Proofpoint Isolation

Protect users from advanced web threats and malicious URLs in corporate and personal email

Key Benefits

- Inspect all web content in real time
- Defend against ransomware and zero-day URL attacks
- Isolate malicious URLs in all apps, including secured social media and collaboration apps
- Isolate personal webmail, uncategorized and suspicious sites
- Prevent credential theft and harvesting
- Get inline and real-time DLP for file upload and download
- Simplify compliance with regional data privacy regulations
- Deploy quickly and easily from the cloud—no hardware or endpoint agents needed

Proofpoint Isolation secures the web browsing and email activities of your users. It uses cloud-based remote isolation to allow your people to access websites and their personal and corporate email freely, without exposing your organization to malware and data loss.

Proofpoint Isolation helps solve the security, productivity and privacy challenges that come with browsing to malicious websites, targeted phishing attacks and high-risk personal webmail use. It is fully cloud-based, so it is simple to deploy, manage and support. Proofpoint Isolation is included in the Information Protection and Cloud Security platform.

When your people browse to a risky website or click on a URL in corporate email or webmail, Proofpoint Isolation renders the page in a secure container off your network and off your users' device. This keeps harmful content out of your environment. Users can view and interact with an isolated web page as normal, but malware and other harmful content are removed from the page. Uploads, downloads and input forms may be disabled to prevent data theft and loss. And our proprietary real-time content inspection detects zero-day threats, such as phishing URLs and ransomware. Our solution automatically blocks further use of the page if a threat is discovered.

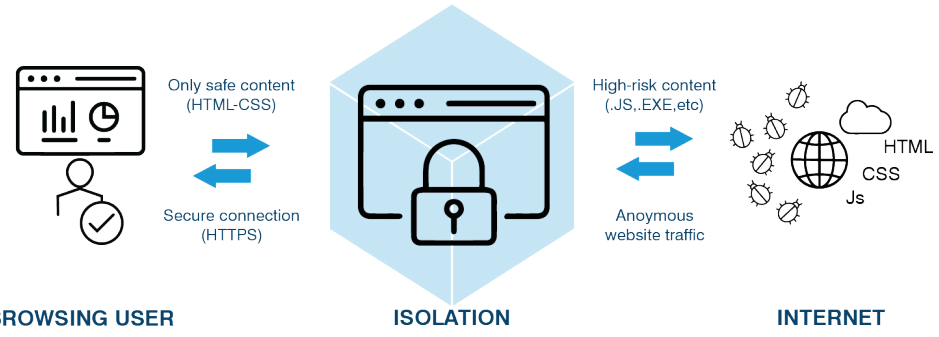

Figure 1: Proofpoint Isolation strips executable code from web pages, then renders safe pages back to the user in the isolation browser.

Leverage Adaptive Security for Risky URLs and Targeted Users

Today's attackers target people in organizations, often through emails that result in compromised accounts, stolen credentials and sensitive data loss. Adaptive controls can help protect your riskiest users as threats evolve. Browsing sessions triggered by URLs in email are isolated automatically based on your policy. You can send high risk and uncategorized sites, including webmail, to isolation.

Through its integration with Proofpoint Targeted Attack Protection (TAP), Proofpoint Isolation can isolate URLs in corporate email sent to your riskiest users. The TAP 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 reveal new threats and lower risk.

Shrink Your Attack Surface

Many organizations allow people to use their personal webmail or browse the internet while on the corporate network. Knowing this, threat actors target specific people using personal webmail to launch sophisticated attacks. More than half of these attacks result from web or personal email use on corporate devices.

Proofpoint Isolation mitigates risk while still letting your people use personal webmail freely and browse the internet safely. You don't have to block access or track users' behavior. You simply redirect traffic to risky websites and cloud apps to an isolated session. This is safely off your corporate environment, in the cloud and off your users' devices. Proofpoint 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 isolated sessions, files with payloads or malicious macros are not downloaded. Proofpoint Isolation dynamically limits user input to reduce browser-based credential theft. It blocks downloads, preventing drive-by malware attacks. It also keeps all kinds of other malicious web content from your endpoints. And it isolates content from trusted sites that have been compromised.

Reduce the Burden on IT

Different users pose different risks and need different levels of access. Sometimes, your people must access unknown URLs and personal webmail. Most solutions require IT teams to decide whether to allow access and accept the risk or block access completely, which gets in the way of users' work. IT is often flooded with requests from individuals and groups for one-off exceptions to access specific sites. Managing these exceptions can be time-consuming and challenging.

Proofpoint Isolation addresses this by letting admins create multiple browsing policies to control groups of users and their access. For instance, 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 needs to actively manage exceptions on a case-by-case basis.

Proofpoint Isolation is integrated with Proofpoint Enterprise Data Loss Prevention (DLP). This provides inline and real-time DLP for uploads and downloads of sensitive data. Our solution provides shared data classification and a single pane of glass for alert management and investigation. You can restrict uploads and downloads by URL, URL category, file type and whether the file contains sensitive data or malware.

Isolated browsing sessions are completely hidden from adversaries, so they can't target your users. Our solution also helps you support local data privacy regulations. That means you'll avoid any employee-privacy issues and compliance violations.

Proofpoint Isolation is easy to deploy and works with the web filter, proxy, gateway and firewall tools you already own

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance 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 75 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**.