Browser and Email Isolation

Organizations are in a constant struggle to protect their users from targeted phishing attacks. Most of these attacks enter corporate environments through corporate email. But users' web browsing and personal email are also fast-growing vectors of compromise.

Research shows that up to 60% of attacks in the enterprise come from web or personal email usage on corporate devices.[1] These channels can be difficult to safeguard at all—let alone in a way that doesn't frustrate users, invade their privacy or impede their workflow. An all-or-nothing approach—blocking personal browsing completely or setting loose an internet free-for-all—is rarely effective.

Proofpoint Email Isolation and Proofpoint Browser Isolation help stop phishing attacks without the productivity-crimping effects of broad website blocks and similar controls. They give IT and security teams an adaptive, risk-based control and added layer of security. With Email Isolation and Browser Isolation, you can stop attacks that target your users in corporate email, personal email and web browsing.

The solutions are simple to deploy, manage and support. Unlike many isolation tools, Email Isolation and Browser Isolation are fully cloud-based and offer hands-free operation. Browsing sessions triggered from uncategorized, potentially risky URLs are automatically isolated from the corporate environment and made safe for users. Users get freedom and privacy. IT and security teams get assurance and visibility into the threats that target their people.

THE DAILY STRUGGLES OF END-USER RISK

Cyber attackers are getting more creative and sophisticated. They're focusing less on infrastructure and more on people. As part of that shift, they're also targeting individuals rather than entire organizations. Here are just a few of the threats organizations face:

Web-based malware attacks

- Drive-by downloads and compromised websites are a way for attackers to infect victims and gather information.
- Credential phishing, malicious reconnaissance and other attacks with no malicious payloads may evade traditional sandboxes.
- Attackers research their targets and target specific users; we call these Very Attacked People™ (VAPs).

Targeted Phishing/URL-based email campaigns

- Legacy tools used to block phishing campaigns have improved. But they still struggle with new and unknown URLs.
- Targeted phishing and state-sponsored attacks often compromise personal email accounts to gain a foothold on corporate assets.

Unknown and uncategorized domains

- Someone always clicks an unsafe URL that reaches the inbox

Heavy burden on internal IT teams

- Managing domain exceptions for blocklists and safelists is cumbersome. And it requires processes, often futile, for dealing with compromised domains.
- Many vendors bundle their web isolation solution with a resource-hogging endpoint agent. That slows users' PCs and hampers work.
- Restricting URLs to a pre-vetted list of allowed sites is a sure way to anger and frustrate users.
- People always try to get around security-mandated roadblocks by moving their work to unprotected personal devices or outside networks.

