FORTRA™

GUIDE (CLEARSWIFT)

Mitigating Information Security Risks in Microsoft 365

The Cloud-Based Productivity Promise of Microsoft 365

With its integrated applications and intuitive capabilities, Microsoft 365 (previously Office 365) has steadily become a corporate productivity juggernaut since its introduction in 2011. In fact, Microsoft's January 2023 Shareholders' meeting just reported more than 63 million subscribers for M365.

M365 offers multiple tiers of capabilities that all leverage the cloud to enable professionals around the globe to create and communicate with ease. But do the native capabilities of the application offer the information security and effective cyber attack prevention required in today's threat environment?

In this guide, we'll examine the cybersecurity functionality built into M365 and where it falls short when considering the strength of security postures required to meet the increasing level of risk we face today.

Today's Threat Environment Poses No Shortage of Business Risks

It's no secret that cyber attacks are a constant threat to businesses and their sensitive information. When it comes to M365, cybercriminals are advancing across several fronts, using different techniques to gain access to valuable data. Some of these techniques include:

- **Phishing Scams**: It's becoming increasingly difficult to spot phishing campaigns geared toward M365 users due to their clever—and realistic—appearance. These masquerade as an innocuous-seeming communication, such as a meeting request from a co-worker or a false live chat. Once the user clicks on the link, he or she is redirected to the phishing site disguised as a M365 page.
- **Malware**: When sent from what looks like a legitimate email address, malware embedded in images or documents can quietly infiltrate a network once a recipient opens the file. This can even happen in preview mode, a security flaw within M365, which doesn't check a document's source prior to launching the preview. Malware is often hidden in documents that employees are accustomed to seeing every day. For example, a PDF of a purchase order could be sent to Finance, or a resume may be emailed to an HR rep. The danger is the recipient has no idea anything is amiss, and these threats can infiltrate a network for days, weeks, or months before they're discovered—**if** they're discovered.
- **Augmenting M365's Supposed Security**: In early 2022, a researcher from WithSecure, a cloud and endpoint protection provider, discovered an unpatchable flaw in Microsoft Office 365's Message Encryption (OME), which enabled a hacker to infer the contents of encrypted messages, implying that the platform could be leaving encrypted emails vulnerable to decryption by hackers at a larger scale. Even worse, though the discovery of the vulnerability was shared immediately with Microsoft when it was identified, they did nothing at the time by way of issuing a fix besides acknowledging the researcher via its vulnerability reward program.

Additionally, in the wake of the COVID-19 pandemic and the dramatic increase in the number of employees remotely, many businesses are overlooking security protocols in favor of rapid M365 deployment, leaving them more vulnerable to attack. In fact, as recent as December 2022, CISA's Vulnerability Bulletin reported 8 remote code execution vulnerabilities in M365 in one week alone!

Inadvertent Data Sharing —Accidents WILL Happen

Other situations highlight accidental but no less harmful forms of having the wrong information sent to the wrong person. Perhaps an account rep shares a file with a customer and doesn't realize there's sensitive PCI, PII, or IP data in a hidden column of a spreadsheet. Or a CEO doesn't realize there is sensitive metadata in the properties field or unaccepted changes still present in the version history of an M&A report.

Perhaps pricing information for one organization isn't deleted from a proposal given to another. And finally, a high-ranking military defense employee could share a document with a photo without realizing the image contains embedded top-secret location information.

Implications of a Data Breach

No matter how it is lost, when data ends up in the wrong hands it can cost the organization greatly. Costs include ransom demands from perpetrators and fines from regulatory bodies for non-compliance with data privacy laws. Cyber attacks with the intention to cause disruption can wreak havoc with internal operations which often leads to customer-facing downtime. All these implications can cause damage to your reputation and ultimately lead to a loss of customers.

Preventing Email Data Leakage

To avoid the risk of a data breach, organizations need to secure their business communication channels. Data leakage through email is commonplace and to minimize the risk, email security tools need to scan deep into messages and attachments to identify any sensitive or critical information before it leaves the organization and ensure that any unwanted data is not received.

M365 is good for dealing with spam and malware and does offer various levels of email security, such as tools to deal with regulatory control through archiving and basic encryption.

Template rule sets are provided to get you started with policies, but these typically do not deliver the deep content inspection required to remain truly secure.

