ZTEdge™
By Ericom Software

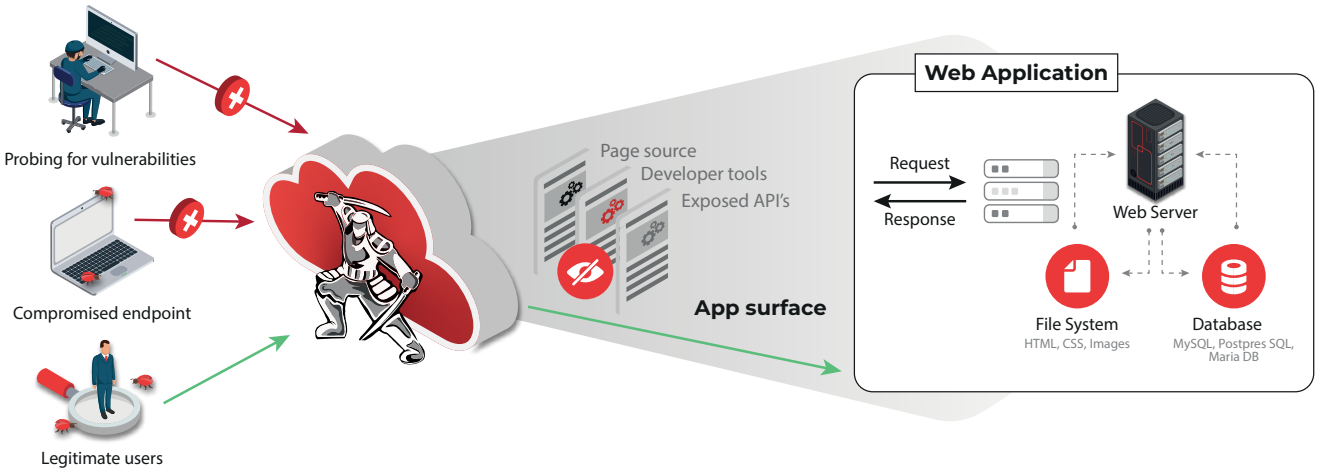
Web Application Isolation Protects Private Web-based Resource Surfaces from Exposure and Attack

Reverse browser isolation approach blocks visibility and access to web application page source and APIs by hackers, bots and compromised devices, and can limit data sharing functionality

Private web-based apps are at significant risk from a host of threats due to their exposed attack surfaces. Compromised unmanaged devices may infect sensitive applications with ransomware or malware; Hackers may deploy bots to probe web app source code for vulnerabilities to discover a "way in" for ransomware injection or to steal valuable customer data.

Many organizations use private web and cloud apps that need to be accessed by third parties, such as contract workers. These third parties may require only limited access, and they may not be using devices that are properly secured from threats. Some organizations choose to host these apps on an internal network, and enable external users to connect via VPN. This approach, however, presents its own risks: Excessive third party visibility into internal networks and potential for lateral movement and attack; Spread of ransomware or other malware to the host network; Data exfiltration; Complex VPN rules and the need to issue/update/disable credentials due to user turnover.

As a work-around to VPNs, organizations can try to host web applications behind a reverse proxy. While this simplifies things for users, it exposes the organization to threats from cybercriminals and attack bots as well as malware from credentialed – but insecure -- user devices.



The Solution: Web Application Isolation

ZTEdge Web Application Isolation secures web-based asset surfaces from malicious actors and bots, while enabling them to provide all intended functionality and services for legitimate users.

Web Application Isolation works much like Remote Browser Isolation, only in reverse: All content from users is routed through a virtual browser located in an container in the cloud. Only safe rendering data reaches the web application. Any malware from the endpoint remains in the container until it is destroyed at the end of the session. Additionally, the data sharing functionality of the application, such as the ability to print pages or copy and paste data from the web browser, can be limited for specific users (like third-party contractors).

Similarly, any document that a user uploads to the website or app is first examined for malware and disarmed within the isolated container by integrated CDR. The safe, malware-free reconstructed document is then transmitted to the site or app with desired native functionality intact.

Hackers or bots that attempt to probe the web app, seeking vulnerabilities that they can exploit, have no visibility into page source code, developer tools or APIs. Instead, they will only see a few lines of ZTEdge Remote Browser Isolation HTML.

For web apps, a reverse proxy comprised of a new-generation firewall and secure web gateway form a pipe that safely communicates access requests to identity and access management and device management systems. Once the user is authenticated and their device validated, network access is established via the application isolation security layer.

ZTEdge™
By Ericom Software

Web and Application Isolation Highlights

- Ideal for protecting private web or cloud apps that service contract workers and other third parties who use unmanaged devices
- Keeps dangerous content from endpoints from reaching a web app. Any malware from endpoints is isolated in the cloud and destroyed when the session ends
- Protects web-facing surfaces from cybercriminals and bots probing for vulnerabilities in page source code, developer tools or APIs
- Limits data sharing functions of web apps for third-parties to prevent data exfiltration
- Reverse proxy including NGFW/SWG enforces secure Zero Trust access to web apps through user verification, device authentication and least-privilege access, for access that is vastly more secure than VPNs
- Integrated CDR disarms documents that are uploaded by users in isolation before transmitting them to web app or website

> *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

ZTEdge Capabilities

Access Security	
DNS Security	SaaS App Access Control
Secure Web Gateway	Identity & Access Mgmt.
Cloud Firewall	Secure Remote Desktop Access
Zero Trust Network Access	SD-WAN

Threat Prevention & Compliance		
Threat Intelligence Network	File Sanitization (CDR)	Cloud Data Loss Prevention (DLP)
Remote Browser Isolation	IDS/IPS	Micro segmentation
Anti-Virus	Ransomware Prevention	Network Traffic Analysis
Anti-Phishing	SSL Inspection	Data Anonymization

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