EXECUTIVE BRIEF

proofpoint™

THE HIDDEN COSTS OF MICROSOFT OFFICE 365 SECURITY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

You've made the big decision to migrate to Microsoft Office 365. Its array of cloud collaboration makes this a great decision. Yet at the same time, Microsoft is also pitching Office 365 as a way to consolidate your security, compliance, and e-discovery platforms. It is promising advanced threat protection, data protection, and an online archive that's all about privacy and meeting robust data-retention requirements. And it's all included. How can you turn down that offer?

On the surface, the prospect of free security for your Office 365 deployment seems promising. Why spend more money on third-party email security or archiving when it comes as part of your Office 365 license? Maybe fresh memories about the data loss prevention (DLP) initiative that never really got off the ground has you questioning whether you really need robust capabilities to protect your sensitive assets.

At a deeper level, you may be asking yourself: "Aren't all email security solutions pretty much the same?"

If it were only that simple. Free Microsoft security may be fine for certain purposes. But it may end up causing more problems and costing more than you bargained for. Not all advanced threat, email security, or archive solutions are created equal.

Consider the childhood story of The Three Little Pigs. In concept, the straw house and the brick house might seem comparable. They both have walls, a roof, and a door. But when the wolf huffed and puffed, only one of them withstood the gusts.

When it comes to truly comprehensive security for Office 365, Microsoft's native security and compliance offerings can't compare with the enhanced protection of an advanced email security solution.

MAKE EMAIL SECURITY FOR OFFICE 365 A TOP PRIORITY

Phishing was first recorded as a term on January 2, 1996. Twenty years later, it has morphed into a highly sophisticated attack used to steal funds and valuable information. Today's phishing is multi-layered. It evades many conventional defenses. The attacks can be broad-based or highly targeted. Many use malware, but others don't. Cyber criminals even deliver phishing email through legitimate marketing services to get past spam filters and other defenses. No wonder 91% of targeted attacks start with email.[1]

Today's creative attackers use automated tools to mine information about their targets from social media profiles, which are often public. 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 a convincing email message to get you to click on a malicious URL or attachment. Once you click, a malicious payload drops on your system.

But, beyond the tactics you're likely familiar with, a new technique has emerged as a serious threat: business email compromise *(BEC)*. BEC

PROVEN SUCCESS AT LEADING ENTERPRISES

"Customer service and support has been excellent. The product works very well and has kept us phish-free for a year now."

—Kenneth Brown, CIO, Whitworth University

"Proofpoint has given us protection from standard bulk campaigns in Office 365 emails, giving us our time back to find more evil things.

—CISO, Global 500 Manufacturer

"Office 365 allowed too many legitimate phishing messages through. We had users fall victim, despite all the end user training to not click and enter credentials. With Proofpoint, efficacy has greatly improved to the point where I can't recall the last time it happened."

—Network Administrator, Private University

"Using Proofpoint to secure our Office 365 email has saved us time and money that would have otherwise been spent on rebuilding compromised systems."

—CSO, Fortune 500 Banking Company

attacks are spoofed emails from someone posing as an authority figure: a CEO, for example, that ask a colleague, such as a staff accountant, to wire funds. Recipients, thinking that they're acting on behalf of a manager, send the funds or information—you guessed it—straight to the cybercriminal impostor. But BEC doesn't stop at fraudulent transfers. The attackers are also tricking recipients into sending PII, payroll information, and more.

Regardless of their tactics, phishing attacks are highly successful. According to the Verizon 2016 *Data Breach Investigation Report*, users opened 30% percent of phishing messages, up from 23% in last year's report.[2] And the SANS Institute reports that 95% of network attacks result from spear phishing.[3]

CYBER CRIMINALS KNOW THAT PEOPLE USE EMAIL MORE THAN ANY OTHER COMMUNICATION TOOL

All this can add up to a big hit to your bottom line. An IBM report released this year reveals that the average total cost of a data breach now stands at $4 million, up 29% from the 2013 average.[4]

How does this relate to your Office 365 migration? The heart of Office 365 is Microsoft Exchange Online email. In a number of areas, Office 365's built-in security, compliance, and archiving capabilities don't meet the needs of enterprise-class organizations.

Too little email protection can lead to costly breaches that taint your brand, damage your reputation and hurt your bottom line. That's why a strong defense for Office 365 email matters.

