

To the Power of Proofpoint

10 Reasons Why Organisations Choose People-Centric Cybersecurity to Enhance their Microsoft 365 Investment



proofpoint.

Introduction

Few tools are as critical to modern business as Microsoft 365. For many organisations, the platform is a key to remote work, global collaboration and the cloud (if not synonymous with these new ways of working).

Unfortunately, the platform’s reach and central role in the workplace also make it a prime target for cyber attackers. Often, it’s the primary vector for compromising their victims. At the same time, remote and hybrid work has only complicated security and insider-led data loss.

While Microsoft 365 is a vital productivity tool, experts such as Gartner and Forrester recommend more complete email, cloud and data security than the platform’s native offerings.^{1 2}

Today’s complex and shifting threat and compliance landscapes call for a new approach to threat protection, data loss prevention and compliance. That’s why we offer a unique people-centric solution that gives you:

- The industry’s most effective threat protection and data loss prevention
- Actionable visibility and context for both internal and external threats
- A modern, integrated approach to threat, data loss and compliance challenges
- An excellent experience for your team—and for end users

Alongside Microsoft as your productivity partner, Proofpoint aims to be your cybersecurity partner. More than 200,000 Microsoft 365 customers already trust us to secure their cloud investment.

Here’s how we can help you enhance Microsoft 365.

1 Mark Harris, Peter Firstbrook, et al. (Gartner). "Market Guide for Email Security." October 2021.
 2. Jess Burn, Joseph Blankenship, et al. (Forrester). "Best Practices: Phishing Prevention." November 2021.

Introduction	Enhanced Threat Protection	People-Centric Data Loss Prevention	Account Takeover Protection	Cloud Visibility and Protection	Incident Response at Scale	Intelligent Compliance and Archiving	Security Awareness and User Behaviour	Integrated Security	World-Class Support	Industry Leadership	Take the Next Steps
---------------------	-----------------------------------	--	------------------------------------	--	-----------------------------------	---	--	----------------------------	----------------------------	----------------------------	----------------------------

REASON 1

Enhanced Protection Against Phishing, BEC and Other Threats

The best cyber defense is one that stops threats where they start. That's why we help more than 200,000 Microsoft 365 customers stop more threats and unwanted email—before they reach users' inboxes.

We catch more threats with multistage sandboxing that uses a blend of static, dynamic and human-analysed code execution. Our AI- and ML-powered detection engine applies advanced behaviour analysis to detect both malicious code and credential phishing websites. It can even detect attacks that use sandbox-evasion techniques that other virtual-machine tools miss.



You also get visibility into:



Which users are targeted with BEC



The top BEC themes directed at your users



How BEC threats are trending over time in your environment

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.

We stop a wide range of other threats, including business email compromise (BEC), supplier fraud and other forms of social engineering that don't always rely on unsafe attachments or URLs.

Trained with trillions of data points, our machine learning (ML) and behavioural analytics detect and block 2.2 million BEC threats every month. We provide detailed forensics so you can understand why a message was deemed unsafe and blocked.

Our integrated solution provides deep visibility into malicious activity and user behaviour to stop most threats. And if something goes wrong, it automates key parts of the incident response process to help you protect your users at scale.

With an average analysis time of less than three minutes, we block unsafe attachments before your users have a chance to interact with them—and without dragging down productivity. We support a wide range of file types, including PDFs and HTML, not just Microsoft Office files.

For high-risk users and websites, our URL isolation solution opens unknown links from email in a safe, self-contained browser window—fully viewable to the user but stripped of potentially harmful content.

And configurable email warning tags with one-click reporting alert users to the fact that they need to be extra cautious and make it easy to report unsafe messages.

