WHITE PAPER:
FINDING EMAIL SECURITY IN THE CLOUD

Finding Email Security in the Cloud

Symantec™

CONTENTS

Introduction

How can you embrace the benefits of cloud-based email and productivity solutions without compromising security or adding risk? Microsoft Office 365, Google Apps, and other cloud-based productivity solutions are clearly transforming the way IT departments deliver apps and services to their users, and adoption of these solutions is continuing to grow. Microsoft CEO Satya Nadella stated there are "nearly 50 million Office 365 monthly active users,"[1] and a Microsoft Ignite 2015 session claimed 35% of the Microsoft Exchange installed base is now on Office 365.[2] Gartner also predicts that by 2018, cloud office systems will achieve a total market penetration of 60%.[3] This rapid and fairly dramatic move to cloud-based productivity solutions makes sense. These hosted offerings provide users with new flexibility and more efficient ways to collaborate, and they offer businesses and IT departments significant cost savings and lower administrative overhead compared to traditional on-premise applications.

But what about security? Exactly how much protection do these next-generation cloud-based email and productivity solutions provide? Microsoft, Google, and other cloud vendors are quick to point out that their cloud-based email offerings include free anti-malware and DLP protection. But how complete and effective are these built-in capabilities? And what else should you consider from a security standpoint as you contemplate the transition to cloud-based solutions like Microsoft Office 365?

Organizations obviously need solid answers to these questions before they can fully embrace cloud-based email and productivity apps. And finding those answers means clearly understanding what today's biggest email security threats are, accurately assessing how much protection today's cloud-based email and productivity solutions can realistically provide, and knowing when and where to turn for additional security capabilities that can enhance and protect cloud-based mailbox solutions.

The average total cost of a data breach is $3.8 million*

Consider the Costs

What kind of impact can malicious emails have on your organization? The costs go far beyond isolation and cleanup:

- IP theft
- Regulatory fines
- Litigation costs
- Lost revenue
- Damaged reputation

**Source: Ponemon Institute; 2015 Cost of a Data Breach Study*

Why "Good Enough" Security is Never Good Enough

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 2015 Symantec Internet Security Threat Report (ISTR), one out of every 244 emails in 2014 contains a malware attack and five out of six large enterprises were targeted by spear phishing campaigns.

This high volume of email threats is certainly nothing new, but the nature of these attacks has also changed dramatically. The number of targeted attacks more than doubled between 2012 and 2014, according to the ISTR, and many of those attacks were introduced through email systems. These advanced targeted and zero-day threats are much more difficult to detect and stop than traditional malware, and standard signature-based anti-malware tools have proven to be largely ineffective against them.

In addition to these elusive and dangerous targeted 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. These new techniques are highly effective at disguising malicious links and fooling traditional link scanning tools.

Finally, it's important to remember that targeted attacks, malicious link redirects, and other malware-related threats aren't the only email security dangers you have to worry about. Data loss through email is another serious issue, so you need to proactively enforce your 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.

[1]Bort, Julie. Here's more proof that companies are jumping on Microsoft Office 365 like crazy. Business Insider. April 24, 2015.
[2]BRK2180 Extending Microsoft Office 365 Visibility, Security and Compliance: Office 365 Management APIs. Microsoft Ignite 2015. May 6, 2015.
[3]New Developments in the Cloud Office System Market. Gartner. 2013.

Mind your security gaps

When you look at today's broad security landscape—and how it applies specifically to email—it quickly becomes apparent that the "baseline" 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.

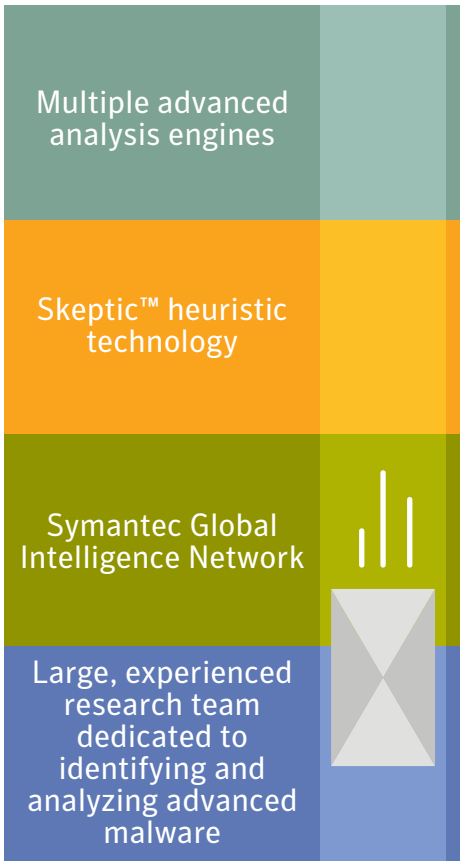
For example, Microsoft Office 365 only includes basic, signature-based anti-malware capabilities, which can't detect or block most of today's sophisticated targeted and zero-day attacks without adding their advanced threat protection solution at additional cost. The phishing link protection in Office 365 is limited to a list of known bad domains, so it doesn't offer much protection against the sophisticated redirect and time delay techniques cybercriminals use to disguise malicious links. And the built-in data loss prevention and encryption capabilities in Office 365 only offer limited policy management capabilities.

