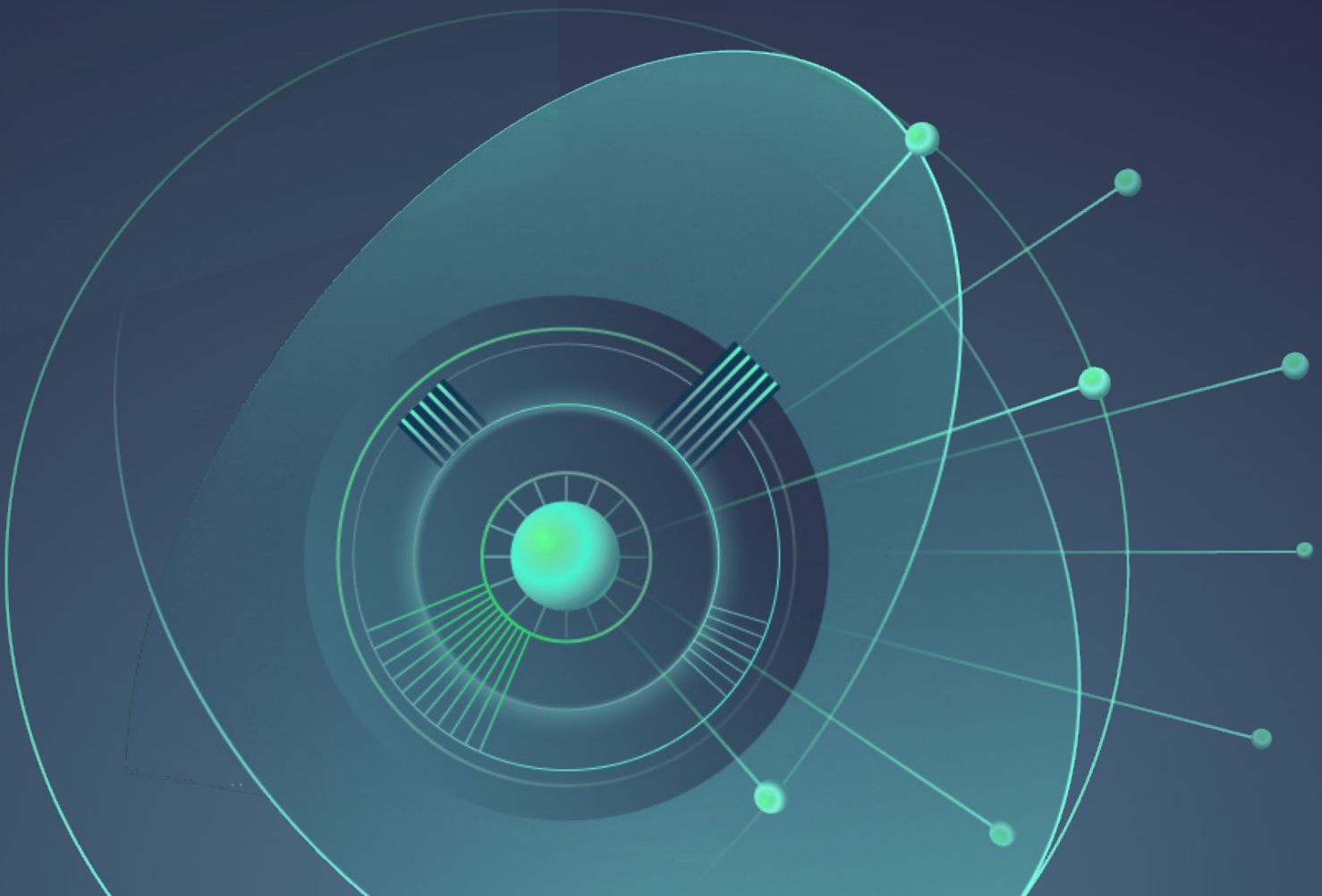




Browser Isolation Buyer's Guide for the Public Sector

What you need to know when selecting an appropriate Browser Isolation solution for Federal, State, and Local Government Agencies



