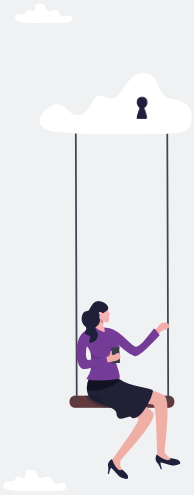
proofpoint.

EBOOK



Securing Microsoft 365

How a dedicated security solution can protect users, safeguard data and enhance the value of your cloud investment

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 those terms).

Unfortunately, the platform's ubiquity and central role in the workplace also make it a prime target for cyber attackers—and often, the primary vector for compromising their victims. At the same time, an accelerated shift to remote and hybrid work has thrust insider-led threats and data loss into the security spotlight.

Today's advanced attacks rely on phishing and social engineering, not just technical exploits. They trick users into installing ransomware and other malware, handing over their credentials, sharing sensitive information and even transferring funds. What's more, threat actors are scaling these people-centric attacks, making them more prevalent, expensive and sophisticated than ever.

Nuisance-level threats, bulk mail and spam also undercut your Microsoft 365 investment. High volumes of these unwanted emails not only hinder worker productivity but can overwhelm already-stretched security and IT teams.

While Microsoft 365 is a vital collaboration tool, experts such as Gartner and Forrester recommend more complete email, cloud and data security than the platform's native offerings.[1,2]

This e-book explores these modern threats, best practices for protecting users and data, and what capabilities to look for when enhancing your Microsoft 365 defences.

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.

SECTION 1

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 huge impact on your bottom line. The average total cost of a data breach stands at a record $4.35 million (USD) globally, up a whopping 43% in the last three years.[3] That figure is even higher in the U.S. at $9.44 million, a 15% jump from 2019.[4]

3 Ponemon. "Cost of a Data Breach 2022" and "Cost of a Data Beach 2019." July 2022 and August 2019.
4 Ibid.

66%

of organisations faced at least one highly targeted spear-phishing attack in 2021

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 data.

Today's phishing is multilayered 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 66% of organisations faced at least one highly targeted spear-phishing attack in 2021; 65% faced at least one business email compromise (BEC) attack.[5] (See "Business email compromise and supplier compromise" on the next page).

Whatever their tactics, phishing attacks are highly successful. A full 83% of U.S. organisations experienced a successful phishing attack last year, up from 57% the year before.[6]

Malware

Every day, the AV-TEST Institute registers more than 450,000 new malware strains and risky apps.[7] But the creativity of malicious actors doesn't stop there.

Attackers are just as creative about finding new targets. They use automated tools to mine information about your people from public social media profiles. They know where your users work. And they know their targets' role, interests, hobbies, marital status, employment history and more.

These details serve multiple purposes: identifying users with the desired data or access and providing fodder for emails convincing enough to get users to click. Once the recipient takes the bait, a malicious payload drops onto the system.

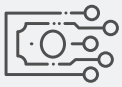
5 Proofpoint. "2022 State of the Phish." February 2022.
6 Ibid.
7 AV-TEST Institute. "Malware (https://www.av-test.org/en/statistics/malware/)." Accessed August 2022.

Business email compromise and supplier impersonation

BEC and supplier impersonation have emerged as new and serious threats. The FBI estimates that these attacks have cost victims upwards of $43 billion (in actual and potential losses) since 2016.

In these attacks, someone poses as an authority figure, business partner, customer or supplier. The attacker might use a spoofed email address or lookalike email domain. In some cases, they may use a legitimate but compromised email account, which is almost impossible to detect with Microsoft 365 alone. No matter what tactic attackers use, the goal is the same: fool the target into sending or diverting funds.

For example, an email that appears to come from a trusted vendor might ask a staff accountant to:



Wire funds

Divert a payment

Change bank account details

In most cases, the money goes straight to the impostor. The average attack nets nearly $180,000.

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

These attackers 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.

Account compromise

Having control over a trusted Microsoft 365 account gives the attacker a trove of information that can be used as a launching pad for all kinds of other attacks.

High-privilege users are often primary targets. With access to a CEO or VP of HR email account, an attacker can access almost any data on the network. What's more, they can exploit the executive's trusted relationships to launch BEC-style attacks on business partners. This not only disrupts normal processes but can damage one of your organisation's most valuable assets—its reputation.

Advanced tactics

Almost all of these attacks use one or more forms of social engineering, the subtle art of manipulation. It's persuasion through deception—coaxing people to do something against their own best interest.

Through social engineering, attackers trick victims into clicking unsafe links, opening malicious attachments, diverting money and sending sensitive data.