Introduction

**Enhanced
Threat
Protection**

People-Centric
Data Loss
Prevention

Account
Takeover
Protection

Cloud Visibility
and Protection

Incident
Response
at Scale

Intelligent
Compliance
and Archiving

Security
Awareness and
User Behaviour

Integrated
Security

World-Class
Support

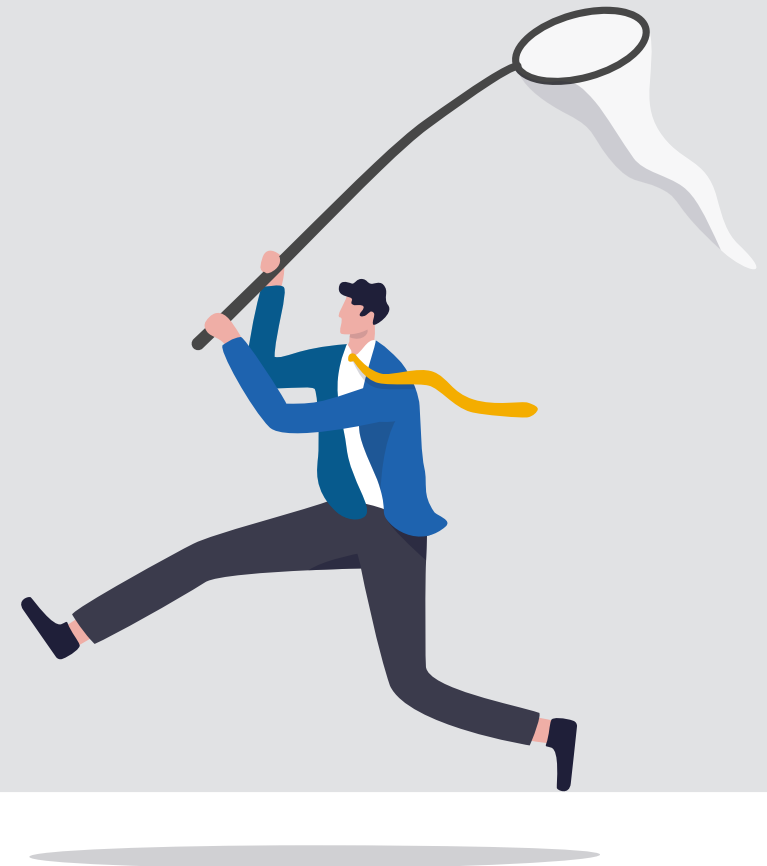
Industry
Leadership

Take the
Next Steps

REASON 2

Modern, People-Centric Data Loss Prevention

The “people perimeter” has replaced the old network perimeter. In an era of remote and hybrid work, your people manage personally identifiable information (PII) and other sensitive data across email, the cloud, the web and endpoints. These trends complicate data loss prevention (DLP) and insider threat management (ITM).



With Proofpoint....

You can easily set and maintain your organisation's unique data policies. Our platform offers the following to make finding, managing and reporting violations easy:

- Native algorithmic analysis
- A smart identifier engine
- Pre-built dictionaries
- Out-of-the-box DLP workflows

We help safeguard data from both external and internal threats with better insight and a streamlined workflow. You get people-centric context that helps piece together the full story behind every DLP alert. Our unique timeline view helps you quickly connect the dots between content, behaviour and threats. It lets you quickly assess user intent, easily collaborate with other teams (such as legal and HR) and take the right course of action.

We also make it simple to create, apply and enforce unified policies across text, email, the cloud, the web and endpoints to keep your data safe and compliant.

Our AI-powered data classification engine discovers, classifies and labels business-critical data to enhance and accelerate your DLP programme. Choose among hundreds of pre-trained classifiers. Or let our AI engine build them from seed documents. Either way, our engine dynamically learns from your data (whether in the cloud or on premises) to suggest dictionaries. You can then apply those dictionaries across all channels with a single click.

Not all DLP incidents are created equal. Our information protection platform connects the dots between content, user behaviour and external threats. This insight helps you tell whether data loss incidents stemmed from careless, malicious or compromised users. Once you know what kind of user you're dealing with, you can respond the right way.

