mimecast

White Paper

Defense in Depth: Closing the Gaps in Microsoft 365 Security

mimecast

Microsoft provides a full set of native security features for Microsoft 365. But are they sufficiently robust to protect your business from a concerted attack?

Overview

Email is the most widely used business application—and the No. 1 vector of cyberattacks. For Microsoft's enormous installed base of Microsoft 365 Exchange email users, the cyber threat is particularly acute. This paper explores the security challenges facing organizations that rely on Microsoft 365 for email and provides recommendations designed to mitigate these risks.

Key challenges:

- Protecting end users from phishing and other email-based attacks
- Guarding against spoofing, lookalikes and other forms of email and website impersonation
- Ensuring true business continuity via point-in-time email recovery and archiving
- Moving beyond event-by-event reporting to obtain a full-forest view of the security landscape
- Justifying the cost of the third-party security solutions needed to mitigate these risks

Chief recommendations:

- Native Microsoft 365 security is good but insufficient. Complement it with best-of-breed secure email solutions
- Use a layered ***defense in depth*** approach to strengthen your security posture and provide a best-of-breed framework for selecting third-party applications
- Adopt a comprehensive strategy of cyber resilience that goes beyond email security and addresses all of your company's data protection requirements
- Don't count on a low profile to keep cyber criminals from targeting your company
- Don't put all your eggs in the same basket of technologies

Lay of the Landscape

Virtually no business can function without email. And among North American organizations, Microsoft 365 is the dominant email service by far.

But while organizations reap many benefits from Microsoft's family of productivity tools, they also incur heightened risk. This is especially true as Microsoft 365 users migrate to cloud-based email. The enormous concentration of corporate email servers this creates presents an irresistible target to would-be cyber thieves and digital saboteurs. Indeed, Verizon's 2019 Data Breach Investigations Report notes that 94% of all malware is delivered by email and nearly half (45%) of malicious email attachments are Microsoft Office files.[1] All told, cyber criminals attack Microsoft 365 far more than any other software environment worldwide.[2]

Globally, between 2016 and 2019 businesses lost $26 billion due to ***business email compromise attacks alone***, according to the FBI.[3] And that's just the tip of the iceberg. Cyber attacks that begin with an email can result in breaches that torpedo a company's operations, cripple it financially and undermine its standing with customers.

To counter this huge threat, companies need to do more than keep a low profile and hope for the best. They must acknowledge the dangers posed by their most important means of communication and prepare to defuse the email-based attacks that are headed their way. For organizations that rely on Microsoft 365 for their email, these are some questions to consider:

- How prepared is your organization to deflect highly targeted phishing attacks?
- Are you confident in your safeguards against spoofing, lookalikes and other forms of email and website impersonation?
- Do your spam filters leave you vulnerable to permanent loss of important business correspondence?
- Is your message encryption reliable and consistent but also user friendly?
- Are the trees obscuring the forest, or does your security reporting system provide you with more than just the details? You need to be able to take in the big picture, so no attack pattern or telltale behavior is overlooked.

However, preventing or limiting the consequences of an attack calls for more than enhanced email security. Preventive measures need to be part of a larger strategy of cyber resilience that embraces backup and recovery, business continuity and compliance, as well as the ability to identify and block threats that originate on the web.

Required: Defense in Depth

Microsoft 365 for email contributes to cyber resilience with an extensive set of protective mechanisms. While these are well engineered and effective, one size simply doesn't fit all and many enterprises will inevitably require a greater degree of control, resilience, and more extensive protections than Microsoft's productivity suite can provide.

For instance, the Advanced Threat Protection (ATP) security service offering for E5-level subscribers provides a degree of protection against malicious URLs, phishing messages and attachments. But it doesn't actively scan all email content for such threats, and its Safe Attachments feature relies entirely on sandboxing to detect malware. Other, more sophisticated techniques, such as deep content inspection, static analysis and multi-stage threat analysis, are not used.

Another example: Examining more than 100 million emails that had been vetted and cleared by the native protection services for Microsoft, the email security experts at Mimecast found that 28% of the spam and phishing threats contained within the sample went undetected. For many companies, this presents an intolerable degree of risk.

