IDC
Analyze the Future

EVENT FLASH

Symantec O3 Strategy Shines Through Cloud Security Market "Smog"

Phil Hochmuth
Charles J. Kolodgy
Sally Hudson
Christian A. Christiansen

IN THIS EVENT FLASH

This IDC Flash discusses Symantec's O3 Cloud Gateway — launched at the 2012 RSA Conference — the first product in the vendor's long-anticipated, and somewhat opaque, O3 cloud security initiative, which it laid out at the RSA Conference one year ago. The "cloud firewall" is targeted at securing corporate SaaS, mobile users, and public/private cloud infrastructures. The O3 gateway is essentially a Web security gateway with a broader range of capabilities for securing end-user activity and data in the cloud. The announcement is the first product launch in what is expected to be a series of subsequent launches as well as strategy and partnership announcements around Symantec's overall O3 strategy and vision.

SITUATION OVERVIEW

The O3 Gateway is essentially a Web security gateway with a broader range of capabilities for securing end-user activity and data in the cloud. The Gateway will use a range of Symantec security infrastructure platforms to deliver these services, such as PGP encryption, DLP, Web/messaging security, SIEM, and SVM and its archiving and data classification platforms. Cloud/federated identity and strong authentication are part of the solution, as well as context-based access control, where the O3 Gateway can use information on device type and physical location to make authentication decisions and determine the risk of end-user connectivity. For these components, Symantec is using its VeriSign VIP two-factor and cloud IAM capabilities, which take advantage of a larger ecosystem federated identity among Internet resources.

Potential use cases for the O3 Gateway include the ability to recognize sensitive data being copied to an external cloud service, such as a simple cloud storage app, or enterprise-focused Amazon EC2 or S3 server or storage platforms. The Symantec appliance could then apply encryption or other DLP enforcement actions on that traffic. An integrated Web single sign-on (SSO) capability provides one log-in window for enterprise end users to connect to an array of approved corporate cloud applications: enterprise-class SaaS, such as salesforce.com, Microsoft Office 365, or NetSuite, or more "consumerized" applications, such as Dropbox, Evernote, and Google Docs.

Back-end log management via its deep site technology can be used on cloud applications such as salesforce.com, allowing for archiving and retrieval capabilities for discovery and other compliance requirements. In addition to securing SaaS and cloud apps, Symantec is also positioning the O3 Gateway for cloud deployment architectures, such as private cloud and hybrid clouds, as well as public cloud infrastructures, such as Amazon EC2.

The Cloud Gateway will be offered as a virtual appliance, allowing it to be deployed on dedicated hardware in an enterprise, as a virtual instance running along other security or edge platform services, or as a cloud instance itself in Amazon's cloud. SSO and access control capabilities, as well as cloud log management and forensic capabilities, are available as of February 28. Support for DLP and encryption features on the O3 Gateway will be available in the fourth quarter of 2012. Symantec is paying careful attention to mobile requirements with the O3 Gateway as well and has created an iOS app for iPad and iPhone, which provide a single window for enterprise users to access corporate-sanctioned or managed cloud resources, via the O3 Gateway. (This app will also be available in the fourth quarter along with the DLP support.)

While the cloud gateway market is largely undefined right now, products and solutions that offer similar capabilities as Symantec's Cloud Gateway are already on the market. Secure Web gateways from vendors such as Websense, McAfee, and Cisco have sophisticated cloud security functions, such as integration with salesforce.com, or the ability to apply DLP policy to cloud applications such as social media or online collaboration and storing tools. Similarly, F5 and Citrix offer Web app delivery access management and control features on their ADCs, which perform similar functions as Symantec's O3 Cloud Gateway. You could also throw in most next-generation firewall providers into the "cloud gateway" category, as many of these vendors — from Palo Alto Networks to Check Point and WatchGuard — have sophisticated Web application control features that can be fine-tuned to provide many of the similar capabilities Symantec is offering. What differentiates Symantec from these competitors is the breadth of services — many of which are already installed widely across its user base. Competitive cloud security offerings can require some heavy lifting to integrate advanced features such as identity and encryption policy management into a Web security platform for cloud.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

Filing Information: March 2012, IDC #233469, Volume: 1

Security Products: Event Flash

One of the underlying assumptions with the O3 Gateway is that cloud providers won't do enough to protect customers in the first place. However, Symantec's go-to-market strategy with the O3 also considers the other side of the equation: the public cloud security infrastructure market. To that end, Symantec is targeting several tier 1 service provider and cloud hosting solution partners for the O3 product, with the idea that these cloud providers can resell the Cloud Gateway directly to consumers of their services. Enterprise SaaS platforms such as salesforce.com and other yet-to-be-named SaaS platforms, as well as large system integration partners (deals with those firms are net yet finalized), will be in the mix. So Symantec is thinking about it both ways: how can enterprises protect themselves in the cloud, and how can cloud providers better protect their enterprise customers.

FUTURE OUTLOOK

The introduction of solutions such as Symantec Cloud Gateway will contribute to growth of the overall public and private cloud security markets. IDC forecasts that the market for total security products sold into both public and private cloud environments will grow at a 30% CAGR from 2010 to 2015. While private cloud will account for the majority of cloud security product revenue — as much as three-quarters while spending — public cloud spending on security products will also grow, consuming as much as one-third or more of worldwide cloud security products spending by 2015.

The O3 Gateway is a good start for Symantec in defining its high-level O3 strategy with actual products. To separate O3 from the "smog" of the current cloud security market, Symantec must emphasize its deep security tie-ins to DLP, encryption, IAM, and other services, and the O3 architecture in general, from competitive Web/cloud security solutions. Major vendors from McAfee/Intel to Cisco, VMware, and RSA as well as Web security and next-generation firewall providers are all focusing on the cloud security market. A slew of start-ups, such as CloudPassage, Dome9, MetaFlows, DataLocker, and Porticor, also have offerings addressing many of the same issues as O3. Symantec's leading position in many security submarkets will help the company stand out, but Symantec is late entering a rather noisy, crowded market.

Symantec's O3 and Cloud Gateway launch helps crystallize a potential new market categorization: enterprise cloud CPE, or cloud gateways. It's likely that in the next few years, enterprises connecting to cloud services such as XaaS or public/hybrid cloud architectures without such "cloud CPE" would be similar to corporations connecting directly to the Internet 15 years ago without a firewall or running an email servers 7 years ago without spam filters — not unheard of, but certainly unwise.

