

SOLUTION BRIEF

# Proofpoint User Protection

Empower your employees and extend protections against account takeover and phishing beyond email

## Key benefits

- **Extend phishing protection** beyond email
- **Enhance your protection** with integrated threat intelligence from Proofpoint
- **Guide your employees** to make safer choices when faced with threats
- **Automate your responses** to account takeovers

Cybercriminals continue to use social engineering to target your people. These tactics trick or threaten users into revealing their credentials or executing malicious code. Email remains the main threat vector for such attacks. However, attackers now exploit many other digital channels. These include collaboration and communication tools, such as Slack, Microsoft Teams, LinkedIn, Zoom and more. These attacks aim to compromise user accounts and take them over. Proofpoint research in 2024 showed that 99% of organisations are regularly targeted for account takeovers. In addition, nearly 62% are impacted by such attacks.<sup>1</sup> These findings show that organisations need a holistic approach to protecting their people and reducing the risks of account compromise.

Proofpoint User Protection gives your users an extra layer of protection beyond email. It automates risk-based learning for your Top Clickers and Very Attacked People (VAPs). With a seamless user experience, it blocks malicious URL links that are delivered in messaging and collaboration applications. It also uses AI-based detections and automates remediations to defend against account takeovers, accelerating threat response.

1. Proofpoint Research, sample size n > 5000 organisations, 2024

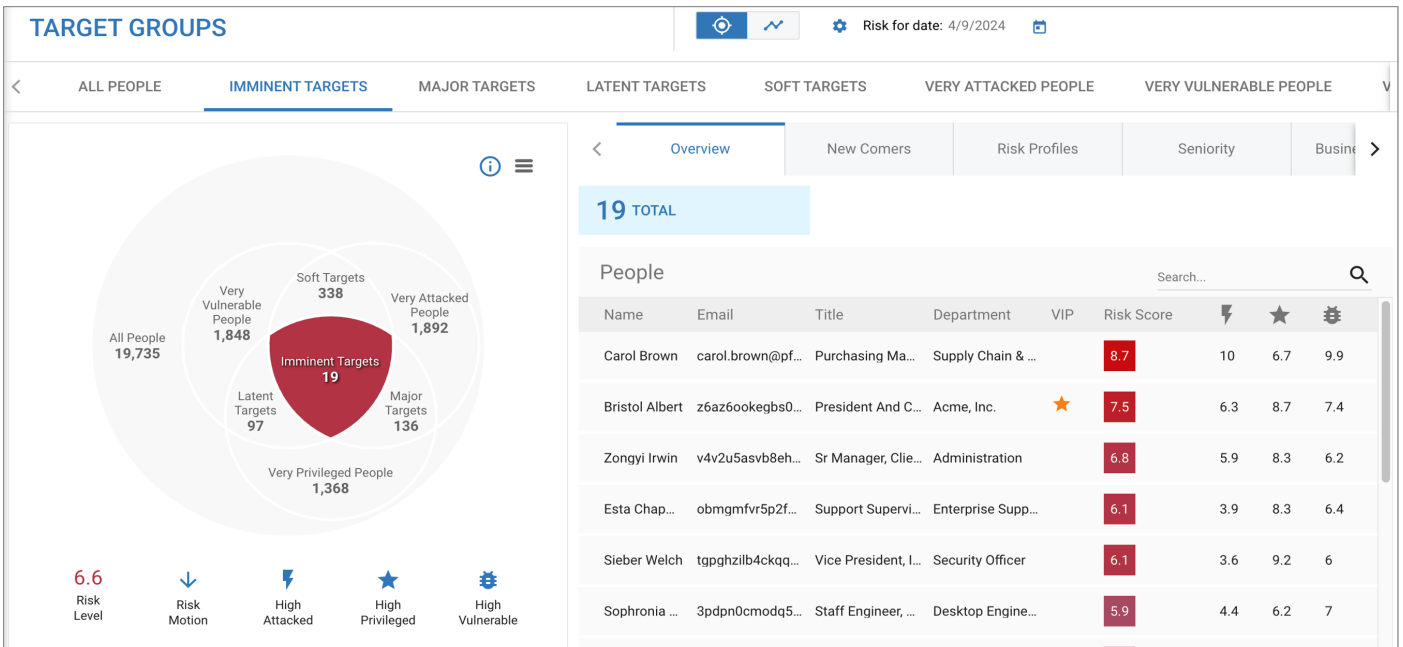
## Stronger protection with better visibility

With User Protection, you unlock the potential of the Proofpoint human-centric security platform. With our integrated threat intelligence and risk insights, you get stronger protection and deeper visibility of high-risk individuals and malicious activities.