As great power competition in the cyber domain escalates and near-peer actors become more sophisticated in their attacks, it's increasingly critical that Federal, state, local, tribal, and territorial governments and other public sector entities not only protect sensitive data, but also protect their networks from web-based threats that could disrupt services or spread disinformation at critical junctures. In many ways, this is a more daunting task for civilian entities than it is for their defense and intelligence counterparts, as the rigorous segmentation from the Internet that defense and intelligence agencies use to protect their most secure networks is impractical to implement for citizen- and research-focused organizations that need access to the Internet to conduct their day-to-day work.

At the same time, it is increasingly difficult to secure the most common touchpoint for employees and the Internet – the web browser. As it stands, most cybersecurity teams are left with a choice between blocking any site they haven't explicitly evaluated – causing unacceptable degradations in user experience or requiring large teams to review allow-listing requests – or simply allowing all sites that aren't known to be malicious – increasing the risk of drive-by and phishing compromises. Remote browser isolation (RBI) provides a third option: isolating webcode processing for all sites that haven't been explicitly reviewed and trusted outside of organizations' systems, removing the risk of technical compromise while providing employees with the access and information they need to effectively and efficiently serve their citizens.

Contents

What is Browser Isolation?.....	04
Why Is Browser Isolation Important to the Public Sector?	05
Full or Partial Isolation?	06
Browser Isolation as part of SWG or SSE	08
How do Full and Partial Isolation compare?	09
Security	10
Useability	11
Cost-effectiveness	12
Ease of Deployment and Maintenance	12
Browser Isolation Solution Requirements	12
About Garrison Technology	12



What is Browser Isolation?

Browser (web) isolation solutions protect the user by preventing the ingest of malware, preventing the covert exfiltration of data and strongly mitigating other web-based threats (e.g. credential harvesting) associated with needing to access non-trusted or high threat systems/networks, such as the public Internet.

To this end, browser isolation creates a full-stack protocol break between the trusted and untrusted/risky execution environments. It also provides a conversion of all non-trusted Internet content to a known good format for delivery to the endpoint device. Both security features must be verifiable and delivered while maintaining an acceptable level of user experience and without introducing an unacceptable level of maintenance and support burden.

The inherent dynamism and patch-centric maintenance of software solutions, along with the intensive compute resources required to create a full-stack protocol break make it clear that hardware security (hardsec)based technologies are the optimal solution, allowing government agencies to take a stringent

allow list-based approach, removing endpoint code execution privileges for all but corporately-vetted and trusted websites while removing the user issues and administrative overhead normally associated with an allow list-only solution. Garrison ULTRA®, which is based on Garrison's *hardsec* technology hosted in Garrison-leased datacenters, can provide the technology that government needs to secure its critical work while allowing departments and agencies to benefit from the data, capabilities, and innovation associated with free access to Internet resources.

Why Is Why is Browser Isolation Important to the Public Sector?

Use of the Internet is part of the day-to-day economic and social fabric of American life. Without the ability to access the Internet, civil servants would not be able to keep up with critical developments in news, research, and procurement. They would also be less capable of interacting with the citizens they serve.

But with the benefits of Internet access come serious risks. Most modern browsers – users' key interaction points with the Internet – are built on dozens of open-source libraries, all of which are subject to compromise. In 2023 alone, eight zero-days, many of which allowed remote code execution, were disclosed in the Chromium stack (the backbone of more than 70% of all browsers). Because browsers also have relatively high levels of privilege on their endpoints, public sector organizations should buy down the risk posed by browsers by using RBI to:


- **Render Unevaluated Sites Safe:** While cybersecurity teams may be responsible for risk evaluations and have contractual protections in place for a few dozen business-critical webapps, timeliness and resource constraints prohibit them from evaluating every site an employee might visit. Unlike URL categorization, risk scoring algorithms, and EDR/XDR products, all of which depend on after-the-fact indicators of compromise to a website, endpoint, or system, the most robust RBI solutions

