ZTEdge™
By Ericom Software

ZTEdge Web Isolation for VM Series NGFWs

Remote Browser Isolation for Palo Alto Networks VM Series Next Generation Firewalls

Protection from web delivered zero-day threats targeting your users and network

Web browsers are the most vulnerable endpoint attack vector. They are essential links in almost all cyberattack chains, and the prime attack vector through which zero-day exploits compromise organizations. Attacks may originate from malicious code embedded in website resources (e.g., scripts, images, ads, fonts), from phishing URLs embedded in emails or social media messages, or from downloads that have been weaponized to contain malware.

Fast, secure web access is essential for every user today. But security teams are hard-pressed to protect users from advanced threats hidden in website code, especially for sites with limited reputational history or those accessed through legitimate platforms, such as Twitter®, LinkedIn®, or web-based email services. Blocking access creates friction and productivity loss, but it takes just one click on a seemingly benign website for serious malware, such as ransomware, to make its way into the corporate network. The financial and reputational damage and costs resulting from these attacks can be severe.

```
<html lang="en">
    <head>

    <meta charset="utf-8">
    <!-- WPS Generated -->
    <link rel="dns-prefetch" href="https://securepubads.g.doubleclick.net/"/>
    <link rel="dns-prefetch" href="https://static.doubleclick.net/"/>
    <link rel="dns-prefetch" href="https://bidder.criteo.com/"/>
    <link rel="dns-prefetch" href="https://static.criteo.net/"/>
    <link rel="dns-prefetch" href="https://as-sec.casalemedia.com/"/>
    <link rel="dns-prefetch" href="https://js-sec.indexww.com/"/>
    <link rel="dns-prefetch" href="https://ib.adnxs.com/"/>
    <link rel="dns-prefetch" href="https://hbopenbid.pubmatic.com/"/>
    <link rel="dns-prefetch" href="https://fastlane.rubiconproject.com/"/>
    <link rel="dns-prefetch" href="https://mcclatchy-d.openx.net/"/>
    <link rel="dns-prefetch" href="https://mcclatchy-idahostatesman.zeustechnology.com/"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"/>
    <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
    <meta name="msapplication-TileColor" content="#FFFFFF"/>
    <meta name="msapplication-TileImage" content="https://www.idahostatesman.com/wps/build/images/idahostatesman/windo
    <meta name="apple-itunes-app" content="app-id=390819220, affiliate-data=at=[illegible]&amp;ct=SmartAppBannerBOI, app-
    <meta name="google-site-verification" content="WCAneqvaC[illegible]04Y"/>
    <meta name="googlebot" content="noodp, noarchive"/>
    <meta name="description" content="Follow the Idaho Statesman newspaper [illegible] headlines on Boise Idaho news
    <meta name="keywords" content="news, breaking, sports, crime, Bo[illegible] [illegible]rden City, Idaho />
    <link rel="canonical" href="https://www.idahostatesman.com/"/>
    <meta name="original-source" content="https://www.idahostatesman.com/
    <meta name="title" content="Boise ID Breaking News, Sports &amp; Crime | Idaho Statesman
    <meta property="og:site_name" content="Idaho Statesman"/>
    <meta property="og:title" content="Boise ID Breaking News, Sports &amp; Crime | Idaho Statesman"/>
    <meta name="twitter:card" content="summary_large_image"/>
    <meta property="og:image" content="https://www.idahostatesman.com/wps/build/images/idahostatesman/facebook.jpg />
    <meta property="fb:pages" content="43887022493"/>
    <meta property="fb:pages" content="136604805589"/>
    <meta property="fb:pages" content="119000034787001"/>
    <meta property="fb:pages" content="150267368335431"/>
    <meta property="fb:pages" content="122219744461960"/>
    <title>Boise ID Breaking News, Sports &amp; Crime | Idaho Statesman</title>
    <link rel="alternate" href="https://feeds.mcclatchy.com//idahostatesman/section
<script>
  window.pageInfo = {
    'videoLead': 'false', access.tags': '' , enableConfiant': true, accuweather.apiK[illegible]
    'domainName': 'www.idahostatesman.com',
    'isNewPublicApi': true',
  'marketInfo.adsizes :{'outofpage':{},'wallpaper':{'1600x600':[1600,600],'None':[]},'floorboard [illegible] 285x70':[285
  Object freeze(window.pageInfo);
```

Malware embedded in web pages

ZTEdge Web Isolation Integration

Ericom Software's ZTEdge Web Isolation is a remote browser isolation (RBI) solution that integrates with Palo Alto Networks VM Series NGFWs via standard URL redirection. This integration allows you to:

- Stop ransomware and zero-day threats from uncategorized websites, social media, phishing URLs, and other risky sites
- Remove malware from file downloads
- Eliminate "over-blocking" of web access to improve user productivity
- Free support staff from responding to help tickets to open access to blocked sites
- Prevent credential theft and oversharing of data on the web
- Keep sensitive data from web apps out of the web browser cache on unmanaged devices

How Remote Browser Isolation Works

The ZTEdge Web Isolation cloud service prevents ransomware, advanced web threats, and phishing attacks from reaching user endpoints by rendering web content in a remote, isolated container. Whether users browse a malicious site directly or click a URL embedded in a phishing email or social media site, they are completely safe since no web content ever executes directly on their device. A media stream representing the website is sent to a device's browser, providing a safe, fully interactive, seamless user experience. For additional phishing protection, websites launched from emails and other suspicious sites can be rendered in read-only mode to prevent users from entering credentials. Attached files are sanitized before being transmitted to endpoints, ensuring that malware within downloads cannot compromise user devices.

VM Series and ZTEdge Web Isolation

The integration of Palo Alto's NGFW and ZTEdge Web Isolation provides a multilayer defense that effectively protects your endpoints, networks, and data from the full range of known and zero-day threats while facilitating essential, productive web-based business activity.

The VM Series NGFW detects known and unknown threats, even in encrypted traffic. Based on URL Filtering, requested sites on the allow list are opened natively on the user's endpoint browser while those on the deny list are blocked. Uncategorized or unidentifiable sites, or those in specified categories, are redirected to ZTEdge Web Isolation to be rendered in isolation, safely away from the corporate network and end user devices.

The integrated Palo Alto Networks and ZTEdge Web Isolation solution secures business-critical web-based activity and protects against undetectable threats and human factor vulnerabilities (e.g., users clicking on phishing URLs) by:

- Inspecting and blocking detectable and known malicious content
- Filtering deny-listed URLs and blocking access
- Isolating all active untrusted web content away from endpoints and internal networks
- Sending isolated web content to endpoints as rendering data so no malware can impact devices or networks
- Sanitizing file downloads from the internet to disarm potentially malicious content
- Providing a read-only mode to prevent users from entering credentials on phishing sites

Securing Endpoints with VM Series NGFW-ZTEdge Web Isolation Integration

The integrated VM Series NGFW-ZTEdge Web Isolation solution provides flexible, resource efficient protection for a wide variety of use cases.

1 Use Case 1: Expand Web Access Without Increasing Risk

Challenge

Blocking access to websites with limited reputational history (e.g., “uncategorized” or “unknown” sites) can create significant user frustration and productivity loss as well as burdening operational teams with requests for exceptions. Yet simply enabling access creates very real cybersecurity risk for an organization. Organizations need to be able to offer secure access.

Solution

With the VM Series NGFW and ZTEdge Web Isolation integrated solution, you can design policies to selectively send certain websites or site categories (e.g., uncategorized/risky websites, social media) to ZTEdge to be isolated. Users get access to the websites they need and enjoy a completely normal browsing experience. And security personnel know that endpoints and networks are protected since only safe rendering information representing the website reaches user devices. Any malware on a site remains in the remote isolated container, which is destroyed after the browsing session.

Benefit

The integrated solution offers broad web access for business tasks with no risk of malware compromising devices. IT and Help Desk teams avoid time-consuming policy modifications to selectively enable access to sites.

2 Use Case 2: Secure Access to Web Email and Social Media

Challenge

Users are under constant threat from malicious links embedded in web email and social media sites, leading to sites designed to steal sensitive data (e.g., login credentials) or infect endpoints with malware. As a result, many organizations block or limit access to sites like Gmail® and Facebook®. Users want access to these sites, but many security and IT teams regard the risk as simply too great.

Solution

With the VM Series NGFW-ZTEdge Web Isolation integrated solution, you can set VM NGFW policies to send traffic from social media and web email sites to ZTEdge to be isolated.

The sites are then rendered in an isolated container, and only safe rendering information is sent to the user's device. Newly-created and uncategorized sites may be opened in read-only mode for further protection against credential theft.

Benefit

Users get access to the social media and web email services they need to complete their work, and your Security personnel get the strong web protection your organization requires.

3 Use Case 3: Protect the C-Suite and High-Risk Users

Challenge

Compared to general employees, senior executives are at significantly higher risk of being targeted by cybercriminals via phishing, business email compromise (BEC), social engineering attacks, and more. While you never want any endpoint to be compromised, a successful attack on executives' and high-risk users' devices may spell "game over" due to their privileged access to sensitive data and systems.

