Securing Office 365 with Symantec

February, 2016

Solution Overview: Enterprise Security

Adoption of Microsoft Office 365, Google Apps, and other cloud-based productivity solutions is growing. Microsoft in its Ignite 2015 session claimed that 35% of the Microsoft Exchange installed base is now on Office 365. Gartner also predicts that by 2018, cloud office systems will achieve a total market penetration of 60%.

How can you embrace the benefits of cloud-based email and productivity solutions without compromising security or adding risk?

Smart, comprehensive email security—whether your email system is on-premise, cloud-based, or both—begins with a clear, realistic understanding of what you're up against. Email is still the most popular and pervasive tool cybercriminals use to launch and distribute threats. According to the Symantec Internet Security Threat Report (ISTR), one out of every 244 emails in 2014 contained a malware attack and five out of six large enterprises were targeted by spear phishing campaigns.

- **Polymorphic Attacks:** Cybercriminals are using increasingly sophisticated methods to disguise malicious URL links embedded in email messages. This includes randomly redirecting links to a sequence of different destinations around the world and adding programmed time delays.
- **Advanced Targeted Attacks:** Organizations are increasingly facing highly sophisticated and stealthy persistent attacks that are difficult to detect and stop using standard signature-based antimalware tools. Targeted attacks more than doubled between 2012 and 2014 and were often introduced through email systems.
- **Data Loss and Compliance:** Data loss through email is another serious issue, so you need to proactively enforce security and compliance policies and protect employees when they share sensitive information and attachments over email. And of course, you have to determine how much of your email content you need to encrypt—and then have a reliable solution in place for monitoring and managing those encryption policies.
- **Contextual Access Control:** Finally, you need strong authentication and access control solutions that work across all on-premise and cloud applications such as Office 365, Salesforce, Box, DropBox etc. Authentication and access control need to be both user-friendly and highly secure so the right users can get the right level of access to their applications and content anytime, anywhere and from any device.

Microsoft, Google, and other cloud vendors are quick to point out that their cloud-based email offerings include free antimalware and Data Loss Prevention (DLP). However, when you look at today's evolving threat landscape —and how it applies specifically to email—it quickly becomes apparent that the security capabilities included with Microsoft Office 365, Google Apps, and other cloud-based email and productivity solutions simply aren't fully up to the task of keeping your organization safe.

Achieving a New Level of Security with Symantec

Fortunately, you're not limited to these baseline security capabilities when you make the move to cloud-based productivity and email solutions. Symantec offers comprehensive security solutions for Office 365 that seamlessly integrate with, complement, and enhance the built-in security that's included with cloud-based email and productivity solutions like Office 365, Google Apps, and others.

Symantec

Here's how Symantec extends the "baseline" security capabilities of Microsoft Office 365:

1. Shield Office 365 Email From Spam, Advanced Malware And Phishing Attacks

Keep advanced malware, spam, and malicious links out of your mailboxes with Symantec Email Security.cloud service

Office 365 includes signature-based anti-malware and spam protection capabilities. Additional services/add-ons are required for handling more advanced threats such as zero-day attacks. The built-in security features of Office 365 are not as effective against today's sophisticated attacks. For example, the "click-time" phishing link protection in Office 365 is limited to "blacklists" of known bad URLs, which cybercriminals often avoid by using shortened links that get redirected many times before reaching final destination.

Symantec™ Email Security.cloud extends Office 365 with:

- **Intelligent real-time link following** — that traces full or shortened redirect links all the way back to their final destinations, analyzes the content in real-time, and prevents emails with bogus links from ever showing up in your users' inboxes.
- **Advanced heuristic technology**— **Skeptic™**— that interprets and analyzes more than 8.4 billion email messages and 1.7 billion web requests collected daily by Symantec's Global Intelligence Network to detect and block new forms of malware. This lets us catch and stop zero-day attacks and sophisticated threats that traditional anti-malware solutions typically miss.
- **Industry-leading SLAs with guaranteed results** — credit back or other remedies are provided if performance targets are not met: 100% protection against known and unknown email viruses, no more than .0001% false positives, 99% spam capture, 100% email delivery and service uptime etc.