One of the most unexpected recent developments has been a sharp increase in telephone-oriented attacks. These attacks require a high level of direct interaction; the emailed lures do not contain malware or malicious URLs. And they usually go undetected without added layers of Microsoft 365 security. The goal: persuade the victim to call a fake customer service number.

Once the victim calls, the attacker guides them into giving remote access to their computer or manually downloading malware. Our data shows more than 100,000 attempts to initiate a telephone-oriented attack every day.

SECTION 2

Why 'Good Enough' Is No Longer Good Enough

Microsoft 365's built-in security and compliance features may help in limited ways. But as threats multiply and evolve, you might need other layers of security.

In some cases, cybersecurity may have been a lower-priority concern as organisations scrambled to support remote and hybrid work to stay viable. With the worst of the COVID-19 pandemic behind them, many are now looking to shore up their cloud investment.

Too little protection against cyber threats and data loss can lead to costly breaches that taint your brand, damage your reputation and hurt your bottom line. That's why enhancing your Microsoft 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 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 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)

Granting persistent access to their accounts through OAuth

Once they gain entry to a user's system with malware, stolen credentials or OAuth app access, cyber criminals can threaten your people, data and systems.

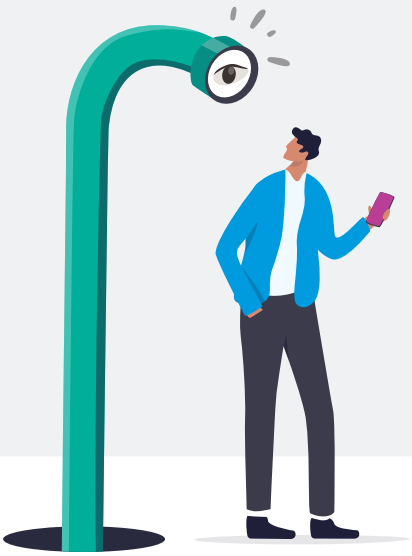
It's no wonder that security has evolved into a boardroom challenge. That's why protecting your Microsoft 365 environment is a business-critical decision. Effective cybersecurity focuses on people first.

You can't protect what you can't see

Safeguarding your Microsoft 365 deployment from both external threats and insider-led data loss stand on a common bedrock: visibility.

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

Blocking threats before they reach a user's inbox has two critical advantages. First, you gain an 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.



By the same token, you can't protect data or respond to data loss incidents without visibility that builds on Microsoft Information Protection (MIP) features. You need insight into where your sensitive data lives and what your users are doing with it. You'll also need context to determine whether an insider risk stems from a careless, compromised or malicious user.

This is even more critical in today's fast-moving business climate. Data evolves as quickly as the next innovation or acquisition. To protect it, you need predictive capabilities to suggest what data is sensitive so the safeguards you deploy get more from your MIP investments.

Siloed security, DLP and compliance is not sustainable

In the ever-evolving threat landscape, cyber criminals coordinate attacks across multiple vectors. Often, they compromise user accounts to exploit insider-level access to critical data, systems and other resources.

That's why an integrated, multilayered defence is vital. An effective solution must integrate with the rest of your security, information protection and compliance ecosystem. That means everything from your email defences to your data loss prevention (DLP) system to your 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.

Threats

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 system may not provide the visibility you need into cyber threats, user activity and data movement across email, the cloud and endpoints.

Data loss

All users pose some degree of risk to your organisation. But everyone is risky in unique and ever-evolving ways. Some users are malicious. Many are negligent. And others might be compromised. That's why one-size-fits-all security and data-access policies don't protect against insider risks and the threats that target people through Microsoft 365.

You need visibility and controls that factor in people, data and threat for context in real time. Only then can you prevent data loss and misuse across the organisation.

Unexpected 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 shouldn't grind your operations to a halt. Look for business continuity features that ensure your users stay productive even when Microsoft 365 is down.

SECTION 3

Calculating the Value of Enhanced Security

Neglecting a dedicated security solution for your Microsoft 365 deployment may appear to save you money on paper.

But not fully securing your investment will likely cost you time, data, 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 attacks push security up to board level, the conversation is not just about efficacy. It's about having the visibility to understand what threats are targeting your people and the inherent risk they pose to the organisation.

Threats

Not having the visibility and insights you need to address security issues can result in lost time. According to Ponemon Institute, detecting and responding to breaches was the biggest part of the cost equation at $1.44 million per breach.[8] That's a 16% jump from the year before and the first time in six years these costs have exceeded lost business due to a breach.