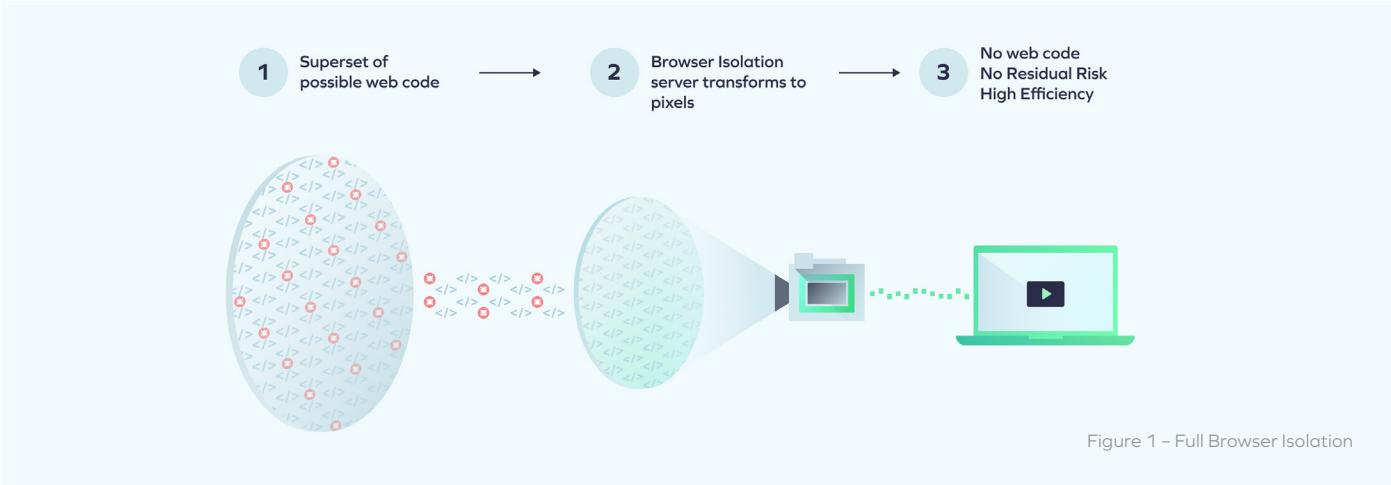
push code processing off of an organization's systems completely, removing the risk of technical exploitation.


- **Reduce the Risk from Phishing Attacks:** Civil servants must review hundreds of emails from citizens, vendors, and professional colleagues every day. As phishing attacks are informed by automated AI reconnaissance and generated by generative AI algorithms, they will become harder and harder to detect. Phishing simulations can only do so much to counter believable emails, and expecting employees to try to discern the difference between (for example) a capital I and lowercase l before clicking on links in their email is taxing, inefficient, and unreasonable. RBI completely removes technical risk from malicious webcode processing and provides real-time user awareness to let them know a site may be trying to harvest their credentials or other sensitive data.

