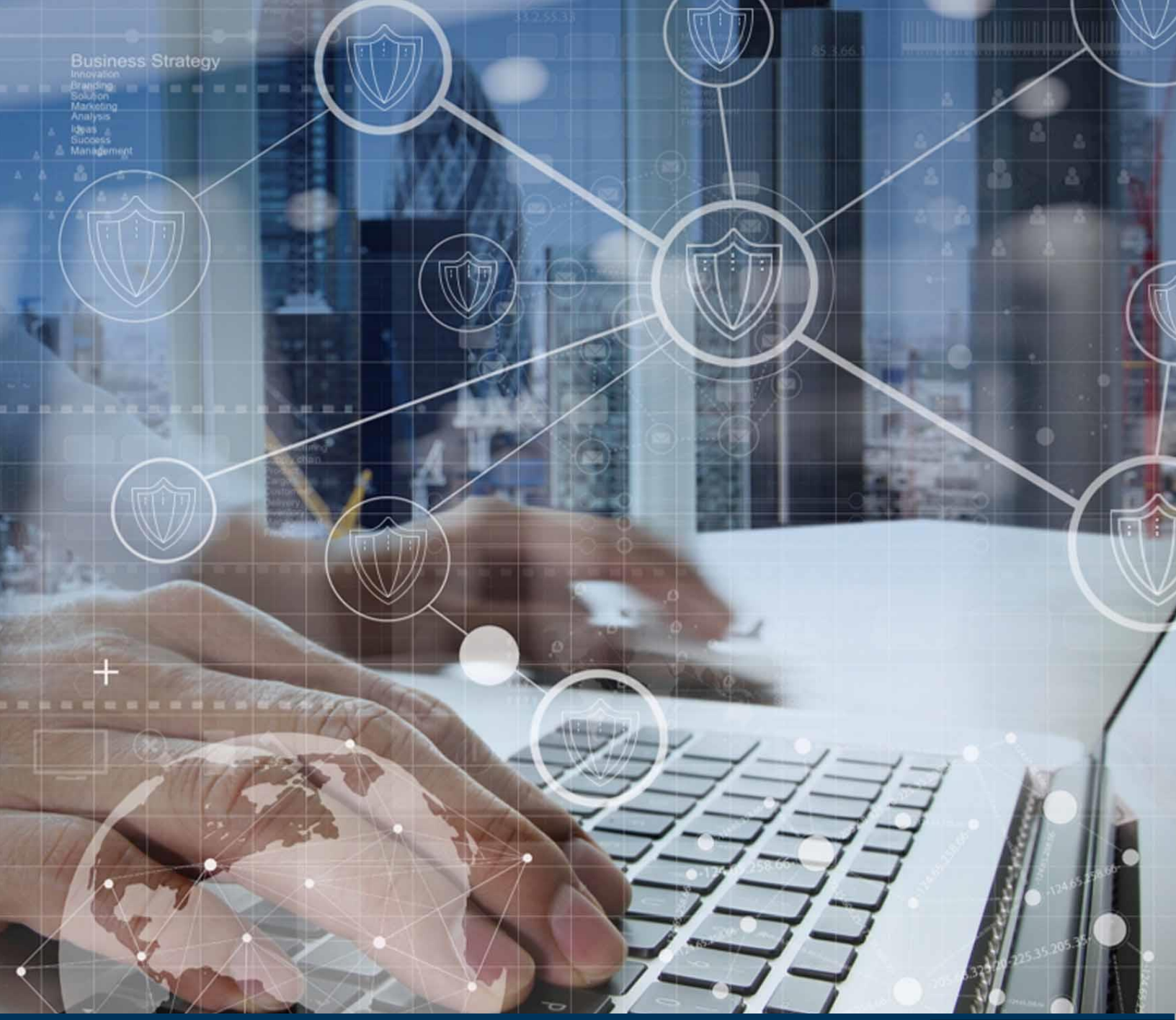


WHITE PAPER

Browsers are the target:

A massive information security challenge

ERICOM

Browsers are the target:

A massive information security challenge

Table of Contents

Almost all successful attacks originate from the public internet, and browser-based attacks are the leading source of attacks on users. Information security architects can't stop attacks, but can contain damage by isolating end user internet browsing sessions from enterprise endpoints and networks[1].

