

SOLUTION BRIEF

Fortinet and Ericom Shield Remote Browser Isolation Solution

Broad, Integrated, and Automated Solution for Secure Web Browsing and Protection Against Zero-day Attacks

Challenges

User endpoints are among the most vulnerable attack vectors, with a majority of both known and unknown malware from the internet penetrating organizations via web browsers. Attacks may originate from a URL link embedded in an email or a message, or from malicious scripts injected into legitimate websites but unnoticed by traditional detection-based measures such as antivirus, firewall, and URL filtering.

Browsing is an essential business practice for almost all organizations. Yet despite the array of products that protect endpoints, users are still susceptible to browser-borne threats. Securing corporate assets from the many threats associated with internet connectivity is a real challenge for InfoSec departments. Some of the highest profile—and costly—recent cybersecurity breaches started with a seemingly benign website visit that introduced malware into the corporate network. The costs and damages associated with recovering from these attacks can be crippling.

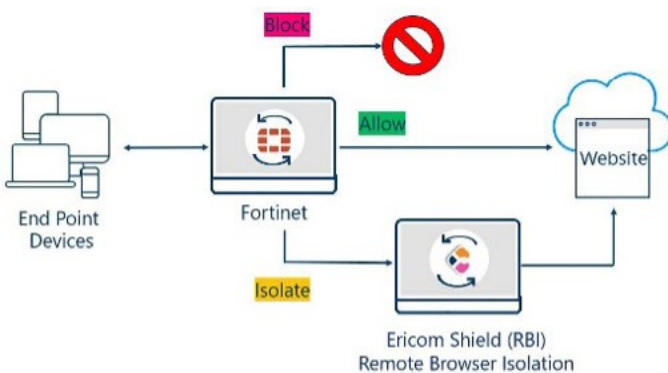
Ericom Software and Fortinet recently established a technology partnership to address these challenges.

Joint Solution Description

The joint solution workflow operates as follows:

- End-user requests a website, using FortiGate as a web proxy
- FortiGate evaluates the request, and if allowed, forwards the request to Ericom Shield
- Ericom Shield navigates to the requested URL
- Ericom Shield virtual browser renders site content in a remote disposable Linux container and sends a safe, interactive visual stream to the end-user's browser
- Once the user stops browsing, or closes the tab or the browser, the Linux container is destroyed along with all site content

Diagram of Joint Solution



Joint Solution Components

- Fortinet FortiGate Next-generation Firewall
- Ericom Shield

Joint Solution Benefits

- Unrecognized, uncategorized, and high-risk rated websites may be browsed freely and naturally, without risk of infection
- Protection from zero-day and file-less malware that evades detection-based solutions
- Clientless—no installation and maintenance required on end-user devices
- Agnostic solution supports all devices, browsers, and operating systems
- Enhances productivity by empowering users to browse without fear of data exploits, ransomware, malvertising, and other threats
- Read-only anti-phishing mode protects against credential theft
- Reduces help desk overhead for browsing exception requests



Solution Components

Ericom Shield

Ericom Shield is an award-winning Remote Browser Isolation (RBI) solution that effectively protects endpoints and networks against web-borne threats. With Ericom Shield, users browse the internet naturally, using any browser. Websites are rendered in an isolated, disposable Linux container in the cloud or DMZ, away from the endpoint. A clean media stream that is transmitted from the container to the browser on the user's device enables full user interaction, while protecting the endpoint and the corporate network from malware, ransomware, malicious cryptomining, and other threats.

FortiGate Next-generation Firewall (NGFW)

The Fortinet enterprise firewall solution offers universal platform support for all types of deployments, giving security professionals maximum latitude across the extended enterprise network. Security managers have the visibility and control they need to counter attackers with one network security operating system across the entire FortiGate family of appliances. And all the FortiGate appliances are interconnected with the Fortinet Security Fabric for automatic distribution of contextual security policy and threat intelligence throughout the enterprise. Using a single-pane-of-glass dashboard, security managers can consolidate their management views and implement security policies concisely.

Use Cases

Use Case 1:

Some professionals, such as cybersecurity researchers, require access to browse the dark web to research new threats. They need to browse safely without themselves being victimized.

Solution: With the Fortinet FortiGate and Ericom Shield integrated solution, URL filtering is tailored for investigators to gather data on relevant dark web sites, which are blacklisted for most users. The FortiGate detects and denies the bulk of the known attacks stemming from those sites. Using Ericom Shield, uncategorized, unknown, and suspicious websites are rendered by an isolated browser remote from the endpoint in the DMZ or cloud, so that any malware that is present cannot infect endpoint devices, and from there, enter corporate networks.

Benefit: Specific users or teams that require open access to the internet to perform their jobs can do so freely without risking penetration of malicious content.

Use Case 2:

End-users are constantly bombarded with phishing attempts to obtain access credentials and enable theft of sensitive data or funds. Eventually, a user will be duped into clicking an email link to a spoofed site, which in turn fools him into entering corporate credentials that can be used to gain access to mission-critical systems and harm business operations.

Solution: With the Fortinet FortiGate and Ericom Shield integrated solution, the bulk of known phishing sites are blocked by FortiGate, while sites that are harder to categorize or have not yet been categorized are opened by Ericom Shield. Ericom Shield's built-in anti-phishing capabilities allow the site to be opened in read-only mode, preventing users from entering sensitive data. If the site is subsequently deemed safe, it can be whitelisted in FortiGate and will be fully accessible to the user the next time they navigate to it.

Benefit: Prevents credential theft via social engineering attacks using spoofed websites. Users can interact with potentially malicious sites to determine if they are safe, while being protected from their own possible errors.



About Ericom

Ericom Software (<https://www.EricomShield.com>) is a global leader in enterprise-grade cybersecurity and connectivity software. Founded in 1993, Ericom provides solutions to a global customer base of more than 30,000 midsize to Fortune 500 organizations. With a focus on secure browsing, application delivery and cloud enablement, Ericom is trusted by customers in over 45 countries and serves more than ten million users at 30,000 organizations of all sizes.



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.