SOLUTION BRIEF

Symantec® Secure Web Gateway

The Advantages of Dedicated Hardware

On-Premises Appliances Offer Reliability, Security, and Control

While the cloud offers numerous benefits concerning flexibility and scale, organizations with lower risk appetites, data residency requirements, or who need to demonstrate network resiliency continue to invest in on-premises and hybrid solutions to address mission-critical network security needs. When it comes to architecting world-class network solutions that depend on hardware, what is true today is the same as it has been for decades—*performance, reliability, and efficacy cannot be compromised.* You need the latest, purpose-built appliances that keep pace with the constantly evolving threat landscape. Now that nearly all malicious traffic can be easily hidden in strong SSL/TLS encryption, hardware-based security solutions must accommodate higher compute workloads yet maintain visibility into all traffic.

However, organizations that demand the unique protections and performance that hardware offers must face the inevitable truth confronting every physical device, they do not last forever. Hardware must eventually be replaced. Most vendors will only offer three years of support, enough time to cover a typical capital depreciation schedule. While refreshed appliances offer benefits of new capabilities and improvements in efficiency, they also allow vendors to lessen the costs of support and software development. This benefits the customer as the cost of supporting old devices would otherwise be passed along to the entire customer base.

Security Virtual Appliance Is the Do-it-yourself Option

Running security software on a preconfigured VM is an excellent option that offers speed, flexibility, and scale. IT and security teams can quickly add virtual appliances (VAs) in new locations or repurpose hardware as requirements change, swapping out one security component for another. Many Symantec customers take advantage of flexible Symantec® Web Protection or Symantec Network Protection licensing that allows them to quickly add VAs as a backup to their Cloud Secure Web Gateway (SWG) deployment to meet resiliency requirements. But while deploying the VAs on their own hardware can initially be an ideal option, there are costs that must be factored into the decision. First, the needed hardware does have a cost, and many organizations do not have racks of VMs waiting around and looking for work. Second, they will likely need to absorb the cost of testing, deployment operations, and maintenance of the devices. Third, they will be responsible for securing the device and any regulatory certification and testing their industry requires.

ADVANCED TESTING AND CERTIFICATION

Symantec appliances are matched, certified and tested for 100% software and hardware compatibility. They also undergo rigorous hardware tests:

- Reliability test
- Highly accelerated life test (HALT)
- Extended temperature test
- Vibration and shock test
- Functional thermal screening tests

Tests ensure appliances maintain 100% performance throughput under normal conditions and a guaranteed 100% performance in all cases. Symantec Security Platform (SSP) appliances also undergo regulatory certifications and testing. Certifications such as Common Criteria and FIPS are must-have requirements for many Symantec customers.

STRONG SECURITY

As a security vendor with decades of delivering advanced on-premises solutions, we understand the importance of ensuring that the security infrastructure itself cannot be compromised. Among many other measures, SSP appliances are hardened from physical attack through BIOS and BMC customization including:

- USB port disable (non-bootable, prevents bad actors from *hijacking* the appliance)
- Secure encryption key management
- Removal of lights-out management (LOM) functionality

SSP appliances undergo penetration testing and employ other proprietary safeguards to prevent a man-in-the-middle attack.

HARDWARE SUPPORT

Our appliances feature five years of hardware support, that is much more than the industry standard of three years. Common components are used for the ease of servicing appliance models at the customer's site. Most importantly, customers can rest assured that there is one responsible party for complete platform delivery (hardware and software) and support. Symantec appliances have integrated customer diagnostics software to troubleshoot any issues that may come up on site. These resources help maximize uptime while minimizing the resources and training a customer would need for a do-it-yourself solution.

Security Virtual Appliance Is the Do-it-yourself Option (cont.)

Every company should evaluate the benefits of VAs, especially when resources allow them to play an important role in their security architecture. However, the role they play will largely depend on an organization's use cases, the people and hardware resources they have available, and how they envision their needs to change over the next three or more years. Very often security teams will realize that a purpose-built security hardware strategy is the best choice, augmented by a mix of cloud and VAs.