ATTACKS TARGET PEOPLE

More attacks come in via email than through any other vector. That's because cyber criminals know that people use email more than any other communication tool.

The bad guys typically target individuals in HR, IT, or finance who have access to high-value data. These clever cyber criminals use social engineering tactics to lure users into giving up assets (i.e. credentials, financial fraud), visiting malicious sites or opening infected attachments. Once the malware gains entry to a user's system, cyber criminals can penetrate corporate networks and exfiltrate treasure troves of valuable sensitive information and assets. That's why deploying a secure email gateway is a business-critical decision. It's no wonder that security has evolved to a boardroom challenge.

YOU CAN'T RESPOND TO WHAT YOU CAN'T SEE

If your email gateway doesn't provide the right insight and deep, detailed reporting, you can't discover and respond to indicators of compromise (IoCs) effectively. You're left searching for the proverbial needle in the haystack.

Blocking threats at the gateway gives you two critical advantages. First, you glean insights about the whole attack, not just the final stages of the attack, when it has reached your network. And by catching threats at the gateway, you can stop them before they have compromised your environment.

SILOED SECURITY IS NOT SUSTAINABLE

Connecting threat intelligence with prevention and response efforts is often labor-intensive, time-consuming and costly. Without smart automated orchestration, efforts to prioritize and contain the impact of threats can be slow and prone to error.

FRAGMENTED DATA LOSS PREVENTION DECREASES YOUR CHANCE OF SUCCESS

Basic data loss prevention (DLP) features are another part of the core Office 365 offering. Already viewed dubiously among many C-level executives, DLP has been known more for its failures than success.

DLP deployments have roughly a 20% success rate, even with immense resource allocation. The likelihood of success is further eroded by single-channel (typically email) point DLP approach. Juggling multiple sets of policies, incident queues, and enforcement tools is not an effective way towards a successful information protection practice.

ARCHIVING MUST BE DEFENSIBLE AND E-DISCOVERY READY

In the same way that you want to ensure that malicious content is kept out of your organization, you also want to ensure that you can retain and archive business-relevant content in a way that's legally defensible. And you'll want to be able to meet your e-discovery obligations quickly, cost-effectively and defensibly.

Complying with archiving and e-discovery rules is about more than just storing unprotected data within the Office 365 ecosystem. It's about email, social media, enterprise collaboration (such as Yammer), and even data stored on users' laptops. Choosing the lowest-cost archive to save some money upfront can wind up costing more in the long run through penalties and higher litigation readiness costs.

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 business-critical email is critical.

CALCULATING THE HIDDEN COSTS OF BUNDLED SECURITY

More often than not, bundled goods may also create significant and sometimes hidden costs with both short-term and long-term consequences. The old adage "You get what you pay for" certainly applies to Microsoft's security offerings. Lack of adequate security for your Office 365 deployment could cost you time, information, money, and even your reputation.

FOR SECURITY TEAMS

Security has always been a tough job. Today's advanced threats make it even tougher. As compliance regulations
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 business. Not having the visibility and insights that you need to address security issues at an organizational level can result in significant lost time.

NOT HAVING THE VISIBILITY AND INSIGHTS THAT YOU NEED TO ADDRESS SECURITY ISSUES AT AN ORGANIZATIONAL LEVEL CAN RESULT IN SIGNIFICANT LOST TIME.

According to Ponemon Institute, the biggest financial consequence to organizations 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 does your team spend investigating, prioritizing, 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 end users?
- How much time is lost from disjointed security enforcement points to contain threats and protect your organization'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? Office 365 downtime is one of the top concerns cited by organizations and leading analysts.[11]

FOR IT DEPARTMENTS

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

> "USING PROOFPOINT TO SECURE OUR OFFICE 365 EMAIL HAS SAVED US TIME AND MONEY THAT WOULD HAVE OTHERWISE BEEN SPENT ON REBUILDING COMPROMISED SYSTEMS."
>
> —CSO, Fortune 500 Banking Company

UPTIME/SERVICE AVAILABILITY

Forrester Research cites availability as one of the top challenges organizations face with Office 365 email.[10] According the most recent industry calculations, the overall cost of an outage is about $5,600 per minute, or more than $300,000 per hour.[5] As you look to boost your Office 365 security and minimize 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 for dealing with these issues:

- How much time can you afford to support 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?
- Are the necessary 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

When email-related security events occur and systems are compromised, IT can spend hours and even days reimaging infected machines. If malicious email content is detected, IT needs to manually remove those emails from user mailboxes after the messages have already been delivered. Failure to do so may result in re-infection when users re-access malicious content—or the potential threat can be propagated if it is forwarded to other users. This process impacts both IT and user productivity, typically a day per incident. Ask yourself:

- How many machines are undergoing unnecessary or avoidable reimaging?
- Does IT have the tools to confirm infections and to prioritize 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 center level, Office 365 complies with major regulations. These mandates include European Union data protection laws, the Health Insurance Portability and Accountability Act (HIPAA), ISO 27001, and others. But Office 365 has some serious flaws when it comes to archiving email data and making it readily accessible when there's a legal dispute or at audit time. Not having legally defensible records retention and workflows can drain time and resources and even result in accusational costs.

The UK Financial Services Act requires its members to retain records for six years. Fines for noncompliance with the Financial Industry Regulatory Authority (FINRA), which aims to protect investors by making sure the U.S. security industry operates fairly and honestly, can run well into the millions.[6] Added 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 organization is involved in a legal dispute, will Office 365 enable you to provide records of all communications and transactions conducted by specific individuals? What happens if you have multiple cases in progress?
- 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 (SLA) agreement 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?

INFORMATION PROTECTION

Breach statistics are staggering across all sectors. Enterprises are always at risk of data loss. Malicious insiders can leak it, external bad actors steal it, and even well-intentioned employees may unknowingly expose vital company assets. The U.S. government suffered 61,000 cybersecurity breaches in 2014 alone.[8] 91% of healthcare organizations have experienced at least one breach over the past two years according to the Identity Theft Resource Center.[7]

Take business email compromise (BEC), which has escalated beyond financial fraud. The spoofers have duped legal departments into sending out sensitive information. They have tricked human resources staff into sending W-2 forms.[9]

Concern about the liability stemming from data breaches has made security a boardroom issue. With this in mind, you need to look at Office 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.

Applying policies to outbound mail, with the workflow to manage incidences serve as an important layer of security, not just compliance.

Here are some specific questions to ask:

- Can you detect sensitive data across the breadth of file types that may contain sensitive information?
- Can you quickly identify 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?
- Where do you need DLP coverage? If you need DLP beyond email, how much effort is required to keep policies consistent and get a consistent reporting across multiple DLP tools?
- 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 to be viewed from mobile devices? What is the recipient experience?