Your team saves time and cuts costs with a single integrated, cloud-native console. Privacy is built in by design, so DLP doesn't come at the expense of user privacy.

We go far beyond native Microsoft 365 security to safeguard users, sensitive data and cloud apps. By identifying your riskiest users, you can apply risk-based controls to keep their accounts safe.

Introduction

Enhanced
Threat
ProtectionPeople-Centric
Data Loss
PreventionAccount
Takeover
ProtectionCloud Visibility
and ProtectionIncident
Response
at ScaleIntelligent
Compliance
and ArchivingSecurity
Awareness and
User BehaviourIntegrated
SecurityWorld-Class
SupportIndustry
LeadershipTake the
Next Steps

REASON 3

Protection Against Account Takeover

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 Microsoft 365 account with real-time alerts of suspicious activity, automated remediation and risk-based access controls.

Robust policies alert you to issues in real time. You can quickly investigate alerts—and any activity that led up to them—with an intuitive dashboard. From there, you can remediate compromised accounts, quarantine unsafe files and apply risk-based authentication as needed.



Integration with Okta helps identify a range of anomalous or unsafe activity, such as:



Successful yet suspicious Microsoft 365 logins



Failed logins



Unexpected access to business applications



Privilege escalations that allow access to critical cloud resources



Escalations that exempt users from the usual authentication factors

REASON 4

Cloud Visibility and Protection



Proofpoint CASB extends our people-centric security to the cloud. We help detect, investigate and defend against cyber criminals seeking access to your data in Microsoft 365 and cloud apps.

Third-party apps add more features to Microsoft 365. But some are poorly built. Others are overtly malicious. Attackers can use third-party add-ons and social engineering to trick your users into granting broad access to your SaaS apps and data.

We can help you discover, assess and control unsafe apps and add-ons. With our powerful analytics, you can grant the right levels of access to apps based on the risk factors that matter to you. User-specific risk indicators with threat intelligence across email, SaaS and others detect anomalies in your cloud apps. These include account takeover, suspicious file activities and more.

With IaaS and SaaS security posture management, we make it easy for you to monitor risky administrative activities. We also help identify misconfigurations and compliance risks to avoid self-inflicted issues.

