

# Proofpoint Email Isolation

## Isolate your people from advanced threats targeting corporate and personal environments

### KEY BENEFITS

- Isolate malicious URLs in corporate email through risk-based adaptive control
- Isolate personal webmail to prevent the 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

Proofpoint Email Isolation lets your people freely access personal email without exposing your organisation to malware and data loss. It uses cloud-based isolation technology to reduce your attack surface and secure users' personal email activity.

Email Isolation renders email sessions in a secure container to keep harmful content out of your environment. Users can view and interact with their email as normal. But malware and other harmful content are removed from the page. Uploads, downloads and input forms are disabled to prevent data theft and loss.

Our unique solution helps you solve the security, productivity and privacy challenges that come with targeted phishing attacks and high-risk personal email use. And it's fully cloud-based, so it's simple to deploy, manage and support.

### Adapt security to risky URLs

Today's attackers target people in your organisation, often through phishing emails. Adaptive controls can help protect your riskiest users as threats evolve.

Email Isolation protects against malicious web-based content in corporate email.

Browsing sessions triggered by URLs in email are isolated automatically based on your policy. You can set Email Isolation to isolate:

- Unknown URLs
- Links from social networks
- Links from online cloud applications

### Adaptive security for targeted users

Through its integration with TAP, Email Isolation can also isolate URLs in email sent to your riskiest users. You can apply isolation to corporate email users based any combination of risk factors.

The integration also provides you with real-time phishing detection and scanning. When an isolated browser session is triggered, it's reported to the TAP dashboard to unearth new threats and track risk. Integrating adaptive, people-centric controls and TAP is an effective way to lower risk.

## Reduce your attack surface

Many organisations allow people to use their personal webmail or browse the internet at work. Attackers know this—and they take advantage of the situation to launch sophisticated attacks. In fact, research shows that more than half the attacks result from web or personal email use on corporate devices.

Email Isolation helps reduce risk while still giving your people the freedom to use personal email. You don't have to block access, inspect files or track users' behaviour. Instead, you simply redirect websites and cloud apps to an isolated session, safely fenced off from your environment.

Our cloud-based solution protects against a wide range of browser-based attacks. These include watering-hole attacks and email links to weaponised cloud apps such as Microsoft SharePoint and Dropbox.

In an isolated session, files and email attachments (with payloads or malicious macros) are never downloaded. User input is limited dynamically to reduce browser-based credential theft. And downloads are blocked, preventing drive-by malware attacks. It also keeps all kinds of other malicious web content away from your endpoints. It even isolates content from trusted sites that have been compromised.

## Reduce the burden on IT

Sometimes, your people need to access personal webmail. With most solutions, IT teams must decide whether to allow access and accept the risk or block them and get in the way of users' work. Often, IT is flooded with requests for one-off exceptions to access specific sites.

Email Isolation provides a better way. It lets users access their personal email freely, safely and privately in an isolated container. It reduces the burden on your IT team, which no longer has to actively manage exceptions on a case-by-case basis. And it frees your organisation from the security, productivity and privacy challenges of employees' personal email use.

Our solution also helps keep you compliant. Isolated browsing sessions are completely hidden from your environment and IT staff. That means you'll avoid any employee-privacy issues and compliance violations.

Email Isolation is easy to deploy because it's fully cloud based. And best of all, it works with the web filter, proxy, gateway and firewall tools you already own.

It all adds up to lower costs, higher IT productivity and better user morale.

## LEARN MORE

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

### ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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 more than half of the Fortune 1000, 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](https://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.