proofpoint.

PROOFPOINT BROWSER ISOLATION

PROTECT USERS FROM ADVANCED THREATS TARGETING CORPORATE AND PERSONAL ENVIRONMENTS

KEY BENEFITS

- Isolate malicious URLs in corporate email through risk-based adaptive control
- Use browser isolation for high-risk web use, such as unknown or new domains
- 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 Browser Isolation, you can allow your people to access the internet securely while defending against malware and data loss.

PRODUCT DESCRIPTION

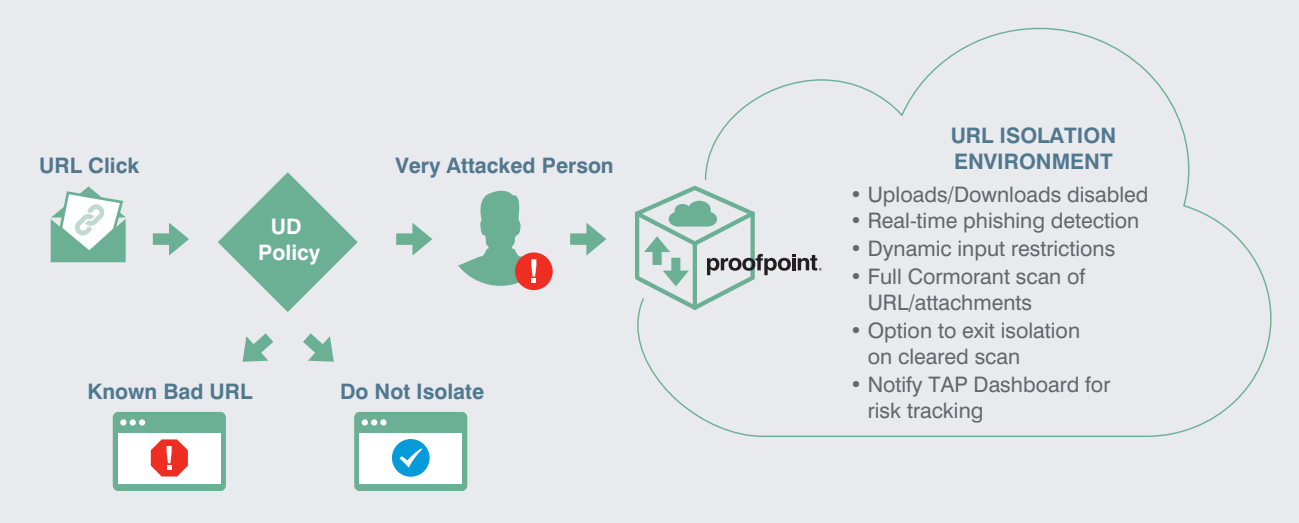
Browser Isolation lets your users access websites, personal email and corporate email safely. It does this by isolating browser sessions in a secure container. This unique solution protects you against malware and malicious content. It disables uploads and downloads. And it prevents theft or loss of sensitive data. Browser Isolation helps you solve the security, productivity and privacy challenges that come with targeted phishing attacks and high-risk web 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 organisation with phishing emails. You need additional adaptive controls to protect your most attacked people. Browser Isolation protects your people from malicious web-based content in corporate email. With Browser Isolation, browser sessions are isolated 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 Browser 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. Isolated browser sessions are reported to the TAP dashboard so that you gain visibility and can track risk.



Reduce Your Attack Surface

Like many organisations, you allow your people to use personal webmail or browse the internet 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 browse the internet and use personal email?

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

Reduce the Burden on IT

You have real concerns about giving your people permission to access uncategorised or unknown URLs and personal webmail. You know how risky that can be. But your people often have good reasons for browsing these sites. With most solutions, IT teams have to 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.

Browser Isolation provides a better way. It solves security, productivity and privacy challenges associated with employee web use. And by keeping browsing sessions in a secure, isolated container, your people can freely access personal webmail and other sites. This also benefits IT because they no longer have to spend their time and effort making exceptions on a case-by-case basis. And it's simple to deploy, manage and support. Your organisation will realize immediate cost savings from higher IT productivity. Plus, you'll boost employee morale by trusting them. You'll also avoid compliance violations by keeping user webmail private. Browser 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.

For more information, visit www.proofpoint.com/uk.