Where M365 Security Falls Short

- DLP controls are less than comprehensive and can be hard to configure effectively
- Policies need to be configured in multiple admin consoles. For example, searching for a keyword requires a Transport Rule to be setup, whereas to detect a credit card number the policy is configured in the Security and Compliance configuration settings
- Unable to detect sensitive information (e.g., PII data) within image files such as screen shots and scanned documents
- Unable to remove meta-data (which might lead to data loss) and malware threats hidden within document and image files
- Even **with** sandboxing to analyze attachments, protection against ransomware is limited
- There can be a delay in the application of outbound mail policy changes that you make to the service
- Does not provide a means to quarantine outbound email; only reject, sender release override, or redirect to administrator
- Can only block file types (by signature) if they are ‘executable’, controlling other file types relies on building policy for extension names, such as Xlsx, Xlsm, Xlsb, etc., rather than “Excel”
- Unable to define new custom file format types (by signature)
- Limited number of notification options (sender, recipient, or admin)
- No re-use of existing lists (profanities, expressions, etc.), however Microsoft does provide some classifiers to cover threat, profanity, resumes, source code and harassment, but are in the process of deprecating their Offensive Language classifier as it was found to generate too many false positives
- No means to duplicate rules, forcing new rules to be created from scratch with different rule criteria (e.g., sender, recipient, or violation action)
- Complex customer configurations may make managing policy difficult
- Unhelpful or misleading error messages, although some may find the tool-tips useful
- Reporting does not provide the level of comprehensive but easy to understand detail required to investigate an information security breach (it should also be noted that any attempt to generate reports on data more than a day old does take significantly longer)
- System logging data is difficult to separate on a per-client basis

Become a Zero-Compromise Enterprise

Fortra Advanced Email Security offers a more comprehensive, secure solution than M365 alone—an important consideration for any IT security professional balancing sensitive and critical information protection and control, with an increasingly cloud-centric infrastructure.

By implementing Clearswift's Secure Email Gateway in conjunction with M365, you will have the missing element required for a robust, comprehensive security posture. And when paired with the additional benefits of Adaptive Redaction, your organization can rest assured knowing sensitive and critical information is secure within the M365 framework. There's no need to compromise collaboration for security as this approach offers the best of both worlds.

The SEG covers all the bases. It features a Deep Content Inspection engine that thoroughly examines message headers, subject lines, message bodies, attachments and contents, image scanning, document headers and footers, and even the metadata within documents. This maximizes the chances of capturing sensitive content such as credit card numbers and banking codes, confidentiality clauses and profanity, customer-defined and regular expressions, and Boolean and positional operator-based expressions.

Furthermore, the solution can be used to **monitor and control internal email**, providing granular controls and advanced data loss prevention functionality to prevent unauthorized data sharing within your business. While organizations control access to file servers and other collaboration services in recognition of the fact that not all information should be available to all people, internal email traditionally lacks these restrictions. This means any employee can send anything to another person inside the organization. The Secure Email Gateway mitigates this type of risk.

Adaptive Redaction in Action

Adaptive Redaction technology is unique to Clearswift and provides cybersecurity protection for email without impacting on productivity. In real time it removes only the information that would cause a data breach or cyber attack, allowing the rest of the communication to continue to its destination. The sender would be notified of the infringement to help inform future choices. Below are its three main features that can be applied to incoming, outgoing, and internal traffic.

DATA REDACTION

Redaction capability in Word, Excel, PowerPoint, and PDF files, as well as email messages to remove sensitive data (e.g., PII, PCI, etc.)

DOCUMENT SANITIZATION

Sanitization capability includes the removal of tracked changes and properties information

