SOLUTION BRIEF

Security Considerations for Microsoft Office 365 Email

Symantec™

Gain the Benefits. Lose the Risks.

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

Microsoft Office 365 adoption is growing rapidly, transforming the way IT departments deliver messaging services to their organizations. Compared to traditional on-premises email, Microsoft's cloud-based email service cuts costs significantly by lowering operational overhead. This is great news! However, your organization cannot afford to overlook security considerations during the evaluation/premigration period.

Office 365 comes with free malware and spam protection; advanced threat protection can be added. But how complete and effective are these built-in capabilities? What security issues should you consider as your organization prepares to migrate to Office 365?

To answer these questions, you must understand today's biggest email security threats, accurately assess how much protection Office 365 can provide, and know when and where to turn for additional security capabilities to protect cloud-based messaging.

Why "Good Enough" Security is Never Good Enough

Smart, across-the-board email security—whether for on-premises, cloud-based, or hybrid email systems—begins with a clear, realistic understanding of what you're up against. Email is the most common way for cyber criminals to launch and distribute threats. According to the 2018 Symantec™ Internet Security Threat Report (ISTR), in 2017 one out of every 412 emails contained a malware attack, 7,710 organizations are hit by a Business Email Compromise Attack every month, and spear-phishing is the most widely used infection vector, being used by 71 percent of targeted attack groups.

As the volume of these attacks increases, so does the attack sophistication. Advanced and zero-day threats are much more difficult to detect and stop than traditional malware, while standard signature-based antimalware tools have proven largely ineffective against them. Attackers now favor targeted spear phishing and business email compromise (BEC) scams. These elusive and dangerous targeted attacks use sophisticated methods including domain spoofing and obfuscation of malicious links embedded in email messages. The losses from these attacks now stands at $12.5bn and grew by 136% over 17 months.[1]

Major email threat groups are also relying on first-stage downloaders to install their final payload, such as using Office documents containing malicious macros and Java scripts. Data loss through email is another serious issue. Mitigating such data loss requires implementing data protection tools and compliance policies.

Mind Your Security Gaps

When you look at today's broad security landscape—and how it applies specifically to email—it becomes apparent that Microsoft Office 365 security capabilities simply may not be up to the task of keeping your organization safe.

[1] FBI, Public Service Announcement, July 2018

> By 2020, 50 percent of organizations using Office 365 will rely on non-Microsoft security tools to maintain consistent security policies across their multivendor "SaaSscape."
>
> **— Gartner, 2017**[2]

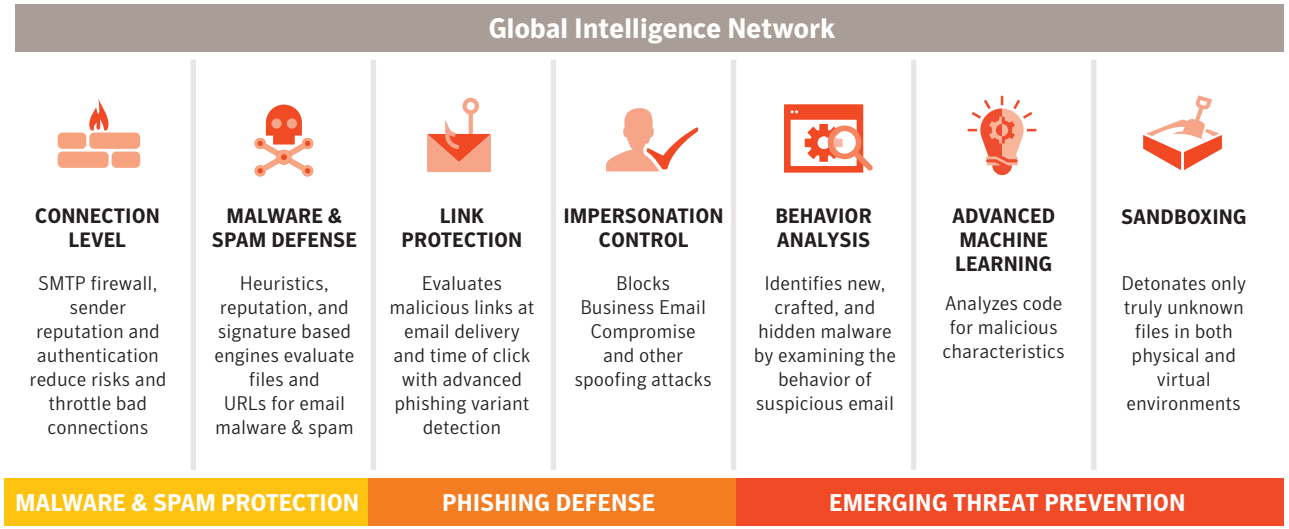
For example, Office 365 cannot effectively detect or block today's sophisticated phishing, ransomware, or zero-day attacks due to its lack of threat isolation and limited link protection capabilities. Moreover, it cannot help customers stop brand impersonation or ensure sender trust by authenticating email senders. Its advanced detection technologies, such as machine learning and behavior analysis, are fairly new and unproven. It lacks rich analytics that provide visibility into threats, a necessity for fast response and remediation. And it offers only basic detection methods, incident management, and remediation workflows for data loss prevention (DLP), leaving organizations open to the risk of data loss.

