Palo Alto Networks and Ericom Software

Remote Browser Isolation to Protect Enterprises from Zero-Day, Web-Based Threats

The Challenge

The web browser is one of the most vulnerable endpoint attack vectors, through which the majority of zero-day exploits compromise organizations. Attacks can originate from malicious code embedded in website resources (e.g., scripts, images, ads, fonts), from phishing URLs embedded in emails or social media messages, or from downloads that have been weaponized to contain malware.

Fast, secure web access is essential for every organization's users—but how can your security team protect users from advanced threats hidden in a website's code, especially when the site has limited reputational history or is accessed through a legitimate platform, such as Twitter®, LinkedIn®, or a web-based email service? Blocking access creates too much business friction and productivity loss, but all it takes is a user's click on a seemingly benign website for a piece of serious malware, such as ransomware, to make its way into the corporate network. As the news shows, the costs and damages associated with recovering from one of these attacks can be severe.

Benefits of the Integration

Ericom Software's ZTEdge remote browser isolation (RBI) integrates with Palo Alto Networks Prisma Access via standard URL redirection (i.e., block page redirect) or IPsec-based service connection. This integration allows you to:

- Stop ransomware and zero-day threats from uncategorized websites, social media, phishing URLs, and other risky sites.
- Remove malware from file downloads.
- Eliminate "over-blocking" of web access, improving user productivity.
- Free support staff from responding to help tickets to open access to blocked sites.
- Prevent credential theft and oversharing of data on the web.
- Keep sensitive data from web apps out of the web browser cache on unmanaged devices.

ZTEdge Web Isolation

ZTEdge™ Web Isolation RBI cloud service prevents ransomware, advanced web threats, and phishing attacks from reaching user endpoints by rendering web content in a remote, isolated container. Whether users browse to a malicious site independently or by clicking a URL embedded in a phishing email or social media site, they are completely safe since no web content is ever executed directly on their device. An interactive media stream representing the website is sent to a device's browser, providing a safe, fully interactive, seamless user experience. Websites launched from URLs in emails can be rendered in read-only mode to prevent users from entering credentials for additional phishing protection. Attached files are sanitized before being transmitted to endpoints, ensuring that malware within downloads cannot compromise users' devices.

Prisma Access

Palo Alto Networks Prisma® Access transforms security with the industry's most complete cloud-delivered platform, allowing you to enable secure remote workforces. Legacy network security products require significant manual effort to deploy, manage, and maintain; do not scale; and leave gaps in coverage that impact productivity and increase risks. Prisma Access provides more security coverage than any other solution, protecting all application traffic to reduce the risk of data breaches while providing guaranteed performance with leading service-level agreements (SLAs) to deliver an exceptional end user experience.

Prisma Access and ZTEdge Web Isolation

The integration of Prisma Access and ZTEdge Web Isolation provides a multilayer defense that effectively protects your endpoints, networks, and data from the full range of known and zero-day threats while facilitating essential, productive web-based business activity.

Prisma Access detects known and unknown threats, even in encrypted traffic. Based on URL Filtering, requested sites on the allow list are opened natively on the user's

endpoint browser while those on the deny list are blocked. Uncategorized or unidentifiable sites, or those in select categories, are redirected to ZTEdge Web Isolation to be rendered in an isolated cloud container, safely away from the corporate network and end user devices.

The integrated Palo Alto Networks and ZTEdge solution secures business-critical web-based activity and protects against undetectable threats and human factor vulnerabilities (e.g., users clicking on phishing URLs) by:

- Inspecting and blocking detectable and known malicious content.
- Filtering deny listed URLs and blocking access.
- Isolating all active untrusted web content away from the endpoint and internal networks.
- Sending isolated web content to the endpoint as a set of rendering information, ensuring no malware can impact the device or network.
- Sanitizing file downloads from the internet, disarming potentially malicious content.
- Providing a read-only mode for websites, preventing users from credential theft attacks.

