Ericom Web Security

ERICOM
Cybersecurity Unit of Cradlepoint
Part of Ericsson

Protect Your Organization from Threats from the Web That Other Solutions Let In

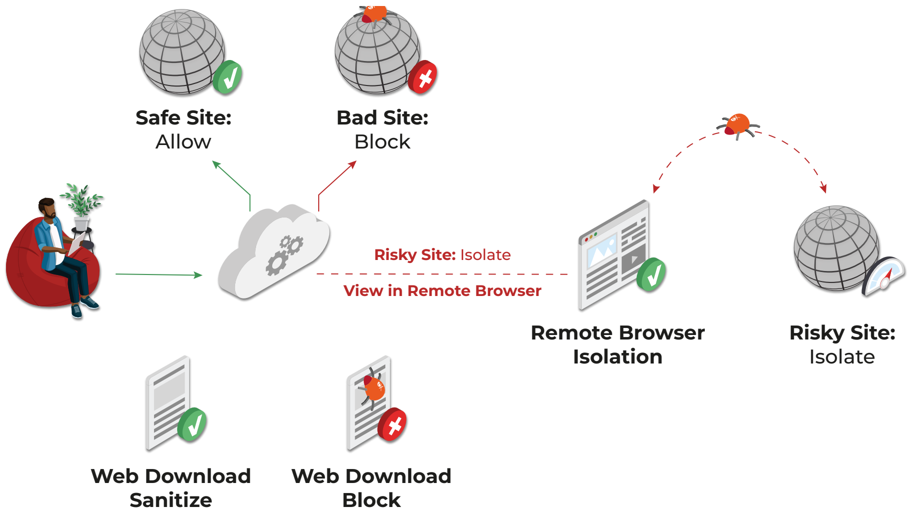
Endpoints and networks are air-gapped from phishing and zero-day exploits, yet users enjoy seamless browsing and email use

Email and the web serve as essential links in the delivery chain for over 90% of successful cyberattacks. Unbeknownst to their owners, legitimate sites may be injected with malware, or host malvertising or malicious downloads, exposing visitors to attack. Phishing emails link to URLs leading to malicious sites that are retired before they can be identified as phishing sites. Social engineering attacks lure recipients into sharing credentials and confidential data or even transferring organization funds. Infected PDFs, Office documents and other files masquerade as legitimate attachments, but deliver malicious payloads when downloaded.

Once even a single one of your user endpoints is infected, ransomware and other malware can move laterally throughout your organization's networks, providing visibility to malicious actors and enabling data theft and pinpoint strikes.

Internet and email are essential tools for your users, yet the defenses that most organizations have on board cannot protect them. Traditional web filtering approaches can, identify the new malware strains that threat actors continually create. Blocking or even limiting user access results in a hit on productivity and complicates basic business functions.

Many organizations count on users to serve as their last line of defense, relying on them to identify and avoid suspicious appeals and links in emails, distinguish between an expertly spoofed site and the real thing, and refrain from downloading attachments that they did not request. Years of user training and millions of dollars have proven that this approach does not work consistently enough to protect organizations from the hundreds of phishing emails delivered each day.



The Solution: Ericom Web Security

Ericom Web Security integrates leading threat prevention technologies to ensure that your users can securely browse the web, click email links, and download files without risk of downloading ransomware or other malware, and are protected from credential theft and zero-day attacks.

Cloud-delivered Ericom Web Security analyzes all web traffic – even encrypted web traffic - and selectively blocks, isolates, and/or sanitizes content, as needed, before it reaches endpoints. Using integrated threat intelligence from a broad set of market sources and real-time data, it optimizes protection for each website, attachment and email to maximize security while delivering a seamless user experience. For additional protection from credential theft, suspected phishing sites can be presented to users in "read-only" mode, preventing them from entering IDs and passwords.

A full range of advanced technologies are integrated in Ericom Web Security to protect your organization from internet-delivered threats, including remote browser isolation (RBI), cloud data exfiltration controls, secure web gateway (SWG), ransomware protection and anti-virus. Content disarm and reconstruct (CDR) and Virtual Meeting Isolation are available as well.

Ericom Zero Trust Web Security Highlights

- Leverages anti-virus and remote browser isolation (RBI) to isolate risky web content away from endpoints
- Prevents advanced malware embedded in risky websites, even zero-days, from reaching networks
- Enables a Zero Trust security approach to web browsing, despite the “unverifiability” of the web
- Applies comprehensive threat intelligence to identify suspicious/ risky sites for isolation
- Displays sites opened via clicks on potentially suspicious URLs in emails in “read-only” mode to prevent credential theft
- CDR examines and, when needed, disarms and reconstructs documents in isolation before downloading them with desired functionality intact
- Optional Virtual Meeting Isolation keeps malware lurking in web clients of solutions like Zoom, Meet and Teams from infecting endpoints

> “
>
> ***Ericom offers a unique value proposition for organizations, delivering a comprehensive set of integrated Zero Trust security capabilities via a simple and affordable always-on cloud platform.***
>
> **Kamalika Sandell**,
> Chief Information Officer
> at the New Jersey Institute
> of Technology
>
> NJIT
> New Jersey Institute of Technology