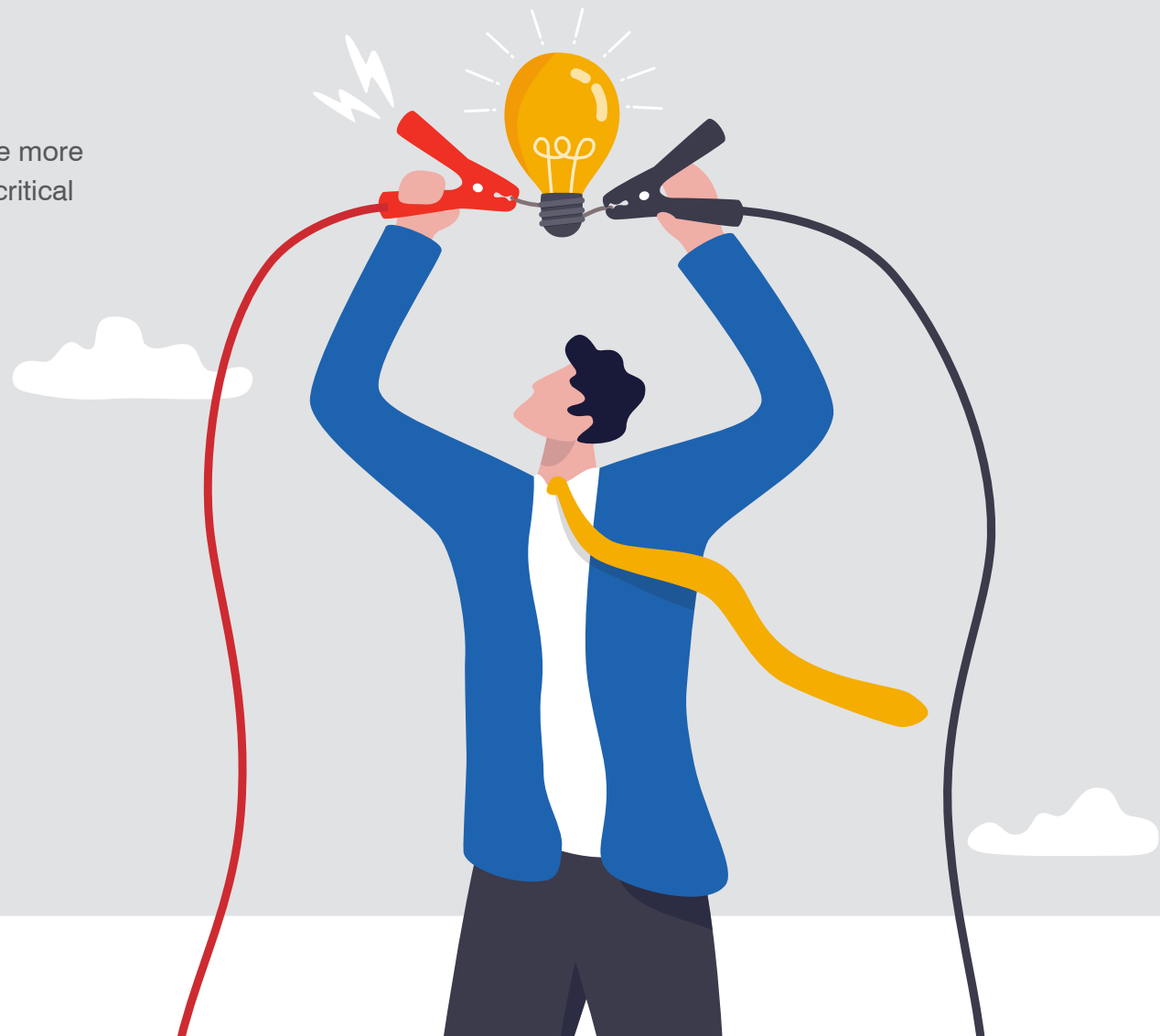


Introduction	Enhanced Threat Protection	People-Centric Data Loss Prevention	Account Takeover Protection	Cloud Visibility and Protection	Incident Response at Scale	Intelligent Compliance and Archiving	Security Awareness and User Behaviour	Integrated Security	World-Class Support	Industry Leadership	Take the Next Steps
--------------	----------------------------	-------------------------------------	-----------------------------	--	----------------------------	--------------------------------------	---------------------------------------	---------------------	---------------------	---------------------	---------------------

REASON 5

Lightning-Fast Incident Response at Scale

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 Microsoft 365 secure.



Threat Response Auto-Pull (TRAP)

Automatically remove malicious email from inboxes with enhanced security alerts and actionable forensics.

Closed-Loop Email Analysis and Response (CLEAR)

Users can easily report suspicious messages, receiving positive feedback to reinforce your security culture.

Our Threat Response Auto-Pull (TRAP) solution automatically removes malicious email from inboxes. These include emails reported by users and those that become unsafe after they've been delivered—even if they've been forwarded to other users.

With Closed-Loop Email Analysis and Response (CLEAR), your users can easily report suspicious messages. Reported messages are quickly analysed to verify and block true threats. And users get positive feedback after reporting to help reinforce your security culture. HTML-based email warning tags alert users to potentially unsafe emails. Together, these features greatly reduce time spent investigating and resolving email threats.

TRAP also enriches security alerts with actionable forensics. That means your security team can verify and resolve incidents faster and more efficiently. TRAP draws on a massive trove of threat intelligence. Our trillion-point threat graph includes real-time data from millions of inboxes around the world, intel from Proofpoint Emerging Threats and third-party sources.

With Proofpoint, you can also remediate Microsoft 365 account takeovers before they cause lasting harm. Finally, we integrate with the security tools you already use, including Okta and CyberArk.