Attackers are subverting the tools your users rely on to get their work done. Whether it's ransoming critical SharePoint files, hosting malicious files through OneDrive or exploiting vulnerabilities in Teams, Microsoft 365 users face a barrage of threats. And they require added layers of security.

Consider the following:

- How much productivity is lost cleaning up email-related incidents that could have been otherwise blocked?
- How much time is spent identifying and remediating compromised accounts? Investigating, prioritising, and confirming threats? Cleaning up emails containing malicious attachments or URLs from your users mailboxes?
- How do you quantify the risk of prolonged user exposure to these emails?
- How much time is lost from a disjointed security response that fails to quickly 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 resorting to personal email when Microsoft 365 email suffers an outage? (A Gartner study once pegged the cost at more than $300,000 per hour.[9] Some Microsoft outages have lasted days.[10])
- How much are you willing to pay to get back files held ransom—and how much can you spend restoring operations if you don't—in attacks not detected by Microsoft 365 alone?

8 Ponemon. "Cost of a Data Breach Report 2022." July 2022

9 Andrew Lerner (Gartner). "The Cost of Downtime." July 2014.

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

Data loss prevention and information protection

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 2021 alone, organisations reported 1,882 data compromises, a 68% jump from 2020.[11] (The figure includes data breaches, exposures and leaks.)

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. Consider augmenting native features with a solution that can apply policies to outbound mail, OneDrive, SharePoint and Teams—and offer visibility from email, endpoints and the cloud.

Data compromises can stem from malicious, negligent and compromised users. So there's no single approach to solving them. Having the context and insight to know which kind of user you're dealing with is critical.

Here are some factors to consider:

- What is the value of the data departing employees take from Microsoft 365 as they walk out the door?
- How much would stolen or exposed data cost if your DLP solution can't protect your most critical assets across the key channels people work? Can you detect sensitive data across email, cloud and endpoints—and the breadth of file types that may contain sensitive information?
- Do you have a centralised way to define policy?
- Can you quickly pinpoint what content and actions triggered a policy alert? Do you have the context you need to tell whether an insider incident stemmed from a malicious, negligent or compromised user and mount the right response?
- Are you confident that your intellectual property (IP) is fully protected?
- Do you have an incident response workflow in place to remediate issues? Does your automated response enable inline blocking or remediation across email, file shares, Teams 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 investigating a DLP alert, do you get a meaningful, easy-to-grasp view of what happened? Is it easy to share with non-technical teams in legal and HR?
- 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?

11 Identity Theft Resource Center. "First Half 2022 Data Breach Analysis." July 2022.

- Beyond using built-in or custom detectors to identify sensitive data, can you dynamically learn from your data through artificial intelligence and machine learning to uncover risk?
- Can it optimise your DLP policies for higher fidelity?

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 Microsoft 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 emerge when well-intentioned users resort to personal email to get work done?

Message trace, non-delivery 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 systems are compromised.

Further, IT should remove these emails to prevent reinfection, which occurs when a user unknowingly reaccesses 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 a serious business. The consequences of failing to comply can be costly and hurt your business. At 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 is limited 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.

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:

- U.S. Financial Industry Regulatory Authority (FINRA)
- U.S. Securities and Exchange Commission (SEC)
- Investment Industry Regulatory Organization in Canada (IIROC)
- U.K. Financial Services Act

These rules aim to protect investors by making sure the U.S., U.K. and Canadian security industries operate fairly and honestly. Fines for non-compliance can run well into millions of dollars. Other costs include those of deploying other security measures, audits and potential reputational damage.

As you assess the default capabilities of Microsoft 365, ask these important questions:

- If your organisation is involved in a legal dispute, will Microsoft 365 enable you to provide records of all communications and transactions from 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?
- Can you capture and preserve all of the compliance content your organisation generates? What about data from social media platforms?
- How well can you supervise and monitor content? (Several regulations require monitoring and sampling content.) Does it use the latest technology, or does it rely on basic keyword matching?

12 Andrew Peck, Jennifer Feldman, et al. (New York Law Journal). "Defensible deletion: The proof is in the planning." January 2021.

13 Chris Matthews (MarketWatch). "SEC fines JPMorgan $125 million for failing to keep records." December 2021.

SECTION 4

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

Today's complex and ever-changing threat and compliance landscapes require a new approach to threat protection, data loss prevention and compliance.

That's why we offer a unique people-centric approach that gives you:

- The industry's most effective threat protection and data loss prevention strategy
- Actionable visibility and context for both internal and external threats
- A modern, integrated approach to threat, data loss and compliance challenges
- An excellent user experience

Here's how we help you enhance Microsoft 365.

