proofpoint.

Securing Microsoft 365

10 Reasons Organizations Choose Proofpoint to Protect Their Cloud Deployment

proofpoint.com

INTRODUCTION

Organizations are moving to the cloud and must support an increasingly remote and distributed workforce. For many, Microsoft 365 is a whole new way of doing business—one that requires a whole new approach to security and compliance.

Today's cyber attacks target people, no matter where they're working or what device they're using. Microsoft 365 customers are turning to Proofpoint for a people-centric approach to security and compliance. Here's why.

Better, faster

email protection

1

The best cyber defense is one that stops threats where they start. That's why we help Microsoft 365 customers stop more threats and unwanted email—before it reaches users' inboxes.

Today's attacks come in many forms. We can help stop all of them.

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. We support a wide range of file types, including PDFs and HTML—not just Office files.

Our malware protection also integrates with our URL-detection features. Our predictive URL analysis scans and neutralizes 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.

But some email attacks don't use malware at all. That's why our integrated, holistic solution also stops business email compromise (BEC) and email account compromise (EAC). We address all attacker tactics. It gives you deep visibility into malicious activities and user behavior. And it automates key parts of the incident response process to help you protect your users at scale.

We catch more URL threats with multistage sandboxing that uses static, dynamic, and analyst-assisted execution. We detect both malicious code and credential phishing websites—even those that use sandbox-evasion techniques other virtual-machine approaches miss.

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

2

Stay compliant and avoid fines without the headaches of traditional DLP. 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 organization's unique data policies.

Our out-of-the-box DLP workflows also make it easy to find, manage and report violations. With our solution, you also get advanced features that take the headaches out of data security and compliance. Here are just a few:

- Read receipts
- Multi-column exact data matching
- Push/pull encryption
- Easy key revocation
- TLS fallback features

No matter how complex your data security needs are, you won't be hindered by technical roadblocks.

Complete protection

against business email compromise and email account compromise

3

Some threats don't use malicious files. Business email compromise (BEC) and email account compromise (EAC) are two sides to a $26 billion problem.[1]

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

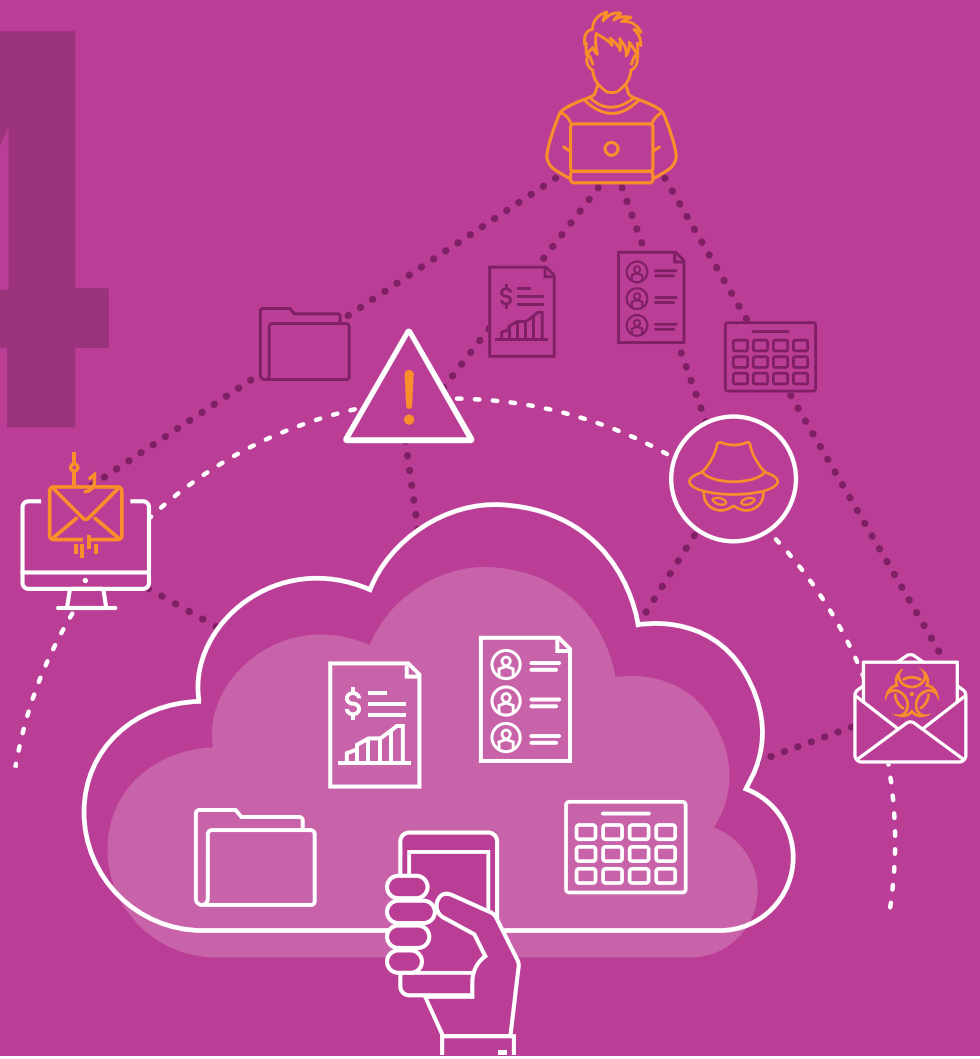
That's why you need a solution that addresses every angle of these deceptive and hard-to-detect threats. Our integrated, holistic solution addresses all attacker tactics. It gives you deep visibility into malicious activities and user behavior. And it automates key parts of the incident response process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

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

Protection against

365 account takeover

4



In the wrong hands, your cloud account can be a weapon.

Cyber attackers who take over your users' accounts have free rein over any sensitive data they have access to. And anyone who controls their email account can exploit people who trust it—inside and outside of your environment.

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

The "people perimeter" has replaced the old network perimeter. Your people share sensitive data without oversight, use unsanctioned cloud apps and countless personal devices.

That's why we take a people-centric approach to protect against cloud threats, discovering shadow IT and governing cloud and third-party OAuth apps.

With rich cross-channel threat intelligence and user-specific contextual data, 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. Classify your sensitive data and detect overly broad file permissions and unauthorized data sharing. Discover what cloud app and services your people are using and govern what data and resources they can access.

Lightning-fast

incident response at scale

6

The longer a threat lingers in your Microsoft 365 environment, the more damage it can do.

That's why fast, efficient incident response is critical to keeping your organization secure. 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. TRAP draws on our massive trove of threat intelligence which includes real-time data from millions of inboxes around the world. We also incorporate intel from Emerging Threats and third-party sources.

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

7

An archive that doesn't let you quickly retrieve the data you need defeats the purpose of having one. No matter how large your archive gets, we guarantee that your searches will take 20 seconds or less—not minutes or hours.

Our cloud-based archive supports more than 500 file types 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).

Security training

that makes users aware, not annoyed

8

Your users are attackers' biggest targets—and your biggest risk. Make them a strong last line of defense with best-in-class security awareness training.

Using proven learning-science techniques, our training helps change user behavior by helping them recognize, reject and report malicious email.

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 organization'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

9

Every purchase includes full installation and customization 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 a yearly renewal rate of more than 90%. It's no wonder that our customers include more than half of the Fortune 100, including:

- The top global banks
- The top global retailers
- The top pharmaceutical companies
- The top research universities

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.

Complete, fully integrated security that streamlines operations

10

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' 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 organizations 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.

0501-003-01-01 08/20