

Remote Browser Isolation

Provide users with safe access to uncategorized sites and known bad sites when necessary by using Forcepoint ONE and other Forcepoint products with Remote Browser Isolation



Challenge

- › User productivity is impacted when access to the web is blocked, but destinations like uncategorized websites and challenging categories like social media are frequently restricted because of security and compliance concerns.
- › C-level execs and users with elevated system privileges are high value targets for web-borne threats.
- › Web-based phishing attacks and credential theft remain key security risks.
- › Sensitive data can be exposed during web interactions.

Solution

- › Adding Forcepoint Remote Browser Isolation (RBI) to Forcepoint ONE and other Forcepoint products prevents web-based threats and phishing sites from compromising endpoints and limits user's data-sharing privileges on the web. This enables you to further advance a Zero Trust security posture by extending Zero Trust principles to secure users from risky web content without blocking or trusting it. Additionally, web applications accessed via the solution do not leave sensitive corporate data in the browser caches of endpoints.

Benefits

- › Users are more productive thanks to expanded access to the web (i.e. uncategorized and newly registered sites), without additional security risk.
- › Users are more productive thanks to expanded access to the web (i.e. uncategorized and newly registered sites), without additional security risk.
- › C-level execs and others with elevated system privileges gain the additional security of having their web traffic isolated from their endpoints.
- › Additional protection from phishing attacks and credential thefts.
- › Prevention of sensitive data leaking to websites.
- › Eliminates sensitive web app data from browser caches of devices.

"Most attacks are delivered via the public internet, through either web browsing or emailed links that trick the user into visiting malicious sites. Simply isolating the browser from the end user's desktop significantly improves enterprise security posture, including protection from ransomware attacks."

— Gartner®, Hype Cycle™ for End Point Security, 2021, Chris Silva, August 11, 2021

Automatically Balance Security and Performance

Forcepoint RBI makes it easy to provide an end-use experience so seamless you won't even notice a difference to native performance, while also enforcing the highest assurance web security technology whenever there is potential risk. RBI provides a Zero Trust approach to web browsing by neutralizing malware through remote isolation without relying on detection. This not only provides malware protection against ransomware, but zero-day threats as well. Forcepoint RBI also utilizes Zero Trust Content Disarm and Reconstruction (CDR) to provide automatic file sanitization for files downloaded during an RBI session. This includes removal of malware embedded in an images file using steganography.

Integrating Forcepoint RBI with Secure Access Service Edge (SASE) solutions from Forcepoint provides a cloud-based, cloud-managed Security-as-a-Service for enforcing Zero Trust access to the web and business resources. By using Forcepoint RBI as an integrated layer of defense along with other cloud-based security and networking solutions you can have confidence in the advanced threat protection that only Forcepoint can provide.

The Secure Web Gateway Service of Forcepoint ONE with Remote Browser Isolation

The integrated solution offers a seamless, native web browsing experience while allowing secure, hassle-free access to websites that users need to successfully perform their jobs. **Links, cookies, bookmarks, clipboards, etc. are fully available via all standard browsers.** RBI with CDR is integrated in the SWG service as a possible action in a SWG content policy, and is invoked based on user group, device posture, location, and website category or risk score.

Key use cases for Forcepoint Remote Browser Isolation:

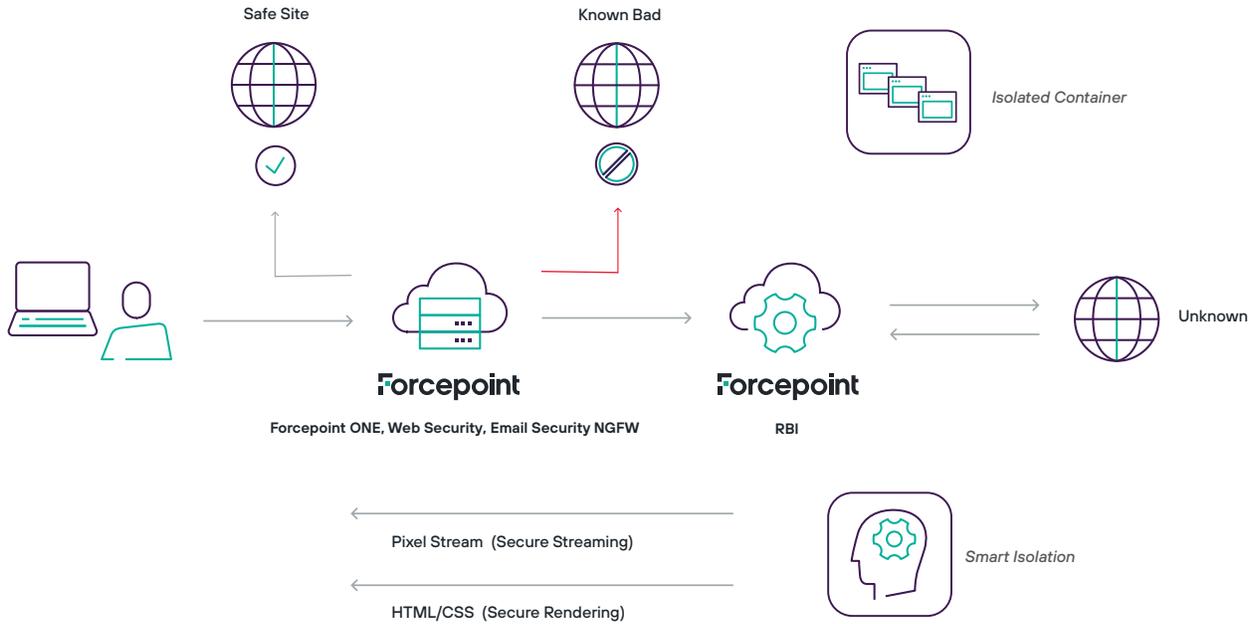
- **Expand Web Access Without Additional Risk.** Securely expand web access to uncategorized and risky sites.
- **Protect C-Level and Other High-Risk Users.** Protect users with elevated privileges by air-gapping their endpoints from web threats.
- **Block Phishing Attacks.** Stop phishing from compromising endpoints, delivering ransomware, and stealing credentials.
- **Prevent Data Loss.** Keep sensitive web app data out of browser caches; limit user data sharing activities on websites.

Table of Features

| FEATURE | VALUE |
|--|--|
| Isolation Modes | |
| Secure Streaming | Secure Streaming provides the highest assurance web security technology available |
| Secure Rendering | Secure Rendering enables a seamless native browsing experience |
| Advanced RBI | |
| Smart Isolation | Smart Isolation intelligently and automatically optimizes RBI delivery to balance performance and security by switching between the two isolation modes based on a given destination's risk |
| Smart Redirection | Smart Redirection automatically determines which links should remain in an RBI session and which should be redirected to Forcepoint SWG for policy enforcement |
| Privacy | |
| Data Sovereignty | Data sovereignty controls give customers control over the duration PII is retained, with the ability to wipe PII data for users on request |
| File Download Security | |
| Zero Trust Content Disarm & Reconstruction (CDR) | Zero Trust CDR automatically sanitizes downloaded documents and images by stripping active content and rebuilding files safely from scratch using only benign elements and maintaining the original file format. This includes removal of malware embedded in an image file using steganography. |
| Antivirus Scanning | An AV scanning engine scans downloaded files that are not supported by CDR for malware signatures to block malicious files |
| Additional Threat Protection | |
| Safe surf | Safe Surf enforces read-only mode to limit interaction with high risk sites |
| Download interception | Download interception prevents drive-by downloads that push malware onto endpoints |
| Threat visibility | |
| Threat Dashboard | View threats prevented across RBI sessions to prove heightened security |
| Enterprise Integrations | |
| IDP Authentication | Integration with SAML compliant IDP providers for end user authentication |
| SIEM Integration | Integrate with SIEM providers to augment security analysis and event correlation |
| Deployment options | |
| Cloud deployment | Leverage cloud delivered RBI to reduce management, never worry about version upgrades again, and conform to Secure Access Service Edge (SASE) architecture |
| On-premise deployment | Deploy RBI on-premises for situations where local legislation or industry policy dictates on-premises ownership of services |
| Additional Deployment options | |
| Stand-alone deployment | Deploy RBI as a standalone solution to secure web traffic |
| Forcepoint Product Integrations | Integrate with Forcepoint ONE or Next Gen Firewall solutions to add the ultimate level of web protection that only Forcepoint RBI can provide |

forcepoint.com/contact

Remote Browser Isolation



Forcepoint ONE and remote browser integration protects browser environments from malware threats.



About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, [Twitter](#) and [LinkedIn](#).

forcepoint.com/contact