proofpoint.

The Hidden Costs of Free

Why Microsoft 365's Native Security Features May Not Be the Value They Seem

Introduction

As more and more organisations make the move to Microsoft 365, the software giant is pitching the platform as a way to consolidate security, compliance and e-discovery. It promises advanced threat protection, data protection and an online archive that's all about privacy and meeting robust data-retention requirements.[1] And it's all included in your 365 subscription plan. How could anyone turn down that offer?

It may seem like a no-brainer. Why spend more money on third-party email security or archiving when it comes as part of your Microsoft licence? Aren't all email, cloud and compliance solutions pretty much the same?

The answers to those questions aren't as simple as they seem. Microsoft security might be fine for some purposes. But it could also lead to problems and cost more than you expect. That's because not all advanced threat protection or compliance archiving solutions are created equal.

Think about the differences between a camping tent and a house. Both can keep you dry during a sudden rain shower. But in a winter storm with gale-force winds, only one of them will make a good shelter.

In the same way, an advanced email security solution can provide better security and compliance defences in today's stormy cybersecurity environment. Microsoft 365's native offerings just may not offer the level of security and compliance you need.[2]

[1] Microsoft. "Microsoft Compliance Manager (preview)." July 2020.
[2] Gartner. "5 Steps for Securing Office 365." December 2019.

Table of Contents

How Attackers Target Your Microsoft 365 Users

It's no surprise that most targeted attacks start with email.

From phishing to malware, email makes it easy for attackers to exploit the human factor and to steal credentials, data and more. These threats can have a big impact on your bottom line. Today, the average total cost of a data breach stands at $8.64 million in the US, up nearly 33% from 2015.[3]

Here are the four primary ways attackers target your Microsoft 365 users:

Phishing

In the 20-plus years since researchers first identified it as a threat, phishing has morphed into a cottage industry of sorts. Cyber criminals use a wide range of techniques for stealing credentials, funds and valuable information.

Today's phishing is multi-layered and evades many conventional defences. Attacks can be broad-based or highly targeted. Many use *malware*, but others don't. Cyber criminals even deliver phishing emails through legitimate marketing services to evade spam filters and other defences.

About 88% of organisations faced at least one highly targeted spear phishing attack in 2019, and 86% faced at least one business email compromise (BEC) attack. (See "Business email compromise" on this page).[4]

Whatever their tactics, phishing attacks are highly successful. A whopping 65% of US organisations experienced a successful phishing attack last year.[5]

Malware

Today's creative attackers use automated tools to mine information about their targets from public social media profiles. That means attackers know where you work. They know your role, interests, hobbies, marital status, employment history and more.

Attackers use these details to craft convincing email messages enticing you to click on a malicious URL or attachment. Once you click, a malicious payload drops onto your system.

Business email compromise

BEC has emerged as a new and serious threat. The FBI estimates that these attacks have cost victims upwards of $26 billion (in actual and potential losses) since 2016.[6]

These attacks use spoofed emails from someone posing as an authority figure. For example, an email that appears to come from the CEO might ask a staff accountant to:

- Wire funds
- Divert a payment
- Change bank account details

In most cases, the money goes straight to the cyber criminal impostor. The average attack nets nearly $130,000.[7]

BEC doesn't stop at fraudulent transfers, either: attackers may also trick recipients into sending personally identifiable information, payroll details and more.

These attacks set their sights on people at all levels of the corporate ladder, no matter what business unit, department or team they belong to. That's why you may need to extend BEC protection to everyone in your environment, not just some of them.

Email and cloud account compromise

A closely related attack called email account compromise (EAC) takes identity deception a step further. Instead of impersonating a trusted person's email account, an EAC attack hijacks it. The email account doesn't just seem legitimate—it's the real thing.

Having control over a trusted account gives the attacker a trove of information to make the BEC-style attacks that much more effective. EAC can also be a launching pad for all kinds of other attacks that steal data, gain a foothold and spread through your environment.

