ERICOM
BE CONNECTED, BE SECURE

Ericom Shield Remote Browser Isolation
Zero Trust protection from web-borne malware and credential theft

Endpoint attacks are on the rise

94% of businesses have had malware delivered by email, and 23% report malware entering via the web*. Detection-based solutions are powerless against unknown or zero-day threats. Credential theft-sites are removed before they can be categorized as malicious – but not before phishing emails lure users in.

Shield your business from web-borne dangers

Ericom Shield Remote Browser Isolation empowers users to securely and efficiently access the essential web-based tools of every modern business – websites and email -- without the risk of malware attacks or credential theft and without investment in costly infrastructure.

Secure Browsing

Ericom Shield renders websites in remote, isolated containers located in the DMZ or cloud, and delivers only a safe interactive media stream to end-users, on their standard browser. No active content ever reaches the endpoint. Users enjoy secure, seamless, hassle-free access to the sites that they need.

Phishing Protection

When it comes to phishing attacks, user training just isn't enough. Ericom Shield executes email-embedded URLs away from endpoints, in remote virtual browsers in the cloud or DMZ, so no malware can reach endpoints. For extra protection from credential theft, the clean media streams can be sent to endpoints in read-only mode, preventing users from entering sensitive data such as user IDs and passwords.

Document-borne Malware Protection

Let users download the files they need from websites and emails, without fear of embedded malware. Ericom Shield content sanitization capabilities disarm embedded threats then reconstruct and deliver safe files, with native functionality intact.

Ericom Shield Remote Browser Isolation

- Websites are rendered in isolated containers in the cloud or DMZ, so no active content ever reaches endpoints

- Proxy-based access – easily integrates with all secure web gateways

- URL redirection to virtual browsers in the cloud or DMZ

- Zero installation on the endpoint

- Works with any endpoint browser, device and OS

- Embedded URL filtering

- Category-based policy management

- Comprehensive activity reporting and logging

- Highly-available distributed cloud platform delivers 99.999% uptime

---

*Verizon 2019 DBIR

Ericom Shield Remote Browser Isolation
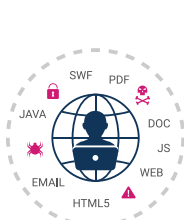
Malware in active web and email content targets enterprises via endpoint browsers

Ericom Shield executes web content in a virtual browser in a isolated container.
a. Download content b. Execute c. Render

Rendered webpages are sent to endpoints as a safe interactive media stream

Users enjoy secure and seamless browsing in their standard browser

Ericom Shield Remote Browser Isolation Improves Security While Reducing Cost and Complexity

- Neutralizes the most prevalent cyber attack vectors -- browsing & email
- Keeps employees productive by providing a secure, cost-effective native browsing experience
- Protects users from sophisticated social engineering, credential theft and phishing attacks
- Air-gaps browser-executable code, email links and downloads away from endpoints
- Opens each tab in a unique, disposable container to eliminate cross-site scripting attacks
- Simplifies IT operations by minimizing false positives and helpdesk calls
- Works with all browsers, devices and operating systems
- Flexibly scales as organizations need to add isolation to cover incremental users

What's Running in Your Browser?

Typical Unsecure Browsing		Ericom Shield Browsing Service	
Java Scripts	152	Java Scripts	4
CSS Scripts	3	CSS Scripts	0
External URLs	22	External URLs	0

Page Source with Unsecured Browsing

Page Source with **Ericom Shield**