Fortunately, you're not limited to these baseline security capabilities when you make the move to cloud-based productivity and email solutions. Symantec offers a security solution—Symantec™ Email Security.cloud—that integrates with, complements, and enhances the built-in security that's included with cloud-based email and productivity solutions like Office 365, Google Apps, and others.

Symantec Email Security.cloud: Comprehensive Security for Cloud-based Email

Symantec Email Security.cloud starts with the same multi-layered approach to blocking malware and elusive targeted attacks that has made Symantec the industry leader in security. This includes multiple analysis engines that are continually updated to scan emails and accurately detect and eliminate known spam and malware threats. This is similar to the anti-malware and anti-spam capabilities you get with Office 365 and other cloud-based productivity tools, but with Symantec, it's just the beginning.

The Symantec Email Security.cloud Difference



Intelligent, real-time protection against targeted threats and zero-day attacks

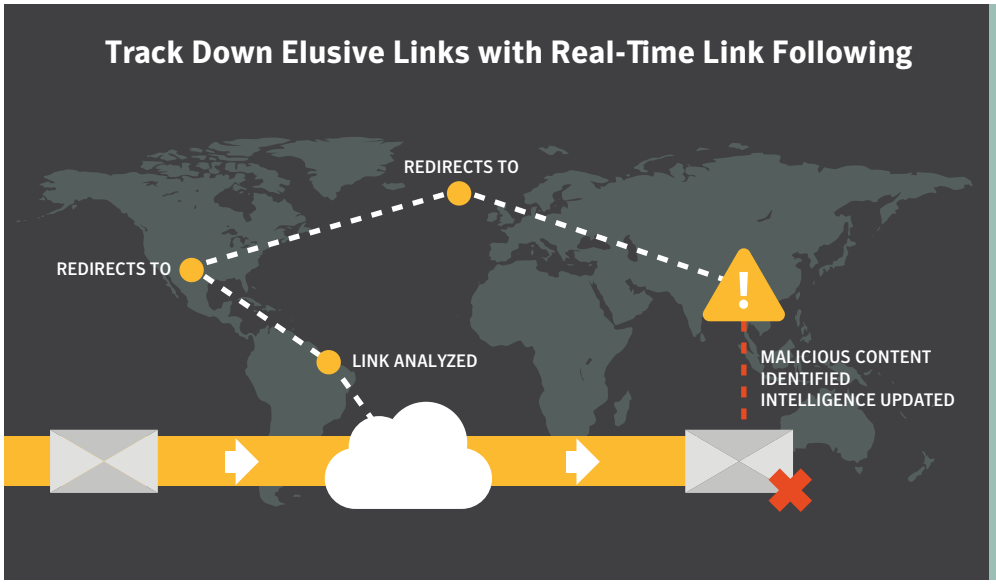
In addition to the industry's most proven and trusted signature-based protection, Email Security.cloud leverages Symantec's advanced heuristic technology—called Skeptic™—to guard against new and advanced targeted attacks. Unlike the anti-malware protection that's included with Office 365 and other cloud-based email solutions, Skeptic interprets and analyzes more than 8.4 billion email messages and 1.7 billion web requests that are collected by Symantec's global intelligence network every day to detect and block new forms of malware. This makes it possible to catch and help stop zero-day attacks and targeted threats that traditional anti-malware solutions typically miss. It also creates an intelligent, adaptable layer of protection that can stop malware as it evolves and changes.

In the very unlikely event that any malware manages to slip through all of these advanced protection technologies, a team of experienced security analysts is always working tirelessly behind-the-scenes to analyze and identify potential new threats and dangers. If they catch something, you'll be notified immediately and provided with fast, effective remediation steps.

