ERICOM
Cybersecurity Unit of Cradlepoint
Part of Ericsson

Web Application Isolation

Protect Your Business from Third Party and BYOD Unmanaged Device Risks

Ericom Web Application Isolation protects cloud and private web applications and sensitive data with clientless security controls

To optimize productivity and competitiveness, modern businesses have transitioned to use of both public cloud applications and private applications, which employees as well as individuals outside of the organization access directly.

The benefits of increased efficiency, reduced manpower and lower capital costs associated with broad application-enabled remote access comes with significant security risks. “Appification" results in customers, contractors and partners accessing applications from devices that are unmanaged and therefore risky. Employees using their own unmanaged BYODs pose similar risks.

Unmanaged devices lack the strong defences organizations require to meet the high security standards they maintain to protect their applications and data. As a result, businesses face the unique challenge of needing to provide access to sensitive data and application, but without being able to de-risk that access. Unmanaged device risks may include:

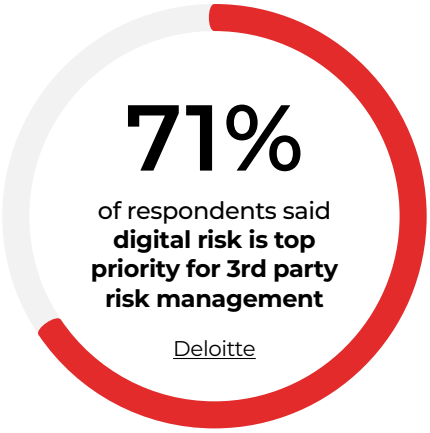
Malware. Infection with malware, which can spread to corporate applications and networks when the device is connected.

Credential Theft. Without security controls and governance, unmanaged devices are easy, vulnerable targets for hackers phishing to steal user credentials for corporate applications.

Data Loss. Once a device is logged into an application, a hacker using a compromised user account can bypass in-app controls to exfiltrate sensitive data using a variety of techniques such as leveraging browser clipboarding functions.

Broad Attack Service. Traditional VPNs and reverse proxies authenticate users but once connected, permit full network access. Users and malware can move laterally through networks attacking all business assets, in violation of the Zero Trust principle of least privilege access.

Inappropriate Data Access. A data breach can result if an unmanaged device with access to corporate data is stolen or lost.



Ericom Zero Trust Web Application Isolation

Cloud-based clientless Ericom Web Application Isolation enables organizations to adopt use of public cloud applications and private or web-based corporate applications while ensuring secure access from unmanaged devices of third parties and employee BYODs.

Users on any managed or unmanaged device may access applications via the Ericom Global Cloud, where isolated containers airgap business applications and data from any malware or security threats on the device. Easy-to-set granular policy controls restrict access and data usage on a least-privilege basis and enforce per-user browser controls to prevent data loss. For instance, an employee working from a BYOD may be permitted to edit a file within O365 but not to download it onto their unmanaged device, while a contractor may be limited solely to viewing data within an app.

Policies also control which content – if any -- can be uploaded to organization networks or web or cloud apps, and by whom. Within the airgap container, content disarm and reconstruct (CDR) is applied to documents to be uploaded to ensure that they are free of malware and pose no threat.

Data filtering and data loss protection (DLP) safeguard against exposure of confidential information and PII. Built-in Identity and Access Management enables quick user onboarding and makes it simple to cancel access privileges when users no longer need it.

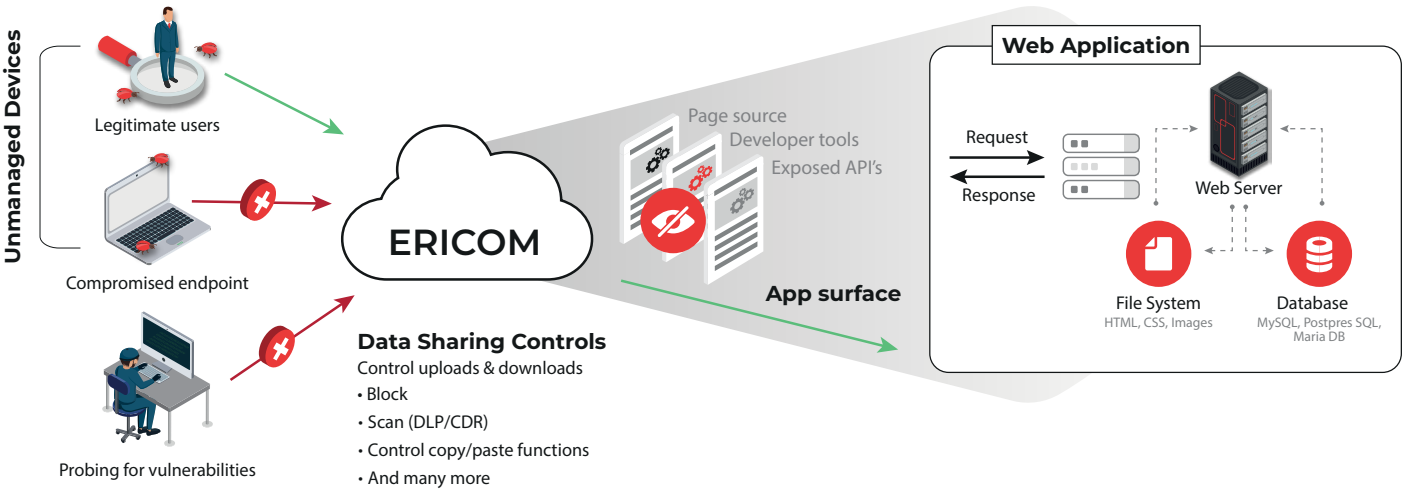
Ericom Web Application Isolation Highlights

- Clientless solution
- Protect data in corporate web apps, private cloud apps, & public apps (O365, Zoom)
- Restrict app access with granular policy-based control of uploads, downloads, 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 Remote Browser Isolation (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

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



Data Sharing Controls Prevent Exposure via Unmanaged Device Access

- Scan permitted downloads and clipboard content with DLP to prevent exposure of PII
- Restrict or block file downloads to unmanaged device
- Optional read-only mode blocks free-form text updates
- Apply granular browser clip-boarding controls including:
  - Limits on amount of data stored in clipboard
  - Restrictions on locations from which data can be copied to clipboard
  - Full or partial restriction of copy/paste and print functions
- Since no data reaches browser cache, it cannot be exposed if device is stolen or lost

Clientless Protection for Web Applications

- Authenticate users with IAM/MFA
- Restrict unmanaged device access to logins via the business's WAI cloud tenant
- Isolate web application access to prevent infection with malware from user device
- Sanitize permitted uploads with content disarm and reconstruct (CDR) to protect app from embedded malware

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