While "good enough" for some low-risk businesses, this degree of email security falls short for companies whose requirements go beyond the basics. Corporate security officers acknowledge this: When decision makers from nearly 1,000 companies worldwide were recently asked whether their organization requires additional layers of email security for Microsoft 365, 81% said yes.[4]

Enter defense in depth, a layered approach to cybersecurity. When used in conjunction with the native security features of Microsoft 365, a defense in depth strategy can buttress a company's security posture and provide a much greater degree of cyber resilience.

With defense in depth, if one security control proves ineffective, others are already in place to fill the breach. By integrating additional protective mechanisms from one or more third-party vendors, the defense in depth model closes any gaps in a company's defenses. Some of the more important elements of a defense in depth strategy include:

- Anti-malware to guard against viruses, spyware and other types of malevolent software. The best of these programs go beyond signature-based detection and include heuristic features that scan for suspicious patterns and activity.
- Network security controls to restrict data and network access. Typically, these are based on an analysis of a network's traffic patterns and used to configure firewalls and intrusion protection systems.
- Data integrity analysis software to spot any data file inconsistencies. Incoming files with discrepancies can be flagged as suspicious—especially when they come from an unfamiliar source.
- Network behavioral analysis software that picks up where firewalls and intrusion protection programs leave off. By identifying aberrant user and network traffic patterns, NBA applications can spot any suspicious activity and take remedial action.

Third-Party Security: More than a Nice-to-Have

The practice of deploying solutions from third parties to shore up the native security of Microsoft 365 is already widespread. Defense in depth gives security professionals an effective way to structure these efforts and optimize their investments.

Defense in depth favors this best-of-breed approach for it has two major advantages:

First, although Microsoft's cloud and application security affords a reasonable level of protection, many third-party solutions perform better and are designed to offer more advanced features than the native security tools of Microsoft 365. For instance, a common complaint from security professionals is that Microsoft's ATP service does not consistently recognize credential phishing attempts that lead to counterfeit Microsoft 365 login screens. Since neither the payload nor link itself is malicious, Microsoft Advanced Threat Protection services offer limited protection for this threat.

What do you like most about using Mimecast with Microsoft 365?

"Above all the security features including the protection against Impersonation."

—Mevin Goonmeter, Infrastructure Operations Manager, IBL LTD

The spam filter of Microsoft 365 is another example. The spam folder can only display 500 messages—there's no way to view more. And while an end user can sort the list to try and locate legitimate emails mistakenly quarantined as spam, the interface and message limit can make it a daunting process. This practically guarantees that a certain number of business messages may be lost forever. A third instance is Microsoft's Message Encryption for Microsoft 365, which has had reliability issues and, like the spam filter, is less than user friendly.

These and other concerns are expressed in Gartner's *2019 Market Guide for Email Security*, which states that "clients report dissatisfaction with [Microsoft 365] natively available email security capabilities."[5] In a similar vein, the Radicati Group's 2019 analysis of secure email gateways finds that Microsoft 365 customers "still report high degrees of spam, malware and other forms of attack."[6] Shortcomings like these explain why nearly two-thirds of corporate IT and security professionals are adding or planning to add a new layer of security for Microsoft 365.

What do you like most about using Mimecast with Microsoft 365?

"The breadth of solutions and the ease of use… both from the user's perspective and from an administration standpoint."

—IT Architect for a mid-size insurance company

The second big advantage to using best-of-breed criteria for selecting email security defenses is that it allows an enterprise to sidestep the limitations of a security monoculture. In effect, incorporating third-party solutions into Microsoft's security environment forces a would-be cyber thief to pick an additional set of locks. If a bad actor is looking for the easiest pickings, then this alone could induce him or her to look elsewhere.

The integration of third-party solutions also undermines a malefactor's ability to target the shortcomings in Microsoft's security arsenal. To learn what they're up against, cybercriminals will often subscribe to Microsoft 365 themselves and conduct dry runs to test the viability of their attack strategies before setting them in motion. Deploying third-party defenses deprives them of this stratagem, forcing them to operate on unfamiliar territory.

Compliance, Backup and Business Continuity

A comprehensive approach to cyber resilience, however, does more than fortify a company's preventive security, as important as that is. It also incorporates the means to backup and protect mission-critical data, maintain compliance with state, federal and agency regulations, and ensure that the business can continue to operate uninterrupted in the event of an outage or while in the midst of a cyberattack.