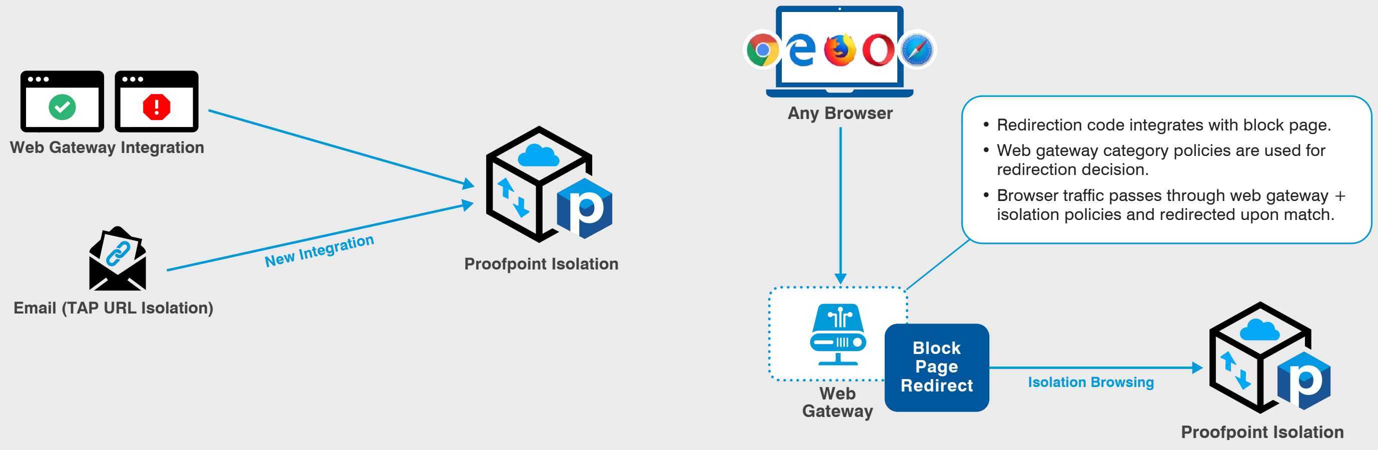
TO ATTACKERS, USERS ARE NOT CREATED EQUAL

When it comes to people-focused attacks, there is no such thing as a silver bullet. Trying to protect everyone to the same degree and in the same way drives up costs and creates needless burdens for low-risk users.

That's because people are unique. So is their value to cyber attackers and risk to employers. They have distinct digital habits and weak spots. They're targeted by attackers in diverse ways and with varying intensity. And they have differing levels of privileged access to data, systems and other resources on the network and in the cloud.

As attackers become more sophisticated, they research and choose specific people in an organization to attack with well-crafted phishing attacks. These VAPs require even more protection.

[1] Osterman Research. "Why You Should Seriously Consider Web Isolation Technology." December 2018.


Web Gateway Integration
Email (TAP URL Isolation)
New Integration
Proofpoint Isolation
Any Browser
• Redirection code integrates with block page.
• Web gateway category policies are used for redirection decision.
• Browser traffic passes through web gateway + isolation policies and redirected upon match.
Web Gateway
Block Page Redirect
Isolation Browsing
Proofpoint Isolation

Proofpoint Isolation—Integrations

THE SOLUTION: ADAPTIVE ISOLATION

Browser and Email Isolation meets organizations' security needs without getting in users' way. Instead of a one-size- fits-all approach to security, the solutions tailor isolation controls according to users' unique vulnerabilities, attack profile and privilege. Everyone stays protected. But users most vulnerable to attack, those targeted more heavily, and those with access to the most sensitive data and systems get an added layer of security.

Browser Isolation and Email Isolation work with the existing web filters you own—whether it's your proxy, web gateway or firewall—in addition to Proofpoint Targeted Attack Protection (TAP). New and unknown URL links are rendered in a managed and isolated browsing session to keep threats out of the corporate environment.

HTML code isn't rendered on their local PC. Instead, isolation uses a remote cloud-based browser to manage users' activity in a secure container. High-risk content, including executable code, is stripped out. A sanitized form of the page is sent to users' browsers. Any unsafe content users would normally encounter never enters the endpoint—or the enterprise.

Users can view the contents of the site as normal. But they can't download or upload content. And if content is restricted based on domain specific settings, they can't input data into forms. At the same time, the website can't:

- Escalate privileges or gain root access
- Execute malicious code
- Make persistent unauthorized system changes
- Alter critical system files

Coupled with our people-centric controls, Browser Isolation and Email Isolation take a tailored, risk-based approach to keeping users safe. You can selectively direct users to the isolation environment based on key risk factors. Suspicious and uncategorized URLs can be accessed safely—even as they're analyzed by TAP in the background. Once TAP has deemed the URL safe, users are given the option of leaving the isolated environment and loading the full version of the website.

Here are the major benefits of adaptive isolation.

Reduces the Attack Surface

Browser Isolation and Email Isolation help organizations take a smarter approach to keeping users' high-risk browsing out of the corporate environment. That gives employees more autonomy and eliminates the risk from uncategorized sites and personal browsing—without the security downsides.

