing. We had to dial down our cipher strength for a short time while the product team updated the software and pushed the update out to customers.

However, rolling out AOSSL wasn't only about problem-solving. Smart planning helped us avoid some issues completely. For example, we chose not to go AOSSL simultaneously around the globe. Instead, we started with the English-language main U.S. site, worked out the kinks there, and then extended AOSSL coverage globally to our three dozen other language- and/or country-localized sites. "It was easy to go AOSSL to the global sites once we knocked out the infrastructure-related problems," Michael says.

Rolling out AOSSL in regional waves also confirmed that our webservers and vendors (such as our media provider and Akamai, our content delivery partner) could handle the extra computing workload that AOSSL required. We were pleased, but not surprised, by the low processing overhead and negligible performance hit.



More than 15 percent of visitors to www.symantec.com in 2015 used Internet Explorer 8, a browser that was released in 2009.

"A few years ago, https was more taxing on the servers than http," Ted explains. "Technology has evolved, and it's much more efficient now." Current CPUs perform the tasks needed for https very quickly, and the additional network round trips required to establish the secure connection also happen very rapidly in most circumstances.

> **"A few years ago, https was more taxing on the servers than http. Technology has evolved, and it's much more efficient now."**
>
> – Ted Garvey, Web Development Manager, Website Security, Symantec

The bottom-line lesson from our experience is this: You can test and test, but issues will probably still arise when you turn on AOSSL. AOSSL is worth the effort because of the benefits it brings, but it requires a change of mindset. Don't think of going AOSSL as a one-time operation, but rather as a lens through which you view every aspect of your website, now and going forward. Then you'll be as successful as we were.

We should add here that our web development team performed all of these experiments–and made the countless small but important changes necessary for AOSSL–in parallel with a major redesign of the Symantec website and the start of its migration to a new, modern content management system. The redesign and migration are ongoing; the team is prioritizing, consolidating, updating, and migrating thousands of pages of still-useful legacy content that originated in a

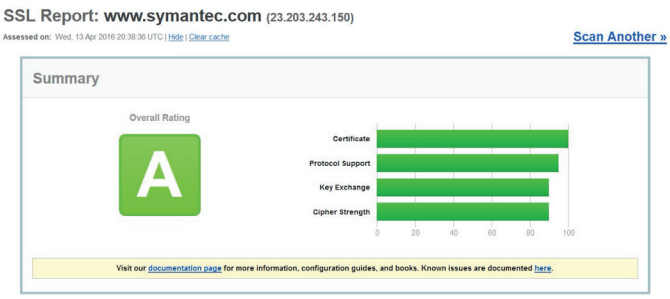
variety of sources over the years. It's a huge, cross-functional task, and one that many organizations face today.

The team may have preferred to change just one thing at a time, but the fast pace of our business today wouldn't permit it. The good news here is that the new content management system we've adopted is far superior to the solution we're migrating from. It will eliminate some nagging issues altogether (such as those related to video players) and is much easier to secure than the old one. As a result, when all of our legacy content is migrated our website security and SSL certificate environment will be simpler and easier to manage.

The hard-won lessons we've learned in this process can help you take your site AOSSL, too. To talk to our experts about website security, visit our Executive Briefing Centers at our U.S. headquarters in Mountain View, California, or in Reading, U.K., or call Symantec at +1 866-893-6565 or +1 520-477-3111. We'll customize a briefing to meet your specific goals, and give you a sneak peek at new challenges and technologies on the horizon.

Thanks to our team's hard work, https://www.symantec.com now earns an A grade from SSL Labs. (Our score is pictured above right, but you can check it yourself–and grade your own site–at https://www.ssllabs.com/ssltest/.) "This was a personal challenge for me," Michael says. "We all want to get the best score. It's been my goal to increase our grade to an A. And we've done it."

Good grades are fine, but in truth the most important measure is our customers' confidence. We went AOSSL because Symantec wants to remain the world's most trusted advisor in cybersecurity.



In early 2016, our website went AOSSL and earned an A rating from SSL Labs.

And that means we must set an example. As Ted, who initiated and pushed for AOSSL says: "To be the leader, we have to be Always-On SSL. That's the bottom line."

> CONTACT SYMANTEC TODAY

SYMANTEC SOLUTIONS AND PRODUCTS IN THIS PAPER

Secure Site Pro with EV SSL Certificates: Secures your website and gives your customers confidence that their transaction is safe and secure.

Encryption Everywhere: End-to-end security for web hosting partners, providing a unified approach to security integration, automation, and management.

1. Google Security Blog, "HTTPS as a ranking signal," https://security.googleblog.com/2014/08/https-as-ranking-signal_6.html
2. Online Trust Alliance (OTA), "Protecting Your Website With Always On SSL," https://otalliance.org/system/files/files/resource/documents/ota_always-on-ssl-white-paper.pdf
3. CA/Browser Forum, "About EV SSL," https://cabforum.org/about-ev-ssl/
4. Learn more about Encryption Everywhere at https://go.symantec.com/encryptioneverywhere

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.