ZTEdge™
By Ericom Software

Zero Trust Web Isolation for Film, Animation, and Visual Effects Company Trusted Partner Network (TPN) Programs

Boost Productivity with MPA Best Practice-Compliant Internet and Email Access that Eliminates the Risk of Exposure via the Web

Secure Web Access from Workstations, Without Risk of Content and IP Exposure

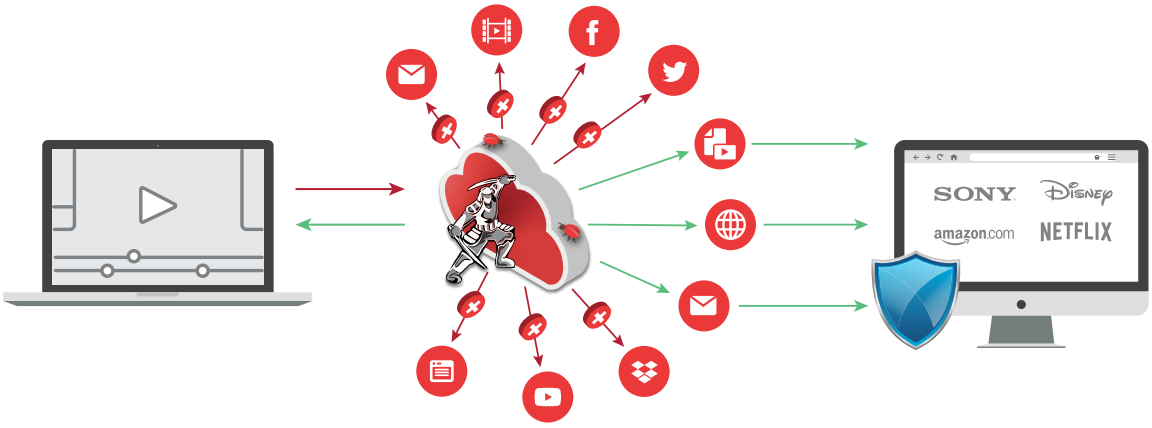
In an important update to the MPA Best Practices Guidelines, Version 4.09 recommends that studios and distributors consider adopting Remote Browser Isolation (RBI) as a best practice for enabling internet and email access from production devices for both internal and third-party uses, without risking exposure of high-value intellectual property (IP) and pre-release content.

For film, animation and visual effects companies who are Trusted Partner Network (TPN) vendors, as well as the TPN Qualified Assessors community and providers, creators, and owners of content, this represents an important opportunity to increase productivity and reduce user frustration.

As a feature-rich, high-performance solution using policy-based remote browser isolation, ZTEdge Web Isolation streamlines operations and improves the user experience for entertainment industry employees and independent artists. It enforces rigorous, granular controls to protect content while protecting workstations and networks from ransomware and phishing – all in full compliance with MPA Content Protection Best Practices.

ZTEdge Web Isolation

- Access SaaS apps, websites and email from production workstations, while preventing content from being exposed via the web
- Enhances productivity and reduces user frustration
- Granular, policy-based control of upload and browser functions by website, category, and file characteristics or size
- No-hassle uploading to approved destinations and downloading from approved sources
- Works with all standard browsers, devices and OS
- Comprehensive activity monitoring, reporting and logging
- Cloud-based and on premise options
- TPN Assessment-approved



ZTEdge™
By Ericom Software

How ZTEdge Web Isolation Supports TPN Programs

Prevents exfiltration of high-value IP via email or the web

ZTEdge Web Isolation provides airtight protection of content and IP through granular group- or category-based policies that block users from uploading content on endpoints and networks to websites and/or attaching files to emails. Browser clipboard functions (copy, cut, paste, print) may be completely disabled, disabled for specific websites or website categories, or otherwise restricted to providing limited, controlled copy functions for only specified websites. This allows necessary data copying while protecting against loss through, for instance, peer-to-peer sites. In cases where files are permitted to be shared, policy-based controls can be applied to ensure compliance with restrictions on file size or types, or the amount of copied data. (MPA Content Security Program, Content Security Best Practices Common Guidelines DS-2.0, DS-2.1, DS-2.2, DS-5.0)

Increases productivity by enabling browsing and email from production devices

With RBI, users can browse the internet via their production devices, with no risk to IP or production content on user devices or networks. All website content remains in remote cloud-based containers or on remote servers, safely isolated from production devices and networks. Yet users can freely access their emails and interact with websites they need, without having to switch to a different device. (DS-2.0)

Controls execution of permitted interactions

ZTEdge Web Isolation supports detailed allowlists for no-hassle uploading to approved destinations and to easily enable downloads from approved sources. Policy-based controls allow browser functions such as copy, cut, paste and print to be completely disabled, disabled for specific websites or website categories, or to allow copying between websites without allowing that data to flow to/from local applications. This allows necessary data copying while protecting against loss through, for instance, peer-to-peer sites. In cases where files are permitted to be shared, policy-based controls can be applied to ensure compliance with restrictions on file size or types, or the amount of copied data. (DS-5.0)

Isolates all web content, including ransomware and other malware, from production systems and networks

ZTEdge Web Isolation runs all website code (which potentially includes hidden ransomware or other data-stealing malware) in a virtual isolated browser in the cloud or on a remote server, essentially air-gapping production devices from the web. The web page content is rendered into an interactive media stream representing the website and sent to the usual browser on the user's device, providing a safe, fully interactive, seamless browsing experience, with no code from the web ever reaching endpoints or networks. ZTEdge Web Isolation also filters for potential phishing emails and malicious domains. All attachments permitted in accordance with policies undergo content disarm and reconstruction (CDR) before being downloaded to user devices to eliminate any malware potentially within. Finally, suspicious sites may be opened in read-only mode to prevent credential theft. (DS-2.1, DS-2.2)

