

# PROOFPOINT EMAIL ISOLATION

## ISOLATE YOUR PEOPLE FROM ADVANCED THREATS TARGETING BOTH CORPORATE AND PERSONAL ENVIRONMENTS

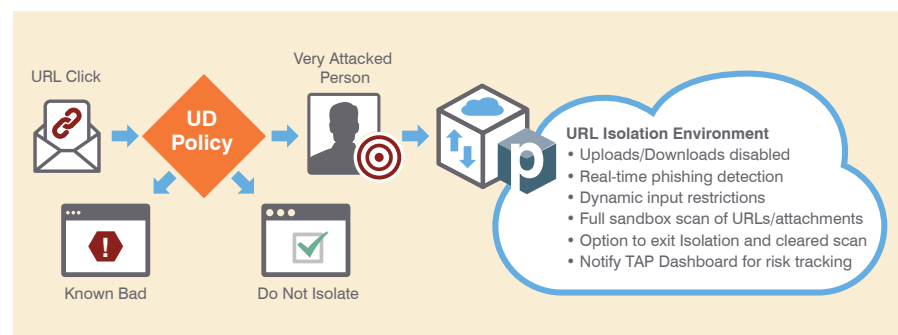
### KEY BENEFITS

- Isolate malicious URLs in corporate email through risk-based adaptive control
- Isolate personal webmail to prevent spread of threats to corporate devices
- Prevent credential theft and harvesting
- Deploy quickly and easily from the cloud—no hardware or endpoint agents needed
- Provide your people with a seamless browsing experience
- Simplify compliance for EU GDPR

It's an ongoing struggle to protect your people against targeted phishing attacks and credential theft. To make matters worse, attackers are quickly getting the upper hand by using malicious URLs for large-scale campaigns. How do you protect against these growing threats? With Proofpoint Email Isolation, you can allow your people to access their personal and corporate email securely while defending against malware and data loss.

### PRODUCT DESCRIPTION

Email Isolation lets your users access their personal email and corporate email safely. It does this by isolating personal email sessions in a secure container. This unique solution protects you against malware and malicious content. It disables uploads and downloads. And it prevents theft or loss of sensitive data. Email Isolation helps you solve the security, productivity and privacy challenges that come with targeted phishing attacks and high-risk personal email use. Plus, it's simple to deploy, manage and support.



### FEATURES AND BENEFITS

#### Adapt Security to Risky URLs and Targeted Users

Today's attackers are targeting specific individuals in your organization with phishing emails. You need additional adaptive controls to protect your most attacked people. Email Isolation protects your people from malicious web-based content in corporate email. It isolates browser sessions based on policy to protect you and your people from high-risk URLs. These include unknown URLs, social networks and online cloud applications.

Integration with Proofpoint Targeted Attack Prevention (TAP) allows current TAP customers to leverage Email Isolation for corporate email. People-centric controls combined with TAP are an effective way to lower risk. You can select

users for the isolation environment based on risk factors in your corporate email. Integration with TAP provides you with real-time phishing detection and scanning. The solution reports isolated browser sessions to the TAP dashboard so you gain visibility and can track risk.

### Reduce Your Attack Surface

Like many organizations, you allow your people to use personal webmail at work. Attackers know this and leverage this to launch sophisticated attacks. In fact, research shows that up to 60% of attacks result from web or personal email use on corporate devices. How do you reduce risk while still giving your people the freedom to use personal email?

With Email Isolation, you can choose to isolate user access to personal email sites. While your people safely access personal webmail, you improve your organization's security posture. There's zero risk to corporate assets. Inspecting files and tracking your users' behavior are not necessary. Plus, personal email attachments with payloads or malicious macros are never downloaded. The solution even isolates content sent via corporate email from trusted sites that have been compromised. This safeguards you from watering-hole attacks and email links to weaponized cloud applications like Microsoft SharePoint, Dropbox and others. Through dynamic input restrictions, browser-based credential theft is also reduced. Additionally, Email Isolation prevents drive-by downloads. And it keeps other malicious web content sent via email away from your endpoints.

### Reduce the Burden on IT

You have real concerns about giving your people permission to access personal webmail. You know how risky that can be. But your people often have good reasons for accessing personal email on their corporate device. With most solutions, IT teams must decide whether to allow or block these sites. If all these domains are blocked, IT is flooded with requests for one-off exceptions to access specific sites.

Email Isolation provides a better way. It solves security, productivity and privacy challenges associated with employee personal email use. And by keeping browsing sessions in a secure, isolated container, your people can freely access personal webmail. This also benefits IT because they no longer spend their time and effort making exceptions on a case-by-case basis. And it's simple to deploy, manage and support. Your organization will realize immediate cost savings from higher IT productivity. Plus, you'll boost employee morale by trusting your users. You'll also avoid compliance violations by keeping user webmail private. Email Isolation is easy to deploy because it's 100% cloud-based. And you can integrate it with your own web filter, proxy, gateway and firewall.

## LEARN MORE

For more information, visit [www.proofpoint.com](http://www.proofpoint.com).

#### ABOUT PROOFPOINT

Proofpoint, Inc. (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 to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. More information is available at [www.proofpoint.com](http://www.proofpoint.com).

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