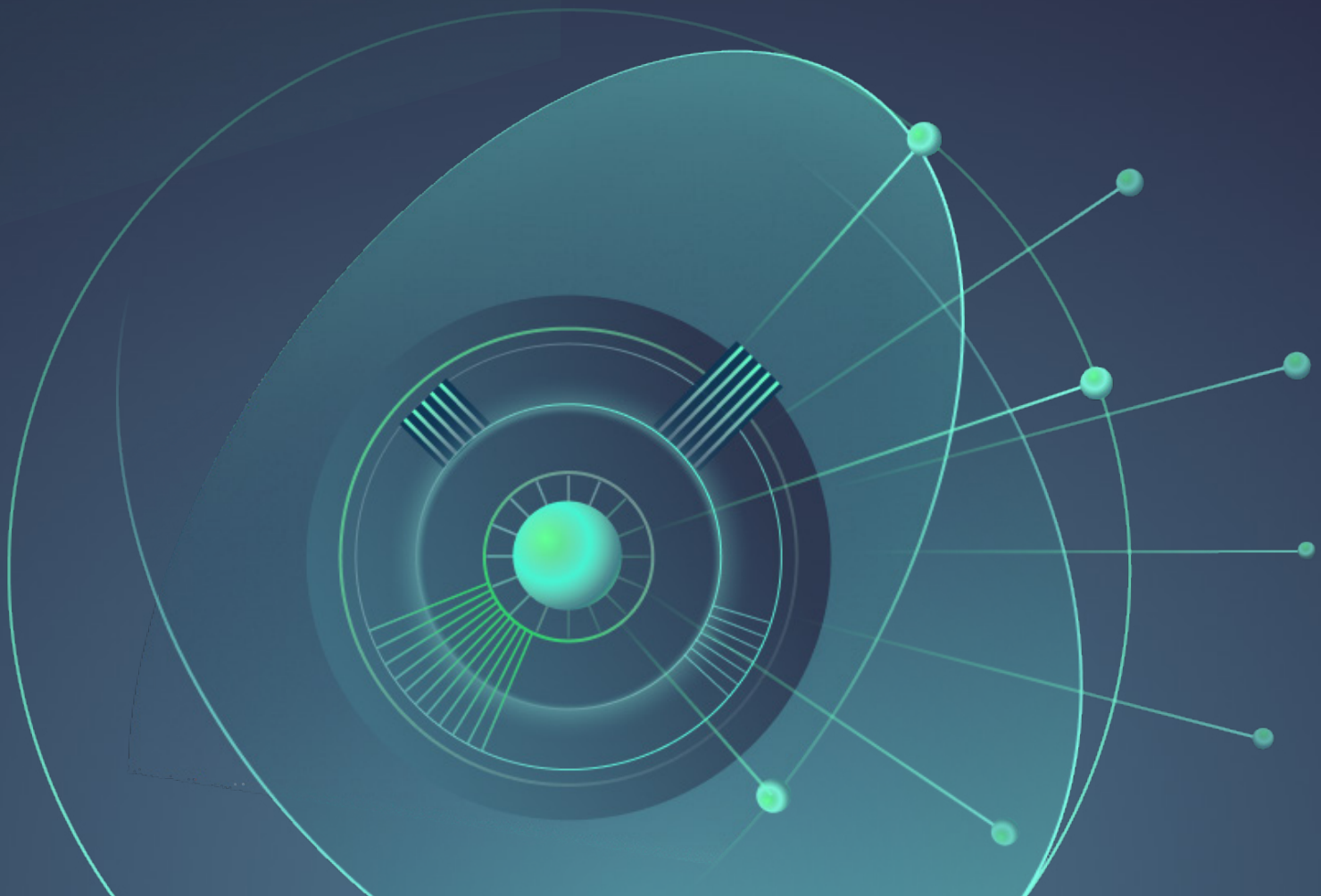
GARRISON

Partial vs Full Web Isolation: Which is right for your enterprise?

Everything you need to know about choosing the best Web Isolation solution to protect your users as they browse the web



If you're one of the growing number of Chief Information Security Officers considering Web Isolation to protect your organization from threats like ransomware and phishing, you're far from alone. But the technology you choose can have implications for security, usability, management overheads, and cost.

It's easy to see why Web Isolation (or Remote Browser Isolation) is such a critical technology. Threats on public web pages are growing and, while firewalls, proxies, user training, web filters, and other tools can help, there is always still a risk that malicious code can make its way onto your endpoints. This guide explores everything you need to know about choosing the best Web Isolation solution to protect your users as they browse the web.

Contents

What is Web Isolation?

Web Isolation (or Remote Browser Isolation) solutions protect users from ransomware, phishing and other web-based threats while they browse the web or click links in emails. It's often used to secure vulnerable or high-risk users, such as senior management, system administrators, or anyone whose job might involve visiting untrusted sites.