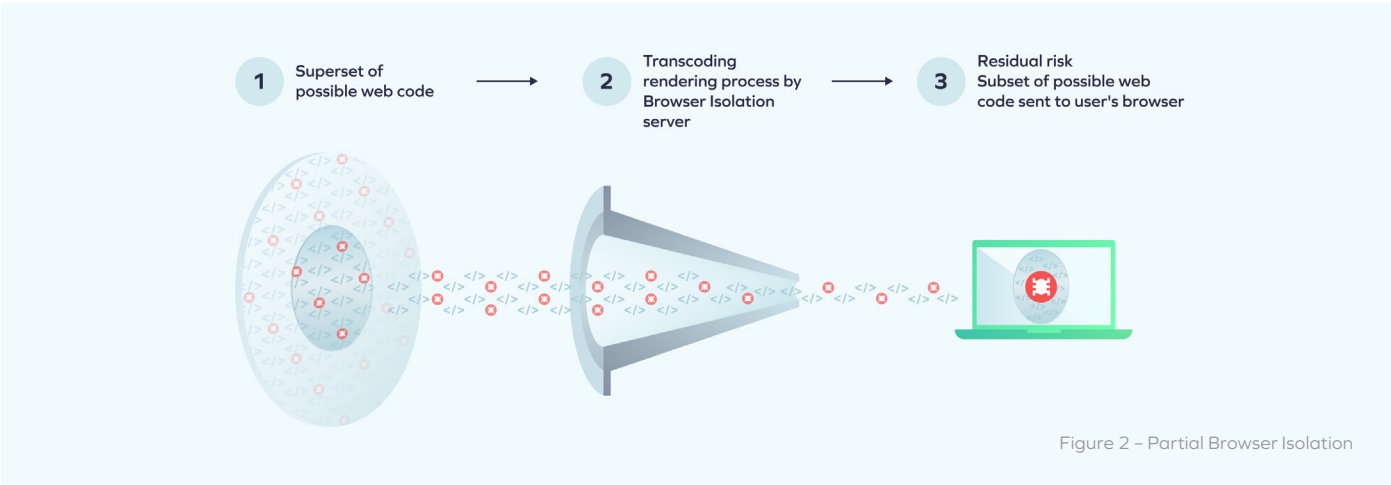
Full or Partial Isolation?

Two forms of browser isolation exist on the market today:

 **Full isolation**, which adopts a process called 'pixel pushing' to render Internet content into an interactive pixel stream rather than processing code on the user's endpoint and applies this process to all Internet content. In addition to pixel pushing, full isolation requires a separate system processing remote browsing activity to avoid the chance that malicious code escapes the containerization or virtualization solution used to process it.



 **Partial isolation**, which adopts 'DOM remodeling/transcoding' and similar algorithms to transform code into less-risky code that is still processed on the user's endpoint, and applies this process to only the Internet content that the vendor deems risky.



Pixel pushing, the process of converting 100% of all web traffic into nothing more than an interactive video stream, is extremely compute intensive but is the pinnacle of browser isolation solutions as this process ensures that zero web content is delivered to the end point. Some pixel pushing solutions attempt to carry out this process in software, which degrades user experience. Furthermore, because the process itself is governed by software, the software must be tested thoroughly and updated frequently to prevent the process itself from being compromised. Using a hardware-based browser isolation approach can alleviate both these issues.

Partial isolation allows vendors to reduce this compute/processing burden by using a policy-based approach whereby the vendor uses proprietary algorithms to decide what Internet content needs to be converted due to risk and what can be passed straight through to the user's endpoint. Such an approach inherently increases the cyber risk to the endpoint and requires trust not only in the vendor's underlying technology, but also the threat intelligence and detection algorithms they use to determine what content needs to be processed. Full isolation, on the other hand, enforces pixel pushing on all presented content, thereby stopping any processing of potentially malicious code from occurring within the network.

Browser isolation solutions that use dedicated pixel pushing hardware, such as Garrison ULTRA, don't suffer the same user experience challenges and therefore are able to deliver extremely strong and robust full isolation while maintaining a good user experience at scale.

What is a Verifiable Pixel Gap?

"Pixel pushing" converts the entirety of a remote browser session into an interactive stream of known good pixels (and associated audio) that ensures that no actual web code is processed on an endpoint.

A Verifiable Pixel Gap is a particular instantiation of a fixed-function protocol break and a fixed-function content conversion mechanism that implements a pixel-pushing approach to providing secure remote Browser Isolation. To have a gap, the browser isolation platform must have two systems: an untrusted system that connects to the Internet and processes web code, and a trusted system that connects to the user's endpoint.

