clearswift
by HelpSystems

GUIDE *(Cybersecurity)*

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 reported 200 million monthly users in its FY20 Q1 results, with commercial use up 19% year over year as of FY20 Q4 results.

Microsoft 365 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 Microsoft 365 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 Microsoft 365, 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 Microsoft 365 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 Microsoft 365 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 Microsoft 365, 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.
- **Bypassing 365 security:** In the 2019 NoRelationship attack, hackers completely bypassed the native Microsoft 365 filters, which don't always scan full documents to determine threats. Instead, it uses xml.rels files to catalog a file's external links. In this attack the cybercriminals removed these files to keep filters from sounding the security alarm.

Additionally, in the wake of the COVID-19 pandemic and the dramatic increase in the number of employees working from home, many businesses are overlooking security protocols in favor of rapid Microsoft 365 deployment, leaving them more vulnerable to attack. In a survey of 250 financial services CISO/CIOs in the US, UK, The Netherlands, Germany, and Australia, almost half of the participants agreed that COVID-19 has brought forward digital transformation-related plans, such as a move to Microsoft 365 and 56% will focus investment on cloud/Microsoft 365 security as well as email security in the coming year. 45% of large financial organizations have seen an increase in cybersecurity attacks since the onset of COVID-19.

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 intellectual property 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 reap 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 Data Leakage via Email

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.

Microsoft 365 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 Microsoft 365 Security Falls Short

All Microsoft 365 customers are automatically protected by anti-virus and anti-spam capabilities, but the level of protection depends on the package your company uses. When it comes to data loss prevention, cyber threats, and administrative functions, Clearswift customers have reported numerous concerns.

- 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
- 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). Microsoft does provide some classifiers to cover threat, profanity, resumes, source code and harassment. However, they 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

Clearswift offers a more comprehensive, secure solution than Microsoft 365 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 the Clearswift Secure Email Gateway in conjunction with Microsoft 365, 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 Microsoft 365 framework. There's no need to compromise collaboration for security as this approach offers the best of both worlds.

The Clearswift Secure Email Gateway 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 at a Glance:

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. Its three main features include:

- **Data Redaction** of Word, Excel, PowerPoint, and PDF files as well as email messages to remove sensitive data (e.g., PII, PCI, etc.)
- **Document Sanitization** including removal of tracked changes and properties information
- **Structural Sanitization** of documents to remove active content and other potentially malicious components from files such as Advance Persistent Threats (APTs), ransomware, etc.

These features can be applied to both incoming, outgoing, and internal traffic.

Plugging Information Security Gaps in Microsoft 365

Introducing Clearswift's technology enables your organization to take a strong stance against cyber-attack 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.

- **Flexible and granular DLP policy control:** Set rules for different senders, recipients, domains, and departments. Ready-to-use policies for regulations such as GDPR, custom token dictionary, and 200+ pre-configured tokens
- **Optical Character Recognition (OCR)** functionality detects sensitive information (e.g., PII, PCI, etc.) in images and scanned documents
- **Anti-steganography** functionality prevents exfiltration of sensitive information within image files and strips incoming embedded threats
- **Structural Sanitization** feature provides additional protection against APTs and ransomware
- Emails are quarantined, with options for redaction, sanitization, or hold for detailed investigation and can be managed by admins, line managers or end users depending on the type of violation
- Recognizes executable, image, document, and multimedia formats by file signature
- A customizable **Missing Manager** policy allows an administrator to define a manager/compliance officer for each user and inspects CC and TO fields for their email address. Emails are reviewed for release by manager/compliance officer
- Manage policies easily using reusable policy objects without incurring additional overhead costs
- The ability to define custom file type detection to block files that are too sensitive to rely on extension-based controls
- **Comprehensive reporting** with full track and trace
- Real time **message tracking** without any noticeable delay
- Access to all logging data is available as you are the exclusive tenant

Integrating Microsoft 365 with the Clearswift Secure Email Gateway

The Clearswift email security solution can be deployed alongside Microsoft 365 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 in Figure 1:

- **Email traffic scanning:** The Clearswift Secure Email Gateway can scan inbound, outbound, and internal email traffic for comprehensive protection.
- **Hybrid deployments:** The Clearswift solution can be deployed as a hybrid configuration if your organization uses both Microsoft 365 and an on-premise email solution.
- **An adaptive approach:** Microsoft 365 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.

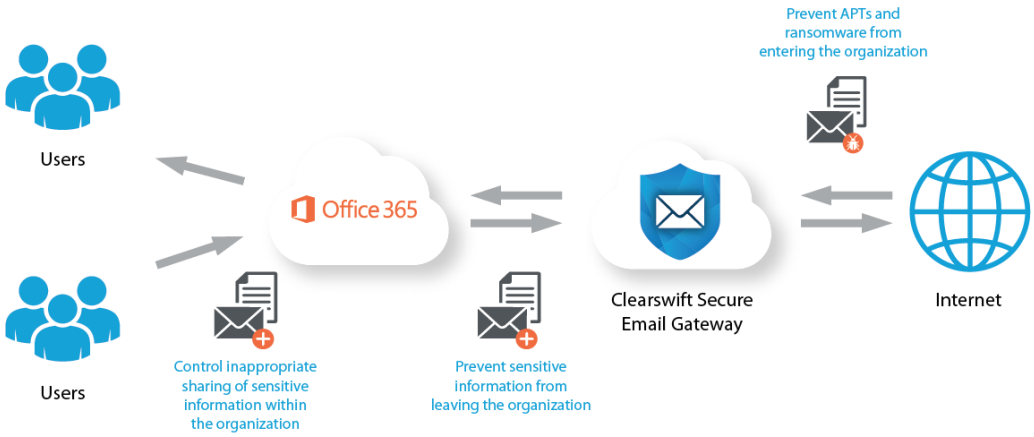

Figure 1: Clearswift Secure Email Gateway integrates with Microsoft 365 to plug information security gaps

Summary

With cyber criminals becoming increasingly creative in their delivery of sophisticated threats, and data protection laws becoming tighter, organizations that store and process sensitive and critical information in Microsoft 365 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.

Clearswift offers the proven security solution you need to integrate seamlessly with Microsoft 365 to enable advanced threat and data protection. The powerful combination of Clearswift alongside Microsoft 365 technologies closes security gaps and mitigates risk for your business.

For more information on cloud-based security, visit www.clearswift.com/solutions/cloud-security. For a deeper dive, watch our on-demand webinar, or request a demo from the team.

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.