Remote Browser Isolation

Work has become a dynamic activity - at home, in the office, and on the go. This shift to work-from-anywhere means more employees connect, create, and collaborate online than ever before. However, increasing reliance on the Internet and browser-based productivity apps like email, instant messaging, and cloud collaboration tools also means there's an expanding external attack surface with new potential entry points for threat actors.

At the same time, adversaries have matured their approach to web attacks with as-a-service offerings, hacking kits, advanced social engineering, and even malicious generative AI tools to deliver more effective and targeted web attacks. In the first half of 2022, over 67 million malicious domains were created[1]; and in 2023, over 74% of successful breaches included the human element[2]. This unprecedented level of volume and social engineering sophistication, coupled with a skyrocketing internet-facing attack surface, means that organizations and high-value employees are at heightened risk.

1. 2023 Recent Trends in Internet Threats - Unit 42
2. 2023 Verizon Data Breach Investigations ReportEv

Isolation Protection From Zero-Day Threats

Remote Browser Isolation (RBI) technology air-gaps a user's web session from their local browsers and is a powerful way to mitigate the risk of internet-borne attacks. By executing web content in fully isolated environments—separate from local devices and networks—organizations can prevent unsanctioned plug-ins, stop accidental data loss, and protect users from zero-day vulnerabilities and web threats like ransomware, malware, and phishing.

Shortcomings of Existing RBI Solutions

While isolation technology can protect businesses from a wide array of web attacks, it is equally imperative to deliver seamless, near-native user workflows and unhindered access to web applications. However, running browser sessions far away from local devices has the potential to disrupt user workflows and impact productivity. Throughout its evolution, traditional RBI approaches have tried and fallen short when governing this tension between performance and security.

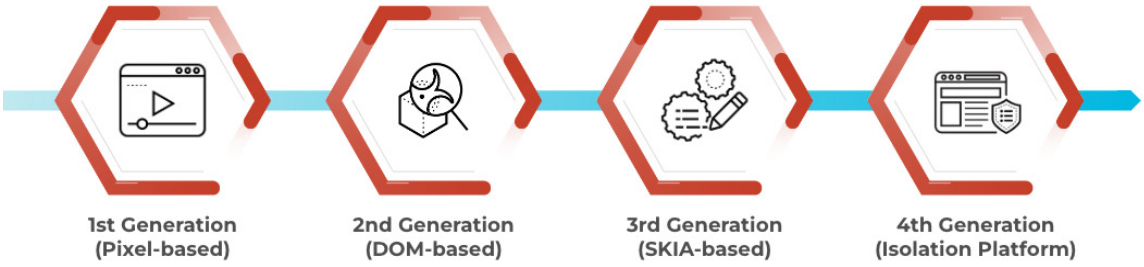

Figure 1: Evolution of Remote Browser Isolation technology

- **First-Generation (Pixel Pushing):** Web content is rendered and processed on a remote server which captures the visual representation of the page and sends it to the users' device pixel-by-pixel. This method provides fully air-gapped security but is bandwidth-heavy, driving up costs and degrading the user experience.
- **Second-Generation (DOM-based):** A Document Object Model (DOM) approach reconstructs the page with HTML elements. It filters and processes web content before rebuilding the page on the user's device. This approach responds better than pixel-pushing but exposes the user to potentially malicious files and zero-day threats.
- **Third-Generation (SKIA):** An open-source 2D graphics library renders the webpage through a SKIA rendering layer to address many of the gaps with pixel and DOM-based approaches. However, SKIA has limited versatility for low-latency, highly dynamic, and interactive real-time applications like O365.
- **Fourth-Generation (Isolation Platform):** Unlike traditional pixel-pushing reconstruction that causes high latency or DOM-based approaches that expose security gaps, a next-generation RBI isolation platform combines the latest vector and pixel-based technologies for superior isolation while simultaneously delivering near-native UX.

How to Approach the Problem

Organizations need a paradigm shift from legacy RBI products to a modern isolation platform with state-of-the-art technology that delivers superior security outcomes, near-native UX, and optimized performance for today's modern SaaS applications.

Zero Trust Security - Keep all or select users and their data safe by neutralizing threats with an added layer of zero trust browser isolation to everything users do online. Improve security while simultaneously alleviating operational burdens with simplified, integrated, and granular controls.

Near-Native Everything - Ensure websites and applications look crisp and feel interactive as if users were browsing websites and accessing SaaS apps natively.

Best UX and Performance - Deliver streaming videos and a wide range of apps—including highly interactive and real-time apps—with low-latency interactivity and seamless transitions into and out of the isolation platform without disrupting user workflows.

The Future is Now. RBI for Prisma Access

RBI for Prisma Access enables users to safely browse the internet no matter where they are. It creates a no-code execution isolation channel between users and browsers to keep zero-day web threats at bay, never allowing malicious files to execute on their machines. Unlike traditional isolation products, RBI for Prisma Access combines the latest isolation technologies with proprietary techniques to deliver near-native user experiences without compromising security.