While Microsoft 365 is generally reliable and does not experience many long-term outages, localized outages are not uncommon. For example, between February 6 and April 30, 2019, the productivity suite experienced 18 separate outages totaling nearly 353 minutes in duration—the equivalent of a 19.6 minute outage every 4.6 days.[7]

Even short outages can have serious consequences. Users, for example, who can't send email from their corporate account, will often turn to their personal email account, bypassing corporate security and increasing the likelihood of a successful email attack or data leakage. Moreover, any business correspondence shared via their personal email will not be captured by their company's archiving and backup systems.

But you can't really fault users for wanting to get on with business. The key issue here is that Microsoft 365 does not include traditional backup and recovery capabilities in the same way as organizations have historically deployed them in on-premises environments.

The cloud-based platform is a live production system that offers recovery of messages and documents only within a limited timeframe, and Microsoft does not offer a point-in-time backup and recovery option. Whether it's due to a careless user, a ransomware attack or a technical failure, once any data stored within Microsoft 365 is gone, there's a good chance that it's gone for good.

A related issue is the limitations to the native search capabilities of Microsoft 365, such as the inability to search email attachments that are password-protected or documents that contain special characters, and the absence of any optical character recognition. There are, however, some third-party archiving solutions that address these drawbacks.

Another concern: The Microsoft Security & Compliance Center generates a variety of threat reports, but these only address specific types of attacks. For a view of the "big picture" across the organization, a security administrator must manually correlate the data within each of these reports.

All of these deficiencies can and should be addressed with best-of-breed third-party solutions. To achieve true cyber resilience, businesses need to work with a limited number of highly trusted vendors who are proficient at integrating their solutions into a Microsoft 365 environment.

What do you like most about using Mimecast with Microsoft 365?

"Archive – simplicity of recovering from the archive plus continuity mode should we lose access to Microsoft 365." *—John Crawley, IT Infrastructure and Security lead, MDSL*

"E-discovery. I can permit access to our outside legal firm to do the necessary e-discovery and know that they have access to ALL email." *—Vice President of IT for a midsize*

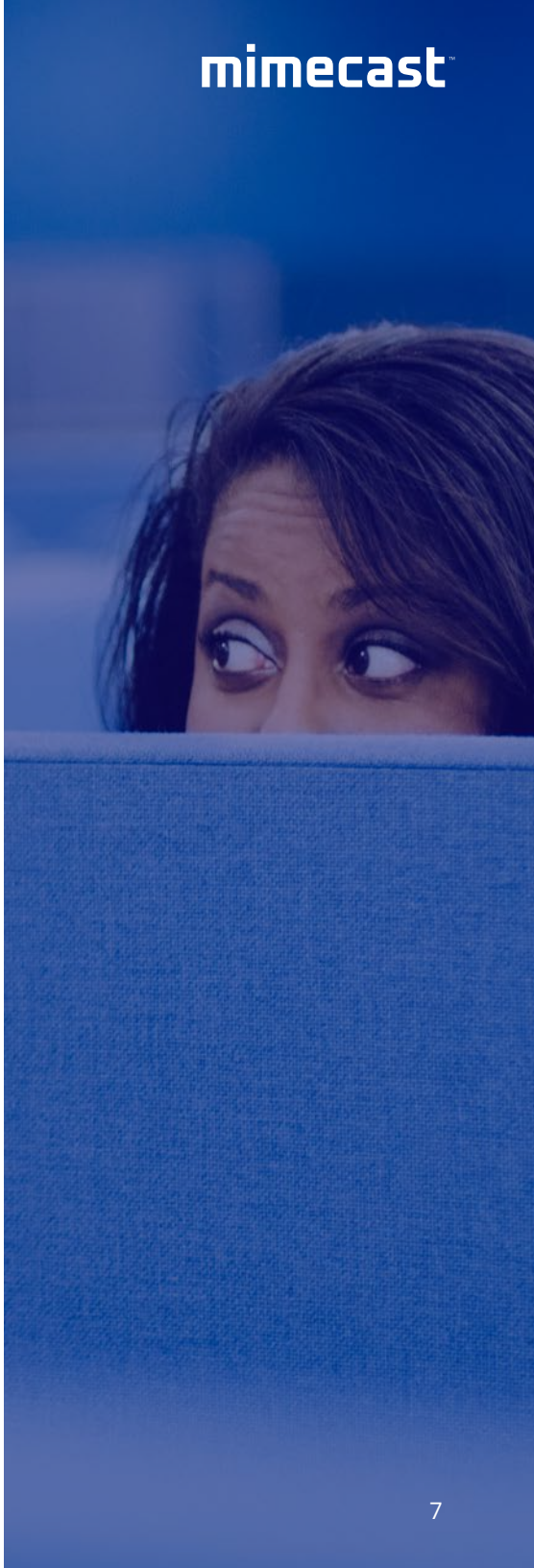
Finding the Money

An often heard objection to adopting a best-of-breed, defense in depth strategy is the additional cost of the third-party solutions. But to gauge the true extent of these costs, they should be compared to the cost of the data breaches these solutions are designed to prevent. And that cost is sky high:

- In 2019, cybercrime cost businesses worldwide more than $2 trillion.[8]
- The FBI estimates that U.S. losses due to business email compromise attacks in 2019 were $1.7 billion. [9]
- Globally, the average cost of a data breach is $3.9 million.[10]
- But in the U.S. it's considerably higher: $8.19 million. [11]

Apart from outright theft, a breach can result in various types of regulatory violations and associated penalties. Even more ominously, it can seriously damage a company's reputation for protecting the welfare of its customers, leading to loss of business. Even a brief email outage can damage customer relationships—or simply nip them in the bud. Emails from existing or potential clients can be lost and their queries never answered. Email outages also impinge on productivity, choking off internal communications and restricting the flow of important information.

Compared to these costs, the additional expense of third-party security and business continuity software is relatively minor, and there are ways to offset it. Forgoing the enhanced but now redundant security features in Microsoft's E5 plan and switching to an E3 plan instead will save a company $15.00 per user per year. There are also considerable savings to be had from phasing out on-premises software and redeploying the services 100% from the cloud. A portion of these can be used to defray the cost of third-party add-ons.



Conclusion: The Path Toward Cyber Resilience

It should be clear by now that counting on obscurity to provide security is naïve, and limiting your defenses to Microsoft's native security mechanism. Instead, companies should seek to strengthen their email fortifications as a key element of a larger and more comprehensive strategy of cyber resilience, and would be well advised to take the following steps:

1. Make an objective assessment of Microsoft 365's security capabilities and limitations with regard to your organization's business needs and risk tolerance.
2. Investigate how third-party data protection solutions can enhance the security features in Microsoft 365 and compensate for their limitations.
3. Adopt a defense in depth framework for integrating best-of-breed third-party applications with Microsoft's native security facilities.
4. Evaluate potential vendors for critical capabilities including:

    - Effective spam and phishing detection with a low false negative rate
    - Enhanced spoofing defenses that encompass lookalike and soundalike domains
    - Robust safe attachment inspection that includes such techniques as recursive analysis and deep content inspection
    - Dynamic site analysis for identifying potential URL-based threats
    - The ability to support and operate effectively in both cloud-based and on-premises environments
    - A redundant architecture that supports uninterrupted business continuity
    - Point-in-time backup and recovery
    - Advanced e-discovery and search capabilities

Microsoft 365 has become the *de facto* standard for business email and collaboration, but for enterprise customers this ubiquity also means heightened risk. Despite a robust set of native security features, gaps and limitations to Microsoft's email defenses leave many businesses vulnerable to a crippling data breach or cyber attack. Deploying suitable third-party solutions within a best-of-breed, defense in depth framework, however, can compensate for these deficiencies and fortify a company's defenses against the growing onslaught of cyber intrusions.

1 ***"2019 Data Breach Investigations Report,"*** *Verizon*

2 ***"Most commonly exploited applications worldwide as of 3rd quarter 2019,"*** *Statista*

3 ***"Public Service Announcement,"*** *Federal Bureau of Investigation*

4 ***"State of Email Security 2020,*** *Mimecast*

5 ***"The 2019 Gartner Market Guide for Email Security,"*** *Gartner Group*

6 ***"Information Archiving. Solved. Mimecast Named a Radicati Market Quadrant Top Player,"*** *The Radicati Group*

7 ***"Ten Questions to Ask About Your Office 365 Deployment,"*** *Osterman Research*

8 ***107 Must-Know Data Breach Statistics for 2020,"*** *Varonis*

9 ***2019 Internet Crime Report,*** *Federal Bureau of Investigation*

10 ***"Cost of a Data Breach Report,"*** *IBM Security*

11 ***"How much would a data breach cost your business?"*** *IBM Security*

mimecast™

Mimecast was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together.

We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.