Fortunately, Symantec Email Security.cloud integrates with, and enhances, the built-in security and DLP capabilities built into Office 365 email. Symantec Email Security.cloud is an integral part of the Symantec Integrated Cyber Defense platform, which delivers complete, multichannel protection—threat analysis, blocking, remediation, and more—across web, endpoint, and email.

Get Proven Protection Against Spam and Evolving Malware

Symantec Email Security.cloud stops spam and evolving malware by inspecting links and attachments with technologies such as reputation analysis, antivirus engines, and antispam signatures; connection-level throttling reduces the risk of spam and malware by slowing and dropping anomalous SMTP connections. These analysis engines are continually updated.

This protection is powered by insights from the world's largest civilian threat intelligence network, the Symantec Global Intelligence Network (GIN), which offers visibility



[2] How to Enhance the Security of Office 365, Gartner, November 2017, G00345278

In 2017, one out of every 412 emails contained a malware attack.[4]

into the threat landscape worldwide. The GIN helps ensure better security outcomes through telemetry distilled from over 175 million endpoints, 80 million web proxy users, and 57 million attack sensors in 157 countries.

In contrast, Office 365 email security relies on third-party antispam and antivirus engines that can't match the efficacy of Symantec Email Security.cloud, which in our testing provides the highest effectiveness and accuracy of any email security on the market.[3]

Block the Most Threats with the Fewest False Positives

Symantec Email Security.cloud blocks new and sophisticated email threats (such as spear phishing, ransomware, and BEC) using advanced multilayered detection technologies (such as machine learning, behavior analysis, link protection with URL isolation, impersonation controls, and sandboxing) that analyze every email characteristic including delivery behavior, message attributes, and attachments while sniffing out social engineering tricks. Further, Symantec Email Fraud Protection enables organizations to automate Sender Authentication enforcement using DMARC, protecting all recipients from impersonation attacks.

Malicious attachment defense

Malicious attachment defense begins with deep code analysis that blocks new variants of ransomware and zero-day attacks by determining if an email contains any previously identified malicious code. File decomposition detects malware hidden within attachments, stopping threats that use evasion techniques such as obfuscated malware. Symantec Email Security.cloud also applies advanced machine learning, behavior analysis, and network analysis designed to identify command and control traffic. Suspicious files are detonated using physical or virtual sandbox execution, and our environment mimics human behavior to coax 'virtual machine-aware' malware into executing.

Microsoft detects and blocks signatureless files with Office 365 Advanced Threat Protection (ATP) Safe Attachments, which includes machine learning, behavior analysis, and sandboxing. But Microsoft's implementation of this technology is new and unproven. And its sandboxing is limited to virtual machine (not physical) execution, allowing virtual machine-aware threats to slip through. This is a significant efficacy gap given that 28 percent of malware is virtual machine-aware.[4]