Key Use Cases

Isolate all unknown and risky web content	Stop browser vulnerabilities, patient-zero infections, ransomware, phishing, and other zero-day attacks hidden in unknown or risky web content.
Secure high-value users	Add a layer of security for high-value users and groups that are frequently targeted by threat actors. Also, prevent high-value users from accidentally leaking sensitive data.

How it Works

RBI natively integrates with Prisma Access to apply Isolation Profiles to existing security policies. Isolation Profiles can be used to prevent data loss by restricting user controls such as copy/paste actions, keyboard inputs, and sharing options (e.g., email, print, etc.). RBI also creates an isolated graphical stream between end users and their remote browsers by preventing code (HTML, CSS, or JS) from directly executing on their machine; effectively retaining and isolating any malicious code within the air-gapped RBI environment.

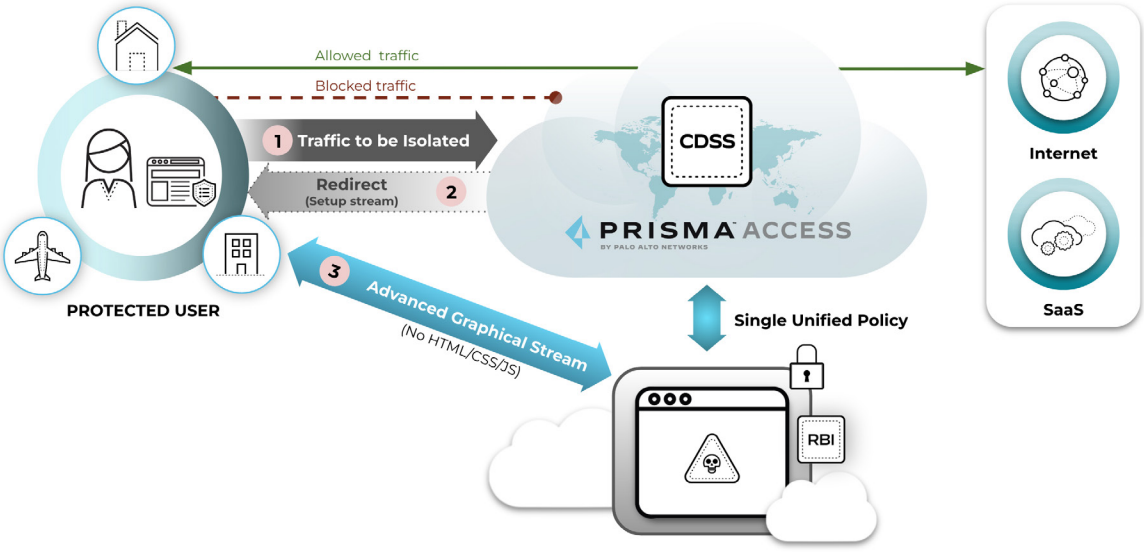

Figure 2: Palo Alto Networks RBI Solution Architecture

Features and Capabilities

Browsers and Platforms	RBI supports major browsers like Chrome and Edge on Windows, and Chrome and Safari on MacOS.
Flexible Deployment	RBI supports all onramps including GlobalProtect, Explicit Proxy, and Remote Networks. RBI leverages Prisma Access compute locations that are closest to the end user's geographic location to minimize latency.
Cloud-Delivered Security Services	All security profiles–Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire®, SaaS Security, and Data Loss Prevention–are supported on the web traffic from RBI to the destination.
Data Loss Prevention	RBI supports granular data leak controls including cut, copy, paste, print, keyboard input, and remote rendering of files.
User Experience	Next-generation isolation combines multiple technologies and custom transformers to enable near-native user experience on highly dynamic and real-time applications that require low-latency interactivity.
Single Pane of Glass	Native integration with Prisma Access provides single-pane-of-glass monitoring, centralized policy enforcement, and dynamic security posture management. Traffic redirection to RBI is policy-driven and natively integrated into Prisma Access policies.

Key Benefits

- **Strongest protection against zero-day web attacks** with the most advanced isolation technology to prevent data leaks and patient zero.
- **Enables workforce and digital transformation** with an RBI solution that seamlessly embeds into existing workflows with near-native web browsing and user experience.
- **Low cost, effort, and complexity to maintain RBI** with uniform policies, centralized enforcement, and single-pane management, all natively integrated with Prisma Access.

Global Customer Services

Global Customer Services delivers the guidance, expertise, and resources necessary for maximizing the value of your RBI investment. Professional Services, Customer Success, support, ongoing education, and adoption tools ensure protection from intruders at every stage of your cybersecurity journey. Contact your Palo Alto Networks account manager to obtain the services that fit your needs.

Deploying a consistent and integrated RBI solution—as part of an SSE or SASE architecture—will not only stop sophisticated cyberattacks but streamline operations and improve user experiences. Securely connect users to the internet and all business-critical SaaS apps, irrespective of location, with the highest level of security without compromising user experience.

To learn more about Palo Alto Networks RBI, visit our webpage or contact your Palo Alto Networks representative.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com