> *"When users are on the workstations that we provision, their internet access is very strictly controlled. The IP and data on those workstations are the crown jewels and they need to be safely guarded. What can get in or out is very tightly regulated by us, on a practical basis. That's where ZTEdge comes in, to help us meet our compliance requirements. ZTEdge is a very high-performance solution that enables browsing to feel native. It makes users' lives better. If people are looking for a high-performance solution in this space, Ericom ticks the boxes."*
>
> **Jeremy Smith**,
> Chief Technology Officer, Jellyfish Pictures

ZTEdge™
By Ericom Software

Remote Browser Isolation: What It Is and How It Works

ZTEdge Web Isolation uses RBI to isolate websites from the end user production environment by air-gapping and rendering the website content, and then applying organization-defined policies to restrict certain browser functionality. This protects the organization while also providing the user with policy-controlled access to websites that they might otherwise not be able to access. Enabling users to view, use and interact with the websites they need on their usual browsers, as they normally do, increases productivity and reduces user frustration.

With ZTEdge Web Isolation, when a user browses to a website or clicks a link, a virtual browser is created in an isolated container in the cloud or on a remote server. Website code executes in the virtual browser, where it remains: Content is rendered into an interactive media stream representing the website and sent to the regular browser on the user's device. When the user stops browsing a site, the isolated container is destroyed, along with the virtual browser and all website content within—including any malware or ransomware that may have been on the site.

Because websites do not execute on the endpoint, no content is left in the browser cache of the user device. If a device is stolen, lost or breached, content that has been uploaded to or downloaded from the web can't be retrieved from the browser cache.

Web Usage Controls and Reporting that Go Beyond the RBI Basics

A number of key capabilities and features make ZTEdge Web Isolation particularly relevant and valuable for entertainment industry organizations and TPN vendors needing to comply with MPA Best Practice Guidelines for Digital Security.

A wide range of policy controls

ZTEdge Web Isolation enables granular, policy-based controls that simplify compliance with email and browsing restrictions. For instance, access can be fully blocked to prohibited sites such as web-based email, peer-to-peer sites, digital lockers, and known malicious sites to prevent content exfiltration and theft.

In addition, for permitted sites, browser capabilities such as printing, downloading and copy/pasting content to or from websites may also be restricted via policy-based controls.

Reporting and auditing

The centralized ZTEdge administration console provides full audit trail and reporting capabilities, including historical web access data, upload and download activities, user activity reports, risk analysis, security events, and more. Security admins can drill down into report data to reveal patterns and define custom reports to get maximum insight from historical organizational data. Data can also be automatically exported to an external SIEM for archiving and further analysis.

End user experience

Unlike remote desktop approaches, which involve numerous steps to first launch a remote desktop, and only then open a protected browser, ZTEdge Web Isolation works with standard browsers on users' regular device or desktop. While some alternative RBI solutions limit browser choice by requiring browser-specific configuration, or utilize kludgy, confusing and often imprecise browser-in-browser technology, ZTEdge Web Isolation fully protects users, on any browser they choose, at any time. It provides an excellent end user browsing experience -- even HD video plays smoothly and on-page navigation is extremely precise.

> ***"We have seen a number of studios using the Ericom solution, including Jellyfish Pictures, and are pleased with the role the technology plays in satisfying key parts of their TPN security compliance requirements."***
>
> convergent
>
> **Mathew Gilliat-Smith**,
> EVP, Convergent Risks

ZTEdge™
By Ericom Software

Protection from phishing emails and sites

ZTEdge Web Isolation protects against phishing by opening URLs in emails in isolated containers in the cloud, away from endpoints. New, uncategorized sites are opened in read-only mode to protect users who might be lured into entering credentials on a phishing site.

Protection from infected attachments

ZTEdge Web Isolation's content disarm and reconstruction (CDR) capabilities examine attachments and remove any malware embedded before downloading to endpoints. Policies may be set to restrict downloads based on user, site or type of attachment – or block all attachments.

Virtual Meeting Isolation

Like all other websites, web portals of virtual meeting solutions are vulnerable to infection with malware, which can then be passed to meeting participants via their browsers. In addition, malware has been identified which can take control of user cameras and expose private chats via virtual meeting solutions.

ZTEdge Web Isolation is the sole browser isolation solution in the market that secures virtual meetings conducted via Zoom, Microsoft Teams, Google Meet, Webex and similar meeting browser portals using a patent-pending proprietary technology supports key collaboration elements like screen sharing, and microphone and video-camera use.

Integrates easily with current and planned security systems

ZTEdge Web Isolation integrates simply with a wide range of the firewalls and secure web gateways in use today, and is also compatible with new generation SASE platforms and security solutions. Organizations that are considering updates to their security stacks can adopt the ZTEdge Web Isolation now, without locking into any specific security vendor.

TPN Vendors and Content Owners

Discover how content can be protected, MPA requirements met, and eliminate frustrating restrictions for employees.

Contact us now

TPN Qualified Assessors

Learn more about how this innovative technology can ease frustrating restrictions for your clients while protecting valuable IP.

Contact us now

Technology Resellers and Service Providers

Contact us to learn more about ZTEdge Web Isolation and how you can become a ZTEdge partner.

Become a partner

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