Web Isolation solutions effectively remove the browser from the user's device, isolating that user from any risks on the web. Different solutions then use different approaches to relay the browsing session back to the user.

Applied correctly, Web Isolation can potentially remove a whole class of cyber threat – which is why so many organizations are exploring it, whether for high-risk users and sites or across the enterprise. However, not all web and Remote Browser Isolation tools use the same techniques and technologies.

Full isolation technologies use pixel-pushing techniques to offer robust security and high levels of compatibility. Partial isolation through transcoding uses different isolation techniques that traditionally offer lower costs and bandwidth requirements.

Now, new hardware-based pixel-pushing like Garrison ULTRA® allows full isolation solutions to offer a powerful mix of security and usability alongside lower costs and management overheads.

This ebook explores the differences between these competing Web Isolation technologies and gives you the information you need to decide which is the best fit for your organization.

Why are organizations adopting Web Isolation?

Web browsing poses a significant risk to any security-conscious enterprise. And as phishing scams and ransomware become increasingly sophisticated, the threat to your users only grows.

For instance, Verizon's latest Data Breach Investigations Report found that 36% of cyber security breaches involve phishing attacks; 11% more than the previous year[1]. And today, Google Safe Browsing lists just under 2.1 million websites as dangerous[2]. Crucially, Google's list only includes the dangerous websites we know about. The unknown threats could be far greater in number.

Protecting users from the growing ranks of malicious pages is notoriously difficult, as user behavior always includes elements of unpredictable human error.

There are only a handful of ways to *truly* secure a user that browses the public internet. You can use a carousel of separate sacrificial devices (and deal with the costs and administrative burden of constantly replacing malware-infested hardware). Alternatively, you can adopt a Web Isolation solution. Any other method, whether it be firewalls, secure web gateways, or web filter lists, still involves your users directly accessing web pages with their devices – which could present a risk.

Web Isolation avoids these issues entirely by ensuring your users' endpoints never connect to the web page at all. Instead, a remote machine accesses web pages on your users' behalf and delivers a separate, clean version of the web page.

[1] https://www.verizon.com/business/en-gb/resources/reports/dbir/
[2]https://transparencyreport.google.com/safe-browsing/overview?hl=en_GB&unsafe=dataset:1;series:malwareDetected,phishingDetected;start:1148194800000;end:1612080000000&lu=unsafe

Full or partial isolation: similar names, very different results

There are two general schools of thought around how to isolate users' web browsing:

Partial Web Isolation strips the website code down to a smaller subset of information to remove malicious code or other parts of a website that could be compromised. That data is then reconstructed to better resemble the original website before being sent to the user. This type of process is enabled by transcoding technologies such as DOM remodelling and network vector rendering.

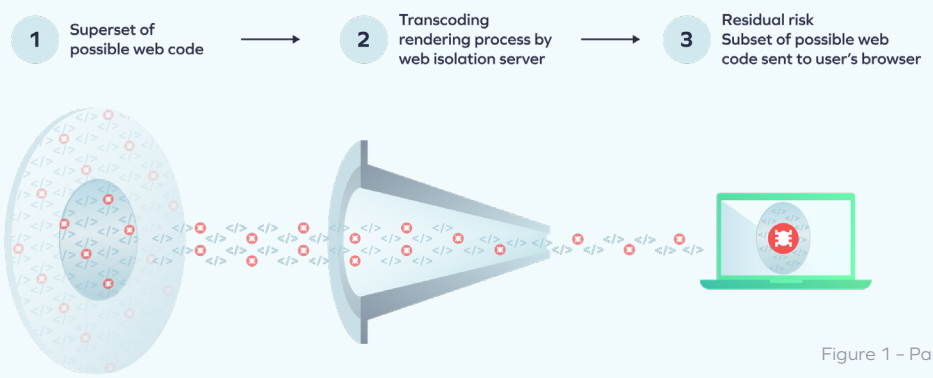


Figure 1 – Partial Web Isolation

Full Web Isolation involves completely separating users from the websites they browse. The Web Isolation solution handles the browsing in its entirety, and delivers the information to users as a video stream that includes none of the website's original code. This is enabled by a technology called pixel-pushing. Traditionally, video streams are encoded and delivered via software, but more modern solutions like Garrison use dedicated hardware to improve the user experience and reduce the cost.

Of course, both approaches have the same end goal: delivering a secure web browsing experience. But they offer different results in terms of the web experience your users receive, your IT management and costs, and – most critically – the level of security you can provide.