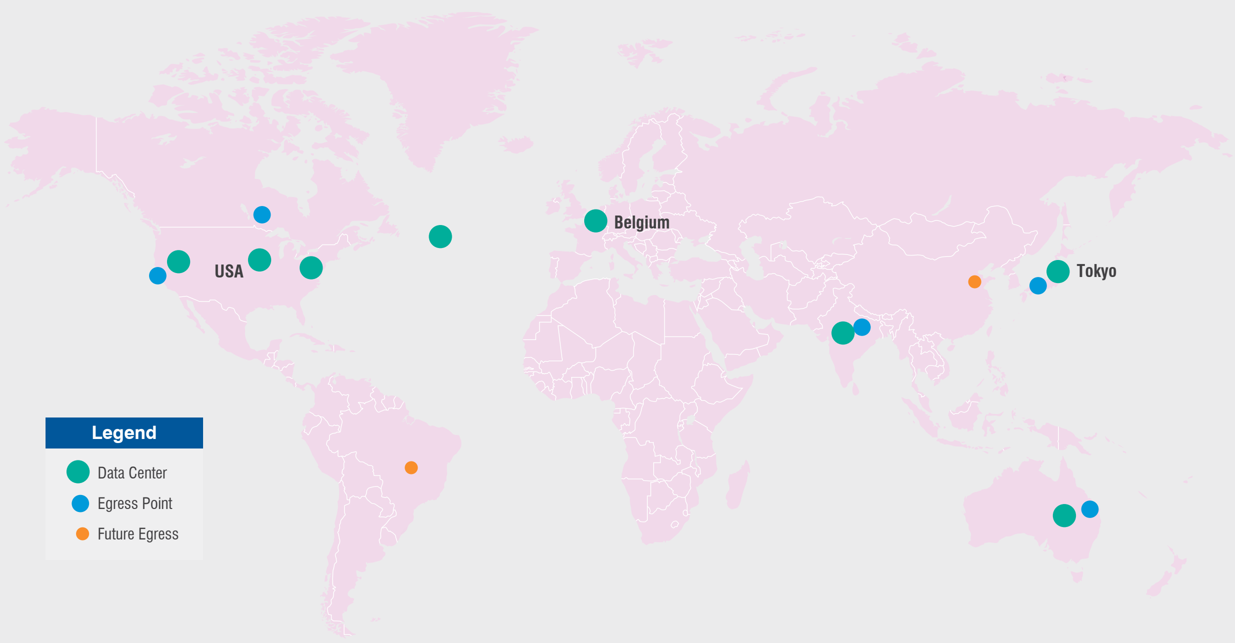
Here's how Browser Isolation can enhance your security posture:

- Near-zero risk to corporate assets. No need to inspect files and track user behavior.
- No downloads of files or email attachments with potential payloads or malicious macros.
- While in an isolated browser session, files are re- rendered and sanitized into safe HTML5 content for viewing and printing.
- Browser-based credential theft is reduced in the isolated session through dynamic keyboard input restrictions.
- Drive-by downloads and other malicious web content cannot be executed on users' local endpoint.
- Isolates content from potential compromised trusted sources, such as watering-hole attacks and email links to weaponized cloud apps (including as SharePoint, Dropbox and OneDrive).

Reduces the Burden on Internal IT Teams

With other traditional URL filtering technologies, IT teams must decide to either allow or block all uncategorized URLs, personal webmail or other risky sites. If all these categories are blocked, IT teams are often flooded with requests from users for one-off exceptions for specific sites.

With Browser Isolation, IT teams no longer spend time managing exception requests. All URLs can be safely viewed in an isolated browser—and used in full once they're deemed safe.



Proofpoint Isolation Across the Globe

For organizations, that means:

- Immediate IT cost savings. No need for one-off exceptions of uncategorized URLs or personal webmail sites.
- Higher employee productivity and morale. Users aren't frustrated by blocks or burdened with creating support tickets.
- Employee privacy while in isolated browser sessions; compliance with worker privacy rules.
- Simplified deployment and integration with your existing web filter (proxy, gateway, firewall)— leverage what you already own.
- Full cloud-based deployment—no hardware or endpoint agents to install. Setup is fast, and time-to- value is almost immediate.