The use of fixed-function hardware rather than potentially vulnerable code and escapable containerization guarantees the integrity of the pixel-pushing process, and therefore the integrity of the browser isolation solution. Moreover, it is straightforward to verify. Garrison ULTRA is the only browser isolation service on the market today that meets this requirement and provides a browser isolation control.



Browser Isolation as part of SWG or SSE

Sometimes a vendor will include browser isolation as part of a suite of other security tools. Such an approach increases the risk of inappropriate vendor-lock and, because most such isolation products do not take a hardware-based approach, also has the potential to introduce concentrated risk into public sector networks.

The use of a “best of breed” browser isolation technology such as Garrison ULTRA, which readily integrates with any proxy server, SWG, or firewall on the market using basic redirection capabilities and is available as a web app via Chrome, Edge, or Safari, provides a more cost effective and secure approach that will be broadly accessible to departments and agencies.

Using a “best of breed” solution for departments’ and agencies’ connection to the untrusted Internet also mitigates the risk of a homogeneous tech stack. While a single-vendor solution may seem convenient to departments and agencies, enabling access to unevaluated Internet sites for users poses a unique risk.

Using a separate service to secure this access point avoids the risk that an advanced actor could use a platform-based browser isolation software as a foothold to exploit the common framework underlying the broader security solution.

How do Full and Partial Isolation compare?

There are four main criteria for comparison and evaluation of Browser Isolation solutions/services:



Security



Cost-effectiveness



Usability



Ease of integration

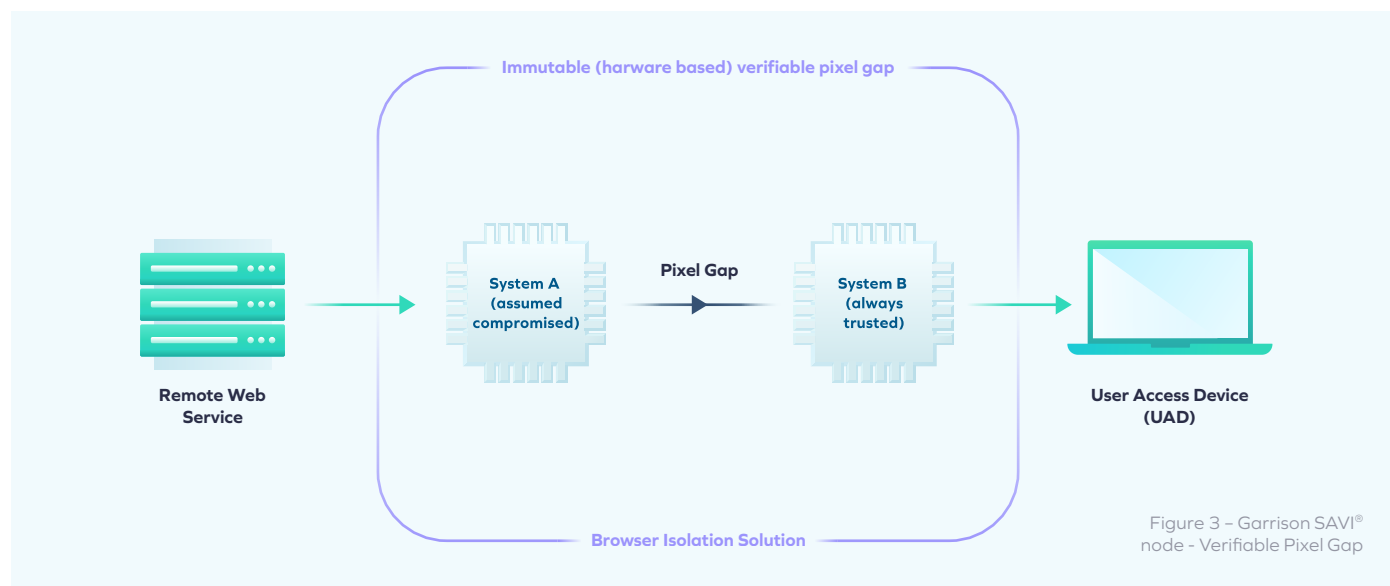


Security

Robust browser isolation is an enterprise cybersecurity control that removes the risk of nation-state web threats hosted on open Internet sites that have not been explicitly evaluated and trusted by your cybersecurity team.