Malicious link defense

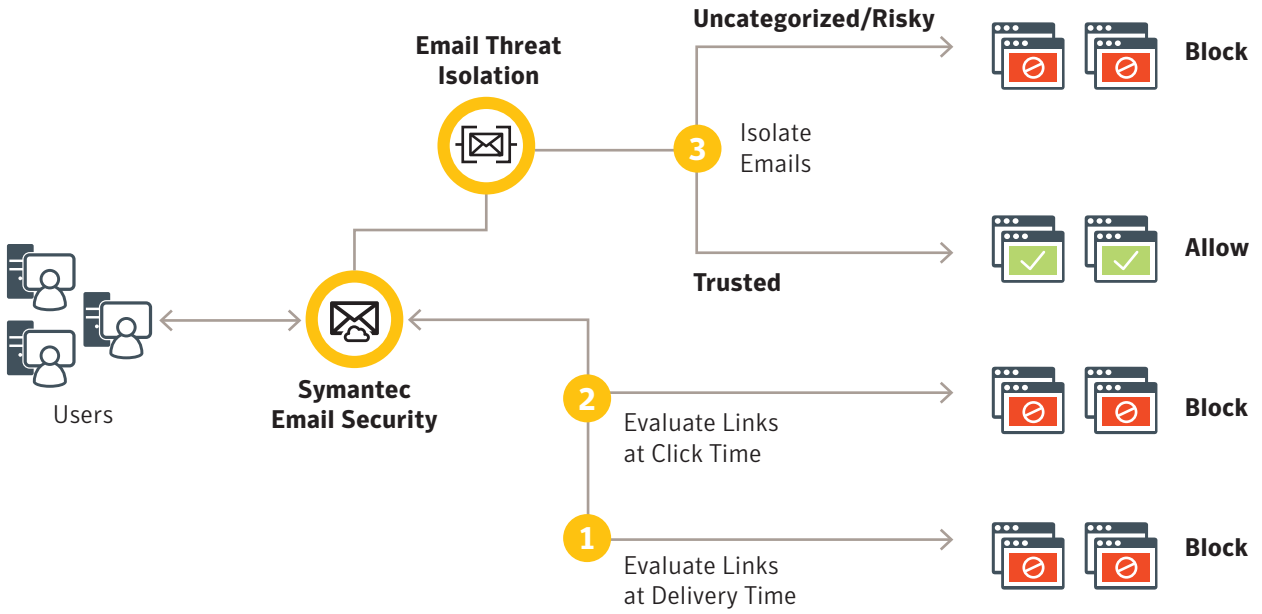
Symantec Email Security.cloud stops malicious links used in spear phishing and targeted attacks, with real-time protection that analyzes links before an email is delivered and again at time of click. It follows links to their final destination even when attackers try to bypass detection using sophisticated techniques such as multiple redirects, shortened URLs, link variants of known phishing sites, and time-based delays.

Link protection from Office 365 email security, featured as 'Safe Links,' is limited to checking rewritten URLs, only at click time, against reactive blacklists.

[3] Symantec Blog: "How Does Symantec Email Security Stack Up Against the Competition?", November 28, 2017
[4] Symantec ISTR 23

Office 365 email security offers no threat isolation capabilities.

Strongest protection against malicious URLs



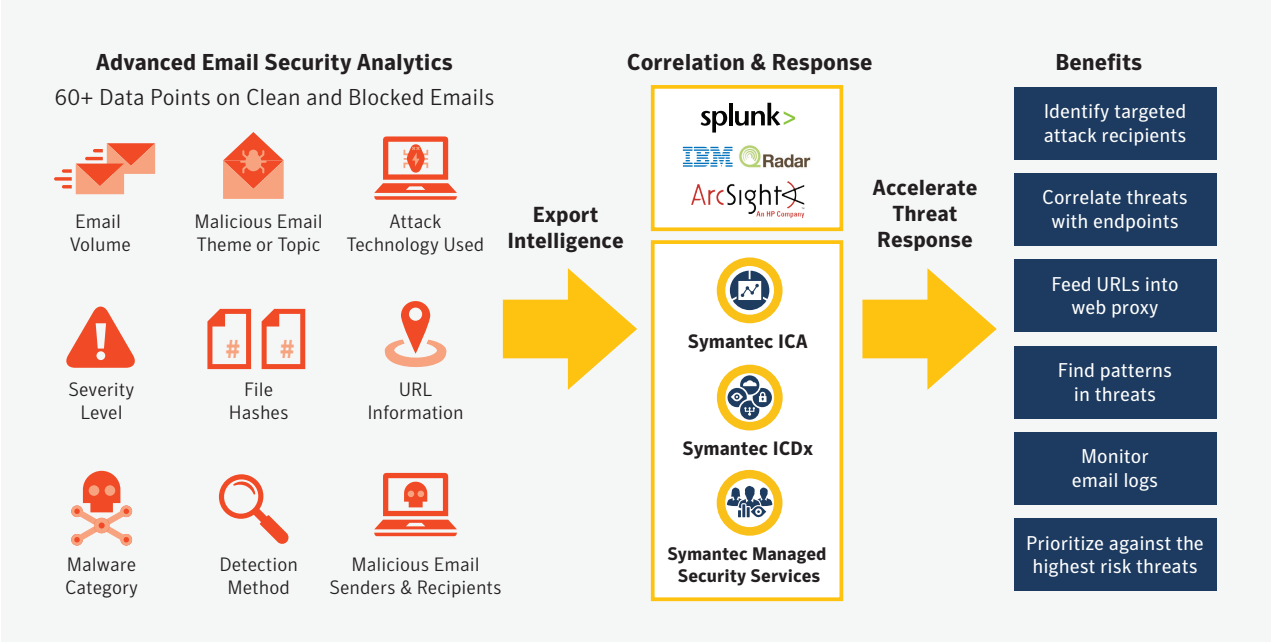
Safe browsing with email threat isolation

Symantec is the only email security vendor to offer integrated isolation technology, which executes suspicious links remotely for even stronger protection against spear phishing and targeted attacks. These capabilities send only safely rendered information to browsers, thereby preventing any zero-day malware delivered via email links or downloads from reaching users. Email threat isolation capabilities also stop credential phishing by rendering suspicious websites in read-only mode, blocking users from submitting sensitive information such as corporate credentials and passwords. Office 365 email security offers no threat isolation capabilities.