DIFFERENTIATORS

Here's how Browser Isolation and Email Isolation are more effective than legacy isolation tools.

- Time to Value and Ease of Deployment
  - 100% cloud—No on-prem hardware or software requirements
  - No endpoint agent needed
  - No special browser configuration (such as proxy configuration)
- Ease of Integration
  - No complex proxy chaining required
  - Leverage existing investments for integrations (proxy, web gateway, firewall, endpoint web filtering, Proofpoint Protection and TAP)
- Threat Detection and Intelligence
  - Real-time phishing detection and deep scan sandboxing with Proofpoint Protection and TAP
  - Proofpoint Isolation uses the same threat intelligence that protects the Proofpoint ecosystem and corporate email
  - The depth and breadth of Proofpoint intelligence is unmatched in the industry
- Privacy
  - The only web isolation service that has prioritized user privacy to meet strict European privacy laws
  - Blind to web traffic outside of isolated sessions

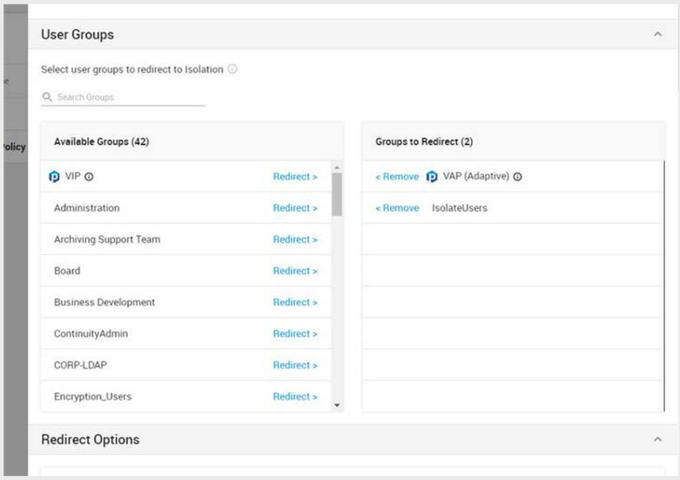
REQUIREMENTS FOR INSTALLATION

Browser Isolation and Email Isolation are cloud-based solutions, fully available anywhere you are. That means you don't have to install anything on endpoint devices or on your network.

From users' view, little changes. They browse the web as they always have—on their preferred browser over the usual corporate network. In the background, their browser traffic redirects to our production domain. Users' web pages are isolated within a remote cloud-based browser. All active content, such as scripts, are executed there. Only safe HMTL, CSS and static content, such as images, are sent to users' local browser.

Proofpoint Browser Isolation supports all modern web browsers, including:

- Internet Explorer 11 on Windows 7, 8 and 10
- Edge on Windows 10
- Safari on Mac OSX
- Firefox on Windows 10, Mac OSX
- Chrome on Windows 10, Mac OSX



User Groups

Select user groups to redirect to Isolation

Search Groups

Available Groups (42)	
VIP	Redirect >
Administration	Redirect >
Archiving Support Team	Redirect >
Board	Redirect >
Business Development	Redirect >
ContinuityAdmin	Redirect >
CORP-LDAP	Redirect >
Encryption_Users	Redirect >

Groups to Redirect (2)	
< Remove	VAP (Adaptive)
< Remove	IsolateUsers

Redirect Options

WEBFILTER INTEGRATION

We can integrate with all of your existing infrastructure, whether it's your proxy, web gateway, firewall, endpoint web filtering, Proofpoint Protection or TAP. Users can be registered in Browser Isolation two ways.

The first is to access our production domain with their default browser. You can send a direct link from a dedicated corporate email address or on an initial visit to an isolated domain.

The second is through the public IP address space for the domain in your Browser Isolation configuration. This way, all users coming from the configured address space are automatically sent into the isolation environment.

