proofpoint.

BUYER'S GUIDE

The definitive guide to stopping human-centric threats

Key capabilities

Here's a look at the capabilities that you need to protect your organization from human-centric threats. They fall under five categories:

1. Comprehensive threat visibility and risk insights
2. Automated threat protection for email and beyond
3. Security for trusted business communications
4. Guidance for employees
5. Account takeover protection

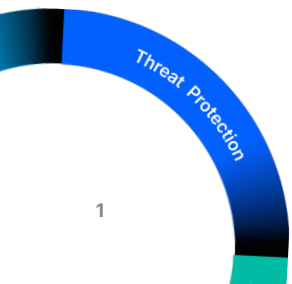
Overview

Threat actors continue ramping up their efforts at exfiltrating data and exploiting business communications for financial gain. And while the number of these threats keeps growing, threat tactics remain largely unchanged. Phishing, malware, ransomware, business email compromise (BEC) and social engineering are all still popular ways to target people.

What has changed, however, is that cybercriminals no longer limit their attacks to inboxes. They have followed users to expanding digital channels—just as they have followed users to the cloud. Digital platforms like Microsoft Teams, Slack, Zoom, LinkedIn and WhatsApp are now prime attack vectors, too.

In this guide, we'll explore the key capabilities that you need to build a strong defense against all human-centric threats—both email-based and beyond. We'll also suggest what to look for as you're choosing a human-centric security platform that's right for you.

Figure 1: Threats and risks across digital workspaces.



$4.88M

is the average cost of a data breach in a phishing or BEC attack.[1]

1: Comprehensive threat visibility and risk insights

To stop human-centric threats, you need to understand which of your users are being targeted—and how. This enables you to apply adaptive security controls to protect the people who are most at risk.

Comprehensive visibility into threats across email and digital channels gives you a complete picture of your vulnerabilities.

Here's what you want a solution to show you:

- **Who is being targeted**, including the threats that they face and whether they have engaged with attackers
- **Forensic details**, including threat actor, threat family, affected users, attack techniques and themes and attack campaign objectives
- **At-risk users**, identifying the people who pose risk to your organization and why
- **Threats within trusted business communications**, including look-alike and spoofed domains or websites that could harm your brand reputation
- **Behavioral changes and threat intelligence**, which can reveal signs that one of your suppliers or a trusted third party may be compromised
- **Suspicious activities**, which indicate potential active account takeovers

Visibility isn't just important for initial deployments; it needs to be ongoing. This ensures that you can continuously adjust your level of protection as attacks change.

2: Automated threat protection for email and beyond

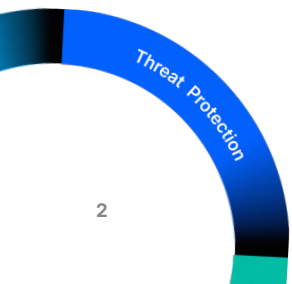
The threat landscape is constantly evolving. Unfortunately, organizations often lack the security talent and the resources to keep up. As a result, it's common for teams to simply not have the time to investigate every security event. What's more, the cost of these events is rising. The latest figures show that the average cost of a data breach in a phishing or BEC attack comes in at $4.88M.[1]

That's why you need a solution that can accurately and efficiently detect and stop threats— without impacting productivity.

Here's what you want a solution to do automatically:

- **Stop threats pre-delivery** with an efficacy of at least 99.99% so that they never reach your users' inboxes
- **Analyze behavioral patterns of internally sent emails**, using threat intelligence technology to detect lateral phishing activities
- **Inspect and block malicious URLs in real time** to ensure that they don't reach users through email or messaging and collaboration platforms
- **Analyze suspicious QR codes pre-delivery** with behavioral AI and semantic analysis and provide sandboxing
- **Detect and responds to compromised identity provider (IdP) accounts** that are hosted in the cloud
- **Insert warning tags** into suspicious messages

When an attacker successfully gains initial access, it's essential to detect and respond to that threat quickly. Doing so can mean the difference between a minor incident and a full-scale breach.



1. IBM. *Cost of a Data Breach Report*. 2024.

71%

of employees admitted to engaging in risky behaviors such as reusing passwords or clicking unknown links.[2]

3: Security for trusted business communications

Digital communications are the lifeblood of organizations. So it makes sense why bad actors would work so hard to infiltrate trusted communications. When recipients can be tricked into thinking that they're interacting with trusted sources, attacks like BEC, phishing and ransomware are more successful.

To maximize their chances of tricking people, bad actors use a wide range of impersonation tactics. It's essential to have multiple layers of protection to stop them.

Look for a solution that:

- **Enables email authentication** for both user and application-generated emails
- **Provides a secure, dedicated environment** for relaying application-generated transactional emails
- **Assists with DMARC implementation** to maximize the effectiveness of email authentication and ensure full DMARC compliance
- **Protects against look-alike domains**, including detection and assistance with blocking or physically shutting them down
- **Monitors for compromised supplier accounts** and takes automated actions to defend against them

When you safeguard your trusted business communications, you not only protect your employees, but you also protect your business partners and customers.

4: Guidance for employees

Even if technology blocks 99% of threats, that remaining 1% can still lead to a major incident. This is where human behavior becomes the deciding factor. Threat actors generally need your people to assist in their malicious campaigns.