Neil MacDonald – VP Distinguished Analyst – Gartner

Introduction

It's a fact of life that in large groups, someone is invariably going to feel left out. They often ask rhetorically: why am I always the last to know something? When it comes to today's Internet and network security threats and vulnerabilities, far too many CIOs, CTOs, and CISOs are often kept in the dark, and are last to know what is going on within their corporate network.

When it comes to corporate networks, it's a dangerous situation when IT support teams don't know what information security issues are occurring within their end users' browsers. Over time, browsers become a target of vulnerable plugins, malware, ransomware and other types of risky software. Add to the matrix end users who are often overly click-happy, along with an environment where browsers are not regularly updated and patched, and you have yourself a perfect information security storm. All these factors add far too many threat vectors into the already dangerous browser environment.

The truth is that it's actually very easy to make all of those problems go away. For starters – ban the use of browsers. This is the moment where readers should raise an eyebrow. Indeed, this would solve the problem, but it's obviously neither practical nor feasible anymore.

So, how can enterprises achieve security, scalability, operability, and a high degree of transparency in a complex network environment? It's called Browser Isolation.

[1] Gartner, It's Time to Isolate Your Users From the Internet Cesspool With Remote Browsing, 30 September 2016

Think about it. If you could simply move security measures from the local user device to a remote, isolated browser—similar to what a hospital does when a patient is diagnosed with a highly infectious disease—that could be a game-changer from a security perspective. In a hospital, isolation precautions help stave off the spread of germs from one person to others. The goal is to protect patients, families, visitors, and healthcare staff by preventing germs from spreading within a healthcare setting. When a similar approach is taken in corporate IT, it protects the network, devices, and users from a different type of infection—in the form of malware, ransomware, viruses, and other cyber threats that place an enterprise at risk.

Browser insecurity

Many security breaches, incidents, and phishing attacks can be traced back to browser-based vulnerabilities that have been exploited. It comes down to this: enterprise security will be greatly improved if you can secure the browser. Browser vulnerabilities are an inevitability. Consider that as of this writing, Mozilla is shipping version 54 of Firefox and Google Chrome version 59. Microsoft is at Internet Explorer 11; let that sink in. It's not that the version numbers are so high; it's the never-ending struggle of Patch Tuesday, and then dealing with the fallout on Exploit Wednesday.

CIOs and CISOs also must contend with zero-day vulnerabilities. At a high-level, targeted attacks from adversaries and governments with sophisticated levels of technical knowledge place enterprises at significant risk, since zero-day attacks can often bypass existing security hardware and software tools. This is especially true for those tools that rely on identifying known threat signatures to detect and respond to attacks.

The browser is a particularly sweet target for attackers with zero-day malware (and in the era of The Shadow Brokers, the size of that community has grown exponentially), since almost every desktop computer has at least one browser installed. When end users visit a rogue website, as they often do, malware can exploit vulnerabilities in these browsers. External threats such as zero-day attacks and APTs (Advanced Persistent Threats) take advantage of internal vulnerabilities to compromise systems, including operating systems and networks.

But even meticulously patching the browser is just the beginning. There is so much malware on the web, it's a given that infections are but a click away. Even if 99.8% of the devices in an

enterprise are secured, all it takes is one malware attack on a single device to spread mayhem throughout the rest of the organization.

That makes web browsing one of the biggest security risks in an organization. But at the same time, it's required for business as usual.

The May 2017 WannaCry outbreak and other ransomware attacks clearly demonstrate how difficult it is to deal with this menace. WannaCry targeted older versions of the Windows operating system. Evolved versions of the WannaCry ransomware may also contain a payload dropper that can be used to deliver additional viruses to the infected host. While antivirus vendors are doing a better job of identifying ransomware, ransomware creators are also becoming much more inventive. This makes it harder for antivirus tools to fully identify the many ransomware variants in real-time.

