ZTEdge™
By Ericom Software

ZTEdge Web Isolation

Protect Your Organization's Networks, Data and Users from Ransomware and Phishing

Stop web-borne malware – even zero-day threats – with remote browser isolation, without limiting web and email use

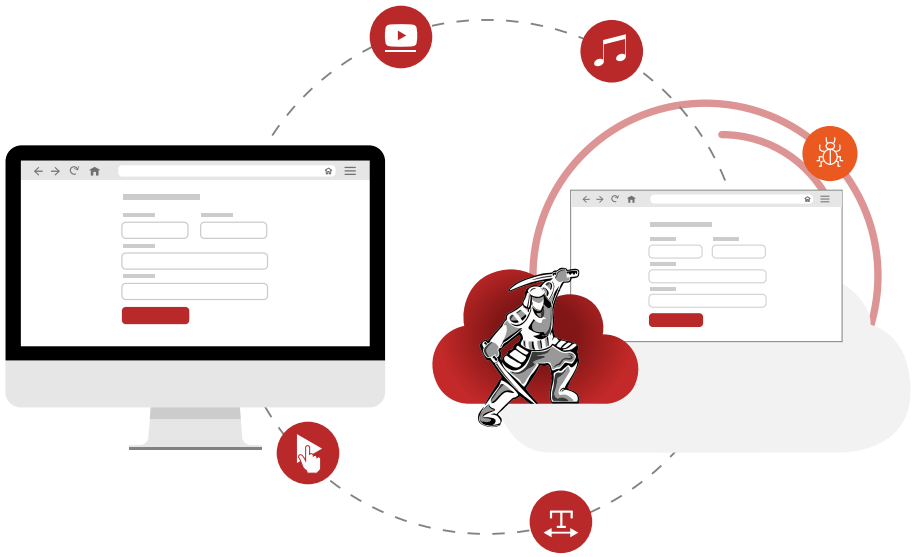
Over 90% of successful cyberattacks depend on email and the web as essential delivery channels. Even legitimate sites may be injected with malware, or host malvertising or malicious downloads, exposing your organization's networks when a user visits or clicks on a link. Phishing emails contain links to purpose-generated malicious URLs, leading to sites that are retired before they can be identified as phishing sites – but not before they download malware to users who click. Business email compromise (BEC) and other social engineering attacks lure recipients into sharing credentials that enable hackers to penetrate your customers' systems and steal confidential data. Infected PDFs, Office documents and other files masquerade as legitimate attachments, but deliver malicious payloads when downloaded.

Once even a single one of your users' devices is infected, ransomware and other malware can move laterally throughout your organization's networks.

Internet and email are essential tools for your users, yet the defenses that your organization has on board are most likely insufficient to protect them. Web filtering approaches cannot catch new malware variants or zero days. Blocking or even limiting user access to email or websites frustrates users, reduces productivity and impinges on 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.

Airgap Devices from Malware



The Solution: ZTEdge Web Isolation

ZTEdge Web Isolation leverages 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, protected from credential theft and zero-day attacks.

Cloud-delivered ZTEdge Web Isolation executes active web content in isolated cloud-based containers, remote from endpoints. Only safe rendering data is sent to whichever browser each user has on their endpoint, where users interact with the site just as they normally do – only risk-free. For additional protection from credential theft, suspected phishing sites can be presented to users in "read-only" mode, so they cannot be manipulated into entering sensitive data like IDs and passwords.

To protect your organization from malware hidden in files attached to emails or downloaded from websites, ZTEdge Web Isolation includes content disarm and reconstruct (CDR) capabilities. Files are downloaded to an isolated cloud-based container where they are examined for malware and, if necessary, disarmed. The files are then reconstructed with (desired) native functionality intact and delivered to endpoints. Additional options include Virtual Meeting Isolation and Identity and Access Management (IAM).

ZTEdge Web Isolation Highlights

- Leverages 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
- Integrated CDR examines and when needed, disarms and reconstructs documents in isolation before downloading them with desired functionality intact
- Displays sites opened via clicks on potentially suspicious URLs in emails in "read-only" mode to prevent credential theft
- Integrates easily with your organization's existing secure web gateway (SWG)
- Optional Virtual Meeting Isolation and Identity and Access Management (IAM) may be added as well

> *ZTEdge 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

Additional ZTEdge Security Solutions for Organizations Adopting A Zero Trust Security Strategy

ZTEdge Web Security

Intelligent remote browser isolation-based web security that allows your organization to protect users and data from ransomware and phishing, with integrated SWG

ZTEdge ZTNA, Apps and Network

A simple, modern and secure approach to remote access that enables your organization to retire costly, complex and vulnerable VPNs

ZTEdge Desktop

A Zero Trust solution that eliminates the remote desktop access vulnerabilities that leave your organization's networks and data exposed

www.zerotrustedge.com

info@zerotrustedge.com

Americas:
T +1 (201)767-2210

UK & Western Europe:
T +44 (0)1905 777970

Worldwide:
T +972-2-591-1700

Follow us