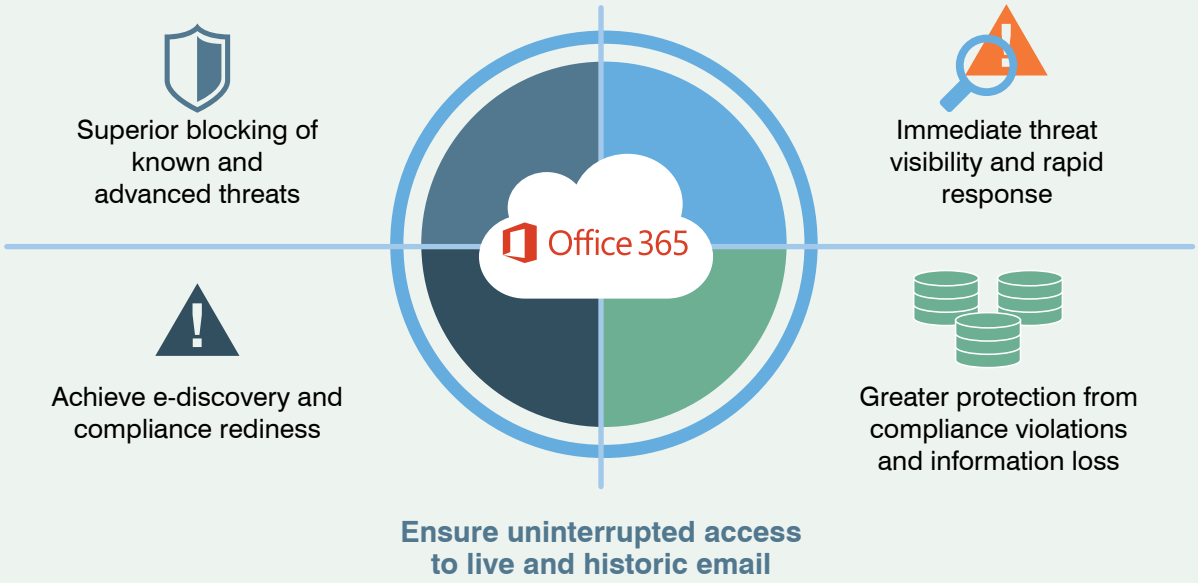
THE PROOFPOINT DIFFERENCE

Today's complex and ever-changing threat landscape requires a new approach to threat protection. When it comes to email, you need much more than just reputation checks against URLs and archaic message trace capabilities. While important, these techniques alone don't enable threat visibility, provide campaign intelligence, or help you verify and contain compromises.

Superior threat protection, immediate threat visibility detection, and rapid response are absolute necessities. Proofpoint's email security technology far surpasses the native Office 365 capabilities, and provides you with the robust protection you need across multiple dimensions. Our award-winning customer support reflects our commitment to your success. With Proofpoint, you get:

- Superior blocking of both known and advanced threats
- Immediate threat visibility to help you respond faster
- Strong data protection to safeguard valuable information and foster compliance
- Capabilities that enable e-discovery and aid compliance
- Uninterrupted access to active and historic email for forensic purposes

HOW PROOFPOINT HELPS



ADVANCED TECHNOLOGIES BOOST YOUR OFFICE 365 DEFENSE

Here's what makes Proofpoint more powerful than Office 365's built-in defenses.

INDUSTRY LEADING EFFICACY FOR ADVANCED THREATS

Security is our business. With the sophistication of today's attacks, more is needed. Proofpoint uses a combination of static and dynamic techniques to catch even the most advanced threats. The sandbox constantly adapts to detect new attack tools, tactics, and targets. It applies to URLs and attachments in email to protect you from banking Trojans, ransomware, and other attacks targeted at your organization.

Our unique predictive analysis preemptively identifies and sandboxes suspicious URLs based on email traffic patterns. This drastically minimizes the risk of a patient-zero case from a previously unknown malicious URL.

IMPOSTOR EMAIL CONTROLS

Drastically reduce exposure presented by advanced spoofing and BEC attacks. We go far beyond Microsoft's suggested use of DKIM/DMARC. Our solutions use proprietary machine learning, communication trend baselining, malformed message attribute analysis, and pre-built policies for holistic detection and visibility.

LOW-PRIORITY INBOX

We provides graymail classification with a high degree of accuracy and responsive learning of individual preferences. Granular visibility via user digests gives employees quick visibility into emails that have been filtered and categorized into low priority inboxes. And as their needs change, they can update their preferences directly through the digest.

DETAILED FORENSICS AND THREAT INTELLIGENCE FOR CAMPAIGN INSIGHTS

Get immediate insight into bad actors, the tools and techniques they are using, and the people they are targeting. You gain an understanding of the bigger picture around the attack campaigns targeting your organization.

AUTO-PULL SAVES CLEANUP COSTS

Save hours per incident, by taking in real-time threat convictions and automatically, or on-demand, remove emails into an user inaccessible quarantine. Works for both Office 365 Exchange Online and Exchange mailboxes.

INTEGRATION WITH YOUR SECURITY ECOSYSTEM

We work closely with a large ecosystem of security vendors to quickly contain threats that have an impact beyond your Office 365 deployment, including:

- Integration with Palo Alto Networks wildfire for additional threat intelligence
- Security information and event management (SIEM) tools, such as Splunk, for threat intelligence and detection. Real-time streaming can help you correlate email with network events to detect and respond to threats faster.
- Yield immediate protection. Apply email threat intelligence seen in your environment at the at the network level, leveraging your existing enforcement tools to close the gap between threat detection and protection. Stop:
  - Infections from spreading from one system to another
  - Control signals from reaching malware
  - Sensitive data from reaching external sites

Proofpoint automates containment, using your existing enforcement tools to close the gap between threat detection and protection.

