ERICOM
Cybersecurity Unit of Cradlepoint
Part of Ericsson

Web Application Isolation

Protect Corporate Apps and Data from Third Party and Unmanaged Device Access Risks

Clientless, cloud-based Ericom Web Application Isolation secures access from unmanaged contractor and partner devices and user BYODs

Third party contractors and employees are increasingly using personal devices to access corporate networks, data and applications, as well as cloud and web apps. This trend, which was dramatically accelerated by pandemic-triggered remote work, brings convenience and productivity benefits to business partners and customers as well as the growing cadre of third party consultants and contractors.

Access to private corporate applications via unmanaged devices, however, poses very real risks for organizations. Devices may be compromised by malware, which could be uploaded to applications and spread across corporate networks, leading to downtime or stolen or corrupted data. In addition, sensitive data and files that are downloaded or copy/pasted onto unmanaged user devices or cached in a device's web browser, may be at risk of exposure, either intentionally or inadvertently.

While many organizations rely on reverse proxies to authenticate users on unmanaged devices for network access, this solution provides little – if any -- control once these users have successfully logged in. They enable third party users to move laterally throughout the network, and view, download and upload data which they have no need to see.

Some newer solutions require users to install software or dedicated browsers on their unmanaged devices. Gig workers as well as employees may be reluctant to load up personal devices with organization-specific software, and equally annoyed to be restricted to an unfamiliar browser.

Organizations face similar concerns regarding public SaaS cloud and web apps. For instance, a third party user with O365 credentials -- or hacker who stole credentials from an unmanaged device -- may be able to log in from any device, exposing the organization to possible uploads of infected files or data loss.

71%

of respondents said **digital risk is top priority for 3rd party risk management**

Deloitte

The Solution: ZTEdge Web Application Isolation

Ericom Web Application Isolation enables organizations to provide simple, secure clientless access, from unmanaged devices, to private and public cloud or web-based corporate applications for 3rd party contractors, partners, customers and employees using BYODs. The cloud-based solution does not require any software to be installed on the unmanaged device, and users browse via their usual browser.

Using remote browser isolation (RBI) and easy-to-set granular, user-level policies, Ericom Web Application Isolation controls which applications each user can access and which actions each individual is permitted to take.

For instance, an employee may be allowed to edit a file in place in O365, but not to download it onto their unmanaged device, while a contractor may be limited solely to viewing the data. Policies also control what content – if any -- can be uploaded to organization networks or web or cloud apps, and by whom. Content disarm and reconstruct (CDR) is applied prior to upload to ensure that all content and files from unmanaged devices are free of malware and threats. Data loss protection (DLP) and filtering can be applied to downloads to safeguard against exposure of confidential material and PII.

To protect against credential misuse or theft, SaaS and web application access may be restricted to logins originating from the dedicated IP address of the Web Application Isolation tenant.

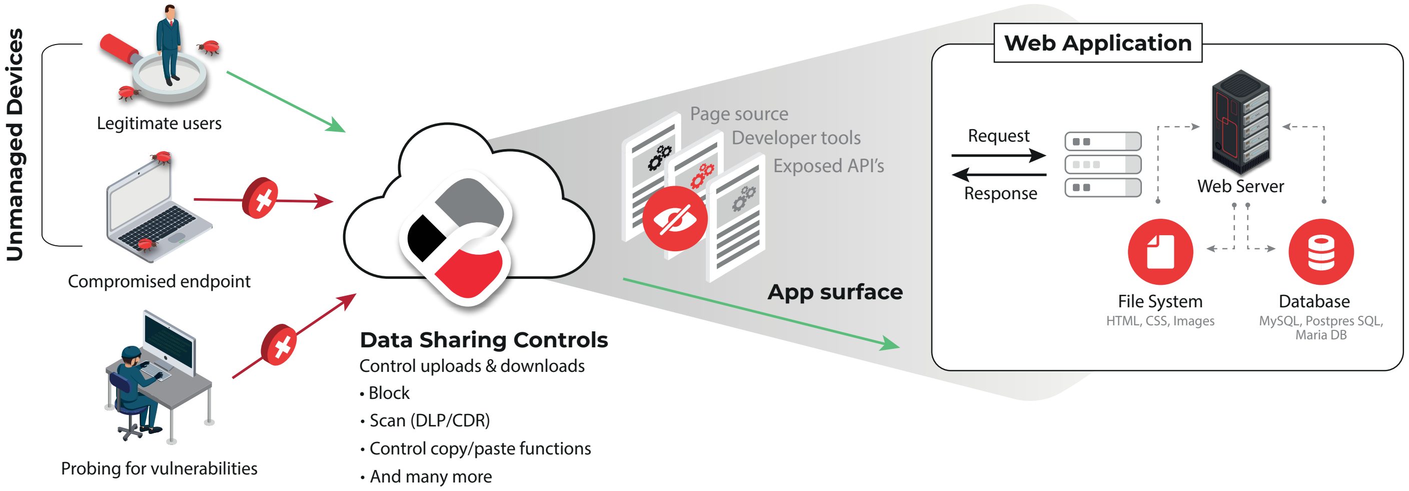
Built-in Identity and Access Management enables quick on-boarding of employees and contractors -- and makes it equally simple to cancel access privileges when contracts end or employees leave.

Ericom Web Application Isolation Highlights

- Clientless solution
- Restrict app access with policy-based controls
- Protect data in corporate web apps, private cloud apps, & public apps (O365, Zoom)
- Granular controls on upload, download, clipboarding and more
- Scan downloads with DLP to prevent exfiltration of sensitive data
- Scan uploads with CDR to block malware
- Open selected web pages in RBI read-only mode to keep sensitive data out of unmanaged device caches
- Cloak app surfaces from exposure on web
- Scalable cloud-delivered service is easy to deploy, install and manage
- Rapid user onboarding

ERICOM
Cybersecurity Unit of Cradlepoint
Part of Ericsson

Web Application Isolation Leverages RBI to Protect Web Apps, Websites and Data from Risky Access via Unmanaged Devices



Data Sharing Controls
Control uploads & downloads
- Block
- Scan (DLP/CDR)
- Control copy/paste functions
- And many more

Security Controls and Functionality

Cloud-based security controls enforce least-privilege access from unmanaged devices and restrict permitted activities to prevent threats, breaches, and data exposure. Ericom Web Application Isolation controls and functionality include:

- User identification and authentication (IAM/MFA)
- Blocking or restricting file uploads and downloads
  - Sanitizing documents OK'd for upload with CDR
  - Scanning documents OK'd for download with DLP to prevent data exfiltration
- Disabling cut & paste (clip-boarding) or restricting based on...
  - Quantity of info
  - Paste destinations (i.e., specific apps)
  - DLP inspection
  - Time in clipboard
- "Read-only" mode for app access (no text updating)
- No application data is cached in unmanaged device browsers
- App access from unmanaged devices is permitted only from IP address of organization's Web Application Isolation tenant

Contact us today to learn more about our cloud-delivered Zero Trust security solutions.

ERICOM
Cybersecurity Unit of Cradlepoint
Part of Ericsson

www.ericom.com

info@ericom.com

Americas:
T +1 (201)767-2210

UK & Western Europe:
T +44 (0)1905 777970

Worldwide:
T +972-2-591-1700

Follow us