And attacks aren't the only concern. Users often sacrifice their organizations' security for the sake of convenience. According to the Proofpoint *2024 State of the Phish* report:

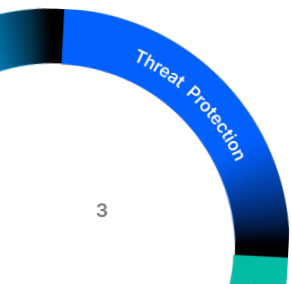
- 71% of employees admitted to engaging in risky behaviors such as reusing passwords or clicking unknown links.
- 96% of those employees knew that their behavior was risky but did it anyway.

When you combine attacks and careless user actions, the chances of a successful breach are compounded. That's why you need to educate your users.

Look for a solution that:

- **Uses your threat data** to identify your most targeted and highest-risk users
- **Provides users with risk-based education** that uses real-life threat examples like the ones that actually target your organization
- **Focuses on behavioral change**, not just checking off a box for your annual security training
- **Motivates employees** by providing visibility into their individual risk scores as well as their impact on your organization's security posture
- **Evaluates effectiveness** and delivers valuable reports that help you to refine your strategy

Strong technology combined with human vigilance is fundamental to stopping human-centric threats. Everyone has a vital role to play in play in securing in your business operations.



2. Proofpoint. *2024 State of the Phish Report.* 2024.

99%

of organizations face regular attempts at account takeovers (ATOs).[3]

5: Account takeover protection

Proofpoint data shows that 99% of organizations face regular attempts at account takeovers (ATOs). These attacks are a form of identity theft where a cybercriminal gains access to or "takes over" an online account. Not surprisingly, cloud-based identity providers—like Microsoft Entra ID, Google and Okta—are most targeted. These accounts serve as single sign-on (SSO) gateways to a user's set of enterprise applications.

And it's not just your accounts that you need to worry about. Cybercriminals also compromise the accounts of trusted business partners to conduct reconnaissance and launch further attacks. These compromised accounts serve as an entry point for multistage attacks that spread across an organization's entire ecosystem as they steal sensitive data, make fraudulent transactions and cause havoc.

AI and machine learning can help monitor all your business communications and automate response.

Look for a solution that:

- **Continuously monitors all accounts** in cloud-based identity provider services such as Microsoft Entra ID, Google and Okta
- **Uses threat intelligence** in combination with behavioral data and machine learning to detect compromised accounts
- **Defends against account takeover attacks** that bypass multifactor authentication (MFA); 65% of hijacked accounts had MFA enabled[4]
- **Accelerates your investigations** by providing a centralized view of post-ATO activities
- **Automates response capabilities** such as account suspension, forced password resets and reverting malicious changes to mailbox rules and MFA settings
- **Removes suspicious third-party applications** as part of post-ATO cleanup

ATOs can be costly and damage your brand. Strong protection is essential to reducing your risk.

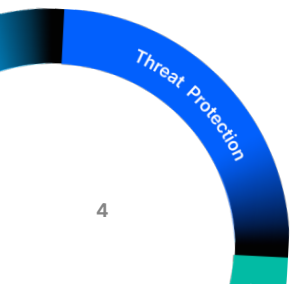
Avoid taking a fragmented approach

As you build out your defenses for email and beyond, point solutions from multiple specialist vendors may seem like the obvious choice. After all, specialist vendors can seem well-equipped to address specific types of attacks. However, this siloed approach has several drawbacks.

For starters, it leads to security blind spots. When tools aren't seamlessly integrated, security teams can find it difficult to get visibility across the security environment. This not only increases the chances that threats will go undetected, but it delays incident response.

It also time-consuming and ineffective for teams to manage multiple security tools. They also must correlate data across siloed control points. And the overwhelming number of alerts that these platforms generate leads to alert fatigue and missed threats. All of this drives up operational costs.

Why not take a more effective approach instead? Adopt a holistic pre-integrated security platform that addresses all human-centric threats. When you work with a single trusted partner, you not only get streamlined management, but you get financial benefits as well.



3. Proofpoint research.
4. Ibid.

Conclusion

A comprehensive human-centric security strategy can protect your organization from a wide array of threats. As you take your first step toward this goal, you should start with the right solution. Look for one that aggregates threat intelligence across email, collaboration tools, messaging platforms and cloud applications. It should also provide key insights into risky user behaviors and help boost your security culture.

Is your current solution limited to just email? Or do you rely on fragmented point solutions? If so, you have room for improvement. Now is the time to assess how well your security protects against all human-centric threats, for email and beyond.

Consolidate with Proofpoint

Proofpoint Prime Threat Protection delivers a pre-integrated threat protection platform to provide complete security. Prime blocks threats across modern workspaces, including email and digital channels. Not only does it protect against the widest array of threats but does so with unrivaled detection accuracy. It also provides deep insights into human risk and strengthens user resilience. And it defends against both compromised user and supplier accounts to keep your trusted business communications safe.

Proofpoint delivers the only modern security architecture with an adaptive approach to protecting your greatest assets and biggest risks: your people. That's why almost 2 million customers of all sizes, including 85 of the Fortune 100, rely on Proofpoint.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →

0203-010-01-01