Forcepoint

Datasheet

Remote Browser Isolation

Key Benefits

- **Risk Reduction** – Prevent malware in web content from contaminating endpoints or your network. Sanitize every webpage for complete assurance.
- **Productivity** – Provide your team with information and tools they need from new or unreputable sites. Access to uncategorized sites reduces over-blocking and relieves system admins from being overburdened with policy exception IT tickets.
- **Optimize Savings** – Reduce costs by using web security to handle most of the traffic, only sending unknown and risky sites through isolation.
- **C-level Security** – Use full isolation only for individuals that are highly valuable targets, and targeted isolation for the rest of the user population.
- **Streamline Compliance** – Prevent sensitive information from getting into the endpoint browser cache.

Allow users to access uncategorized and known bad sites while preventing malware, zero-day exploits, and phishing threats. Forcepoint Remote Browser Isolation (RBI) renders risky sites in a remote virtual container ensuring malicious code does not infect the endpoint. It features Zero Trust Content Disarm and Reconstruction (CDR) to sanitize documents at download and prevent steganographic upload. Forcepoint RBI integrates with Secure Access Service Edge (SASE) solutions from Forcepoint to provide cloud-based enforcement for Zero Trust access to the web.

As organizations embrace the proliferation of cloud migration, cloud-based apps, and work from anywhere with BYOD, the complexity of maintaining web security has increased. As a result, organizations are exposed to new security vulnerabilities. Embedding malware and other malicious code into websites is the latest vector used to infiltrate organizations. All that is needed is for a user to visit a compromised website to deliver zero-day malware. The unsuspecting user does not need to click on a link or download a document. Malware embedded on the website loads directly into the browser on the user's device as the user arrives at the site.

Forcepoint RBI delivers secure access to risky or uncategorized websites without relying on legacy threat detection tools. By isolating web content from end-user devices using a virtual container, Forcepoint RBI prevents contact between the device and any malware running on the website. After the session ends, the container is deleted along with any malware. This instantly sanitizes unsafe sites, giving organizations the flexibility to allow employees to access previously restricted sites.

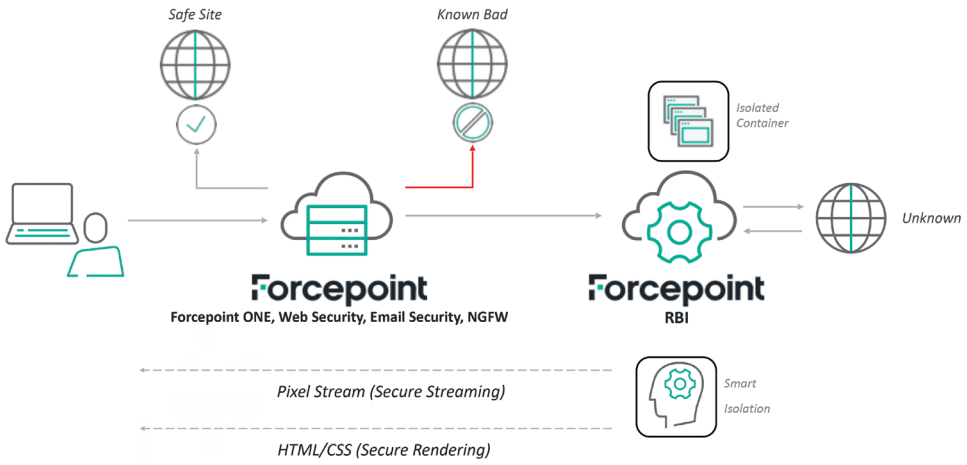

Figure 1: Forcepoint ONE ecosystem with Smart Isolation technology automatically adjusts between two rendering modes based on potential risk or verified trust

Built on a Zero-Trust Framework

Forcepoint Secure Web Gateway (SWG) is enhanced with RBI and Zero Trust CDR to enable Zero Trust Web Access. It uniformly enforces web policies in the cloud for sites and on the endpoints, helping organizations simplify their transition from remote workforces to hybrid workforces.

Forcepoint RBI and Zero Trust CDR makes web browsing and document upload and download safe and simple for distributed businesses and government agencies. They provide employees the ability to safely visit any website and download documents without fear of malware being installed on their devices.

Zero Trust Content Disarm and Reconstruction (CDR)

Forcepoint Zero Trust CDR solution was built around the zero trust framework, meaning it assumes nothing can be trusted and does not detect malware. Instead, it extracts valid information from documents (either discarding or keeping the original), verifies the extracted information is well-structured, then reconstructs a brand-new, fully functional document to carry the information to its destination. As a result, document-borne risks are eliminated.

Unlike legacy detection-based processes, zero-day threats cannot evade Zero Trust CDR. With near real-time performance, end users gain peace of mind that all potential threats are eliminated without impacting user productivity.