Enhanced protection against phishing, BEC and other threats

Our AI-powered detection engine uses advanced behavioural analysis to stop a wide range of threats—including hard-to-detect threats that don't use malicious attachments or URLs, such as BEC attacks.

Using ML and behavioural analytics that are trained with trillions of data points, we detect and block 2.2 million BEC threats every month. We provide detailed forensics so you can understand why a message was identified as BEC and blocked.

You also get visibility into:

- Who in your organisation is targeted with BEC
- The top BEC themes directed at your organisation
- How BEC threats are trending over time for your organisation

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

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.

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 Office files.

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.

And configurable email warning tags with one-click reporting alert users to take extra caution and makes it easy for them to report potentially malicious messages.

The industry's most effective data security

Safeguard data from external and internal threats with people-centric context that connects the dots between content, behaviour and threats. Our timeline view pieces together the story behind every DLP alert. You can quickly assess user intent, easily collaborate with other teams such as legal and HR and take the appropriate course of action.

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

Our AI-powered data classification engine gets your DLP programme running quickly and streamlines your workflow. You can choose among hundreds of pre-trained classifiers or let our DLP engine build custom classifiers from seed documents. The engine dynamically learns from your data in the cloud and on-premises repositories to suggest dictionaries. You can apply them across all channels with a single click.

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.

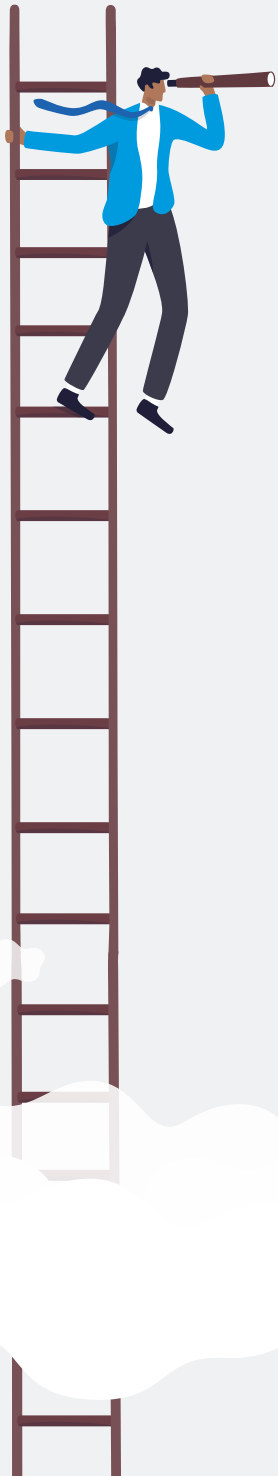
Protection against account takeovers

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.

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.

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

- Successful but suspicious Microsoft 365 logins
- Failed login events
- Unexpected access to business applications
- Privilege escalations that allow access to critical cloud resources
- Escalations that exempt users from the usual authentication factors



Enhanced cloud visibility and security

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 Microsoft 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

Automatically remove malicious email from inboxes, including those reported by users or detected as unsafe after these messages have been delivered. When malicious messages are detected, we automatically remove them from users' inboxes—even if they've been forwarded to other users. This feature greatly reduces the time your security and messaging teams spend investigating and resolving email threats.

We also can remediate account takeovers before they cause lasting harm to your data, operations, business relationships and reputation.

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.

Our cloud-based archive supports more than 500 files 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 awareness programmes that change user behaviour

We offer a vast library of engaging content based on real-world attacker 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 organisation's unique security challenges and fit into users' schedules.

Beyond foundational awareness education, 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

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

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 half of the Fortune 100.

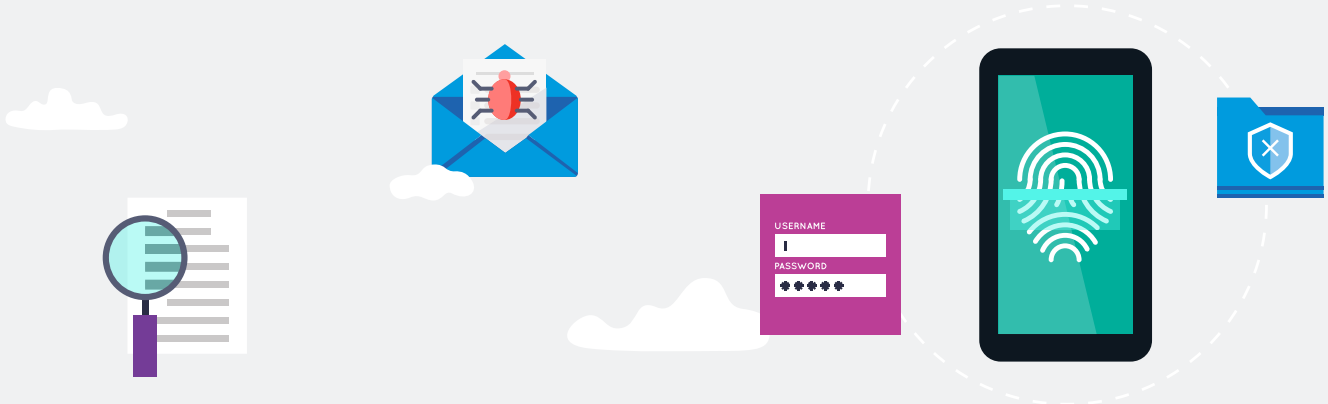
Complete, fully integrated security that streamlines operations