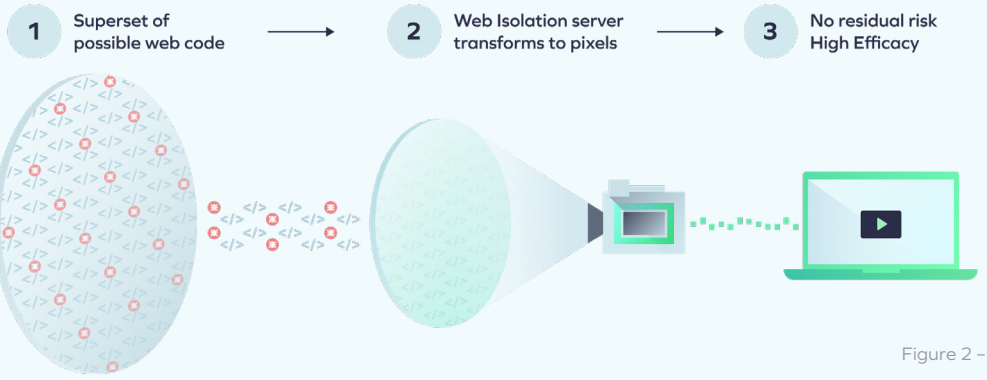


Figure 2 – Full Web Isolation

How do full and partial Web Isolation compare?

There are four main criteria for judging the quality of a security solution:

- Security
- Usability
- Cost-effectiveness
- IT simplicity

How do full and partial Web Isolation compare across these four points?

Security

Nobody considers Web Isolation technology unless they're serious about securing their key users. The first criteria, then, is what protection the solution offers.

Web Isolation solutions work by keeping your user away from potentially harmful website code. So when you're considering how effective they are, the main question is what code – if any – still makes it through to the user's device.

Partial Web Isolation

Because transcoding presents a subset of the original code to users, it's inherently porous. The effectiveness of the security depends on which parts reach the user, and what gets stripped out. You're likely to have questions about these decisions, as they determine the potential for malicious code to slip through the net or for attackers to exploit the site in a new way.

Unfortunately, transcoding is generally a black box: solution providers rarely explain exactly what subset of website code gets used. Security is a matter of trust.

Full Web Isolation

Full isolation technologies like pixel-pushing are inherently non-porous because they prevent users from interacting directly with any website code. They therefore offer far more comprehensive security.

What to look out for:

- Security-conscious enterprises will want to look for the improved protection and transparency that full Web Isolation offers.
- If you're interested in partial isolation solutions, make sure your provider can offer transparency around how their transcoding works and what website code it lets through to users.

Usability

Web Isolation can have two main impacts on usability:

1. **Incompatibility with websites can break the user experience.**
2. **Sending traffic between the client and the Remote Browser Isolation solution can add latency.**

These are both key issues. If your users don't enjoy their browsing experience, they may try to find a way around your Web Isolation solution – creating new security risks.

Partial Web Isolation

In some cases, partial isolation technologies offer acceptable latency levels. But this is situation-specific: in many cases latency can be poor and variable, particularly where technologies use protocols that aren't optimized for real-time communication. Transcoding can also create significant compatibility issues. Some kinds of content – like video playback, for example – may not work at all, or only function with a limited set of features.

And as website and plugin developers constantly update their code, transcoding solution providers must continually update their systems to keep pace. When they fall behind, website features (and even entire websites) can stop working, significantly degrading the user experience.

Finally, for some websites, transcoding solutions can be bandwidth-intensive, meaning they don't work well under poor network conditions. This is particularly noticeable on sites where transcoding tricks don't work well. In these cases, providers have to fall back to pixel-pushing – for which their technology is typically not optimized, unlike true pixel-pushing solutions.

Full Web Isolation

Pixel-pushing technologies avoid compatibility issues as they don't interact with website code – they instead turn the content into a video stream that's sent to the user in real time.

Historically, these streams demanded high bandwidth resulting in significant latency and a degraded browsing experience. This remains true of many software-based pixel-pushing solutions, but new, hardware-based solutions mitigate much of these bandwidth requirements.

This is the approach we take with Garrison's Web Isolation solutions, using specialized hardware to compress and stream video feeds more efficiently to help reduce latency and deliver a seamless browsing experience. And by hosting our solution in the cloud with Garrison ULTRA®, enterprises can get the security and usability benefits of modern pixel-pushing without worrying about deploying and maintaining hardware.

What to look out for:

- Hardware-based pixel-pushing solutions can offer the best balance between latency and compatibility – and the most consistent user experience.
- Many vendors will lock you to pre-set web addresses for their trial period – limiting your ability to test the service in normal browsing conditions. So, when assessing solutions for usability, make sure any demos or trials let you test the service on all websites.
- Ultimately, usability is subjective. The only way to decide which experience your users will enjoy is by testing different solutions. That's why we offer a **free trial** of our hardware-accelerated, cloud-based Garrison ULTRA® solution, so you can see how far pixel-pushing has come. And yes, you can use it with any website you like.

