IDC TECHNOLOGY SPOTLIGHT

Sponsored by: SonicWall

Adopting cloud to improve security — particularly the software-as-a-service (SaaS) model — is a growing trend. But this adoption is not without risks and responsibilities for end-user organizations. This IDC Technology Spotlight looks at the role of SaaS security providers, particularly SonicWall and its Cloud App Security (CAS) solution.

Optimizing Cloud Security: Extend and Standardize Protection

September 2019

Written by: Chris Rodriguez, Research Manager, Cybersecurity Products, and Rob Westervelt, Research Director, Security Products

Introduction

After years of speculation, tentative adoption, confusion, and lessons learned, cloud services have gained broad mainstream acceptance. IDC's *CloudView Survey* found that across 12 tiers of business size ranging from small business to enterprise, 64% of end customers are using SaaS. This number climbs to 81% when we add in respondents that expect to implement SaaS within a year. In the survey, 42% of respondents cited "improved business agility" as the leading benefit of SaaS adoption, while 39% of respondents also noted the benefit of "reduced total size of IT budget." Notably, respondents cited "improved IT security" as the second most anticipated benefit of public cloud adoption.

AT A GLANCE

KEY STATS

- IDC survey respondents cited "improved IT security" as the second most anticipated benefit of public cloud adoption.
- 64% of businesses (of all sizes) are using SaaS. This percentage rises to 81% when we add in respondents that plan to adopt SaaS within a year.

SaaS adoption has swelled as business leaders eagerly anticipate the potential advantages of public cloud services. However, the need for security has emerged as a key lesson learned. Simple mistakes such as misconfigurations in AWS S3 buckets led to a rash of data breaches in 2018, including large multinational corporations and U.S. federal agencies.

Thus, cloud providers now offer built-in security capabilities with their cloud services. For many organizations, built-in security may prove adequate. However, SaaS providers cannot ensure against all forms of threats, leaving businesses to identify and fill the gaps — a task that is massively complicated for organizations relying on multiple SaaS platforms, each with varying degrees of protection and different policy engines and interfaces. While cloud providers have made great strides to secure their services, customers are increasingly recognizing the need to take a role in securing their cloud environments.

SaaS Offers Potential Business Benefits

The benefits of cloud are numerous and well documented, including business agility and lower costs. The outsourcing of IT responsibilities is a significant aspect of the business value for the SaaS model — businesses need not worry about patching or updating SaaS applications. However, IDC notes the negative implication of the cloud model: This outsourcing fundamentally represents a loss of centralized IT organizational control over data and user activities compared with traditional computing models.

The security industry has responded by introducing solutions that return a level of control to the IT security organization. For example, a cloud access security broker (CASB) enables IT organizations to gain visibility into the cloud applications that their users and data are accessing. CASB solutions can be used to control the applications that users access as well as how they use the applications and what data they access, upload, modify, or share. Based on these capabilities, CASB has become an increasingly important component of an enterprise data protection strategy.

The adoption of better security controls and tools is essential to reduce barriers to cloud adoption. IDC notes that "security, once a significant inhibitor of cloud adoption, has become a key driver." In IDC's *CloudView Survey*, respondents indicated that "improved IT security" was the single most anticipated benefit of public cloud adoption, second only to "improved business agility."

SaaS Risk Trends Span Email and More

As cloud adoption has increased, cybercriminals have noticed. New categories of risk have emerged that are unique to cloud environments. For SaaS, the reuse of credentials is a major security challenge, as attackers test combinations of stolen credentials from previous and unrelated data breaches to gain access to accounts. Account takeover is especially pernicious as attackers can instantly gain access to sensitive data based on the permissions and privileges associated with the account. A single compromised account can grant attackers access to email, SharePoint, and OneDrive files. These breaches can be difficult to detect as actions from the compromised account appear legitimate.

Yet, IT organizations continue to face familiar threat vectors as well. The move to SaaS email is accompanied by the familiar set of threats, including spam, phishing, malware, social engineering, and fraud. For example, business email compromise (BEC) remains a common and costly email-borne threat. The FBI Internet Crime Complaint Center (IC3) reported that BEC attacks accounted for $1.3 billion in losses in 2018 (https://pdf.ic3.gov/2018_IC3Report.pdf), or an average of $63,000 in losses per incident.