ENFORCEMENT DEVICES

- Cisco ASA
- Palo Alto Networks
- Check Point
- Cisco IOS
- Juniper SRX (JUNOS)
- Fortinet FortiGate
- Blue Coat
- Microsoft Exchange/ O365
- OpenDNS
- CyberArk
- Imperva

ENDPOINT FORENSIC COLLECTION AND COMPROMISE VERIFICATION

Not all attacks result in compromise. That's why you need insight into where to prioritize efforts. Automatic IoC forensic collection from the endpoint lets you compare a forensic snapshot of the endpoint to a sandbox forensics version to help verify infections and gain threat insights. You can also check for evidence of past infection on the target machine, and scan on demand to check for IoCs on other machines. Automating data collection improves your quality of response.

EMAIL DATA LOSS PREVENTION

DLP projects are prone to failure. Focusing on the channels you care about most with a unified set of policies and incident response queues dramatically increase the likelihood of success. We protect multiple content types, not just Office 365 files. Beyond "set-and-forget" DLP, we also offer deep insights into compliance violations. Policies can be fine-tuned to meet your organization's needs and priorities. A robust incident response workflow for administrators and users makes it easier to take swift action when incidents arise.

> "OFFICE 365 ALLOWED TOO MANY LEGITIMATE PHISHING MESSAGES THROUGH. WE HAD USERS FALL VICTIM, DESPITE ALL THE END USER TRAINING TO NOT CLICK AND ENTER CREDENTIALS. WITH PROOFPOINT, EFFICACY HAS GREATLY IMPROVED TO THE POINT WHERE I CAN'T RECALL THE LAST TIME IT HAPPENED."
>
> —Network Administrator, Private University

EMAIL CONTINUITY

Keeps users connected and productive in the event of an Office 365 email outage. This always-on insurance policy for critical business communications enables users to continue sending and receiving email without requiring any action from IT. End users get full access either natively within Outlook or via Web portal. The most recent 30 days of email can be made available in the end user inboxes. All emails are restored, with headers intact, to the email server. That means archiving and forensics for legal purposes are never a problem.

EMAIL ARCHIVING

Most organizations are requires to ensure legally defensible retention of content in Office 365, including Exchange Online, OneDrive for Business, and Skype for Business. The archive features provided by Microsoft are much more about storage management than e-discovery and compliance.

We go far beyond Microsoft Exchange Online Archive. We guarantee immutable archive storage and exhaustive indexing of more than 500 attachment types, including non-proprietary Microsoft file formats. The robust e-discovery workflow and guaranteed 20-second search performance makes forensics faster and easier. Our proprietary Double-Blind Key Encryption architecture ensures that you retain complete control over the encryption key for data kept in our cloud-based storage.

STEP UP YOUR OFFICE 365 SECURITY WITH PROOFPOINT

Microsoft may insist that all the security you'll ever need is available for with your Office 365 license. But as we've seen, the hidden costs and risks can be significant. As the volume and sophistication of advanced threats continues to evolve more rapidly than even before, you must protect your people, data, and brand from advanced attacks and compliance risks.

Our security solutions provide with industry-leading security, compliance, and email continuity capabilities for your cloud-based Office 365 deployment that far exceed Microsoft's native protection. With Proofpoint, you can take advantage of the freedom, flexibility, and cost savings of Office 365—without sacrificing your ability to keep users connected and protected.

For more information, visit: www.proofpoint.com/o365

[1] Kim Zetter (Wired). "*Hacker Lexicon: What Are Phishing and Spear Phishing?*" April 2015.
[2] Verizon. "2016 Data Breach Investigations Report." April 2016.
[3] Neal Weinberg (Network World). "*How to blunt spear phishing attacks*." March 2013.
[4] Ponemon Institute. "2016 Cost of Data Breach Study: Global Analysis." June 2016.
[5] Andrew Lerner (Gartner). "*The Cost of Downtime*." July 2014.
[6] Financial Industry Regulatory Authority (FINRA). "*FINRA Fines Scottrade $2.6 Million for Significant Failures in Required Electronic Records and Email Retention*." November 2015.
[7] Identity Theft Resource Center.
[8] Ian Bremmer (Time). "*These 5 Facts Explain the Threat of Cyber Warfare.*" June 2015.
[9] FBI. "*FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals*." March 2016.
[10] Proofpoint. "*Six Key Capabilities for Securing Office 365 Email*." May 2016.
[11] Proofpoint. "*Is Microsoft Office 365 Secure*?" 2016.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint™ www.proofpoint.com