[3] Ponemon. "Cost of a Data Breach 2020" and "Cost of a Data Breach 2015." July 2020 and May 2015.
[4] Proofpoint. "2020 State of the Phish." January 2020.
[5] Ibid.
[6] FBI. "Business Email Compromise: The $26 Billion Scam." September 2019.
[7] Darla Mercado (CNBC). "New online financial scam costs victims $130K per attack." February 2018.

Why Microsoft's Built-In Security May Not Be Enough

Microsoft 365's built-in security and compliance features may help in limited ways. But they simply may not meet the needs of enterprise-class environments.

Too little email protection can lead to costly breaches that taint your brand, damage your reputation and hurt your bottom line. That's why enhancing your 365 defences is critical to staying secure and compliant.

Today's attacks target people

Cyber criminals know that most people across your organisation use Microsoft 365—including email and cloud apps—more than any other business tool. Many of these users have access to funds or high-value data. But others have vulnerabilities, attack profiles and access privileges that may not always be as obvious.

Attackers use social engineering tactics to lure users into:

- Opening infected attachments
- Visiting malicious sites
- Giving up assets (such as credentials or financial data)

Once they gain entry to a user's system with malware or stolen credentials, cyber criminals can penetrate your environment.

It's no wonder that security has evolved into a boardroom challenge. That's why protecting your Microsoft 365 email and cloud apps is a business-critical decision. And effective cybersecurity focuses on people first.

You can't respond to what you can't see

To discover and respond to attacks effectively, you need the right insights. Unless you have a protection that provides you with deep, detailed reporting, you'll be left searching for the proverbial needle in the haystack.

Blocking threats at the email gateway and in the cloud has two critical advantages. First, you gain understanding about the whole attack, not just the final stages of it after the damage is done. Second, by catching threats early—ideally before they reach your users—you can stop them before they compromise your environment.

Siloed security, access and compliance is not sustainable

In the ever-evolving threat landscape, cyber criminals coordinate attacks across multiple vectors. That's why a well-orchestrated defence is vital to a good security posture.

An effective solution must integrate with the rest of your security, access control and compliance ecosystem. That means everything from your email gateway to your data loss prevention (DLP) system to cloud access security broker (CASB) to your identity management platform.

Smart and automated coordination can help you prevent, detect and respond to threats that target people through Microsoft 365.

Security

As users migrate to OneDrive, Teams and other Microsoft 365 productivity apps, data security can be a challenge. You need to be able to identify and defend the data that your people create, access and share.

That's not always easy with Microsoft 365 alone. The platform's native threat detection may not provide the visibility you need into cyber threats, user activity and data movement across email, the cloud and endpoints.[8]

Access

All users pose some degree of risk to your organisations. But everyone is risky in unique and ever-evolving ways. That's why one-size-fits-all security and data-access policies don't protect against threats that target people through Microsoft 365.

You need access and data controls that factor users, groups, threat intel and context in real time. Only then can you prevent and respond to data misuse across channels, including cloud apps and email.

Adaptive access and data controls are based on users, groups, threat intel and context. You may need granular control for some groups and wider-scale controls for larger groups of users. In either case, being able to easily adjust security as needed helps you prevent and respond to data misuse across channels, including cloud apps, email and endpoints.

Compliance

Juggling multiple sets of policies, incident queues and enforcement tools is not an effective way to protect your sensitive information and stay compliant.

Complying with archiving, data-retention and e-discovery rules is about more than just storing unprotected data within the Microsoft 365 ecosystem. It's about email, social media, enterprise collaboration (such as Yammer and Teams) and even data stored on users' devices.