Business email compromise defense

Symantec provides the strongest protection against BEC and other spoofing attacks by blocking threats that impersonate a user or domain in your organization. These impersonation controls identify and prevent BEC scams by using a sophisticated impersonation engine and linguistic analysis to sniff out attacks that masquerade as a specific user or spoof a legitimate email domain in your organization. In addition, Symantec Email Fraud Protection enables organizations to automate sender authentication using multiple standards (such as DMARC, DKIM, and SPF). In contrast, Office 365 has no sender authentication capabilities.

Office 365 offers little security analysis and does not include important Indicators of Compromise (IOCs).



Uncover, Prioritize, and Remediate Advanced Attacks

Symantec Email Security.cloud accelerates your response to targeted and advanced threats with advanced analytics that provide the deepest visibility into email attack campaigns. This intelligence includes insights into both clean and malicious emails as well as more Indicators of Compromise (IOCs) than any other vendor: 60+ data points such as URLs, file hashes, and targeted attack information. Using an API, you can stream this data to your Security Operations Center to quickly determine the severity and scope of any targeted or advanced attack. Symantec's Integrated Cyber Defense Exchange collects, filters and forwards data to facilitate this analysis.

Office 365 offers little security analysis. It does not include important IOCs such as URLs, file hashes, method of attack, and action taken. This lack of visibility limits your organization's ability to uncover, prioritize, and remediate advanced attacks.

Data Loss Prevention and Policy-based Encryption

Symantec Email Security.cloud integrates with Symantec Data Loss Prevention and policy-based encryption services to prevent private or compliance data from

Symantec protects over 163 million email users and scans more than two billion emails per day.

leaving your network through email messages or attachments. Symantec Data Loss Prevention analyzes messages before any data leaves Office 365 email, including content (header, body, and metadata) and context. Multiple, sophisticated content detection engines—including fingerprinting, vector machine learning, and form recognition—rigorously examine structured and unstructured data. This data includes regulated data and intellectual property, such as personally identifiable information, financial reports, plans, source code, product designs, electronic forms, and images. Granular policy definition, clear incident reporting, and powerful remediation workflows deliver very effective data protection for all your organization's channels from a single control point.

In comparison, Office 365 DLP capabilities provide only basic content detection methods and cannot detect most structured and unstructured data. Its policy definition, incident reporting, and remediation capabilities are considerably immature.

Integrated Cyber Defense

Symantec Email Security.cloud belongs to the Symantec Integrated Cyber Defense Platform, working alongside other Symantec products to protect endpoints, web, and Office 365 files (scanned by Symantec Cloud Access Security Broker) while strengthening your overall security posture. Underpinning our Cyber Defense Platform is the Symantec GIN, powered by threat information discovered and blocked by Symantec product data feeds (email security, web proxy, endpoint protection, and cloud access security broker), which push out real-time blacklist updates to other channels to prevent further infection.

The Industry's Strongest SLAs Guarantee Results

Symantec protects over 163 million email users and scans more than two billion emails per day—protection we back with the industry's most stringent and aggressive service level agreements (SLAs). In addition to providing 100 percent virus detection efficacy, Symantec is the only email security provider to guarantee 99+ percent spam effectiveness (for English-language spam; we also guarantee spam capture efficacy for spam in other languages). We're so confident of our ability to meet performance levels that we include money-back remedies if we fall short. In fact, Symantec is the only email security vendor that will provide 100 percent service credit for threat efficacy after just one infection during a calendar month. In contrast, Microsoft limits payment to a 25-percent service credit—even after multiple infections in a month.

Symantec is the only email security vendor that will provide 100 percent service credit for threat efficacy.

Safely Transition to Office 365 with Confidence

Most organizations transition from on-premises to cloud-based email gradually. Symantec Email Security.cloud is built to protect all the email solutions running in your environment, including Microsoft Office 365, Google Gmail, and other hosted mailboxes, and traditional on-premises email systems such as Microsoft Exchange. Symantec wraps a unified protection layer around all your different systems, so nothing slips through the cracks as your email environment changes and evolves.

Symantec is ready to help you confidently transition to Office 365 email without any security compromises. Symantec Email Security.cloud enables your organization to tap into all the advanced security technology, global resources, and proven expertise needed to stay safe from today's most advanced and sophisticated email threats—and stay a step ahead as those threats evolve.

To learn more about Symantec Email Security.cloud, please visit symantec.com/products/email-security-cloud

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

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

Copyright © 2019 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

19D210754_SB_SECURITY_CONSIDERATIONS_O365