User Protection is powered by Proofpoint Nexus®. Nexus is a comprehensive threat intelligence platform that is powered by AI, machine learning and real-time threat intelligence. User Protection extends this industry-leading threat-detection stack to block all malicious URL links, however they are delivered. It accurately identifies account takeovers in tools such as Microsoft 365, Google Workspace

and Okta. User Protection also helps you uncover your high-risk users. It does this by analysing your users' behaviours and their performance in security training and threat simulations. This risk analysis also looks for indicators of active account compromises.

With this improved visibility of human risk, you can apply adaptive security controls to users with varying risk profiles. For example, you can automatically enrol your VAPs, Top Clickers or Imminent Targets into tailored security training. You can also enforce automated remediation actions after an account has been taken over. These actions include revoking access, resetting passwords and quarantining accounts. They also include revoking access to third-party apps and reversing malicious changes to mailbox rules.



**Figure 1:** User Protection identifies your high-risk users through enhanced human risk scoring. This improved visibility enables you to prioritise security efforts, apply adaptive security controls and provide additional education to those most at risk.

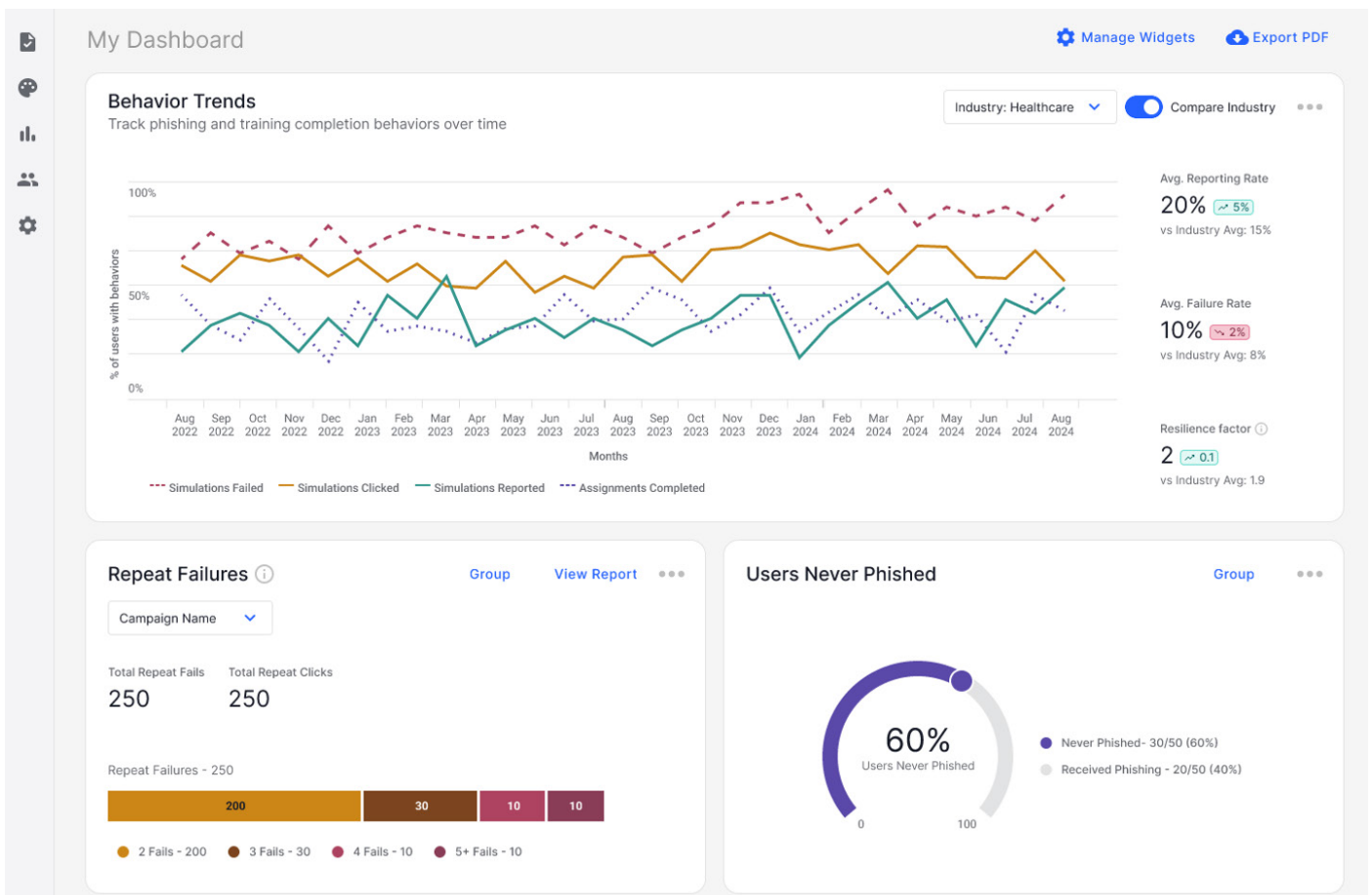
## Help users build resilience against emerging threats

User Protection gives your employees the tools, knowledge and motivation to be more resilient against evolving social engineering tactics.