WannaCry may also introduce various browser hijackers or other extensions to the browser, which can be used to harvest stored account credentials, cookies, and web search history. While the browser was not the primary target of these attacks, it is still a target.

Speaking of browser hijackers, these are yet another instance in which malicious browser extensions not only change the settings of the installed browser, but also engage in other dangerous actions — including retrieval of sensitive information such as stored account credentials, cookies, and web search history.

There are a number of other serious browser issues that plague enterprises. Perhaps the most problematic in this context is that Windows[2] lacks a mechanism for process isolation. This means that there is no way to segregate the browser from critical system processes. In other words, a security issue in the browser can place the entire operating system at risk.

To demonstrate the issue, and building on the analogy from earlier in this white paper, modern hospitals do a good job of isolating highly contagious patients, which is why they can have infants and infectious patients in the same building. But imagine if they put vulnerable newborns and contagious patients in the same unit. No one would tolerate that. But the same thing occurs in both the operating system and browsers, and it's tolerated every day.

[2] Windows certainly isn't the only operating system in use. But this white paper focuses on Windows, given its dominance in the consumer market.

Browser isolation — a better and more secure browsing experience

This paper opened with an observation from a Gartner report, appropriately titled *It's Time to Isolate Your Users From the Internet Cesspool With Remote Browsing*. One does not have to be a distinguished analyst to realize that, unless the browsing experience is cleaned up, enterprises are at risk for a myriad of security issues.

Browser isolation means many things to different people. Gartner terms it *remote browsing*. They note that this approach reduces the impact of browser-based attacks by isolating the act of browsing from the user device, as well as the rest of the enterprise network and systems. Browser isolation works using the same method as a hospital putting an infectious patient in isolation, away from the rest of the healthy population.

As long as contagion persists, family and friends can interact with infectious patients via windows and speakers, while safeguarded from dangerous germs. When the patient is cured, he's released, free of infection and ready to go. His isolation chamber is quickly returned to a pristine and germ-free condition, ready for the next patient: Germ-ridden items are disposed of and surfaces scrubbed, with dangerous agents eradicated before they can possibly escape.

Similarly, isolating browsing makes risk-laden sessions accessible to users as a safe visual stream, free of all malware. When relevant, items for download are sanitized fully as they're delivered. And once the need for isolation is over, unlike costly medical equipment, remote isolated browsers are simply destroyed, along with all infectious malware generated during the session, and a new one created for the next browsing session..

The ROI and ROSI (return on security investment) of browser isolation is compelling. Since most attacks originate from the Internet, the mere act of shifting the browsing process off the endpoint and into a safe zone reduces the attack surface. Gartner estimates that firms that isolate browsing will see a *70% reduction in attacks* that compromise end user systems.

While browser isolation is effective, it can never guarantee 100% security. Aside from the proverbial death and taxes, nothing is certain in this world. But what browser isolation can indeed provide is a method to significantly reduce the impact of a malware outbreak and minimize the risk of such an outbreak traversing throughout the enterprise network. Pragmatic firms know that attacks are inevitable. The differentiator is how well a firm can minimize the attack surface and aftermath of the attack. That is why isolation and containment are so important, as they limit the ability of an adversary to wreak havoc.

By adding that layer of isolation, enterprises add a barrier between the endpoint and the insecure frontier of the Internet. The user has the same browser experience, but the risks of attack and malicious infections are significantly minimized.

In infectious disease practices, the goal is to isolate the infection so it will stop spreading. The same holds true for computer viruses — isolate them and then eliminate them. When malicious software is isolated, it can't harm the enterprise. Using the same strategy, when a compromised browser operates in an isolated environment, it also can't do damage to the enterprise. This secure environment isolates the end user browsing session, which makes for a safe computing environment.

The security and technology benefits of browser isolation are many. A few of the more compelling ones include:

- *Minimizes the attack surface* – While web-based attacks on users can't be completely eliminated by having browsers isolated and secured, the attack surface is significantly reduced.