2. Protect Against Advanced Threats And Targeted Attacks

Uncover, prioritize and remediate advanced email-based threats rapidly with Symantec Advanced Threat Protection (ATP)

Built-in security offered with Office 365 or other collaboration services are largely ineffective against advanced targeted attacks that organizations face today. They lack the ability to correlate events across email, endpoints and network to detect attacks that are highly stealthy and persistent. They also lack the capabilities to quickly "drill into" the details of an attack and see how all events are related, and search for any attack artifacts across control points. This inhibits the ability to "connect the dots" and get visibility into suspicious activity in their environment. Further, prioritizing events, quickly containing and remediating these attacks across your entire organization is not possible.

Symantec ATP extends Office 365 with:

- **Automated and improved detection** — **Cynic™** — an entirely new cloud-based sandboxing and payload detonation service that can execute suspicious files in both virtual and "bare metal" environments to uncover even those "virtual machine-aware" attacks[1] that would evade detection by traditional "virtual-only" sandboxing technologies offered natively by Office 365. Cynic leverages advanced machine learning-based analysis and combines local customer context with Symantec's global intelligence to detect sophisticated attacks. Further, our ATP customers benefit from the ongoing investigations of new and unknown malware by our global team of threat researchers, who detect and alert customers about targeted attacks by comparing malicious activities across industries and geographical regions.
- **Critical events prioritization** — **Synapse™** — our new cross-control point (email, endpoint, network) correlation engine that prioritizes the most important security events across the organization, allowing SOC analysts to "zero in" on just those events of greatest risk to the organization**.** A single console showing all suspicious events across the organization allows you

1. Symantec ISTR: 28% of today's advanced attacks are "virtual machine-aware"

to quickly "drill into" details of an attack, lets you see how all events are related and search for attack artifacts across control points.

- **Fast remediation** — Symantec ATP provides one-click containment and remediation across control points. For example, with a single click, the analyst can: "Remove BAD.EXE from all endpoints, block incoming e-mails containing BAD.EXE, and prevent BAD.EXE from entering via web downloads". Or, they can go one step further and totally isolate the compromised machine from the organization's production network. Symantec ATP also provides unique visualization of related Indicators-of-Compromise (IoCs) of an attack, with a graphical view of how all IoCs are connected to each other.

3. Safeguard your Sensitive Information in Office 365 Exchange

Prevent sensitive information from leaving your organization with DLP Cloud Service for Email

Microsoft's built-in data loss prevention and encryption capabilities within Office 365 are rudimentary and basic. They don't meet the advanced compliance and complex intellectual property use cases and requirements of enterprises. Office 365's limited content detection methods (simple regex, some document fingerprinting and basic watermarking) lead to a high number of false positives, increasing the burden on IT. With Office 365, incident remediation and workflow options are limited to basic notification and blocking, which makes it difficult for enterprises to respond effectively to data loss incidents. Additionally, most organizations have a heterogeneous, hybrid IT environment with multiple cloud applications deployed along with on-premises applications. Office 365 lacks a unified set of Data Loss Prevention controls and a management interface outside of the Microsoft ecosystem. Symantec DLP (nine time Gartner MQ leader) simplifies policy management, reporting, and incident remediation by providing a single management console with the most advanced detection technologies across different cloud ecosystems and on-premises applications.

Symantec extends Office 365 with:

- **Enterprise-strength data protection** — **Symantec™ DLP Cloud Service for Email** — a new cloud-based service built on Symantec's market-leading data loss prevention technology offering the broadest content detection capabilities including described content matching (keywords, expressions), data fingerprinting (structured data and unstructured documents), and machine learning (for content such as source code and forms). These advanced detection technologies are coupled with support for over 360 different file types. It offers sophisticated policy management, reporting, and incident remediation workflows.

  Customers who wish to manage their own DLP installation may still use Symantec DLP Cloud Prevent for Office 365.

- **Single console and unified set of DLP controls for all cloud services and on-premises environments** — Unlike Microsoft's multiple management interfaces and disjoint controls, Symantec's solution provides robust and unified security controls for heterogeneous environments and hybrid deployment models. This allows you to extend your security infrastructure and policies to Exchange Online and a range of non-Microsoft applications & mobile devices environments. The Symantec Enforce management platform provides a unified, easy-to-use management console across all DLP channels, including Office 365 Exchange, and other cloud apps and on-premises deployments.
- **Seamless policy-based encryption** — that uses a policy based approach to encrypt emails based on message attributes or message content in a manner that is totally transparent to the sender. Unlike that of Office 365, Symantec's encryption solution does not require encrypted message recipients register or use a Microsoft account, or use one-time passcodes to access encrypted messages. Symantec Policy Based Encryption also works with all types of mobile devices and does not require apps like the Office Message Encryption (OME) Viewer to access encrypted messages.