Informed by Proofpoint global threat intelligence, our solution gives you immediate insights into the ever-changing threat landscape. With these insights, you can educate your users on trending and emerging threats. You can deliver targeted

education, including training, threat simulations and notifications, to your VAPs on specific threats that they face. You can also tailor the training to suit users' roles, behaviours and unique risk profiles.

With the Adaptive Groups and Pathways features, you can automatically enrol your high-risk users into targeted campaigns. This saves you time and effort in building a robust behaviour change programme. It also guides your users to make safer choices in the face of threats.

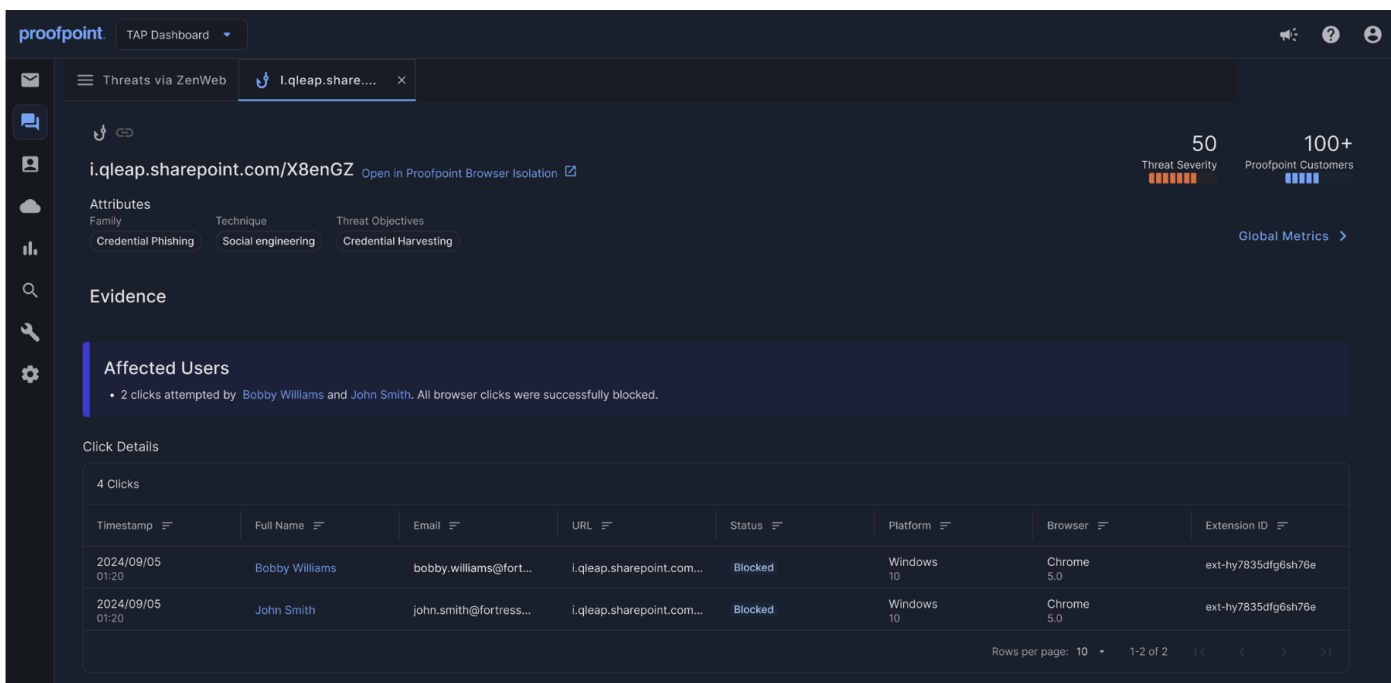


**Figure 2:** User Protection is informed by Proofpoint global threat intelligence. It gives you insights about the ever-changing threat landscape. You can educate your users on new threats while capturing behaviour trends over time.

## Block malicious links across multiple platforms

Cybercriminals now exploit digital channels other than email. These include Microsoft Teams, Zoom, Slack, LinkedIn and other social media platforms. User Protection gives you extended protection by blocking malicious URLs in all of these channels.

