Zero Trust Web Isolation for Film, VFX and Post-Production Trusted Partner Network (TPN) Programs

MPA Content Security-Compliant Internet and Email Access that Boosts Productivity and Eliminates Risk of Content Exposure

MPA Content Security Best Practices, Version 5.2 recommends that studios adopt Remote Browser Isolation (RBI) to meet Technical Security Guidelines for Information Systems and Network Security. RBI enhances productivity and reduces capital costs while securing high-value pre-release content from potential exposure via the web.

For Trusted Partner Network (TPN) vendors, content owners and especially creative staff, RBI is the solution of choice due to its powerful combination of secure, air-gapped protection and frictionless use.

Ericom Web Isolation: Productivity, Content Control, and Defense Against Cyberattacks

As a feature-rich, high-performance RBI solution with a wide range of flexible, granular data sharing controls, Ericom Web Isolation is used by industry-leading studios worldwide to eliminate the inefficiencies, delays and high costs associated with dedicated, separately staffed and equipped networks for downloading and uploading content.

While fully implementing MPA Content Security Program Best Practices for corporate email and web filtering and internet access Ericom Web Isolation provides a seamless, excellent user experience for artists and entertainment content creators. It also defends studios against email and web-delivered cyberattacks as well as content loss, and enables secure use of collaborative productivity-enhancing web platforms such as O365 and Teams.

ericom security by cradlepoint

Ericom Web Isolation for MPA Content Security Program Compliance

- Access SaaS apps, websites and email from production workstations, while preventing content exposure
- Enhances productivity, lowers costs and reduces user frustration
- Granular, policy-based control of uploading based on website, category, file characteristics, and file 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

©Cradlepoint. All Rights Reserved. | cradlepoint.com

How Ericom Web Isolation Supports TPN Programs

Corporate Email Filtering (TS-1.8)

Ericom RBI strengthens email filtering to ensure secure email use from production environments. Links are opened in isolation and only safe rendering data reaches user workstations. Undetectable threats like zero days are isolated in the Ericom Cloud and then destroyed. To prevent transmission of sensitive assets and materials, policy-based content sharing controls and DLP are applied to all outgoing emails and attachments. Attachments may also be restricted by size and file type.

To protect against phishing, links from emails are opened in isolation, so no malware can be triggered. Unknown sites can be opened in read-only mode to prevent users from entering credentials on even expertly spoofed sites. Email links to sites known to contain malware, viruses or phishing threats are simply blocked.

Email attachments are secured through policies that include:

- Blocking of incoming attachments at the point of download based on AV scan, file type, and other threat data
- Previewing content of attachments within an isolated session
- Sanitization of attached files using content disarm and reconstruct (CDR) to remove threats in weaponized documents

All activity is audited to identify which websites or files are accessed by which users.

Internet Access (TS-2.8)

Ericom Web Isolation's strong security approach and extensive content controls effectively isolate user production devices from the internet and protect studio and creative content through three key measures:

1. Web browsing sessions are executed within remote isolated containers to create and maintain airgapped seperation between the user's device and the internet, and to protect studios from ransomware and other web threats.
2. Granular policy controls curtail specific functionalities, based on user identity and type of website. These controls restrict activities such as uploads, downloads, clipboard interactions, printing, copy/pasting, screenshot capturing, and more. Websites may also be restricted to being viewed in a read-only state, enhancing security to an even greater extent. This comprehensive approach fortifies the digital environment and substantially mitigates potential risks and vulnerabilities.
3. File sanitization (CDR) is applied to web downloads and email attachments to remove threats in weaponized documents.

All activity is audited to identify which websites or files are accessed by which users.

Web Filtering (TS-2.10)

Web filtering is a baseline capability of Ericom Web Isolation. A categorization engine enables policies to be set specifically for high-risk sites like file sharing services and social media platforms. DNS filtering is likewise an integral function of the RBI service.

Ericom Web Isolation protects against ransomware and other web threats by isolating web content in remote cloud containers, away from user devices. Known malicious websites are systematically classified as high or medium risk, allowing for implementation of differential measures based on the risk profile of each site. Organizations may choose to prohibit access to these sites outright or confine access within an isolated environment, with constrained privileges.

This risk-based approach provides a heightened level of security, shielding systems from potential threats originating from these sites and preventing data exfiltration. Alternatively, studios may choose full internet isolation for maximum security and control.