Solution

With the VM Series NGFW and ZTEdge Web Isolation integrated solution, VM NGFW policies can be set to send all web and cloud application traffic from executives or high-risk users to ZTEdge to be isolated. These sites are rendered in an isolated cloud container, and only a safe, fully interactive media stream is sent to the user's device. Remote browser isolation protects these users' endpoints from 100% of the malware they may encounter on a website, in a social media stream, or in a URL or attached file they click on in an email.

Benefit

Protect executives and high-risk users who are targeted at elevated rates. Isolating all their traffic "air gaps" their endpoints from 100% of malware, giving them the strongest protection while preserving their web browsing experience.

ZTEdge™
By Ericom Software

4 Use Case 4: Prevent Loss of Sensitive Data via Endpoints

Challenge

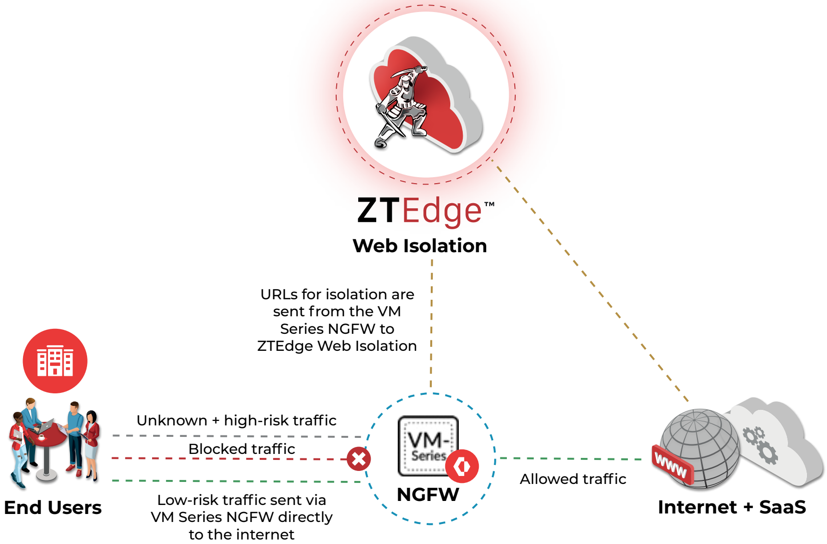
As organizations embrace digital transformation initiatives, it is growing more difficult to maintain control over sensitive information. Users' interactions with web- and cloud-based applications present a significant data loss risk because data is left in the browser cache on each and every endpoint device each time it's used to access private web apps. Equally concerning is the significant risks of data leakage via "footprint" from public software as a service (SaaS) apps, such as Salesforce®, if endpoints are compromised.

Solution

With the VM NGFW-ZTEdge Web Isolation integration, access to web and cloud applications may be only via Isolation mode. Since no web content or code is ever downloaded or stored on the user's endpoint, no data footprint is created and data cannot be lost if the device is ever compromised. Web Isolation also provides additional powerful data sharing controls, such as the ability to restrict browser functionality like screen capture, copy/paste from a clipboard to local storage, and file download/upload for specific sites or categories.

Benefit

Prevents sensitive data from being leaked to the web via web browsers due to inadvertent (or purposeful) exposure by employees.


ZTEdge™
Web Isolation
URLs for isolation are sent from the VM Series NGFW to ZTEdge Web Isolation
Unknown + high-risk traffic
Blocked traffic
Low-risk traffic sent via VM Series NGFW directly to the internet
VM-Series
NGFW
Allowed traffic
www
End Users
Internet + SaaS

Solution architecture overview

About ZTEdge Web Isolation from Ericom Software

Ericom Software is a leading provider of cloud-delivered, Zero Trust cybersecurity solutions that protect today's digitally distributed organizations from advanced security threats. The company's ZTEdge™ Web Isolation is an industry leading remote browser isolation (RBI) solution that protects organizations from web and email based threats. The award-winning solution is available via on-premises or via the Ericom Global Cloud, a distributed high-availability elastic cloud platform. Ericom's cybersecurity solutions protect tens of thousands of businesses and millions of end users worldwide. The company has offices around the world and a global network of distributors and partners.

www.zerotrustedge.com

Americas:
T +1 (201)767-2210
E-mail: info@zerotrustedge.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: info@zerotrustedge.com

Worldwide:
T +972-2-591-1700
E-mail: info@zerotrustedge.com

Follow us