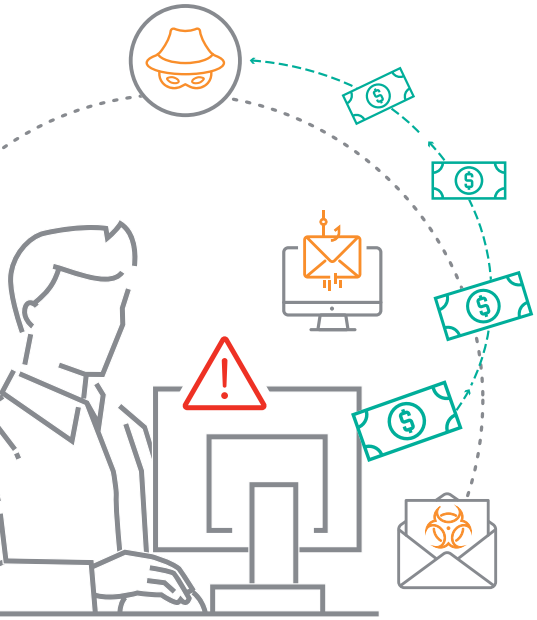
Choosing the lowest-cost archive to save some money upfront can wind up costing more in the long run. That's especially true for organisations with complex compliance, supervision and e-discovery needs.

Unanticipated email outages can have huge business impact

Today's business depends on reliable email access. An unexpected outage could have costly consequences. That's why ensuring around-the-clock access to email is critical.

Microsoft 365 outages are a fact of life. But they don't have to grind your business to a halt.

[8] Osterman Research. "Using Third-Party Solutions with Office 365." September 2019.



Calculating The Hidden Costs Of Microsoft 365 Security

The old adage "You get what you pay for" applies to Microsoft's security offerings. Lack of adequate security for your Microsoft 365 deployment could cost you time, information, money and even your reputation. Here's how augmenting Microsoft 365's native capabilities can keep you more compliant and secure.

For security teams

Security has always been a tough job. Today's advanced threats make it even tougher. As compliance regulations and high-profile breaches push security up to the board level, the conversation is not just about efficacy. It's about having the visibility to understand what threats are targeting your people.

Not having the visibility and insights that you need to address security issues across the organisation can result in lost time.

According to Ponemon Institute, the biggest financial consequence to organisations that experienced a data breach is lost business.[9] These costs can vary widely based on the quantity and type of assets lost.

Consider the following:

- ☐ How much productivity is spent cleaning up damages from compromises by preventing threats that could have otherwise been blocked?
- ☐ How much time is spent identifying and remediating compromised accounts?
- ☐ How much time does your team spend investigating, prioritising and confirming threats? (This can range from 2–16 hours per targeted user.)
- ☐ How much time is spent cleaning up emails containing malicious attachments or URLs from your users' mailboxes?
- ☐ How do you quantify the risk introduced as a result of prolonged exposure with these emails accessible to users?
- ☐ How much time is lost from disjointed security enforcement points to contain threats and protect your organisation's reputation? (This can range from hours to days per alert.)
- ☐ How much extra time does limited visibility add to your efforts trying to understand threats targeting your environment?
- ☐ What is the security impact of users going to personal mail when Office 365 email experiences an outage? (One survey pegged the cost for high-priority app downtime at $67,651 per hour.[10] Some Microsoft outages have lasted days.[11])

[9] Ponemon. "Cost of a Data Breach Report 2020." July 2020.

[10] Scott Bekker (Redmond Channel Partner). "Study: Hourly Cost of Application Downtime Nearly $68K." June 2020

[11] Ed Targett (Computer Business Review). "Microsoft Office 365 Outage: Day Two as Enterprise User Grumbles Grow." January 2019.

For IT departments

If you're an IT administrator, consider the costs of outages and support.

Uptime and service availability

While Microsoft 365 promises a 99.99% uptime, it does have outages. (A quick glance at Microsoft's own status Twitter feed shows just how common service issues are.)

As you look to boost your Microsoft 365 security and minimise these costs, ask yourself these questions:

- ☐ How heavily does your business rely on email? What is the impact if emails from customers or prospects are lost due to email outage?
- ☐ How often is your Office 365 email flow interrupted?
- ☐ How quickly is IT alerted of an outage?
- ☐ Do you have enough data and visibility to set expectations on when service will be restored?
- ☐ What security and compliance risks are introduced when well-intentioned users resort to personal email to "get work done?"