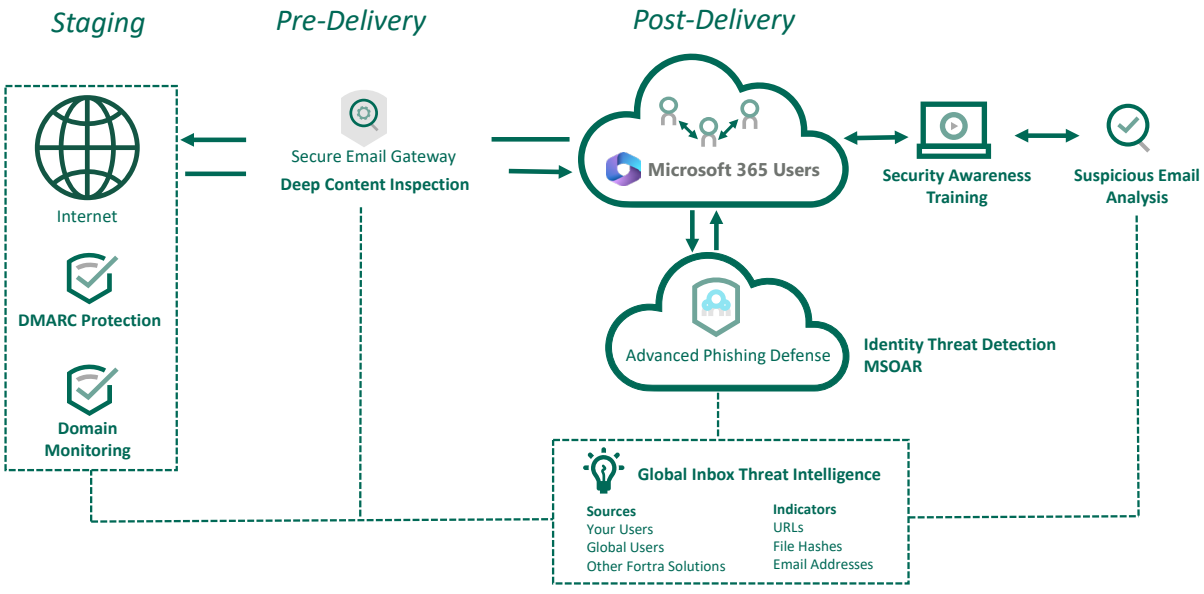
STRUCTURAL SANITIZATION

Sanitization capability to remove active content and other malicious components from files, such as APTs, ransomware, etc.

Plugging Information Security Gaps in M365

Introducing Fortra's technology enables your organization to take a strong stance against cyber attacks and data loss. This is possible with capabilities and controls that close gaps against the efforts of external cybercriminals as well as malicious—or well-meaning, but careless—employees.

- *Granular DLP policy control* allows you to set flexible or custom rules for different senders, recipients, domains, departments & apply hundreds of preconfigured tokens from a dictionary or policies for regulations like GDPR
- *Optical Character Recognition* (OCR) detects sensitive information (e.g., PII, PCI, etc.) in images & scanned documents
- *Anti-steganography* functionality prevents exfiltration of sensitive data within images & strips embedded threats
- *Structural Sanitizing* provides additional protection against APTs & ransomware
- *Email quarantining*, with options for redaction, sanitization, or to hold for detailed investigation by end user
- *Recognition of file signature* in executable, image, document & multimedia formats
- *Missing Manager policy feature* so an administrator can define a manager or compliance officer to check for violation by end user, and inspect email header fields if needed
- *Easily reusable policy objects* without incurring additional overhead costs
- *Define custom file-type detection* to block files that are too sensitive to rely on extension-based controls
- *Comprehensive reporting* with full tracking & tracing capabilities
- *Real-time message tracking* without any noticeable delays
- *Full-access, easy-to-find logging data* as you are the exclusive tenant
- *Integrating M365* with the Clearswift Secure Email Gateway



Clearswift's Secure Email Gateway, along with Agari Phishing Defense & DMARC Protection, PhishLabs' Suspicious Email Analysis & Domain Monitoring, and Terranova's Security Awareness Training, integrates with M365 to fill email security gaps.

Fortra's comprehensive email security solution can be deployed alongside M365 to ensure your organization's valuable information remains secure—whether it's housed on-premise, in the cloud, or in a hybrid environment.

Additional considerations as illustrated the infographic:

- **Email Traffic Scanning**: The SEG Secure Email Gateway can scan inbound, outbound, and internal email traffic for comprehensive protection.
- **Hybrid Deployments**: The Fortra solution can be deployed as a hybrid configuration if your organization uses both M365 and an on-premise email solution.
- **An Adaptive Approach**: M365 offers a comprehensive hosted email and SharePoint solution with variable levels of security. To truly feel confident your sensitive and critical information is secure, it's important to enhance these security capabilities with an adaptive approach.

Conclusion

With cybercriminals becoming increasingly savvier in their delivery of sophisticated threats, and data protection laws becoming tighter, organizations that store and process sensitive and critical information in M365 need to weigh the benefits of the platform and the cyber risks associated with it. Even with the most advanced offering, the Microsoft solution still has security shortfalls that need to be plugged.

Fortra's Advanced Email Security offers the proven comprehensive security solution you need to integrate seamlessly with M365 to enable advanced threat and data protection. The powerful combination of Fortra alongside M365 technologies closes security gaps and mitigates risk for your business.

Discover how Fortra Email Security solutions can augment M365!

GET THE GUIDE

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.