

## Meet MPA Content Security Program Best Practice Common Guideline Recommendations with RBI

[MPA Content Security Best Practice Common Guidelines V4.1](#) implementation guidance suggests that organizations involved in the production of entertainment related content evaluate the role that remote browser isolation(RBI) can play in satisfying content security requirements. This chart highlights how Ericom ZTEdge Web Isolation aligns with MPA best practice recommendations. Learn more [here](#).

MPA Security Guidelines	Recommendations	Ericom ZTEdge Web Isolation (Ericom's RBI Solution)
<b>MPA DS-2.0 BP:</b>	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application / desktop session	Ericom RBI Isolates or 'air gaps' the users production desktop environment from the internet, by 1. Executing all web browsing sessions in remote isolated containers 2. Enforcing policy controls to restrict certain functions of each website
<b>MPA DS-2.0 IG-(a)</b>	Utilize Browser Isolation via an isolated virtual environment, which allows isolated Internet browsing and email access. This must be completely isolated from the production network (e.g., Ericom RBI, McAfee Light Point, Zscaler, Palo Alto Prisma, Menlo Browser Isolation)	This includes uploads, downloads, clipboard, printing, etc
<b>MPA DS-2.0 IG-(b)</b>	Access to restricted or malicious sites is prohibited	Known malicious sites are categorised as high/medium risk so that policies can be applied to either block access or isolate with restricted access
<b>MPA DS-2.0 IG-(c)</b>	Restrict content from being transferred to or from the system	Files can be blocked and controlled by domain name from being transferred to or from the system
<b>MPA DS-2.0 IG-(d)</b>	Review system activity regularly	Audit reports are available showing full user activity including session browsing, uploads, downloads, administrative functions, etc
<b>MPA DS-2.0 IG-(e)</b>	block the download/upload, block copy and paste functions to the Internet gateway system from the production network	Uploads/downloads can be blocked; Clipboard controls can be restricted in mutiple ways, including • copy to/from desktop/device • copy between isolated websites • by size of data • by text vs images

MPA Security Guidelines	Recommendations	Ericom ZTEdge Web Isolation (Ericom's RBI Solution)
<b>MPA DS-2.1 BP:</b>	Implement - corporate filtering software or appliances that block the following: <ul style="list-style-type: none"> <li>• Potential phishing emails</li> <li>• Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.)</li> <li>• File size restrictions limited to 30 MB</li> <li>• Known domains that are sources of malware or viruses</li> </ul>	Ericom RBI can ensure that even after email filtering has been performed, users can safely access email from production environments in isolation, with additional protection around <ul style="list-style-type: none"> <li>• downloading email attachments</li> <li>• uploading documents to be attached to outgoing emails</li> <li>• restriction of file sizes, attachment types</li> <li>• protection against unknown phishing sites through read-only policy</li> <li>• blocking access to sites that have known malware/virus/phishing threats</li> </ul>
<b>MPA DS-2.1 IG(a)</b>	Identify restricted content types for email attachments	Email attachments can be controlled through policies, to <ul style="list-style-type: none"> <li>• block at the point of download based on AV scan, file type, etc</li> <li>• allow previewing within an isolated session</li> </ul>
<b>MPA DS-5.0 BP:</b>	Implement - corporate filtering software or appliances that block the following: <ul style="list-style-type: none"> <li>• Potential phishing emails</li> <li>• Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.)</li> <li>• File size restrictions limited to 30 MB</li> <li>• Known domains that are sources of malware or viruses</li> </ul>	Ericom RBI incorporates additional features for web filtering as well as browser isolation. Through DNS categorisation of websites, policies can be set to <ul style="list-style-type: none"> <li>• block high risk sites or known malicious domains</li> </ul>
<b>MPA DS-5.0 IG:</b>	Implement - corporate filtering software or appliances that block the following: <ul style="list-style-type: none"> <li>• Potential phishing emails</li> <li>• Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.)</li> <li>• File size restrictions limited to 30 MB</li> <li>• Known domains that are sources of malware or viruses</li> </ul>	<ul style="list-style-type: none"> <li>• protect medium risk websites by isolating sites that may have yet unknown malware.</li> <li>• protecting against known or unknown phishing sites by either blocking or forcing the site to read-only</li> </ul>
<b>MPA DS-5.0 BP:</b>	Designate specific data I/O systems to be used for uploading / downloading content from / to external networks (Internet)	Ericom RBI can restrict downloads and uploads to only specific authorised external websites
<b>MPA DS-5.0 IG:</b>	Implement allow listing to restrict content downloads and uploads to only authorized external sources and destinations	

The below is also referenced for non-production users

MPA Security Guidelines	Recommendations	Ericom ZTEdge Web Isolation (Ericom's RBI Solution)
<b>MPA DS-6.2 BP:</b>	Scan all content for viruses and malware prior to ingest onto the content / production network.	All content can be scanned prior to download through any combination of these options <ul style="list-style-type: none"> <li>• multiple AV scans</li> <li>• block by file type</li> <li>• file structure check to ensure file type (extension) is correct</li> <li>• CDR (Content Disarm and Reconstruction) to remove active content prior to downloads to stop the threat of Malware within documents</li> </ul>
<b>MPA DS-6.2 IG:</b>	Perform scans on a system that is not connected to the content / production network	RBI protects users on both the production and non-production back-office networks, so that any downloaded content is scanned for AV & malware

### About ZTEdge Web Isolation from Ericom Software

Ericom Software is a leading provider of cloud-delivered, Zero Trust cybersecurity solutions that protect today's digitally distributed organizations from advanced security threats. The company's ZTEdge™ Web Isolation is an industry leading remote browser isolation (RBI) solution that protects organizations from web and email-based threats. The award-winning solution is available via on-premises or via the Ericom Global Cloud, a distributed high-availability elastic cloud platform. Ericom's cybersecurity solutions protect thousands of businesses and millions of end users worldwide. The company has offices around the world and a global network of distributors and partners.