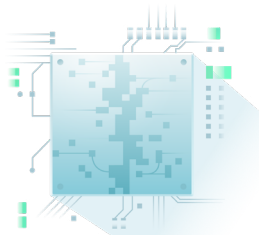
As described above, however, pixel pushing technology and a Verifiable Pixel Gap are the only ways to ensure full isolation from an APT-level adversary, who could bypass DOM remodeling/transcoding, subvert pixel conversion software, or evade threat intelligence or detection-based filtering approaches.

For full browser isolation to be able to include a Verifiable Pixel Gap, the product internal architecture must include **two segregated systems between which establish the conversion and verification aspects of the pixel stream.**



For the Verifiable Pixel Gap to meet the fixed-function protocol break and fixed-function content conversion requirements it is necessary for the product internal architecture to be based on hardware. The use of hardware to implement robust security enforcing functions is described as *hardsec*.

Instead of CPUs, hardsec uses lower-complexity (non-Turing-machine) digital logic to implement security, avoiding the inherent vulnerability that lies in the flexibility of software. By making use of FPGA silicon, hardsec can deliver security while maintaining flexibility to address real-world cybersecurity problems in a cost-effective manner.



Garrison's hardsec technology, as assessed under LBSA by NSA's NCDSMO, is at the core of the Garrison ULTRA browser isolation service. **More information about hardsec can be found at <http://hardsec.com>**



Enhanced User Risk Awareness

Traditional browser isolation solutions have often aimed to obscure non-trusted browsing sessions from users with the aim of attempting to make the isolated browsing an 'invisible' user experience. However, this approach poses a danger, as when users navigate to sites that are not trusted, they are likely to be unaware that they are now browsing to the 'risky Internet' and therefore may inadvertently enter sensitive information, such as passwords, procurement data, or even CUI data.

For effective browser isolation, it's essential to establish a distinct and noticeable browsing environment for untrusted websites as a human interface control for the flow of CUI. This ensures users receive a subtle yet clear cue, prompting them to be cautious and refrain from entering sensitive information. Garrison ULTRA achieves this using a Chrome, Edge, or Safari pop-up window, creating an easily usable but visually separated browsing environment. This isolated browsing session will soon have enhanced visual cues to continue to alert users to the fact that they are operating in a non-trusted environment.



Usability

Browser isolation can have two main impacts on usability:

- 1 **Incompatibility**
- 2 **Performance/latency**



Partial Isolation

Partial isolation solutions try to maintain acceptable levels of performance and latency by minimizing the use of pixel pushing specifically and remote content processing in general. This obviously comes at the cost of significantly reduced security. This detection-based approach, which causes parts of a web page to be processed and rendered differently depending on the perception of risk as determined by a vendor's proprietary algorithms, also causes issues with overall page compatibility, often perceived by the user as slow, stuttering, or incomplete page loads.



Full Isolation

Full isolation treats all remote content as equally untrusted/risky and therefore fully converts the entire web page to a safe pixel stream in real time, which avoids the page compatibility issues of partial isolation.

Full isolation using hardware for the conversion processing achieves the highest level of security while strongly reducing the additional latency that processing introduces. The use of hardware and *hardsec* technology further reduces the latency introduced into the solution via the use of dedicated hardware for video compression and delivery.



Cost-effectiveness

Typically, commercial cybersecurity solutions license on a one size fits all licensing model. For a browser isolation solution, this would introduce unnecessary cost, as not all users who are licensed will require the concurrent use of the browser isolation service. This is especially true for the diverse workforce of government agencies, where some employees may spend most of the day conducting Internet research, whereas others' Internet activity may be more incidental.

