IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Symantec's New Web Protection Suite: Providing Choice

March 01, 2021

By: Frank Dickson, Christopher Rodriguez

IDC's Quick Take

On March 1, 2021, Broadcom Software delivered its new Symantec Web Protection Suite offering. The strength of the suite approach is that it provides flexibility and choice to organizations. Security can be applied by an on-premises appliance, via an edge proxy via cloud proxy or all three in a hybrid approach that is dynamically configured based on policy. It provides choice to enterprise customers that may have had few viable alternatives in the past.

Event Highlights

On March 1, 2021, Broadcom delivered its first new security offering since the formation of its new Software Group in December 2020. The solution is a hybrid approach which delivers web security by an on-premises appliance via an edge proxy, as an IaaS-deployed virtual appliance, or via cloud proxy. It can even be all three in a hybrid approach that is dynamically configured based on and with universal policy enforcement. The flexibility of the solution allows organizations that may require on-premises, appliance-based provisioned security in some parts of the organization from either accepting the expensive and slow back-hauling of traffic for the entire organizations or implementing a multi-vendor solution that also results in a multi-policy nightmare. Additionally, a single hybrid suite approach provides flexibility for those looking to migrate to a cloud solution. Migrating 5,000 or 500,000 endpoints to a new solution-without the right tools- can be daunting. Not having options, and migrating on someone else's timeline, may be even less palatable. The solution is offered on a simple per user pricing basis, obfuscating many of the budget issues that are likely to derail security tool migrations. Regardless of where security is provisioned, the suite is offered as a single per user price. The list price is $75 per user (contract terms and volume clearly will be influencing factors).

The Symantec branded Web Protection Suite includes the following features:

- Secure Web Gateway delivered as an on-premises appliance, private cloud and SaaS
- Security Intelligence
- Browser isolation (based on the Fireglass acquisition)
- Web Content Analysis
- Centralized Management & Reporting
- Web Application Firewall (WAF)

It is important to note that the security intelligence integrates with the browser isolation solution. Let's face it, browser isolation solutions require compute overhead; isolating 100% of traffic is either expensive or taxing on the endpoint CPU. The Symantec solution isolates based on a configurable risk score, allowing security professionals to balance risk with cost/performance to achieve the desired balance.

IDC's Point of View

The age of digital transformation has resulted in sensitive data residing across on-premises and distributed environments as well as cloud applications carrying different risk levels and approaches to mitigate the risk to critical data. Compounding the complexity of protecting these assets is employee demand for ubiquitous access to corporate resources, regardless of the device they are using, their connectivity, or their location.

Traditional security solution platforms were designed decades ago to reduce the risk to traditional network perimeter architectures. This perimeter-based security was applied in silos for policy enforcement at ingress and egress points and to attempt to detect data theft and prevent accidental data loss and exposure.

These issues have been validated in many of the key findings in Data Security Survey, 2020. The survey found that, while a quarter of sensitive data still resides in on-premises datacenters, the sensitive data making up the other three quarters is spread evenly across desktops and laptops, smartphones, and public and private cloud environments. And approximately 30-35% of this data is encrypted, according to this survey of 620 IT and IT security practitioners across North America and Europe. Tracking and controlling sensitive data is a significant challenge because data owners are often remote and working with external customers, contractors, and business partners. The most sensitive data resides at the endpoint, with more than 64% of those surveyed indicating data there to be very sensitive or extremely sensitive.

Pervasive Data Defense (PDD) platforms provide perimeter-free protection over critical data assets across hybrid and multicloud environments by leveraging cloud-based platform and often delivered as SaaS. These emerging platforms represent the convergence of cloud security gateways, data loss prevention platforms, and secure web gateway functionality. And this security market convergence enables enterprise security teams to leverage a single unified policy engine, a single management console, centralized analytics, and a consolidated reporting framework.

Once converged, pervasive data defense and response solutions may collect and share rich telemetry on employees, business partners, customers, and connected systems and applications. The exchange of contextual information into how people and applications access, manipulate, and share structured and unstructured data strengthens policy-based enforcement mechanisms and provides a mechanism for unifying forensics and auditing.

Symantec, now a Division of Broadcom, offers a PPD solution that provides cloud-native security that enables consistent data and threat protection controls from devices to cloud services. Symantec tightly integrated its Elastica cloud security gateway (which came to Symantec via a Blue Coat acquisition) and its Blue Coat ProxySG secure web gateway that enables customers to centralize policies and reporting capabilities. The solution includes its DLP Cloud Service for Email (which is optional) and its CloudSOC cloud security gateway integration, which provides data discovery via API integrations to cloud services including Office 365, Box, and Dropbox and the ability to reuse existing DLP policies and workflows.

Delivering PDD as SaaS Doesn't Work for Everyone

Delivering security as SaaS can provide extremely compelling value. When IDC spoke with organizations about their experiences of using cloud enterprise security solutions (specifically iboss cloud),

interviewed adopters reported that they linked the use of cloud based SaaS security to establishing a more cost-effective security environment by optimizing their use of hardware appliances and bandwidth. Benefits included

- Improving employee productivity levels by reducing latency and delivering more bandwidth, leading to improved application performance, especially for mobile users
- Generating efficiencies for security teams by providing visibility into and actionable detail on network traffic, allowing IT teams responsible for security to react more efficiently and effectively to threats
- Lowering security-related costs by avoiding the need for hardware appliances, reducing bandwidth consumption for backhauling network traffic, and retiring less cost-effective security solutions

That being said, delivering security as SaaS does not work for everyone. Broadcom's software customers are in most major industries including banks, insurance companies, other financial services providers, government agencies, information technology service providers, telecommunication providers, transportation companies, manufacturers, technology companies, retailers, educational organizations and health care institutions. Additionally, Broadcom's focus is on large enterprises that have computing environments from multiple vendors and are highly complex. Security delivered as SaaS is simply not a possibility for 100% of endpoints for these types of customers. If your organization is result of several acquisitions which resulted in a network "duct taping" together of several solutions, a single vendor, single product solution might not work. Additionally, if your endpoint is PC in customer service applications, SaaS would likely work. What if your endpoint has extreme security requirement likely an actively deployed tank in a hostile theatre? SaaS delivered security may not be practical and/or culturally viable.

The strength of the Broadcom Web Protection Suite approach is that it provides flexibility and choice to organizations. The web security is not a vanilla, one size fits all approach. Security can be applied by an on-premises appliance, via an edge proxy via cloud proxy or all three in a hybrid approach that is dynamically configured based on policy. Simply put, it provides choice to customers that may have had few viable alternatives in the past.

Subscriptions Covered:
Data Security