Zero Trust CDR on Upload

Forcepoint RBI provides organizations the ability to process documents and images with Zero Trust CDR on upload. This protects data loss via steganographic content, an approach often employed as part of industrial espionage and intellectual property leaks as most steganographic content is undetected by legacy security solutions such as antivirus.

Smart Isolation

An industry first, Smart Isolation eliminates the need for administrators to decide which rendering mode is suitable for their security needs. It automatically adjusts between two rendering modes based on potential risk or verified trust of the page and associated content. End users benefit from increased native-level responsiveness on safe sites and 100 percent secure browsing on new websites, unknown and potentially malicious sites.

Secure Rendering

Traditional RBI solutions stream sequences of images or pixels of an isolated website to the end user's browser. This is a highly secure mechanism to deliver web content. However, since it is a stream of images, it consumes a high amount of network bandwidth. With Secure Rendering, Forcepoint RBI disarms a website of its potentially malicious executable content like .js files and delivers HTML and CSS to the end user's browser. The local browser then renders it using its DOM, delivering a fast native browsing experience.

Secure Streaming

Secure Streaming converts website content into a visual stream of content. The user experience is close to native browsing, except that instead of the standard right-click menu, it offers a custom menu and limits custom font display. Secure Streaming is the safest isolation mode.

Safe Surf

Safe Surf converts a webpage into read-only mode. It permits functions like hyperlinks and navigation but restricts entering data into text fields and downloads/uploads of documents. Organizations can customize a destination's threat level, and once the user access that destination, Safe Surf is automatically activated. Ensuring user credentials and other sensitive user data are not shared or exposed within a Forcepoint RBI session.

Clipboard Control

Organizations can restrict or permit access to the copy-and-paste functions between their endpoint and the remote browser. These controls are set at the policy level, so it can be customized for specific users and user groups, giving admins greater policy enforcement.

System requirements for endpoints

DESCRIPTION	SPECIFICATION
Processor	Intel i3 2.5GHz or better
RAM	4 GB
Free Disk Space	25 MB

For latest requirement please refer to Forcepoint support page **here**

SUPPORTED OPERATING SYSTEMS	SUPPORTED VERSIONS
Microsoft Windows	Windows 10
Apple macOS	macOS 10.7 or later

Forcepoint RBI supports all HTML5-compatible web browsers, including Chrome, Edge, Firefox, and Safari.
For latest requirement please refer to Forcepoint support page **here**

Integration

PRODUCT	BENEFITS
Forcepoint ONE Web Security Forcepoint Web Security* Forcepoint FlexEdge Secure SD-WAN Forcepoint Next Generation Firewall (NGFW)	Zero Trust Web Content: Enhance web security by redirecting web traffic to RBI service, isolating any potential risks.
	Protect against advanced Web Threats such as HTML Smuggling and Drive By Downloads.
	Zero Trust File content: Sanitize file upload and downloads with RBI's CDR to prevent file related malware and data exfiltration.
	Increased Production: Increase web access securely via RBI.

* Cloud, On premise, Hybrid

PRODUCT	BENEFITS
Forcepoint Data Loss Prevention (DLP)	Full DLP visibility of isolated traffic for consistent policy enforcement
	Enhance DLP capability to detect data theft via steganography
	Control file uploads and HTML POSTs to prevent data exfiltration
	Prevent Stenographic Data loss by sanitizing document and image uploads with CDR.
	Utilize RBI security controls to limit permissions from risky users by controlling access to System Clipboard, File Uploads and Downloads, and print functions within isolated sessions.

Reporting

Reports provides comprehensive reports about the downloads, uploads, and browsing activities of your users.

TYPE	DESCRIPTION
Browse/Web Activity	Generate a report that shows the web browsing activity per user.
Downloads	Generate a report that shows the document downloads per user.
Uploads	Generate a report that shows the document uploads per user. Includes analysis carried out and analysis results.
Security Threat	Generate a report that shows the threat score for each website viewed through the remote browser.

Dashboard

Dashboards provides interactive, real-time graphical information about the status and activity in Forcepoint RBI.

TAB	DESCRIPTION
System	Provides system license and active session details.
Web Security	Provides comprehensive information about the range of threats encountered by Forcepoint RBI. The Web Security tab opens by default when you sign in to Forcepoint RBI.
Network	Provides usage statistics for each user, browser type, and browsing category.

CDR DOCUMENT TYPE SUPPORT
Supported document Types: For the most up-to-date list of supported file types, visit **here**[1]

[1] https://threat-removal.deep-secure.com/faq

To learn more about Remote Browser Isolation or schedule a free demo please visit **Remote Browser Isolation.**