SaaS Introduces New Complexity Challenges

The cloud model introduces unique requirements that complicate the security architecture and force organizations to adapt their security practices. Consider the following germane example: Email security gateways are giving way to cloud-based email security solutions that are better suited to the anywhere, anytime, any device nature of SaaS solutions. Traditional on-premises and message transfer agent (MTA)–based approaches present limitations in terms of the type of messages that can be secured or trade-offs in the ability to leverage native built-in protections or purpose-built third-party security technologies. Following a traditional on-premises approach would require IT organizations to route traffic back to their datacenters, thereby adding latency to the connection. This approach also bypasses any built-in protections included with the email service and would leave IT organizations blind to threats transferred by internal messaging.

As SaaS email is increasingly bundled with other productivity applications, security solutions that offer only email security are proving to be too narrow in scope to offer comprehensive protection. Traditionally, email security solutions are designed to address email threats only. However, the Microsoft Office 365 suite of SaaS applications consists of more than email, including productivity, sharing, and collaboration applications. This evolution of email requires an equal evolutionary "leap" in email security solutions that are capable of addressing broader SaaS security requirements.

Growing Risk Drives Security Awareness and Best Practices

Under the shared responsibility model, cloud service providers acknowledge the need to secure their platforms. For example, while Microsoft has worked to secure its Office 365 platform, the cloud service has become a rich target for attackers. Attacks such as baseStriker, ZeroFont, Z-WASP, and PhishPoint demonstrate that attackers are actively probing ways to bypass Office 365 built-in protections. Though Microsoft is working to add enterprise security natively into its Office 365 platform, the most advanced protections require customers to upgrade to the Microsoft 365 E5 license, with an additional fee per user per month.

But cloud service providers are actively reminding their customers that they remain responsible for security of their own data and usage. The security requirements for each platform will vary, but IDC stresses the importance of understanding risk and responsibilities associated with SaaS use. Compared with infrastructure as a service (IaaS) or platform as a service (PaaS), SaaS leaves customers with the least amount of security responsibilities. However, customers that overlook these responsibilities are exposing their organizations to massive risks, as evidenced by the numerous misconfigurations of S3 buckets that led to massive data breaches in 2018 and 2019.

Compared with IaaS or PaaS, SaaS leaves customers with the least amount of security responsibilities. However, customers that overlook these responsibilities are exposing their organizations to massive risks.

Considering SonicWall Cloud App Security

The SonicWall Cloud App Security (CAS) solution offers protection for SaaS applications, including email services and other popular office productivity applications. The SonicWall CAS solution is designed for a multicloud world, leveraging an API-based architecture to deliver a much-needed layer of protection for organizations moving to the cloud, whether partially or completely, or using multiple SaaS services. The SonicWall solution supports popular enterprise SaaS email, collaboration, and productivity applications, including Microsoft's Office 365 Email, SharePoint, and OneDrive as well as Google's G Suite. The SonicWall CAS suite of protection capabilities includes email security as well as DLP, CASB capabilities, and other advanced capabilities.

Protection Suite for SaaS Email and More

The SonicWall CAS solution delivers enterprise protections for SaaS email, including antiphishing and URL scanning, DLP, and sandbox-based analysis for detection of advanced threats in malicious attachments. Additional advanced capabilities include protection against BEC and fraud attempts, using advanced analytics and over 300 threat indicators. SonicWall CAS leverages machine learning and AI capabilities to block impersonation attacks.

Beyond email, SonicWall CAS offers account takeover protection to safeguard many popular SaaS platforms. The solution uses machine learning to profile user behavior, including retroactive scanning of activities. In the case of stolen credentials, user profiling and behavior analytics technologies are necessary to determine if an account is being accessed and abused by cybercriminals.

For SaaS applications such as OneDrive and other file sharing applications, the SonicWall CAS solution applies sandboxing and real-time antivirus scanning to detect threats. The solution can scan files and data that are already in the cloud, or that move from one cloud service to another. Additionally, the solution offers DLP for data at rest, as well as analysis of

configurations and permissions, along with policy templates. The solution helps prevent sensitive data exposure by limiting access to only sanctioned applications and by preventing unauthorized uploads of sensitive data to the cloud.

Cloud-Native Design and Advantages

SonicWall CAS features an API-based architecture that offers numerous advantages over traditional appliance-based or MTA-based email security solutions. For example, the solution does not "hold" mail or add latency. By using APIs, the solution avoids the latency associated with proxy-based approaches. The solution does not represent a potential point of failure and can fail open if needed.