Message trace, non-deliver report (NDR)

"What happened to my email message?" is a common question fielded by email IT and security professionals every day.

Take a deep look at your process and ask:

- ☐ How much time can you afford to spend supporting these issues?
- ☐ How often are message logs indexed? How long are logs retained?
- ☐ Are search query results returned in minutes or hours?
- ☐ Does the search experience differ in older versus newer logs?
- ☐ Do you have the required search criteria available to find logs quickly? Are the details returned from the search sufficient?
- ☐ What is the process for calling support for more detailed information?
- ☐ What is the impact of the false positives on the volume of message traces and time required?

Time spent on email and machine cleanup

IT can spend hours and even days reimaging infected machines when email-related security events occur and systems are compromised.

Further, IT should remove these emails to prevent re-infection, which occurs when a user unknowingly re-accesses the content, or even forwards it to another user.

This process hurts both IT and user productivity, typically a full day per incident. Ask yourself:

- ☐ How many machines are undergoing unnecessary or avoidable reimaging?
- ☐ Does IT have the tools to confirm infections and to prioritise machines that were exposed but not compromised?
- ☐ How much time does IT spend on message cleanup?

For compliance staff

Compliance is serious business. The consequences of failing to comply can be costly and hurt your business.

Archiving

At the data centre level, Microsoft 365 complies with major regulations. These mandates include Europe's General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), ISO 27001 and others.

But the platform has some serious flaws when it comes to archiving and supervising email data and making it readily accessible when there's a legal dispute or when it's audit time. Not having legally defensible records retention and workflows can drain time and resources. It may even result in litigation costs.[12]

You'll likely need a Microsoft 365 plan that includes compliance features or purchase them as an add-in subscription to fully comply with mandates from any of the following:

- US Financial Industry Regulatory Authority (FINRA)
- US Securities and Exchange Commission (SEC)
- Investment Industry Regulatory Organisation in Canada (IIROC)
- UK Financial Services Act

These rules aim to protect investors by making sure the US, UK and Canadian security industries operate fairly and honestly. Fines for non-compliance with can run well into the millions.[13] Other costs include the cost of deploying additional security measures, audits and potential reputational damage.

As you evaluate the capabilities of Office 365, ask these important questions:

- ☐ If your organisation is involved in a legal dispute, will Office 365 enable you to provide records of all communications and transactions conducted by specific users including social media and enterprise collaboration platforms? What happens if you have multiple cases in progress?
- ☐ How well are you able to put content on legal hold when a legal dispute happens?
- ☐ How much time does it take for IT to perform e-discovery and data export? How quickly do searches execute? Does Microsoft offer a service level agreement (SLA) that defines the parameters of this key capability? Where does the processing of the search occur?
- ☐ Once you determine the data set that you want to export, can you upload the files to a specified FTP site in an automated way? Or do you need schedule time to finish this part of the workflow manually? What are the consequences of delay in getting the required data to review teams?
- ☐ Are you able to capture and preserve all of the compliance content your organisation generates? What about data from social media platforms?
- ☐ How well are you able to supervise and monitor content? Several regulations require the monitoring and sampling of content. Does it use the latest technology, or does it simply rely on basic keywords matching?

[12] Osterman Research. "Using Third-Party Solutions with Office 365." September 2019.

[13] Ann Marsh (Financial Planning). "Interactive Brokers fined $38M by 3 regulators for compliance lapses." August 2020.

Information protection

Breach statistics in all sectors are worth paying attention to. Enterprises are always at risk of data loss. Malicious insiders can leak it. External bad actors can steal it. Even well-intentioned employees may unknowingly expose vital company assets.

In 2018 alone, 79 data breaches hit US military and government entities, exposing 5,302,846 records.[14] Overall, the total number of reported breaches rose 17% in 2019 to 1,473.[15]

Take business email compromise (BEC) and email account compromise (EAC), which have cost victims more than $26 billion in potential losses since 2016.[16] Spoofers have tricked victims into wiring money, diverting payroll, sending vendor payments to the wrong account and exposing sensitive information.