Introduction

Enhanced
Threat
ProtectionPeople-Centric
Data Loss
PreventionAccount
Takeover
ProtectionCloud Visibility
and ProtectionIncident
Response
at ScaleIntelligent
Compliance
and ArchivingSecurity
Awareness and
User BehaviourIntegrated
SecurityWorld-Class
SupportIndustry
LeadershipTake the
Next Steps

REASON 6

Intelligent Compliance and Archiving

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 with Proofpoint, 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 it's 10,000 mailboxes, 100,000 mailboxes or more.

Introduction	Enhanced Threat Protection	People-Centric Data Loss Prevention	Account Takeover Protection	Cloud Visibility and Protection	Incident Response at Scale	Intelligent Compliance and Archiving	Security Awareness and User Behaviour	Integrated Security	World-Class Support	Industry Leadership	Take the Next Steps
--------------	----------------------------	-------------------------------------	-----------------------------	---------------------------------	----------------------------	---	---------------------------------------	---------------------	---------------------	---------------------	---------------------

REASON 7

Security Awareness Programmes That Change User Behaviour

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 behaviour by helping them recognise, reject and report malicious email.

We offer a vast library of engaging content based on real-world attack techniques. It's informed by our own threat intelligence and your users' unique knowledge gaps. And it's flexible enough to be tailored to your unique security challenges and fit into your users' schedules.

But we go even further. Phishing simulations based on real-world threats and techniques test users' ability to spot the latest attacks. For users who fall for the bait, point-in-time feedback and follow-up training help turn mistakes into teachable moments. We make it easy to track and report progress over time to help identify areas of improvement—and build a culture of security awareness.



REASON 8

Complete, Fully Integrated Security That Streamlines Operations



Our complete security platform blends powerful, effective email, cloud and data protection to solve today’s biggest security and compliance 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 Microsoft 365 investment.

Our proven approach to security and compliance for Microsoft 365:

-  Reduces your risk
-  Frees up critical security and IT resources
-  Cuts costs
-  Makes your security operations more effective and efficient

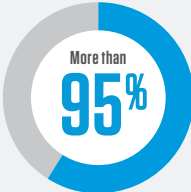
Introduction	Enhanced Threat Protection	People-Centric Data Loss Prevention	Account Takeover Protection	Cloud Visibility and Protection	Incident Response at Scale	Intelligent Compliance and Archiving	Security Awareness and User Behaviour	Integrated Security	World-Class Support	Industry Leadership	Take the Next Steps
--------------	----------------------------	-------------------------------------	-----------------------------	---------------------------------	----------------------------	--------------------------------------	---------------------------------------	----------------------------	---------------------	---------------------	---------------------

REASON 9

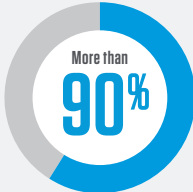
World-Class Support

We fully install and customise your deployment, drawing from the latest industry trends and best practices. And after deployment, we offer 24/7/365 support—no complicated service add-ons.





sustained customer satisfaction rate



yearly renewal rate



of the Fortune 100 are our customers

We have earned a sustained customer satisfaction rate of more than 95% and yearly renewal rate of more than 90%. It's no wonder that our customers include more than 80% of the Fortune 100. We serve:



The top global banks



The top global retailers



The top pharmaceutical companies



The top research universities

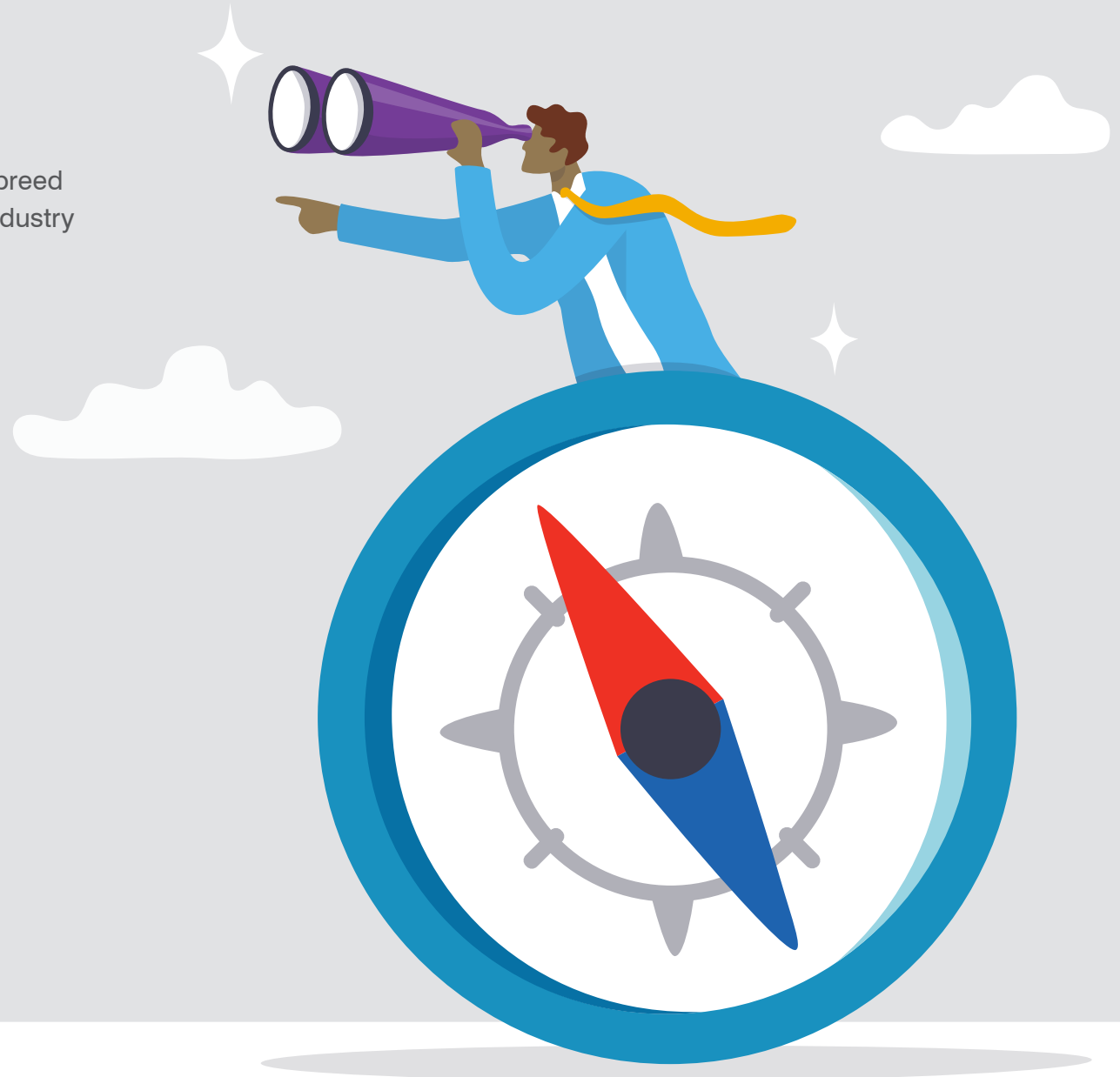
Most of these organisations are also Microsoft 365 E3 or E5 subscribers. So while they rely on Microsoft as their productivity partner, they turn to and Proofpoint as their security partner.

Introduction	Enhanced Threat Protection	People-Centric Data Loss Prevention	Account Takeover Protection	Cloud Visibility and Protection	Incident Response at Scale	Intelligent Compliance and Archiving	Security Awareness and User Behaviour	Integrated Security	World-Class Support	Industry Leadership	Take the Next Steps
--------------	----------------------------	-------------------------------------	-----------------------------	---------------------------------	----------------------------	--------------------------------------	---------------------------------------	---------------------	---------------------	---------------------	---------------------

REASON 10

Industry Leadership

With Proofpoint, you don't have to choose between best-in-breed technology and a fully integrated solution. We're a proven industry leader across cybersecurity, DLP and compliance.



