Zero Trust, Air-Gapped Protection from 100% of Advanced Web Threats

Prevent even zero-day exploits that bypass traditional web defense solutions

Why Is Your Business Still Experiencing Cyberattacks?

For most enterprises, internet access remains stubbornly Zero Trust-proof: Standard solutions filter for known malware and ransomware, but are powerless to stop unknown threats, like the zero-day exploits that are increasingly used in cyberattacks. Since web content cannot be verified as free from those threats, organizations committed to Zero Trust security principles should, by all rights, prohibit all use of the web.

Instead, organizations blocklist only known-bad sites, filter content for known threats, trust that websites that are not proven risky are secure and depend on users to identify the very social engineering emails that are designed to fool them. What they do NOT do is assume content is risky unless verified safe.

That's why, despite great strides in enterprise Zero Trust journeys and significant investment in web security solutions, the overwhelming majority of enterprises that experience cyberattacks can trace those attacks back to a click on acompromised website or a malicious link in a phishing email.

ericom security
by cradlepoint

Ericom Remote Browser Isolation highlights

- Air-gap user devices from risky sites to keep malware away
- Open suspicious sites in read-only mode to prevent credential theft
- Prevent phishing even when users click
- Sanitize downloads to keep weaponized files off devices and networks
- Prevent data loss and exposure with granular browser controls
- Enforce acceptable web use policies
- Per-user policy controls restrict web access

Ericom Web Isolation: Air-Gapped Zero Trust Internet Access

Ericom Web Isolation is the only solution to provide full, seamless Zero Trust access to all websites, including virtual meetings, instant messaging sites and more. Since no content from the web can be verified as safe, Ericom Web Isolation air-gaps all web content away from the user device. As a result, users can securely interact with even known-dangerous sites:

- When a user clicks a link or types a URL, Ericom Web Isolation opens the site in a cloud container, remote from the device browser.
- All active website code remains within the cloud container and never reaches the endpoint.
- Safe rendering data is sent from the cloud container to the device browser, where the user interacts just as they would with native site content.
- Granular policy-based controls can restrict which sites each user can visit and limit browser clipboarding activities for users, site categories or individual sites. DLP prevents exfiltration of sensitive data.
- No dedicated enterprise browser is required.
- Clientless options are ideal for third-party contractors and users who connect from unmanaged devices.

©Cradlepoint. All Rights Reserved. | cradlepoint.com

How Ericom Web Isolation Eliminates Trust from the Browsing Equation

From their usual browser, users navigate to the websites they need as they always do — by clicking a link or typing a URL.

Website content is rendered within an isolated container in the Ericom Cloud.

All active content remains sealed within the container in the Ericom Cloud.

Only safe rendering data is sent from the cloud-based container to the browser on the user device.

Users interact with the visual site representation via their browsers, in an experience that is indistinguishable from unisolated browsing. All user actions — clicks, scrolling, and so on — are transmitted to the website via the Ericom Cloud.

Files attached to emails or websites are downloaded via the isolated container, where content disarm and reconstruct (CDR) technology strips out any malware and reassembles the file with desired functionality intact before downloading it to the user.

Easy-to-manage granular controls protect stop users from exposing of sensitive data via the web. Browser print and clipboarding (copy/paste) activities can be restricted or disabled on a per user/per site/per content basis. DLP prevents exposure of PII, even in applications with end-to-end encryption (E2EE) like IM sites.

Suspected credential theft sites are opened in read-only mode to protect users who mistake spoofed sites for legitimate ones and attempt to enter credentials.

When the user leaves the site or moves on to a different activity, the cloud container, along with all content within, is destroyed.

To learn more about our cloud-delivered Zero Trust security solutions, request a live demo at **ericom.com/contact-us.**

©Cradlepoint. All Rights Reserved. | cradlepoint.com | R122023

cradlepoint PART OF ERICSSON