Meet MPA Content Security Program Best Practice Recommendation with Ericom RBI

MPA Content Security Best Practices v5.2 recommends that organizations involved in production of entertainment content adopt remote browser isolation (RBI) to meet technical information system security and network security requirements. This chart highlights how Ericom Web Security aligns with MPA best practices and additional recommendations.

MPA TECHNICAL SECURITY GUIDELINES	BEST PRACTICES	ADDITIONAL RECOMMENDATIONS	SITE	CLOUD	ERICOM WEB ISOLATION FOR MPA/TPN COMPLIANCE
Information Systems, Corporate Email Filtering (TS-1.8)	Establish and regularly review a process for Corporate Email Filtering to detect, report, and block the following: • Phishing emails • Malware/ransomware • Transmission of sensitive asset/content material • Executable file attachments	Incorporate into Incident Response process for reporting	✓	✓	Ericom RBI further strengthens email filtering to ensure that users can safely access email from production environments in isolation, without concern about threats that filtering misses. Additional protection include: • Sanitizing email attachments prior to download • Applying DLP and sharing controls to documents to be attached to outgoing email messages • Restriction of attachment file sizes and types • Protection against unknown phishing sites through read-only policy • Blocking access to sites linked from emails that have known malware/virus/phishing threats Email attachments can be further controlled through policies to: • Block at the point of download based on AV scan, file type, etc • Allow previewing within an isolated session • File Sanitization (CDR) - Web downloads and email attachment may be sanitized to • remove threats in weaponized documents **All activity is audited to identify which websites or files are accessed by which users.**

ERICOM SECURITY: REMOTE BROWSER ISOLATION ALIGNMENT WITH MPA GUIDELINES

MPA TECHNICAL SECURITY GUIDELINES	BEST PRACTICES	ADDITIONAL RECOMMENDATIONS	SITE	CLOUD	ERICOM WEB ISOLATION FOR MPA/TPN COMPLIANCE
Network Security, Internet Access (TS-2.8)	Establish and regularly review a policy and process for Internet Access in production networks and all systems that process or store digital content, to include the following: • Prohibit directly accessing unauthorized Internet sites, resources, or services • Prohibit direct email access • Implement firewall rules to deny all outbound traffic by default, including to the Internet and other internal networks	For isolated web browsing/ email access: • Browser isolation tools via a virtual environment that is not on the production network	✓	✓	The stringent Ericom RBI security approach effectively isolates the user's production device -- laptop, workstation, or mobile -- from the internet and protects studio and creative content through four key measures: 1. Web browsing sessions are executed within remote isolated containers, ensuring a strict barrier between the user's device and the internet. 2. Imposing granular policy controls that curtail specific functionalities of each website. These controls apply to 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, substantially mitigating potential risks and vulnerabilities. 3. File Sanitization (CDR) - Web download and email attachment are sanitized tremove threats in weaponized documents. • Isolating risky web content in remote cloud containers protects endpoints from ransomware and other web threats in addition to enforcing strict separation. **All activity is audited to identify which websites or files are accessed by which users.**
Network Security, Web Filtering (TS-2.10)	Establish and regularly review a process for corporate Web Filtering to address the following: • Peer-to-peer file sharing • Malware/ransomware • Malicious sites	Recommend implementing the use of DNS filtering	✓	✓	Ericom RBI includes web filtering categorization, enabling policies to be set specifically for file sharing sites and other high-risk sites. DNS filtering is provided as an integral part of the RBI service. Ericom RBI protect against ransomware and other web threats by isolating risky 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 precise measures. Organizations can choose to prohibit access outright or confine access within an isolated environment, with constrained privileges. This proactive approach assures a heightened level of security, shielding your system from potential threats originating from these sites. File Sanitization (CDR) sanitizes web downloads and email attachments to remove threats in weaponized documents that have been shared.