Use Case 1: Expand Web Access Without Security Risk

Challenge

Blocking access to websites with limited reputational history (e.g., "uncategorized" or "unknown" sites) can create significant user frustration and productivity loss as well as put added burden on operational teams to selectively allow access. Meanwhile, simply enabling access creates very real cybersecurity risk for an organization. Organizations need to be able to offer secure access.

Solution

With the Prisma Access and ZTEdge Web Isolation integrated solution, you can design policies to selectively send certain websites (e.g., uncategorized/risky websites, specific categories like social media) to ZTEdge Web Isolation to be isolated. Users get access to the websites they need and enjoy a completely normal browsing experience, but your Security personnel know the users are completely safe since only a safe set of rendering information representing the website is sent to users' devices. Any malware on a site remains in the remote isolated container, which is destroyed after the browsing session.

Benefit

The integrated solution offers broad web access to complete business tasks with no risk of malware compromising devices. IT and Help Desk teams avoid time-consuming policy modifications to selectively enable access to sites.

Use Case 2: Enable Access to Web Email and Social Media Sites

Challenge

Users are constantly under threat from malicious links embedded in web email and social media sites aiming to steal sensitive data (e.g., login credentials) or infect endpoint devices. As a result, many organizations block or limit access to sites like Gmail® and Facebook®. Users want access to these sites, but many Security and IT teams determine that the risk to the business is just too great.

Solution

With the Prisma Access and ZTEdge Web Isolation integration, you can set policies in Prisma Access to send traffic from social media and web email sites to ZTEdge Web Isolation to be isolated. These sites are rendered in an isolated container, and only safe rendering information is sent to the user's device.

Benefit

Users get access to the social media and web email services they need to complete their work, and your Security personnel get the strong web protection your organization requires.

Use Case 3: Protect the C-Suite and High-Risk Users

Challenge

Compared to general employees, senior executives are at a significantly higher risk of being targeted by cybercriminals via phishing, social engineering attacks, and more. While you never want to see any endpoint compromised, if an endpoint belonging to an executive or high-risk user is compromised, the sensitive nature of data and systems they have access to may spell "game over."

Solution

With the Prisma Access and ZTEdge Web Isolation integration, you can set policies in Prisma Access to send all web and cloud application traffic from executives or high-risk users to ZTEdge Web Isolation to be isolated. These sites are rendered in an isolated cloud container, and only a safe, fully interactive media stream is sent to the user's device. Remote browser isolation protects these users' endpoints from 100% of the malware they may encounter on a website, in a social media stream, or in a URL they click on in an email.

Benefit

Executives and high-risk users being targeted at an elevated rate. Sending all their traffic to isolation "air gaps" their endpoints from 100% of malware, giving them the strongest protection while preserving their web browsing experience.

Use Case 4: Prevent Loss of Sensitive Data

Challenge

As they embrace digital transformation initiatives, many organizations are concerned about maintaining control over sensitive information. Users' interactions with web- and cloud-based applications represent a significant data loss risk because data gets left in the browser cache on each and every endpoint device each time they access private web apps. Perhaps more worrying are the significant security concerns of public software as a service (SaaS) apps, such as Salesforce®. This "footprint" of data can be leaked if the endpoint ever gets compromised.

