ZTEdge™
By Ericom Software

Web Application Isolation

Protect Corporate Apps and Data from 3rd Party and Unmanaged Device Access Risks

Cloud-based ZTEdge Web Application Isolation secures access from unmanaged devices, without special software or browsers that must be installed

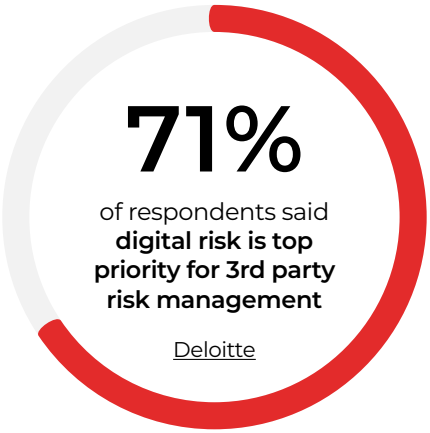
What was once touted as "Bring Your Own Device" (BYOD) now goes without saying: Both 3rd party contractors and employees are increasingly using personal devices to access corporate networks, data and applications, as well as cloud and web apps. This trend, which was dramatically accelerated by pandemic-triggered remote work, is one that many IT organizations are working to support since it brings convenience and productivity benefits to their business unit partners as well as the growing cadre of 3rd party consultants and contractors they work with in today's gig work economy.

Access to private corporate applications via unmanaged devices, however, poses a number of very real risks for organizations. Devices may be compromised by malware, which could be uploaded to applications and spread across the corporate networks, leading to downtime or worse yet, stolen or corrupted data. In addition, sensitive data and files that are downloaded or copied/pasted onto unmanaged user devices for legitimate use, 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. Unfortunately, 3rd party users are able 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 3rd party user with Office 365 credentials may be able to log in from any device, exposing the organization to possible uploads of infected files or breaches, in the case of credential theft or misuse.



The Solution: ZTEdge Web Application Isolation

ZTEdge Web Application Isolation enables organizations to provide simple, secure access, via unmanaged devices, to the private and public cloud or web-based corporate applications and data users need for their work, regardless of whether they are 3rd party contractors or employees. The cloud-based solution does not require any software or clients to be installed on the unmanaged device, and users are free to browse via their usual browser.

Using remote browser isolation (RBI) and easy-to-set granular, user-level policies, ZTEdge Web Application Isolation controls which applications the user can access, how they can access each one, and which actions each individual is permitted for each resource.

For instance, an employee may be allowed to edit a file in place in Office 365, 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) 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 Web Application Isolation tenant dedicated IP address.

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.

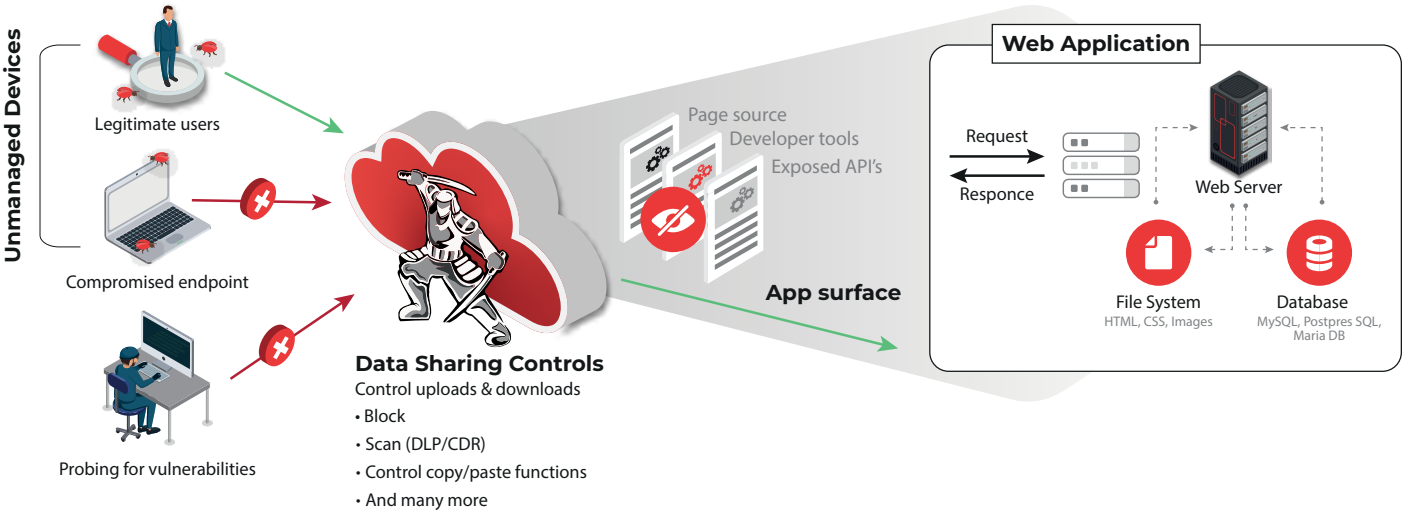
ZTEdge Web Application Isolation Highlights

- No special software or browsers to install on devices
- Restrict what apps each user can access
- 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
- Cloaks web-exposed app surfaces
- Scalable cloud-delivered service is easy to deploy, install and manage
- Rapid user onboarding

ZTEdge™
By Ericom Software

Web Application Isolation

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



Security Controls and Functionality

Cloud-based security controls enforce least-privilege access from unmanaged devices and restrict permitted activities to prevent threats, breaches, and exposure of resources to attack. ZTEdge 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 of malware and/or scanning with DLP to prevent data exfiltration
  - Sanitize documents OK'd for download of malware and/or scanning 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

www.zerotrustedge.com

info@zerotrustedge.com

Americas:
T +1 (201)767-2210

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

Worldwide:
T +972-2-591-1700

Follow us