- *Simplifies effective management* – Not every firm has a centralized update server to ensure that browser updates are rolled out across the organization. Browser isolation means that you no longer have to worry about what version of Firefox, IE or Chrome each employee is using. Just update once and the job is done.

- *Promotes defense-in-depth* – This is an information security concept in which multiple layers of security controls are placed throughout the enterprise. It provides redundancy in the event that a security control fails or a vulnerability is exploited, such that there's

no single point of failure that exposes the network to a broad scale attack. Isolation is an additional layer on the information security tool belt.

- *Plays nicely with other solutions* – Browser isolation complements existing core security solutions such as secure web gateways (SWG), firewalls, intrusion detection (IDS), data loss prevention (DLP), and file integrity monitoring (FIM). Further, remote isolation augments existing classification measures.

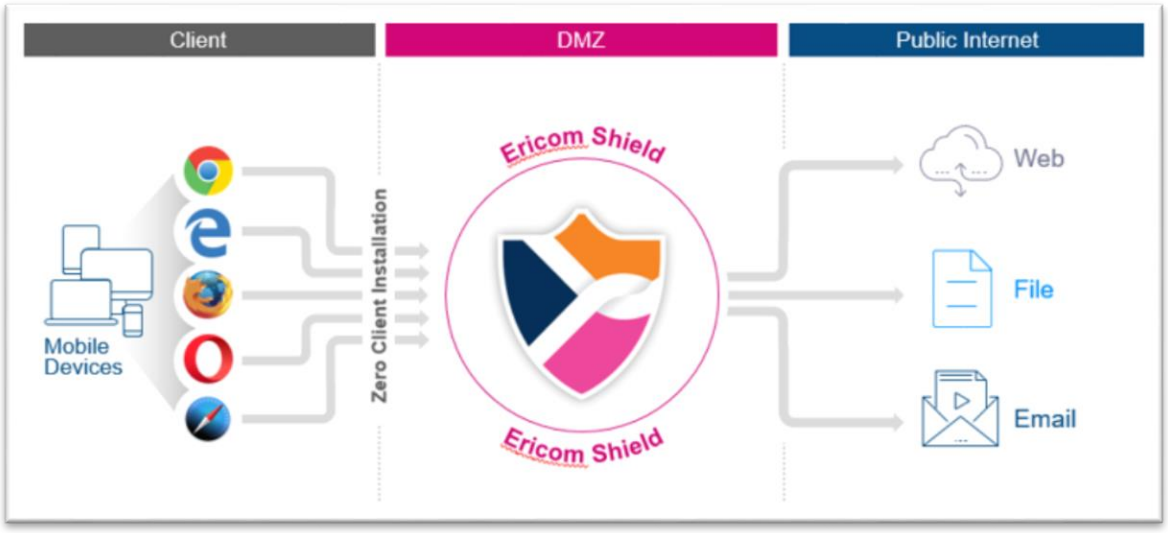
- *Helps reduce support costs* – Browser isolation reduces the variability between different employee browsing setups. Often the most vexing and time-consuming part of a technical support call is understanding what is going with the end user's browser configuration and setup. If that element can be eliminated, support calls will be shorter, costs will be slashed, and productivity can increase — which adds up to a compelling value proposition.

- *Helps reduce cyber-insurance costs* – Firms that are able to show that they have an effective and formal information security program are often able to negotiate more favorable rates from their cyber-insurance carriers.

Introducing Ericom Shield™ for Secure Browsing

Ericom Shield for Secure Browsing is an enterprise-grade security solution that remotely isolates web traffic. Ericom Shield is a clientless solution that can easily be deployed in the largest of enterprises with significant scalability.

The beauty of Ericom Shield is that it enhances security without degrading the end user browsing experience. Its efficient container-based architecture spins up a brand new virtual container for every browser tab users open. Moreover, each web session is rendered remotely in a contained virtual environment, while safely delivering a visual stream of interactive web content in real time, for a seamless, native end user browsing experience.