4. Control Access With Strong Authentication

Ensure the right people, and only the right people, have access to your Office 365 deployment with our Symantec VIP

Identity protection is the lock on the cloud's front door. It keeps attackers out and ensures that workers have access to the cloud apps they need. Done properly, it also improves the user experience by enabling a transparent login process. With Office 365, the authentication is limited to options such as out-of-band (text and voice) and mobile notifications, which means safer, or more convenient options such as biometrics, risk-based and hardware credentials are not available. Office 365 provides Single Sign-On and authentication for only Office 365 applications. It only supports Active Directory (AD) and Microsoft Identities. This is not enough for customers who see authentication and access controls as part of their strategic security policy instead of specific to individual applications.

Symantec extends Office 365 with:

- **Increased security without reducing user convenience — Symantec™ VIP (Validation and ID Protection Service)** — a cloud-based service offers robust multi-factor authentication that meets diverse needs and supports hardware tokens, one-time password (OTP), out-of-band (OOB), mobile Push, Apple Watch Push, passwordless fingerprint authentication (TouchID) and more. Furthermore, Symantec for Office 365 offers robust risk-based authentication that is not limited to just geo-location. It also leverages data from Symantec's Global Intelligence Network and uses a purpose built login anomaly engine to more accurately detect suspicious behavior.
- **Better and streamlined audit & access control for Office 365 and other cloud services — Symantec™ VIP Access Manager** — a cloud-based service that offers Single Sign-On and user management capabilities for Office 365 and other cloud applications thus improving control, convenience and compliance for end users and administrators. It comes configured with the most common enterprise applications including Office 365 and supports a variety of identity services including Microsoft Active Directory, LDAP, Oracle and more. Easily accessed by a diverse array of mobile devices including smartphones and tablets – giving users access to applications they need to be productive anywhere, anytime, with any device.

Transition to the Cloud with Confidence

As your business explores the advantages of moving to a new generation of cloud-based email and productivity solutions, Symantec is ready to help you make that transition confidently and without making any security compromises. With Symantec Office 365 security solutions, you can tap into all of the advanced security technology, global resources, and proven expertise you need to keep your organization safe from today's most advanced and sophisticated email threats—and stay a step ahead as those threats continue to evolve.

Competitive Analysis of Office 365 Protection

The following table provides a comparison of select security providers including Microsoft Office 365 security, to help you gain a deeper understanding of the various offerings.

SOLUTION AREA		SECURITY PROVIDERS			
		Symantec (ATP, Email Security.cloud, DLP*, VIP)	Microsoft (E5)	Proofpoint (Enterprise)	Cisco (CES)
Advanced Threat Protection	Detects, prioritizes, and remediates advanced threats	Across endpoints, email, and network control points	Email only	Email only	Email Only
	Targeted attack identification by security researchers	✔	✖	✖	✖
	Virtual and physical cloud-based sandboxing	✔	Virtual only	Virtual only	✔
Email Security	URL protection with real-time link following	✔	✖	✖	✖
	Threat detection via heuristics	✔	✖	✔	✔
Data Loss Prevention	Email & cloud app DLP monitoring	✔	Limited to O365	✖	✖*
	Comprehensive content detection with machine learning technology	✔	✖	✖	✖
User Authentication	Robust MFA: mobile, biometircs, risk-based	✔	Limited 2FA	✖	✖
	Extensive cloud apps support	✔	Requires Azure AD Premium	✖	✖
	SSO for SaaS applications	Unlimited	10 apps/user	✖	✖

*Symantec is an 9-time Leader in the Gartner Magic Quadrant for DLP
*Cisco uses RSA DLP (End of Life, March 2015)

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist

US: Call toll-free 1 (800) 745 6054 | Outside the US: For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

350 Ellis St. Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

21363340 02/16