©Cradlepoint. All Rights Reserved. | cradlepoint.com

Remote Browser Isolation: What It Is and How It Works

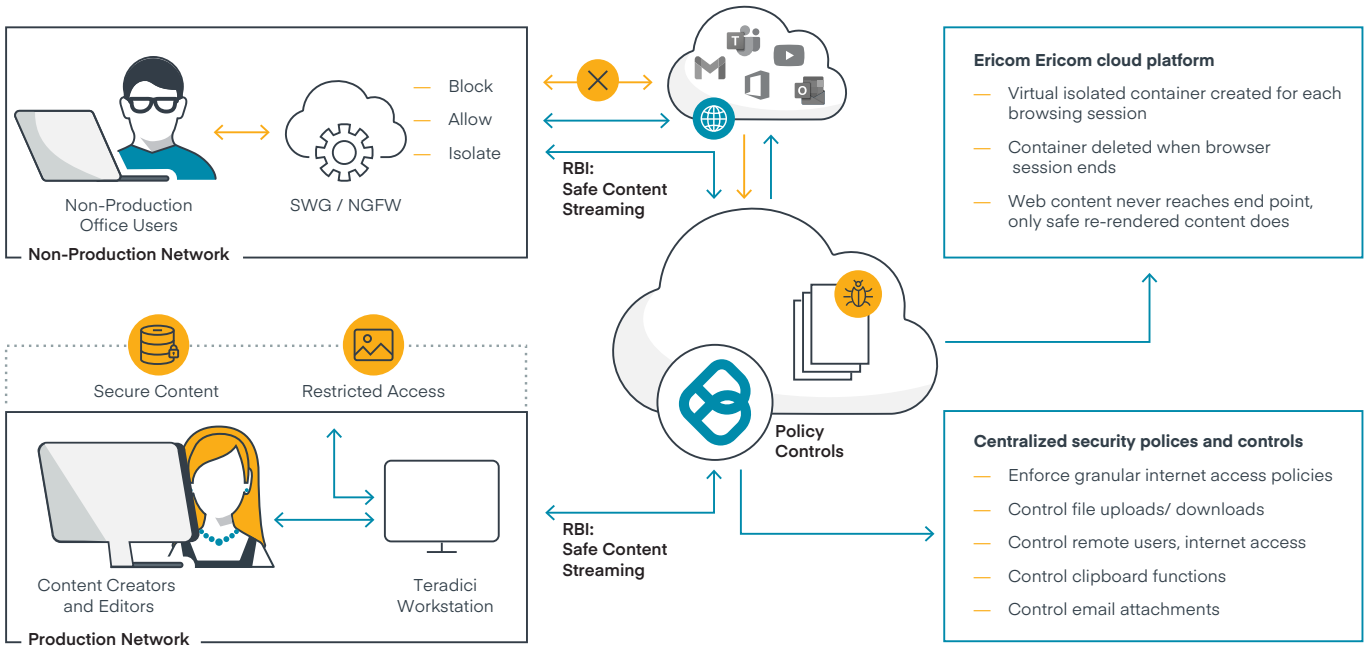
Ericom Web Isolation isolates websites from the end user production environment by air-gapping and rendering the website content in the cloud, and applying organization-defined policies to restrict selected browser functionality. This protects the organization while also providing the user with policy-controlled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

With Ericom 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.

"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 Ericom comes in, to help us meet our compliance requirements. Ericom 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



©Cradlepoint. All Rights Reserved. | cradlepoint.com

Web Usage Controls and Reporting that Go Beyond the RBI Basics

A number of key capabilities and features make Ericom 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

Ericom Web Isolation includes a range of 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 Ericom admin 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

Ericom 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, dedicated enterprise browsers, or utilize kludgy, confusing and often imprecise browser-in-browser technology, Ericom Web Isolation fully protects users, on any browser they choose. It provides an excellent end user experience -- even HD video plays smoothly and on-page navigation is extremely precise.

Protection from phishing emails and sites

Ericom Web Isolation protects against phishing by opening URLs from emails in isolated containers in the cloud, away from endpoints. New, unknown 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

Ericom 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.

Integrates easily with current and planned security systems

Ericom 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 Ericom Web Isolation now, without locking into any specific security vendor.

©Cradlepoint. All Rights Reserved. | cradlepoint.com

> **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."**
>
> **Mathew Gilliat-Smith,** EVP, Convergent Risks

convergent

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.

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

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 Ericom Web Isolation and how you can become a Ericom partner.

Become a partner

Discover how Ericom Remote Browser Isolation for TPN Compliance can empower your studio to increase productivity, reduce costs and protect sensitive data.

Contact us today for a personalized demonstration or to learn more about our scalable cloud-delivered service at ericom.com/contact-us.

©Cradlepoint. All Rights Reserved. | cradlepoint.com | R010824

cradlepoint PART OF ERICSSON