Once configured, organizations can issue a block page depending on the website category. Most customers choose to seamlessly redirect users into an isolated environment. They configure the block page as a "speed bump" to let users know they are entering an isolated environment and why.

SERVICE ARCHITECTURE

Isolation operates across several global and regional cloud services.

The global services manage user- and account-related activities (identification, presences and personal data) and geolocation redirection. They allow users from around the globe to use the system from anywhere in the world; traffic is routed from the nearest data center to your local egress point.

The regional service provides the isolation and egress features. It operates in several locations to provide a faster user experience. Advanced settings (Research mode) allow users to manually select the geolocation of the remote Egress service and specify the HTTP headers as well as the server they'd like to access a website from.

SECURITY EFFECTIVENESS

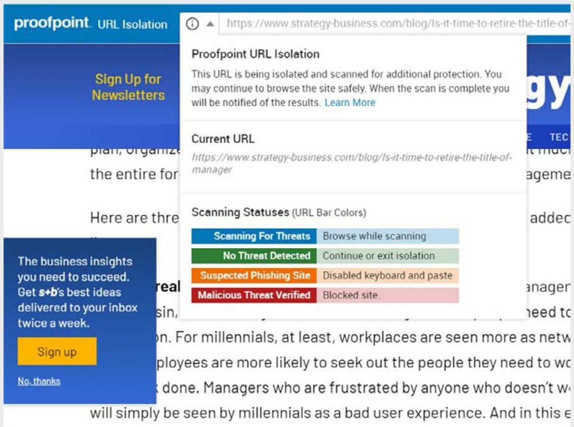
Our adaptive isolation capabilities draw on threat intelligence we glean from corporate email. We automatically isolate suspicious URLs, especially those sent to your most vulnerable, attacked and privileged users.

This adaptive control mechanism complements Proofpoint Email Protection and Targeted Attack Protection. Users can fully access and interact with most websites. For sites deemed suspicious by initial scans, they can view the site in read-only mode while a full threat analysis is performed.

Applying Granular Controls to Existing User Groups

As the threat landscape shifts, not everyone needs the same isolation experience for links in their corporate email. Trying to protect everyone to the same degree and in the same way drives up your costs and creates needless burdens for your low-risk users. Browser Isolation and Email Isolation give you the ability to quickly adapt to these threats and modify policies for existing user groups. This provides more granularity for your entire organization. All user groups from Proofpoint Email Protection will be added automatically to Browser Isolation and Email Isolation in the URL Isolation Policy settings. You can also import your VIP user list from User Center and the VAP list from TAP to set isolation policies for those groups specifically. This policy flexibility allows you to create customized isolation settings for specific groups, giving your users the freedom to access the sites they wish. And all while protecting them from unsafe URLs and web-based threats.

Browser Isolation and Email Isolation give you the capabilities to quickly shift and apply granular isolation policies to existing groups with high-risk profiles as needed. This helps you reduce your attack surface by ensuring the right protection is provided to your users.


proofpoint. URL Isolation
https://www.strategy-business.com/blog/Is-it-time-to-retire-the-title-of-
Sign Up for Newsletters
The business insights you need to succeed. Get s+b's best ideas delivered to your inbox twice a week.
Sign up
No, thanks

Proofpoint URL Isolation

This URL is being isolated and scanned for additional protection. You may continue to browse the site safely. When the scan is complete you will be notified of the results. Learn More