Concern about the liability stemming from data breaches has made security a boardroom issue. With this in mind, you need to look at Microsoft 365 security with a critical eye. Review its ability to find sensitive data (including multiple file types), resolve issues across all channels and enforce and report policy issues. Being able to apply policies to outbound mail, with the workflow to manage incidences, should serve as an important layer of security, not just compliance[17]

Here are some questions to ask:

- ☐ Can you detect sensitive data across email, cloud and endpoints—and the breadth of file types that may contain sensitive information?
- ☐ Can you quickly pinpoint what content triggered a policy alert?
- ☐ Do you have an incident response workflow in place to remediate the situation?
- ☐ Does your automated response enable remediation across multiple channels, including email, file share and Microsoft SharePoint sites? Do you need a separate DLP solution to reduce the attack surface across each of these channels? How are you keeping these policies synced and reporting consistent?
- ☐ When sensitive data is detected, how is encryption handled? What type of granularity do you have to revoke messages to the wrong recipient? What percentage of encrypted emails do you anticipate being viewed from mobile devices? What is the recipient experience?
- ☐ Can you see who has access to privileged data and systems and can you create policies based on individuals and groups of people?
- ☐ Can you quickly identify risky third-party applications your users' access and protect your organisation from these apps?

[14] Identity Theft Resource Centre. "10,000 Breaches Later: Top Five Military and Government Data Breaches." October 2019.

[15] Identity Theft Resource Centre. "2019 End-of-Year Data Breach Report." February 2020.

[16] FBI. "Business Email Compromise: The $26 Billion Scam." September 2019.

[17] Osterman Research. "Using Third-Party Solutions with Office 365." September 2019.

Reduced Risk, Streamlined Operations And Lower Cost—The Proofpoint Difference

Today's complex and ever-changing threat and compliance landscape requires a new approach to threat protection. That's why we offer a unique people-centric approach that gives you:

- The industry's most effective threat protection
- Actionable visibility
- Data access and controls
- Excellent user experience
- A modern approach to compliance challenges

Here's how we help you enhance Microsoft 365.

Better, faster email protection

With an average analysis time of less than three minutes, we block malicious attachments before your users have a chance to interact with them—and without getting in users' way.[18] And we support a wide range of file types, including PDFs and HTML—not just Office files.

Predictive URL analysis scans and neutralises unsafe URLs before they're delivered and when users click. You can block attachments that contain unsafe URLs and rewrite suspicious URLs whether they appear in text files (.txt), rich-text files (.rtf) or HTML.

Our integrated, holistic solution also stops non-malware threats. It gives you deep visibility into malicious activities and user behaviour. And it automates key parts of the incident response process to help you protect your users at scale.

For high-risk users and websites, our URL Isolation technology opens unknown links from email in a safe, self-contained environment to keep threats out of your environment.

Data security across email and the cloud

We make it simple to create, apply and enforce unified policies across email and cloud-based apps to keep your data safe and compliant.

Built-in algorithmic analysis, our smart identifier engine and dictionaries let you focus on setting and maintaining your organisation's unique data policies. Out-of-the-box DLP workflows also make it easy to find, manage and report violations.

[18] Proofpoint. "Proofpoint Email Protection Data Sheet." April 2020.

Complete protection against BEC and EAC

BEC and EAC attacks come in many forms, and no one approach can stop them all. A security tool may stop one or two tactics but still leave you exposed to a multitude of others.

That's why you need a solution that addresses every angle of these deceptive and hard-to-detect threats. Our integrated, holistic solution addresses all attacker tactics. It gives you deep visibility into malicious activities and user behaviour. And it automates key parts of the incident response process to help you protect users at scale.

Protection against 365 account takeovers

Through our multilayered approach, we help you protect your 365 account with real-time alerts of suspicious activity, automated remediation and risk-based access controls.