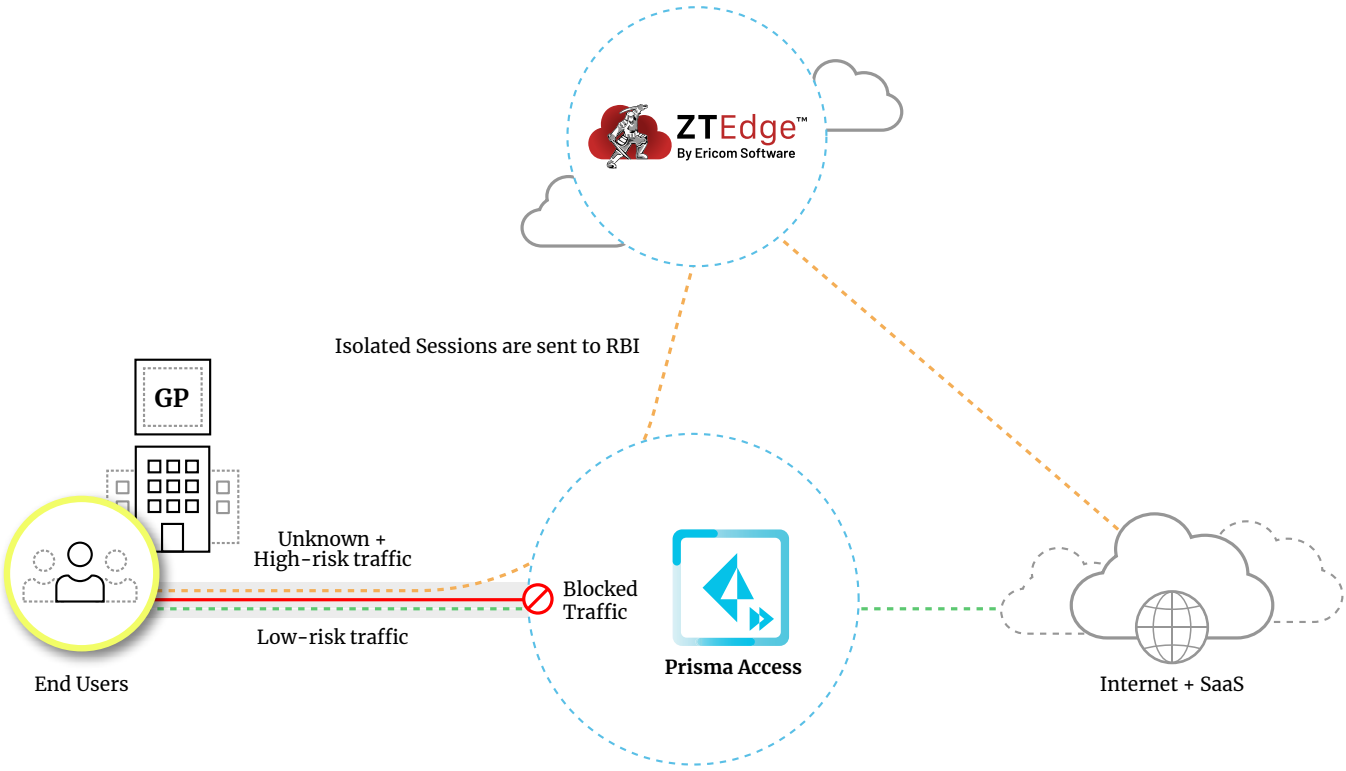

Figure 1: Solution architecture overview

Solution

With the Prisma Access and ZTEdge Web Isolation integration, you can allow users to only access web and cloud applications via Isolation mode. This ensures that no web content or code is ever downloaded or stored on the user's endpoint. Since no data footprint is left, data cannot be lost if the device is ever compromised. RBI also provides additional powerful data sharing controls, such as the ability to restrict users' actions, like screen capture, copy/paste from a clipboard to local storage, and file download/upload.

Benefit

Prevent loss of sensitive data by limiting user operations with web-based applications/websites and blocking sensitive web-app data from being stored in the browser cache of endpoints.

There are two methods available to enable RBI for Palo Alto Prisma Access customers: block page redirection and IPsec-based service connection. The service connection approach is recommended, but you can use block page redirection if you do not use service connections.

About Ericom

Ericom Software is a leading provider of cloud-delivered, Zero Trust cybersecurity solutions that protect today's digitally distributed organizations from advanced security threats. The company's ZTEdge™ Web Isolation cloud service is a market-leading remote browser isolation (RBI) solution that integrates with SASE platforms to protect users from advanced web and email cyber threats. Find out more at www.Ericom.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS | ZTEdge™ By Ericom Software

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