Our complete, integrated security platform combines powerful, effective email, cloud and information 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 environment.

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



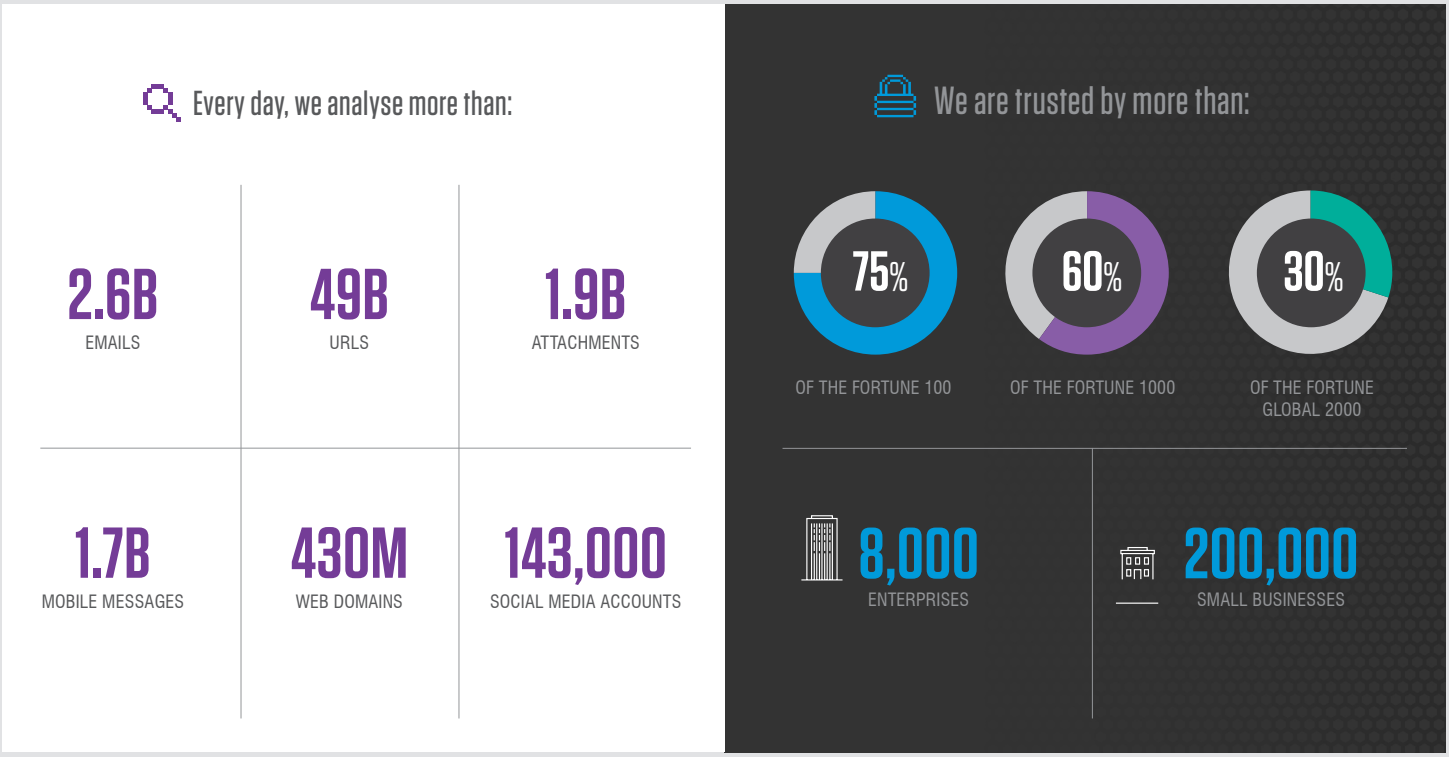
SECTION 5

Take the Next Steps

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

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.



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**.