When incidents occur, you can investigate past activity and alerts with our intuitive dashboard. Our robust policies alert you to issues in real time, remediate compromised accounts, quarantine malicious files and apply risk-based authentication when needed.

Cloud visibility and security that works

We take a people-centric approach to protecting against cloud threats, discovering shadow IT and governing cloud and third-party OAuth apps.

We go far beyond native 365 security to safeguard users, sensitive data and cloud apps from external threats and compliance risks. Identify your Very Attacked People™ and apply risk-based controls to keep their accounts safe.

Lightning-fast incident response at scale

Our Threat Response Auto-Pull (TRAP) solution removes malicious email from your users' inboxes—even if it has already been delivered or forwarded to colleagues.

TRAP also enriches security alerts with actionable forensics intel that lets your security team verify and resolve incidents faster and more efficiently. And we support a wide range of email systems—not just Microsoft 365—and integrate with the security tools you already use, including Okta and CyberArk.

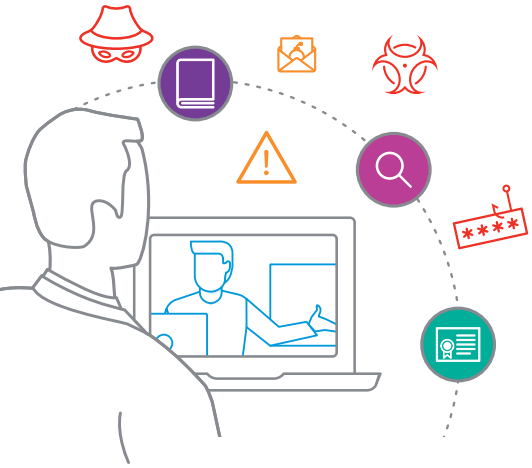
Intelligent archiving at warp speed

No matter how large your archive gets, we guarantee that your searches will take 20 seconds or less—not minutes or hours.[19]

Our cloud-based archive supports more than 500 files types[20] in the cloud and on-premises, not just email. And we don't limit the number of e-discovery cases, legal holds, and data exports you can include—whether its 10,000 mailboxes or 100,000 (or more).

[19] Proofpoint. "Proofpoint Enterprise Archive Data Sheet." March 2018.

[20] Ibid.



Security training that makes users aware, not annoyed

We offer a vast library of engaging content based on real-world attacker techniques. It's informed by our own threat intelligence. And it's flexible enough to be tailored to your organisation's unique security challenges.

Beyond foundational awareness training, we offer phishing simulations and point-in-time follow-up training for users who fall for the bait. We make it easy to track and report progress over time to help you identify areas of improvement and help your users thrive.

World-class support

Every purchase includes full installation and customisation of the solution along with access to the latest industry trends and best practices. We offer 24/7/365 support after deployment—no complicated service add-ons.

Our company earns a sustained customer satisfaction rate of more than 95% and yearly renewal rate of more than 90%.[21] It's no wonder that our customers include more than half of the Fortune 100.

Complete, fully integrated security that streamlines operations

Our complete, integrated security platform combines powerful, effective cloud and email protection to solve today's most pressing challenges. We also integrate with best-in-class security vendors such as Palo Alto Networks, Okta and Crowdstrike to streamline your workflow and help your security team work better and faster.

Together, it all adds up to unified, people-centric security that protects your cloud deployment. Our proven approach to security and compliance for Microsoft 365 reduces your risk, frees up resources, cuts costs and makes your security operations more effective and efficient.

Take The Next Steps

Learn more about Proofpoint and how we can help you enhance your Microsoft 365 deployment with people-centric protect and compliance across email, the cloud and endpoints at https://www.proofpoint.com/us/solutions/microsoft-365-security-compliance.

[21] Frost & Sullivan. "Frost & Sullivan Recognizes Proofpoint as the Global Email Security Market Leader for Fifth Consecutive Year.' August 2019.

LEARN MORE

For more information, visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0501-004-01-01 09/20