Proofpoint Email Isolation

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

Key Benefits

- Isolate malicious URLs in corporate email through risk-based adaptive controls
- Isolate personal webmail to prevent the spread of threats to corporate devices
- Prevent credential theft and harvesting
- Lower risk of data loss
- Simplify compliance with regional data privacy regulations
- Deploy quickly and easily from the cloud—no hardware or endpoint agents needed

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

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

When your people click on URLs in corporate email or webmail, Email Isolation renders the page in a secure container off your network. This keeps harmful content out of your environment. Users can view and interact with their web page as normal. But malware and other harmful content are removed from the page. Uploads and downloads may also be controlled to prevent data theft and loss.

Leverage Adaptive Security for Risky URLs and Targeted Users

Today's attackers often use phishing email to target people in organizations. 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

Through its integration with Proofpoint Targeted Attack Protection (TAP), Email Isolation can isolate URLs in corporate email sent to your riskiest users. You can apply isolation to corporate email for specific high-risk users or URL categories.

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

Shrink Your Attack Surface

Many companies let their people access personal webmail while on the corporate network. Threat actors know this. And they 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.

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' behavior. Instead, you simply redirect webmail sites to an isolated session. This is safely off your corporate environment. It is in the cloud and off your users' devices.

When your people click on a URL in either personal webmail or corporate email, every loaded page is scanned for threats. Uploads and downloads, which may contain payloads or malicious macros, are blocked. User input is limited dynamically to reduce browser-based credential theft.

Reduce the Burden on IT

Sometimes, your people need to access personal webmail. With most solutions, IT teams must decide whether to allow this access and accept the risk, or to block access completely and get in the way of users' work. IT is often flooded with requests from individuals and groups for one-off exceptions to access specific webmail sites. Managing these exceptions can be challenging and time-consuming.

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

Our solution also helps you comply with local data privacy regulations. 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 is fully cloud-based. It 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**.