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 GDPR

Proofpoint Browser Isolation lets your people freely access websites, personal email and corporate email without exposing your organization to malware and data loss. Drawing on threat intelligence from Proofpoint Targeted Attack Protection (TAP) it uses cloud-based isolation technology to reduce your attack surface and secure users' web activity. Used with TAP, you can also isolate unknown and risky web links to stop URL-based threats.

Browser Isolation renders browser sessions in a secure container to keep harmful content out of your environment. Users can view and interact with the web page 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. And our proprietary real-time anti-phishing scan analyses the site and automatically blocks further use of the page if it finds a threat.

**Adaptive security for risky URLs**

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

Browser 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 Browser Isolation to isolate:

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

**Adaptive security for targeted users**

Through its integration with TAP, Browser Isolation can also isolate URLs in email sent to your riskiest users. You can apply isolation to corporate email users based on 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 organizations 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, more than half of the attacks result from web or personal email use on corporate devices.

With Browser Isolation, you don’t have to block access, inspect files or track users’ behavior. Instead, you simply redirect websites and cloud apps to an isolated session, safely fenced off from your environment.

Browser Isolation protects against a wide range of browser-based attacks. These include watering-hole attacks and email links to weaponized 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

All users are not created equal. Different users pose different risks and need different levels of control. And sometimes, your people need to access unknown URLs and 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.

Browser Isolation provides a better way. It allows admins to create multiple browsing policies to control groups of users and their access. You can create and manage access codes that can be shared to grant users access to new policies. Researchers, executives and other users who need broader access can have separate, less restrictive controls.

These adaptive controls help reduce the burden on your team, and IT no longer has to actively manage exceptions on a case-by-case basis.

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.

Browser 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.