WHITE PAPER

In, Out and Around

360° Security for Microsoft 365

Trustwave®

Introduction

The rise and dominance of Microsoft 365 has been significant and shows no sign of stopping. According to Microsoft's 2018 earnings report, Office commercial revenue increased 11%, driven by Microsoft 365 subscriptions growth.

Microsoft Microsoft 365 bundles Office applications, such as Word, Excel, PowerPoint and Outlook with collaboration tools like Skype, Teams and OneDrive. There are a number of different licensing tiers offering varying degrees of data loss prevention capabilities, such as Azure Rights Management Services (RMS), as well as email security features. The possibility of wrapping all of this capability into one licensing entity is causing organizations to rethink their traditional on-premise secure email gateways and how they are deployed.

Therefore, it is important to understand what Microsoft 365 does and doesn't do from an email security, data protection and management perspective. Realistically, no one cloud tool is going to fully replace the coverage provided by multi-layered on-premise administration, security and management tools. So how do you evaluate your risk tolerance and align the appropriate level of coverage?

Trustwave compiled a list of 10 of the most common email security concerns from the requests that we receive from RFP and tender requests, in-bound sales calls and customer consultations. We receive a significant number of inquiries from current Microsoft 365 customers needing to supplement their service with an additional layer of security and more robust management capabilities. In this whitepaper, we will discuss the 10 areas of email security risk and what you can do to protect your Microsoft 365 investment.

Risk Areas

- Spam and False Positive Rates
- Business Email Compromise
- Malicious Spam
- Quarantined Spam Control
- Enforcing Outbound Email Policies
- Data Leakage
- Archived Email
- Policy Management
- Visibility and Reporting
- Licensing Costs

With a clear understanding of what the risks are, you will be better able to align the right coverage to secure **what comes in**, protect **what goes out** and **manage everything around** Outlook on Microsoft 365.

Let's Start With a Checklist

Here is a quick snapshot of email security risk areas. Use this checklist to determine which risk areas are most important to you and read on for more in-depth analysis in this white paper and determine how you can optimize the security, protection, management and cost of your Microsoft 365 investment.

RISK AREA	MICROSOFT 365	THIRD PARTY SECURE EMAIL GATEWAY
Spam Detection & False Positive Rate	May need additional skillsets to create custom rules and staff bandwidth to respond to increased help desk requests.	Can provide industry-standard spam catch rates right out of the gate with less false positives to increase time-to-value.
Business Email Compromise	Traditional detection engines aren't effective at blocking low volume, targeted attacks.	Can provide internet-level protection to eliminate these threats before they ever reach the network.
Malicious Spam	Advanced threat protection is only available at the higher license packages.	A third party SEG may be able to provide better protection and actually reduce your software licensing costs.
Quarantined Spam Control	Limited capabilities for users' self- quarantine management.	Industry-standard SEG providers offer management tools to support native language management, while reducing burden on IT staff.
Enforcing Outbound Email Policies	Has limitations.	If you need something more robust, you'll need to engage a provider that has a robust policy engine.
Data Leakage	If you don't have enterprise wide data loss prevention (DLP), you may want to ensure Microsoft 365 can support the rule sets of your legacy, on-premise email gateway.	The right third-party solution can fill in where there are limitations in Microsoft 356 or enterprise DLP. You may be able to gain the granular protection without having to go on an expensive Microsoft 365 licensing tier.
Archived Email	If advanced eDiscovery support is needed, you may have to go on expensive Microsoft 365 licensing tiers.	You may be able to get improved archiving functionality at a more favorable price point with a third party that can future-proof your investment.
Policy Management	Microsoft 365 has good capabilities here, but many organizations utilize complex policies built up over time in their on-premise software. Be sure Microsoft 365 can accommodate these.	If Microsoft 365 doesn't meet your needs, work with a provider that has deep experience partnering with customers of all stripes, that can help you unravel current policy use cases.
Visibility and Reporting	You may need to go to expensive licensing tiers to get security visibility beyond mere transactional reports.	A third-party solution can provide visibility into security incidents for analysis and response.
Licensing Costs	It may seem attractive to deal with one vendor and one licensing agreement from a simplicity perspective.	Using a third-party security solution can deliver best of breed protection and reduce total cost of ownership.

What is Coming In?