SSP Hardware Is an Optimized Solution

Symantec, through acquisition, has offered purpose-built network appliances for nearly 25 years. In 2001 the Blue Coat Secure Web Gateway (ProxySG) series was introduced, and it quickly became the actual gold standard for on-premises SWGs (a position it continues to hold today). In 2020, the Symantec SSP series of hardware appliances were introduced with a new and innovative approach to on-premises security. After converting legacy network security solutions to a single operating system (Symantec SGOS), customers gained the ability to mix and match software solutions on a standard SSP appliance. This capability offers exponential value when paired with the extremely flexible Web Protection (or Network Protection) software solution, giving unprecedented scale, adaptability, and control of evolving hardware needs. It lessens one of the biggest headaches of buying a purpose-built appliance, precautionary overbuying for what may be needed several years in the future.

Just like the purchase of a smartphone or laptop, the security team expects that the newer device will be much better. SSP hardware does not disappoint. SSP appliances can run multiple network security components including Edge SWG (formerly ProxySG), Content Analysis, Malware Analysis (sandboxing), and Management Center. SSP appliances are one-of-a-kind machines, custom-manufactured with the specifications of the dedicated Symantec hardware engineering team. The team follows a cohesive and disciplined strategy in technology and roadmap planning.

Unlocking New Potential

SSP hardware can offer speed, scalability, and flexibility that can play a key role in any network architecture, whether as a standalone solution or as a mix in a cloud or hybrid environment. It can also be part of high availability or resilience planning decisions. But while the appliances come preconfigured with the latest Symantec SGOS software, a Symantec Web Protection or Network Protection license is needed to tap into its full potential. These licenses offer security teams access to any mix of on-premises, cloud, or hybrid capabilities. Priced with a per-user annual pricing, Symantec Web Protection gives customers the ability to add Edge Proxy, Content Analysis, Malware Analysis, and Management Center to their SSP hardware deployment (regardless of the number of appliances). Moreover, users get access to these capabilities with VAs too.

WHY SYMANTEC CUSTOMERS WIN

When evaluating the purpose-built SSP appliance against a VA, remember that there is no competition for CPU, memory, storage, or network port resources with third-party applications. The SSP appliance is optimized for the precise job it needs to do. But even organizations moving from an older Symantec ProxySG appliance to SSP hardware can realize the benefits of greater flexibility and speed.

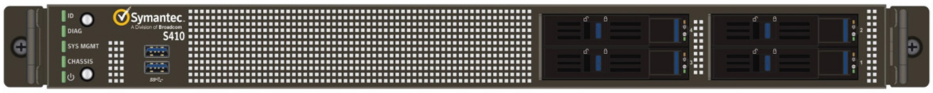
Every situation is different, but when looking at old hardware devices still in use today, consider what SSP can now offer:

- Three times better performance
- Two times more concurrent users
- More than six times rack density improvement
- Compatibility with four Symantec network security products
- Greater uptime and resilience

Unlocking New Potential (cont.)

Companies that have been on Symantec Cloud SWG (formerly called Symantec Web Security Service) or ProxySG hardware should now look to renew or buy new Symantec Web Protection licenses. SSL Inspection, Intelligence Services, Application Visibility and Control, and High-Risk Isolation are also available at no additional charge. Additionally, Symantec Network Protection includes everything in Web Protection with the addition of full remote browser isolation, Zero Trust Network Access, on-premises, customizable sandboxing, and extended report log retention. But what makes the software license truly compelling is that Cloud SWG licensing is included too. Each user can also be protected with the same SWG policies wherever they go. Together, SSP hardware and Web Protection or Network Protection allow you to choose the exact architecture that works for your needs.

SSP Hardware Provides Optimal Performance, Reliability, Scale, and Control for On-Premises SWG Needs



For more information, visit our website at: www.broadcom.com

SWG-ADH-SB100 June 7, 2024