

PROOFPOINT TARGETED ATTACK PROTECTION ISOLATION PERSONAL WEBMAIL DEFENSE

EASILY AND EFFECTIVELY PROTECT PERSONAL WEBMAIL ACTIVITIES

Today's cyber criminals are exploiting people as their favorite way to beat security controls. Email and social media have nearly 100% reach to business users around the world. As a result, 90% of cyber attacks reach victims through these venues. They compromise your network, steal credentials and gain access to your assets.

Since corporate email is now the number one vector for malicious infections, these attackers have now turned their efforts to lucrative opportunities in the personal webmail space. By isolating non-work-related interaction, you can save your organization significant time and money. It substantially reduces the time associated with the SOC, security analyst and incident response investigation time. It also helps you enforce your internal data use policy to keep your agency resources focused on what's important.

Personal Webmail Defense protects you and your employees across personal webmail. It is built with simplicity at its core and based on intelligence from Targeted Attack Protection (TAP). And it empowers you to protect hundreds of thousands of users in days—not weeks or months.

Personal Webmail Defense detects both known and new, never-before seen attacks. These use malicious attachments and URLs to download malware on a device or trick users to share their passwords or other sensitive information.



Personal Webmail Defense gives you visibility into your greatest security risk—your people. We protect them from the threats that target them, protect the data they work with and protect the users themselves.

KEY BENEFITS

Privacy

Personal Webmail Defense allows you to respect your users by giving them the greatest level of freedom, privacy and anonymity. And it provides consistency with your internet acceptable use and security-related requirements. We are committed to protecting your privacy and our solution seeks to provide your users with a limited right-to-privacy for personal communications and web use.

- The only personal information collected about you is the corporate email address used to register (“provision”) your browser for use on our service. The corporate email is used only for provisioning and de-provisioning your access and is not used as part of any ongoing authentication or web use.
- Secure sessions are established to connect to our cloud provisioned container where each user's browsing session is rendered via HTML 5 and Cascading Style Sheets (txt). Using HTML 5 allows us to support XSF stripping and to block active content such as Flash and Silverlight.

Deploy quickly in the cloud. Realize value immediately.

Our cloud architecture provides you with optimal scalability. This allows you to deploy Personal Webmail Defense quickly and derive value immediately.

- Your users can use their personal webmail the way they normally do with their preferred browser. There's no software or special browser required. It provides performance that's comparable to accessing the web directly—with no noticeable difference or latency.
- Personal Webmail Defense is designed to simplify the job of your IT teams managing employee webmail use. Its 100% cloud-based design, ease of use, and streamlined user self-provisioning means it requires minimal time to deploy. And it requires virtually no user training or support.

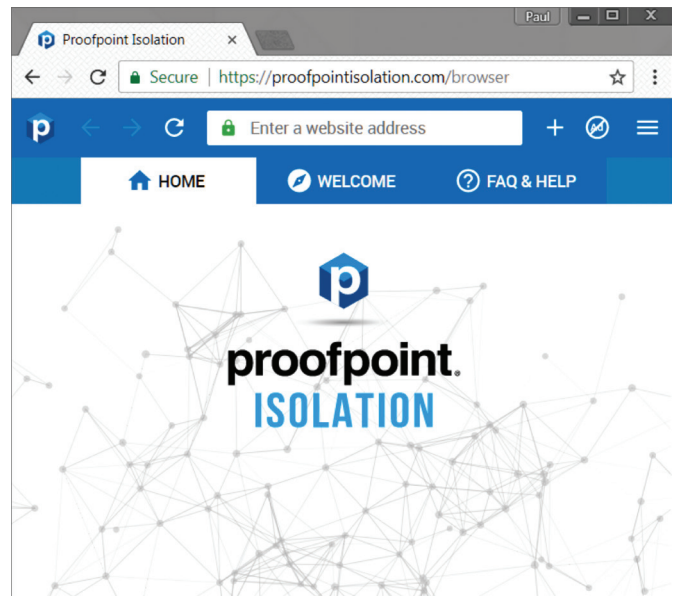
Dynamically provision your users with limited and isolated access to various web mail providers. And do it without changing your security posture.

Personal Webmail Defense helps you meet GDPR regulations. It provides you and your users with compliant, anonymous and protected webmail access. And it does this by directing your user's activity through a secure and isolated container in our off-premise network.

- Through Personal Webmail Defense, user access to webmail services is provisioned without allowing your users to download or upload from the local network environment. It safely renders only passive content (like HTML) to the endpoint.
- Rather than use traditional detect and remove techniques, Personal Webmail Defense isolates personal webmail within our cloud browsers. And it synchronizes only the safe presentation layer (HTML/CSS) back to your user's browser. This prevents any unknown code from being executed on the end-point.
- All potentially risky actions are prohibited. This includes downloads and uploads.

Leverage the power of integrated threat intelligence

It's important to have web isolation technology with integrated threat intelligence. This protects your users from today's sophisticated attacks. We provide an integrated fabric of threat intelligence that gathers data from email, mobile and social threat vectors. And we bring to bear the most powerful database in the industry. Along with our web isolation technology, this protects you across all the ways attackers are targeting your employees and customers.



ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.