Other vendors claim to leverage this kind of global security intelligence. But when you look at the numbers, it's obvious that no other email security company can match the size and scope of Symantec's Global Intelligence Network—which constantly collects massive amounts of data from more than 41.5 million attack sensors around the world and analyzes it using a global team of live security researchers and analysts.

Superior protection against malicious email links

Symantec Email Security.cloud offers equally advanced protection against malicious email links. The link scanning capabilities in Office 365 and other cloud-based email offerings are limited to "blacklists" of known bad URLs, which cybercriminals often avoid by using shortened links that get redirected multiple times before reaching their final destinations. Symantec Email Security.cloud overcomes these advanced evasion tactics 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.



Real-Time LInk Following Gets Big-Time Results

Last year, attackers launched an extensive campaign that consisted of 39 different attacks over a six-week period. These attacks targeted a wide range of different industries, including education, finance, and government, and they all featured emails that contained malicious URL links with multiple redirects. With its advanced Real-Time Link Following capabilities, Symantec Email Security.cloud followed the link redirects back to their sources, identified them as malicious, and proactively blocked the emails—all in real-time.

DLP and Encryption with policy-based controls

Symantec Email Security.cloud goes far beyond the basic signature-based security capabilities in Office 365 to keep your organization safe from targeted malware, zero-day attacks, and elusive email links. But it also enhances your ability to prevent private or sensitive data from leaving your network through email messages or attachments—whether you're working to protect your own intellectual property, comply with government regulations, or both.

Powerpoint with a Vengeance

When a major broadcasting corporation produced a news story on a controversial topic, activist hackers expressed their displeasure by launching a spear phishing attack that featured executable malware embedded inside a PowerPoint email attachment. Fortunately, the advanced heuristic security capabilities in Symantec Email Security.cloud—working together with a team of live analysts—proactively detected the threat and prevented emails with the malicious file from ever reaching their intended recipients.

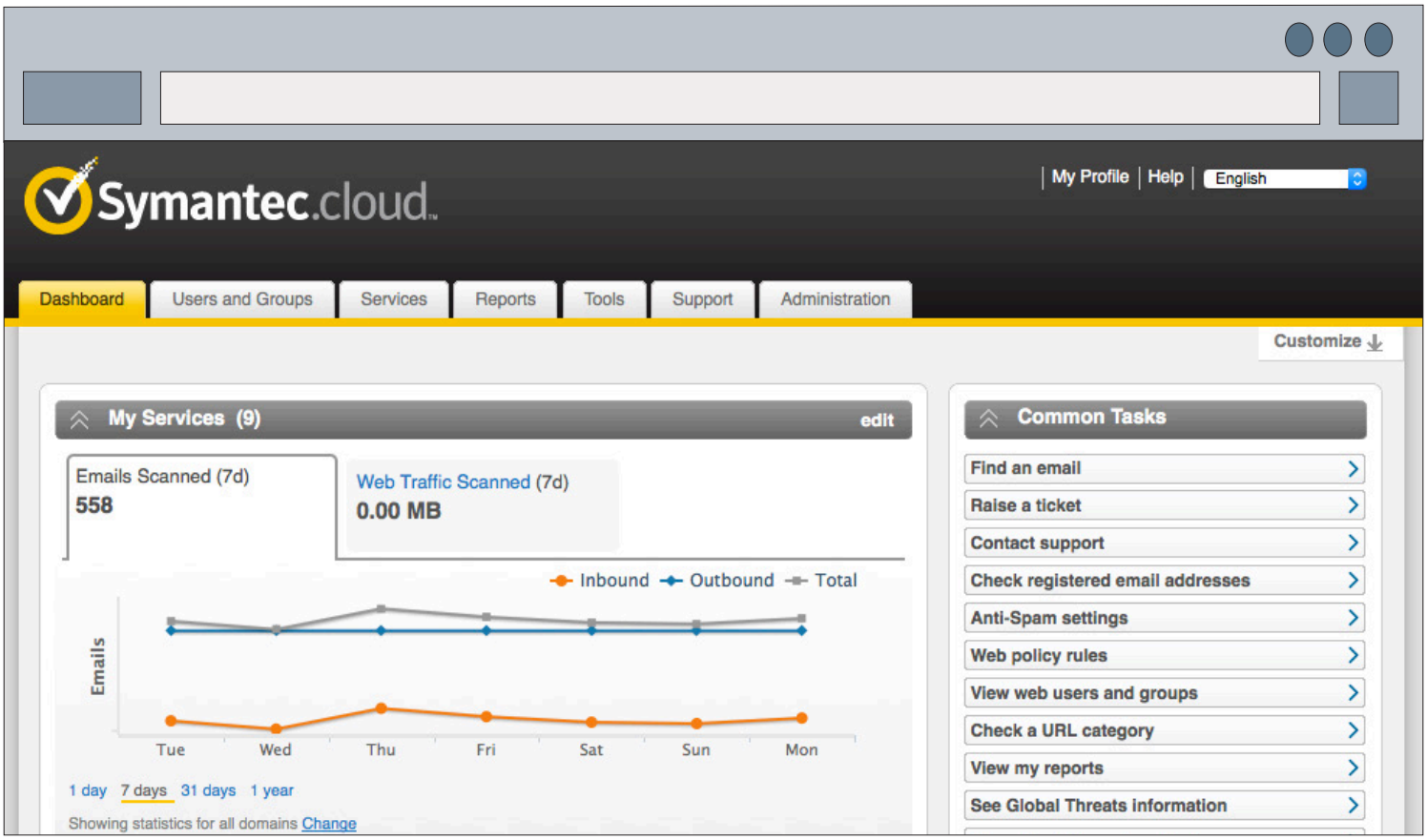
With Symantec Email Security.cloud Data Protection, you can define and enforce granular policies for controlling email-related data loss. This includes leveraging proven libraries and templates based on Symantec's market-leading data loss prevention technology. These flexible policies give you total, customizable control over what types of content and attachments users can email to people outside your organization.