We constantly innovate to keep Microsoft 365 environments protected against a wide range of threats—including new and emerging attack techniques. With one of the largest data sets in cybersecurity, we identify threats faster and respond to them more effectively.

While our ultimate goal is to please customers, here are just a few of the industry accolades we've earned along the way:

- Leader in the 2022 Magic Quadrant for Enterprise Information Archiving for the 10th consecutive year
- 2022 Gartner Peer Insights “Customers’ Choice” for Security Service Edge
- 2022 Cybersecurity Excellence Awards Gold Winner in more than 25 categories, including anti-malware, anti-phishing, artificial intelligence security, AWS cloud security, Azure cloud security, cloud access security broker, data leakage prevention, email security, insider threat solution and security awareness programme
- Winner, 2021 CISO’s Choice Awards for Premier Security Company, Email Security and Cloud Security Solutions
- 2021 Cybersecurity Breakthrough Awards, Overall Enterprise Email Security Solution Provider of the Year (second consecutive year)



Introduction	Enhanced Threat Protection	People-Centric Data Loss Prevention	Account Takeover Protection	Cloud Visibility and Protection	Incident Response at Scale	Intelligent Compliance and Archiving	Security Awareness and User Behaviour	Integrated Security	World-Class Support	Industry Leadership	Take the Next Steps
--------------	----------------------------	-------------------------------------	-----------------------------	---------------------------------	----------------------------	--------------------------------------	---------------------------------------	---------------------	---------------------	---------------------	---------------------

Take the Next Steps

Our complete, integrated security platform combines powerful, effective cloud and email protection to solve today's most pressing challenges. We also offer flexible deployment, including inline and API-based options. That means we can begin protecting your Microsoft 365 environment quickly and easily without disrupting your existing setup.

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 for your cloud deployment. Our proven approach to security and compliance for Microsoft 365:

- Reduces your risk
- Frees up resources
- Cuts costs
- Makes your security operations more effective and efficient



Learn more about Proofpoint and how we can help you enhance your Microsoft 365 deployment. Explore people-centric protection, data loss prevention and compliance across email, the cloud, the web and endpoints.

Visit proofpoint.com/us/solutions/microsoft-365-security-compliance.

About Proofpoint

The Proofpoint Nexus Threat Graph blends the industry’s best security research, technology and threat data to keep you protected at every stage of the attack lifecycle. No one else has better insight into how today’s cyber attacks target people.

 Every day, we analyse more than:

2.6B
EMAILS

49B
URLS

1.9B
ATTACHMENTS

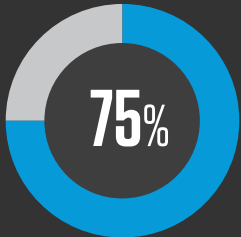
1.7B
MOBILE MESSAGES

430M
WEB DOMAINS

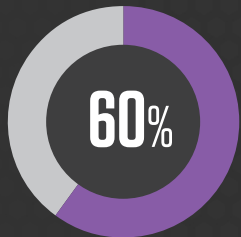
143,000
SOCIAL MEDIA
ACCOUNTS



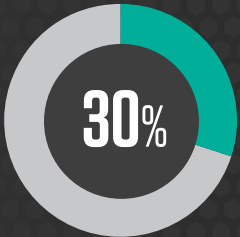
We are trusted by more than:



OF THE FORTUNE 100



OF THE FORTUNE 1000



OF THE FORTUNE
GLOBAL 2000



8,000
ENTERPRISES



200,000
SMALL BUSINESSES

LEARN MORE

For more information, visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance 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 75 percent of the Fortune 100, 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, Inc. Proofpoint is a trade mark of Proofpoint, Inc. in the United States and other countries. All other trade marks contained herein are property of their respective owners.