Current URL

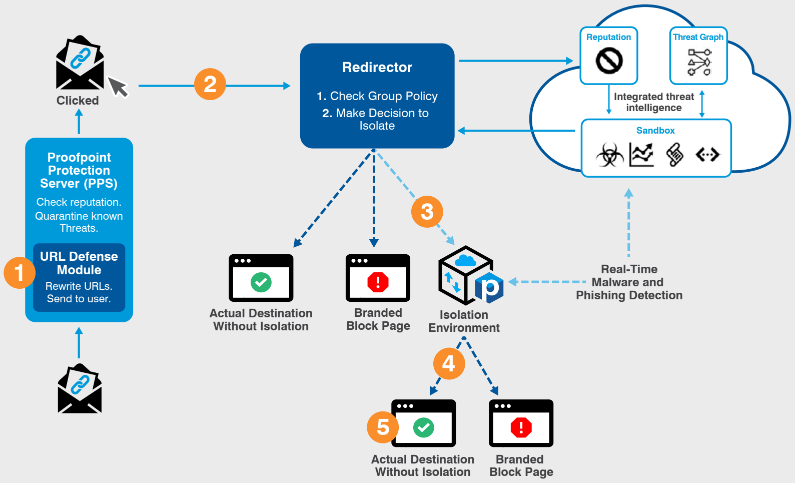
https://www.strategy-business.com/blog/Is-it-time-to-retire-the-title-of-manager

Scanning Statuses (URL Bar Colors)

Scanning For Threats	Browse while scanning
No Threat Detected	Continue or exit isolation
Suspected Phishing Site	Disabled keyboard and paste
Malicious Threat Verified	Blocked site.

Scanning Status for TAP URL Isolation

Browser Isolation and Email Isolation allow your users to browse and interact with personal email and unknown URLs safely while scanning for malicious content that could potentially impact your users and their corporate devices. While each URL is being scanned in Isolation, you may notice several different URL color bars representing a different status. A blue URL bar indicates that the URL is currently being scanned and is safe to continue browsing. A green URL bar means scanning is complete and no threats have been detected. From here you may continue to browse the site or exit isolation. A yellow URL bar indicates that the URL may be suspect for a potential phishing site. If this happens, Isolation will disable all keyboard entries and the ability to paste. Lastly, a red URL bar indicates that a malicious threat was detected and verified. If this happens, Isolation will then immediately block further access to this site.


Clicked
2
Redirector
1. Check Group Policy
2. Make Decision to Isolate
Reputation
Threat Graph
Integrated threat intelligence
Sandbox
Proofpoint Protection Server (PPS)
Check reputation. Quarantine known Threats.
URL Defense Module
Rewrite URLs. Send to user.
1
3
Actual Destination Without Isolation
Branded Block Page
Isolation Environment
Real-Time Malware and Phishing Detection
4
5
Actual Destination Without Isolation
Branded Block Page

Real-Time Phishing Email Scanning

1. URL rewritten in incoming email based on policy routes and domains.
2. URL is clicked and forwarded to the TAP redirector. Redirect policy can be adjusted based on membership in the Proofpoint Isolation User Group.
3. User is directed to the Isolation environment. The website is safely rendered and sends only passive content to the endpoint.
   - **a.** Uploads and downloads are disabled.
   - **b.** Real-time phishing detection and dynamic input restrictions are put in effect.
   - **c.** A policy to disable all keyboard inputs can be made here until a clean result is returned from the sandbox.
4. Option to exit Isolation environment after full sandboxing analysis deems the site safe.
5. User continues to browse as normal.

What Happens During Click Time?

DATA LOGGING

Data security is our top concern. By design, Browser Isolation and Email Isolation minimize the collection of confidential data and personally identifiable information.

- Email addresses are stored as hashed values and used as anonymous user IDs unless you actively request "non-anonymous mode."
- User site cookies are correlated to anonymous user IDs (except in "non-anonymous mode") and stored encrypted in our database.
- Browsing history is correlated to anonymous user IDs (except in "non-anonymous mode") and stored encrypted in our database.
- Only customer administrators use passwords to log into the Isolation console (dashboard). Passwords are hashed using BCrypt.

CONCLUSION

Proofpoint Email and Browser Isolation technologies uniquely strengthen your security posture against complex threats entering your organization. This security platform not only prevents high-risk web browsing, but also secures data leaving the organization, prevents email fraud, and simplifies and automates response actions. This allows you to spend your time and resources focusing on what matters. We reduce the attack surface of your organization by providing a secure and frictionless way for your users to browse the internet.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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 more than half of the Fortune 1000, 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**.