Then, you can use this same policy-based approach to define which emails should be encrypted—based on message attributes or message content—and trigger an automatic, seamless encryption process that is totally transparent to the sender.

Office 365 also includes basic email encryption, but it's linked to the email recipient's password, which means your intellectual property may only be as secure as a contractor's weak password. Finally, it's important to note that Microsoft has no contingency plan if an attacker steals an Office 365 user's login credentials to compromise an account, which actually opens up a totally new attack vector. The Symantec Email Security.cloud approach to encryption eliminates both of these potentially serious weaknesses.

Bringing all the pieces together with a unified management portal

Symantec Email Security.cloud provides all of the advanced security, data loss prevention, and encryption capabilities you need to embrace new cloud-based email and productivity solutions without compromising security. But Symantec is also working to make sure these pieces work seamlessly together and support other aspects of your cloud security infrastructure. This starts with a unified portal for managing all of your Symantec Email Security.cloud services and capabilities from one location, including security, data protection, and encryption settings and policies. Then, you can extend this same intuitive interface to Symantec Web Security.cloud or Symantec Advanced Threat Protection: Email. This gives you a single, convenient way to configure, manage, and report across all of your communication vehicles, which saves time and gives you a more comprehensive view of your overall security posture.



No Patch, No Problem

To exploit a new zero-day software vulnerability before it could be patched, a group of attackers emailed a bogus Word document that contained an embedded malformed TIFF image designed to trigger remote and local code execution. To make this threat even more elusive, the attackers targeted a relatively small number of recipients and sent emails with different subject lines and attachment filenames. Symantec Email Security.cloud—again supported by a team of analysts—proactively identified all of the malicious emails and blocked them before they appeared in their intended targets' inboxes.

Industry-leading SLAs with guaranteed results

It's easy to talk about the advanced security capabilities in Symantec Email Security.cloud. But Symantec also backs these claims with one of the industry's most stringent and aggressive service level agreements (SLAs). Symantec Email Security.cloud is delivered through highly available, top-tier data centers located around the globe. These data centers are highly available, fully redundant, and designed to leave ample headroom for spikes in traffic or unexpected failure conditions. This makes it possible to offer SLAs that include certain money back remedies if world-class performance levels are not met.

Complete protection through every step of your transition to the cloud

For most organizations, the transition from on-premise to cloud-based email is a gradual one. That's why Symantec Email Security.cloud is built to protect all of the email solutions currently running in your environment, including Microsoft Office 365, Google Apps, other hosted mailboxes, and traditional on-premise email systems like Microsoft Exchange. With Symantec, you can wrap a cohesive, unified, and comprehensive layer of protection around all of these different systems, so nothing slips through the cracks as your email environment changes and evolves.

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 Email Security.cloud, 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.

Learn more about Symantec Email Security.cloud

Visit our website
www.symantec.com/email

To speak with a Product Specialist in the U.S.
Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data-intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

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

21344128 06/15