Spam and False Positive Rates

Spam detection should be table stakes now. As an industry, we have been combatting it for more than 15 years and spam volumes have reduced considerably. According to Trustwave's 2018 Global Security Report, spam volumes have dropped from 85% of total email a decade ago to below 40% today. However, when we talk to customers who migrated off legacy email security gateways to Microsoft 365 email security, they tell us they are suddenly getting help-desk calls about increased spam in users' mailboxes. This is a nuisance but what's perhaps more concerning are the reports of legitimate business emails that end up in Junk mailboxes – false positives. No spam engine is perfect and there is always a trade-off between detection rate and false positive rate, but what we are hearing is that the out-of-box catch rate for Microsoft 365 is not aligned with best-in-class third party solutions. So, unless you have the staff bandwidth and skill sets to create custom rules and configurations and respond to increased help desk requests, you may want to consider a third-party secure email gateway solution.

Business Email Compromise (BEC)

Seen in many different aspects from spear phishing to CEO fraud, wire fraud and whaling, no matter what you call it many organizations large and small have been impacted by it.

The reason why Microsoft 365 and many other email security solutions are failing to detect BEC attacks is that they are trying to use their existing detection engines to detect these attacks. Spam engines were designed to detect wide-spread mass volume attacks, or "spray and pray" attacks. This does not apply to BEC. BEC attacks are personalized to the target organization. The criminals use social engineering tactics to impersonate the CEO or some other senior executive and message spoofing techniques to make the recipient believe that the email originated from within the organization or from an address that the executive could be using.

To effectively combat BEC attacks, in addition to user education, you need to use a detection engine specifically designed to spot these attacks.

Product features to look for: When it comes to addressing BEC fraud...

Not all fraud detection engines are created equally. We talk with many organizations that have suffered losses even using an email security platform that markets its ability to detect BEC fraud. When evaluating vendors' products be sure to look for engines that are specifically designed to address BEC fraud. They should have the ability to allow you to add the names of your senior executives. Also, keep in mind that the actual ability of the engine to block what is seen in your environment can only be proven in your environment.

Malicious Spam

While spam volumes are down as previously mentioned, the percentage of malicious email within that spam volume is up, from around 3% in 2015 to just over 25% in 2017, according to Trustwave Global Security Report.

To combat the proliferation of malicious spam, email with malware hiding in attachments or embedded links to malicious sites, it is necessary to layer Microsoft's antivirus scanners with protection that blocks unknown malware. Microsoft 365's base packages rely on blocklists of known malware. Advanced threat protection services are available on the most expensive subscription level, but considering the cost to performance ratio, many customers are finding it more cost-effective to add a third-party security layer to fill.

Product features to look for: When it comes to blocking malicious spam, your email security solution should offer…

- Multiple layers of protection in addition to spam and unwanted email filters
- Options to select from industry-leading antivirus scanners
- Support for Yara rules
- Ability to detect both email and web-based threats
- Support for mobile devices
- Embedded URL rewriting and sandboxing capabilities
- Visibility into attacks

Additionally, it has been well-reported in the media that there has been significant hacker activity attempting different methods to subvert Microsoft's advanced threat protection (ATP) engines. Trustwave has caught examples of this activity in our email filters as well. Being a popular target of phishing lures is one of the unfortunate by-products of Microsoft 365's popularity.

Quarantined Spam Control

In Microsoft 365, users have to manage their own quarantine via their Junk folder. There are only minimal spam filter settings, but no options for allowing users to manage different categorizations of spam – for example newsletters or junk mailers versus inappropriate email.

What is Going Out?

Enforcing Outbound Email Policies

With the increased focus on inbound email security due today's advanced threats, it's easy to neglect outbound email policy enforcement. But with the ever-increasing regulatory requirements around data privacy, such as the European Union's General Data Protection Regulation (GDPR), many organizations are straining to support the increased demands on the email policy engine which oversees outbound email. Unless you are a small company in an unregulated industry, then you will probably find yourself looking for a third-party solution.

Product features to look for: When it comes to outbound email policies…

Be sure the provider offers a broad range of policy conditions and actions to provide maximum flexibility. For example, if you needed to build a new policy from the ground up, does your solution offer the ability to openly create and combine new conditions and actions? Be wary of solutions with "pre-defined" compliance policies, which will likely need to be customized to suit your environment anyway, and, without a flexible policy engine may not even work.