Finally, at the end of each session, the remote container is discharged, preventing attack persistence and blocking drive-by downloads, phishing attempts, and other malware from ever reaching your users or your network.

Ericom Shield provides a number of compelling benefits:

- *Threat mitigation* – CISOs can stop worrying that browsers can easily be used as a point of entry for ransomware and other malicious attacks. By isolating and blocking threats before they reach the endpoint, security incidents will decrease and information security staff can spend their time being more proactive, as opposed to responding reactively to the never-ending wave of new malware outbreaks.
- *Document sanitization* – Ericom Shield helps eliminate the risks from weaponized documents (e.g., *.pdf*, *.doc*, *.xls*, and *.ppt*). First, the file is downloaded to the container being used for that browsing session, where it is examined and sanitized. This provides protection against known and unknown threats by combining security functions such as data sanitization, vulnerability assessment, and multi-scanning; all of which adds up to a security force to be reckoned with. Moreover, Ericom utilizes both Content Disarm and Reconstruction (CDR) and file type conversion for document sanitization. While browsing, file downloads are sanitized in the background without impacting user experience or file functionality.

- *Increased productivity* – IT staff can anticipate a significant decrease in the number of technical support calls dealing with pesky browser issues. By utilizing Ericom Shield as a master "browser in the sky" to which all user browsers are subservient, browser patch management is now consolidated around the proxy. Meanwhile, all content rendering and sanitization happens far away from vulnerable endpoints—undetectable to end users. This is not a trivial point, as one of the reasons for IT and support staff burnout is the need to work on a diverse set of tasks, with frequent context switching.

- *Plugin exploit prevention* – Hosting risky plugins such as Flash and Java on enterprise endpoints presents many challenges for IT organizations, but employees rely on these plugins to run a number of internal legacy apps required for their daily work. These browser applications are popular targets of zero-day attacks, and create significant IT overhead because of their constant need for security updates and patches. By isolating potentially harmful plugins such as Java and Flash in the Ericom Shield safe zone, these plugins can only operate in a contained environment, far away from endpoints. As a result, admins can eliminate Flash and Java installations on endpoint browsers, yet still permit access to Java and Flash content—without the risk of malware.

- *Policy compliance –* Whether in the form of JavaScript, HTML, or Flash components—or file downloads—all risky content encountered during the course of employee browsing is subjected to any existing security policies that define Acceptable Use for your organization (e.g., blacklisted sites or content). Any "undefined" content is downloaded and executed within a dedicated secure container that serves as a barrier between end users and the internet. By isolating all browser tabs in a disposable virtual environment, enterprises are protected from known and unknown threats, as all threats are contained—no detection necessary.

- *Vendor agnostic flexibility and interoperability* – Ericom Shield performs its function irrespective of the underlying browser, hardware, or operating systems. It supports any browser, any operating system, and any device. That's true interoperability.

- *Exceptional user experience* – The user experience remains completely intact. It's seamless and native – users simply click on their chosen browser icon and enjoy the same smooth browsing experience.

Summary

In conclusion, browser isolation is a compelling security solution and is part of a growing trend of non-signature-based anti-malware security alternatives. It isn't the only solution but, like a good camping knife, browser isolation should be one of the many information security tools on an enterprise's Swiss Army knife of protection.

About Ericom

Ericom Software is a global leader in securely connecting the unified workspace. Ericom empowers today's connected workforce and the IT organizations that support them by securing and optimizing desktop, application, and web content delivery to any device, anywhere. Founded in 1993, Ericom provides enterprise-grade secure remote access, desktop virtualization (VDI), and web security solutions to a global customer base of more than 30,000 midsize to Fortune 500 organizations. With a focus on application delivery, cloud enablement, and secure browsing, Ericom advances secure connectivity—providing end users with a superior work experience and optimizing enterprise productivity. With over 8 million end users, Ericom has offices in the United States, United Kingdom and EMEA and an extensive network of distributors and partners throughout North America, Europe, APAC, and Africa.