Cost-effectiveness

Cost will always be a vital concern when assessing security solutions. If a Web Isolation solution's upfront or ongoing costs are too high, it could limit your ability to scale. And if licensing models are inflexible, it can affect how you decide to roll out and deploy solutions across different user groups. And between the technology licence itself, the computing resources, and the bandwidth connectivity costs, there can be a lot to consider here.

Partial Web Isolation

Different partial isolation solutions will use different transcoding approaches to protect users, so ongoing costs can vary between vendors. While some partial isolation solutions may keep bandwidth requirements down, many rely on transcoding approaches that can be compute-intensive – leading to significant infrastructure requirements and costs.

Vendors will also approach licensing and scalability differently, so it's worth calculating the potential costs if you decide to roll the service out to more users than you initially planned.

Full Web Isolation

Traditional, software-based pixel-pushing isolation moves significant data volumes, which can be compute and bandwidth-intensive and lead to high operating costs.

But new, hardware-based full isolation solutions significantly reduce those ongoing costs. And cloud solutions running on purpose-built hardware can offer the same benefits without the need to pay for isolation devices upfront.

What to look out for:

- Hardware-based pixel-pushing solutions can offer lower ongoing costs compared to software-based alternatives or partial Web Isolation.
- Where possible, find a vendor that will offer licensing based on concurrent active sessions instead of per user. This means you can be more flexible in how you deploy your solution (for example, you could have a large group using the solution less frequently or a smaller group of intensive users for a similar cost).

IT simplicity

Whether it's through initial deployment requirements, or ongoing manageability and integration issues, you'll want to be sure your Web Isolation tool keeps things simple for your technical teams – and doesn't divert IT resources from other essential work.

Partial Web Isolation

The key issue with transcoding solutions is that many aren't designed to work alongside existing proxies and secure web gateways. And those that claim interoperability with your security tools may still need extensive configuration to ensure everything integrates and works together correctly.

Even when a solution is properly configured and integrated, the low compatibility of transcoding-based solutions can put pressure on IT to answer a greater volume of support tickets, as users encounter websites that don't work.

Full Web Isolation

Unlike transcoding approaches, full Web Isolation doesn't need to modify entire chunks of website code to deliver pages to users. While there's still a risk of incompatibility, there's a much lower chance of new updates to websites breaking the underlying method of Web Isolation. And that means there's less need to constantly install update patches.

And depending on which vendor you use, the upfront deployment requirements can also be easier than with partial isolation solutions.

Hardware-based alternatives vary in IT complexity, but on-premises options require upfront installation and deployment. By comparison, hardware-based solutions hosted in the cloud don't have this need – although, like any solution, some configuration is still required to ensure interoperability with proxies and other security tools.

What to look out for:

- In general, full isolation solutions are more consistently compatible with websites and more readily designed to integrate with other security tools – so they demand less of your IT department.
- Some organizations will want the additional control of deploying their Web Isolation tools on premises.
- Those that don't have such stringent requirements can further reduce IT management burden by opting for a hardware solution hosted in the cloud.
- But think carefully about how your Web Isolation solution will integrate with other security solutions, such as your proxy and secure web gateway.

Full Web Isolation and full security – without the drawbacks

While partial and full Web Isolation technologies each have their pros and cons, there's no doubt that organizations that put security first are likely to consider the latter.

Some firms may be willing to explore a less secure solution if they believe it will offer other usability, cost and management overhead benefits.

However, for most security-conscious enterprises, hardware-accelerated, full isolation – delivered through the cloud – offers the best combination of security, user experience, IT management, and cost.

If you'd like to see for yourself the user experience and security benefits full Web Isolation in the cloud can offer, we'd be happy to give you a free trial of Garrison ULTRA®.

Garrison ULTRA® uses custom hardware hosted in the cloud to offer secure full Web Isolation with low latency, high compatibility with websites, rapid setup, and simple interoperability with your existing proxy and secure web gateway.

BOOK YOUR GARRISON ULTRA® TRIAL TODAY

Security starts with an informed purchase

If you can assess the security, usability, cost-effectiveness and management burden of different Web Isolation technologies, you can make an informed purchasing decision that keeps your users – and your business – safe.

But while these four pillars are crucial elements of any Web Isolation technology, they're just the start of what to consider when selecting a solution provider.

To learn more about the different Web Isolation technologies available, and how to find the right one for your business, speak to one of our Web Isolation experts.

Contact the team via email info@garrison.com

Email info@garrison.com
UK Telephone +44 (0) 203 890 4504
US Telephone +1 (646) 690-8824

www.garrison.com

© Garrison Technology Ltd 2022

CD00000617 - March 2022