Data Leakage

If you have already deployed and rely on a dedicated data loss prevention platform that integrates with Microsoft 365, you have no issues here. However, if you were relying on the policy capabilities within your legacy email platform, you may find, as did many of the customers we speak to, that only a limited number of policy actions are available. Before you fully migrate to Microsoft 365 be sure to investigate whether its DLP capabilities can handle your existing requirements and definitions.

Archived Email

Having email archiving built into Microsoft 365 makes it easy to enable this capability that many organizations need to do in order to meet compliance requirements.

If you already have email archiving, then moving from on-premise to cloud-hosted email presents a challenge about what to do with your email archives. Users will want access to their old email as soon as you go live on Microsoft 365. Making this available means either importing data to the cloud or running two email systems in parallel. Most of the leading email security vendors offer SaaS-based email archiving, allowing you to streamline your migration to Microsoft 365 and future-proof your move to the cloud.

You'll never have to migrate your archived emails again if you ever decide to leave Microsoft 365 for another cloud platform. Be sure you work with a provider who understands your eDiscovery, data privacy and compliance requirements and perhaps most importantly, provides flexible data import and export options.

360° Management Around Your Email System

Policy Management

Let's face it, business email is not just about sending messages back and forth. Your email system may contain HR information, financial records and other confidential attachments. Or, it may be a part of a larger business automation workflow. Email has been the de facto business communication and collaboration tool for decades. If you think about the various use cases for email in your organization, are you being enabled or limited by your system's policy engines?

Microsoft 365 delivers many great features and if it does all you need then fantastic. But if it's not meeting current and anticipated future needs, you may find yourself looking for a third-party provider that offers mature management capabilities. If that becomes the case, work with a provider that has deep experience partnering with customers of all sizes and industries that can help you unravel your current email use cases.

Visibility and Reporting

Often overlooked in the product evaluation phase, reporting capabilities are how you prove the value and return you are getting for your email security solution. Microsoft 365 gives you visibility into the transactional aspects of email, covering what has been sent, received and read from a mailbox viewpoint. If you want actual email security reports for analysis and incident response, you will need either a third-party reporting solution or use an additional email security layer in front of Microsoft 365 that has the reporting capability (and all the rest of the features) you need.

Product features to look for: When it comes to reporting capabilities…

Look for a solution that goes beyond the transactional reporting capability in Microsoft 365. For detailed threat hunting and incident response, you may need a robust solution with that provides visibility into rule triggers, threats and impersonation attempts.

Licensing Costs

Every organization has different requirements and needs differing capabilities within the Microsoft 365 suite. However, the upper levels of Microsoft 365 can be very expensive. If you are considering – or currently subscribing to – the most expensive licensing tiers just for email archiving or advanced malware detection, then it might be more cost effective to look at an external third-party solution instead.

Trustwave has helped many customers define their productivity, collaboration and security requirements to align their desired service level with the optimal licensing tier. Microsoft 365's highest service tiers may compel customers to buy products/services they don't want in return for added email security. In many cases, however, companies can achieve significant savings by choosing a lower Microsoft Enterprise tier and adding a third-party email security solution.

One more thing...

A recent addition to the standard Microsoft 365 licensing levels, Azure Rights Management Services (RMS) provides an excellent range of additional rights management capabilities that can be assigned to office files and/or the emails they are attached to. The sender can place limits on the ability for a receiver to print or forward content and ensure the email is sent encrypted. Azure RMS is predicted to gain adoption, however, without visibility into RMS-protected attachments, you run the risk of sensitive data leaking from the organization.

While Azure RMS is supported in Microsoft 365 applications, there is limited support when it comes to Outlook 365 outbound email policy enforcement. If fully enabling Azure RMS is important to your business goals, then you may want to investigate Trustwave Secure Email Gateway capabilities. Trustwave's solution goes beyond what the industry, including Microsoft 365 is able to do in terms of unpacking and decrypting attachments, stripping out sensitive data and violations of acceptable use policies and then re-encrypting attachments.

Conclusion

If your current email security doesn't fit your risk profile, consider a third-party solution to enhance what Microsoft 365 offers. Trustwave has more than 20 years of experience providing customers with advanced protection against advanced email- and web-based threats, unmatched policy configuration and in-depth data protection and compliance management.

Please visit our website to learn more about Trustwave email security solutions.

Trustwave®

TRUSTWAVE.COM