User Protection is powered by Proofpoint Nexus, which analyses over 21 trillion URLs. Based on this intelligence, User Protection conducts URL reputation inspection and analyses any URL in the browser. When an employee tries to access a link in a messaging or collaboration tool, User Protection analyses the URL in real time. If it finds that a URL is malicious, it blocks it. In this way, your users stay protected from malicious websites and content.



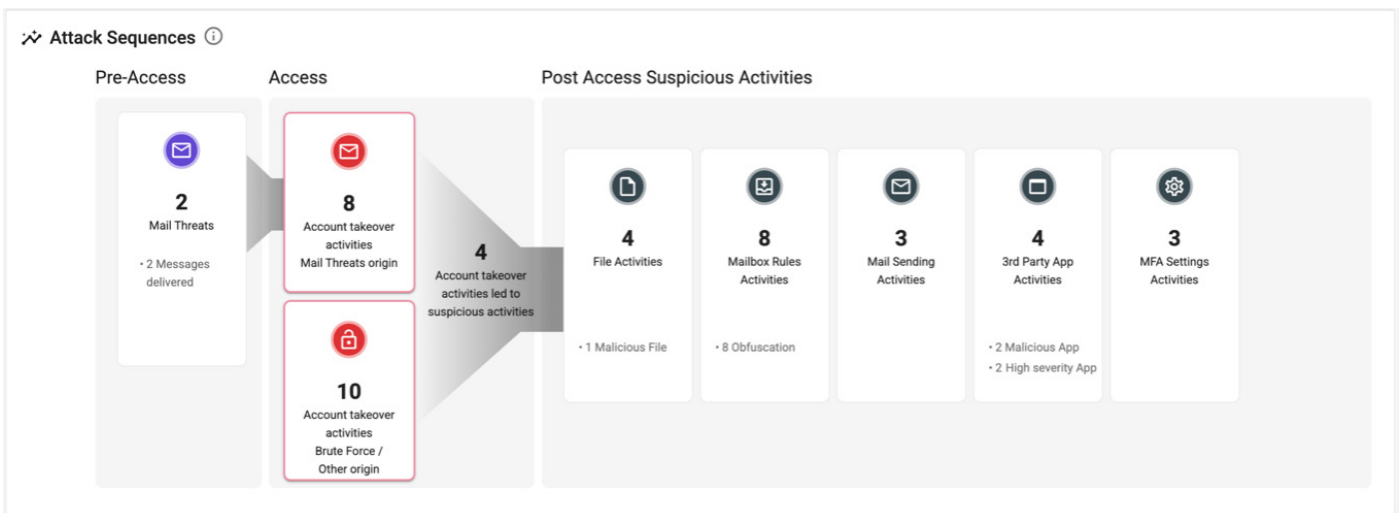
**Figure 3:** Proofpoint extends phishing protections beyond email. It also blocks malicious URLs that are shared in messaging, collaboration and communication platforms.

## Quickly detect and respond to compromised accounts

When your employee's account has been compromised in a tool such as Microsoft 365, Google Workspace or Okta, User Protection gives you peace of mind. It detects and responds to the incident before any damage is done. Using AI, machine learning, behavioural analytics and threat intelligence from Nexus, User Protection detects suspicious cloud account activities. It correlates these with email threats to more accurately identify and reverse account takeovers.

Competitive solutions have limited abilities to respond to post-account-takeover activities. By contrast, Proofpoint speeds up your threat response after it detects an account takeover. It identifies changes made by attackers and removes their access. It forces password resets, reverts updates to mailbox rules and multifactor authentication (MFA) settings and breaks connections to malicious third-party applications. It also quarantines and removes any files that were uploaded by the threat actor.

With User Protection, you can automate all of these actions. This means that you spend less time investigating and responding to account takeovers and minimise the potential damage to your organisation.



**Figure 4:** User Protection shows you pre- and post-access malicious activities for affected accounts.

## Leverage our expertise, optimise your security programme

Technology is crucial for threat protection, but a modern approach must also address people and processes. With the right skillsets, optimised solutions and strong security cultures, organisations can adapt to an evolving threat landscape.

By combining Proofpoint premium services with Proofpoint solutions, you gain access to a team of experts who help deploy and manage a comprehensive, human-centric threat protection strategy for you. From guidance to hands-on system and programme management, the Proofpoint Premium Services team helps deliver real security outcomes and accelerate your time to value.

# 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 cyberattacks. Leading organisations of all sizes, including 85 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](http://www.proofpoint.com).

Connect with Proofpoint: [X](#) | [LinkedIn](#) | [Facebook](#) | [YouTube](#)

Proofpoint is a trademark or tradename of Proofpoint, Inc. in the United States and/or other countries. All other trademarks contained herein are property of their respective owners. ©Proofpoint, Inc. 2025

**DISCOVER THE PROOFPOINT PLATFORM →**