The solution offers significant value for IT organizations that are weighing the benefits of built-in protections of their SaaS platform. SonicWall CAS integrates at the API layer, which allows the solution to work "behind" and out of band of the cloud service rather than "in front" and inline. A major advantage to this approach is the ability to leverage purpose-built capabilities provided in the SonicWall solution as an additional layer of advanced protection in addition to the SaaS-included protections. For example, SonicWall customers can leverage base Microsoft antispam and antivirus capabilities in Office 365 while leveraging the specialized capabilities in SonicWall CAS to stop BEC and account takeover attacks. Essentially, SonicWall CAS works as the advanced protection layer, complementing and extending the built-in protections in Office 365 and other SaaS platforms to block attacks that might otherwise be missed.

The API-based design offers a variety of additional benefits, such as the ability to detect threats in internal messaging. By comparison, email security solutions that rely on appliances can detect messages only as they move "north/south," or inbound or outbound. Similarly, the API-based design allows SonicWall CAS to protect data in SaaS applications in real time, whether moving in or out of a SaaS environment, internally, or cloud to cloud. The API design also allows retroactive scanning of data and files at rest, already in the cloud, as well as retroactive analysis of older messages in the case of SaaS email. This includes the ability to recall delivered messages from inboxes, when needed.

Addresses Cloud Security Standardization and Consistency

In the modern multicloud environment, IT organizations are challenged to standardize policies. Each cloud application provider offers a set of built-in policy controls. However, these controls and their capabilities, as well as how to use them, vary from one cloud service to another. This variation introduces a high potential risk of inconsistent policy or misconfigurations that may lead to sensitive data exposure. Cloud App Security acts as a manager of managers, allowing customers to map and extend upon the built-in controls to achieve consistent protection.

Notably, Cloud App Security is a part of the SonicWall Capture Cloud Platform, which offers a common policy management engine, allowing enterprises to standardize security policies across multiple cloud environments. Customers benefit from a single portal and a unified consistent view of threats, security tools, policies, and defenses.

Challenges

Specialized email security vendors surround their security solutions with complementary offerings that SonicWall does not offer at this time, such as security awareness training for end users. Additionally, as threat actors develop more sophisticated tactics and techniques, technologies such as expert systems for message content and writing style analysis to detect impersonation attacks will be more important for SonicWall to develop going forward. Ultimately, SonicWall continues to add new features to Cloud App Security, with plans to add new capabilities to bring the solution to parity with those of more established competitors.

Conclusion

SaaS is gaining recognition as a critical resource for businesses of all sizes, and threat actors have started to take notice. Popular SaaS providers have already made great strides to secure their platforms. Next, the evolution and cross-pollination of email security and cloud security solutions may help customers confidently embrace public cloud services. Ultimately, IDC believes the adoption of SaaS, including email and other productivity applications, will only continue to increase. However, the ability to secure SaaS applications will determine how painful the journey to the cloud will be.

About the Analysts

Chris Rodriguez, *Research Manager, Cybersecurity Products*

Chris Rodriguez is a Research Manager in IDC's Cybersecurity Products research group focused on the products designed to secure today's complex enterprise networks. IDC's cybersecurity research offerings to which Chris contributes include Endpoint Security; Network Security Products and Strategies; Security Analytics, Intelligence, Response, and Orchestration (Security AIRO); and Identity and Access Management research programs.

Rob Westervelt, *Research Director, Security Products*

Robert Westervelt is a Research Director within IDC's Security Products group. He provides insight and thought leadership in the areas of cloud security, mobile security, and security related to the Internet of Things (IoT). Rob is also responsible for research and analysis around a wide range of evolving security markets, including endpoint security, security and vulnerability management (SVM), and identity and access management (IAM).

MESSAGE FROM THE SPONSOR

SonicWall Capture Cloud Platform

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. The SonicWall Capture Cloud Platform tightly integrates security, management, analytics and real-time threat intelligence across the company's portfolio of network, email, mobile and cloud security products. This approach enables our complete portfolio of high-performance hardware, virtual appliances and clients to harness the power, agility and scalability of the cloud. Core to the platform, SonicWall Cloud App Security delivers easy-to-use SaaS security for Office 365, G Suite, email, messaging, file-sharing services and a range of popular SaaS applications. For more information about SonicWall Cloud App Security, please visit ***www.sonicwall.com/CAS***.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com