A more cost-effective model to license for a heterogeneous group like a government agency is on a consumption basis, where concurrent sessions, rather than individual users, are licensed. This will allow departments and agencies to purchase only the license capacity needed to service their workforces at the busiest times, rather than on the assumption that all users will be using browser isolation at the same time. The licensing model should also allow for easy expansion of licenses should additional capacity be needed – for example, if additional vendors are onboarded or additional use cases are identified.

Garrison ULTRA can license on either a per-user basis based on different profiles of user activity or a seat-based concurrent users basis. Department and agencies can optimize utilization of the service through the concurrent users model, or can purchase per-user licenses to ensure headroom and enterprise-level scalability.



Ease of Deployment and Maintenance

Public sector cybersecurity teams have multiple priorities each day, many of which are related to time-sensitive response and reporting requirements. Ease of deployment and a low-to-no maintenance approach to preventative technologies like browser isolation is important so ongoing implementation doesn't distract your teams from urgent directives.

Effectively implemented browser isolation also reduces the maintenance load for the individuals responsible for IT and cybersecurity. For instance, having an 'Allow' list of trusted sites and web apps (O365, ServiceNow, Salesforce, etc.) and pushing all other web browsing through a full isolation browser isolation solution can eliminate the need to comb through endpoint detection logs and reduce the volume of website investigations for additional sites to be placed on the allow list.

Being able to rely on the strength of mechanism provided by a hardware-based full isolation solution reduces the need to configure and maintain a complex policy definition and enforcement mechanism to control the flow of component parts of web browse requests and responses based on a 3rd party perception of threat.

ULTRA's hardware-based enforcement is also inherently Secure by Design, and eliminates the need for continuous monitoring and evaluation of a software solution for vulnerabilities and patches -- and, more importantly, the risk that one of your critical security solutions will be the subject of a time-consuming Emergency Directive.

Garrison ULTRA is 100% cloud based and can easily be configured for use with any proxy or similar device (e.g., firewalls, secure web gateways). We will make professional services resources available either in workshops for pilot participations or in 1:1 sessions with customers to ensure that our service is deployed and configured correctly. Garrison can also provide an on-premise solution if desired.



About Garrison Technology

Garrison Technology, founded in 2014, has brought together years of cybersecurity and classified government expertise to create the most robust, hardware-enforced, isolation solutions in existence. In addition to our cloud-hosted ULTRA offering for remote browsing, Garrison also offers appliances for cross-domain and rigorously-enforced operational technology (OT) applications.

Browser Isolation Solution Requirements

Based on the above discussion, we suggest the following Security, Cloud Service, Usability, Cost Effectiveness, and Ease of Deployment and Maintenance requirements for consideration in evaluating remote browser isolation solutions.

Security

SR#	Security Requirement	Response Consideration
S.1	The solution shall implement hardware-based full isolation using hardsec architectural principles	Software-based isolation solutions such as virtualization and containerization are vulnerable to escape attacks and other sophisticated nation-state techniques
S.2	The solution shall implement a Verifiable Pixel Gap	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.3	The solution shall implement the Verifiable Pixel Gap between two physically discrete, segregated systems	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation. A single system Browser Isolation platform lacks a pixel gap and introduces unacceptable trust in a remote browsing system that may be compromised through Internet browsing
S.4	The solution shall not permit any bypass of the verifiable, hardware enforced pixel gap	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.5	The solution shall implement full conversion of all remote content	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.6	The solution shall convert all visual content to a verifiable pixel stream	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.7	The solution shall convert all audio content to a verifiable PCM audio stream	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.8	The security enforcing functions of the solution shall have been subject to assessment by NSA, DOD, or equivalent trusted 3rd party	The vendor must be able to provide supporting documentation from the trusted 3rd party assessor
S.9	The security enforcing functions of the solution shall be shown to respond to evolving threats	The vendor must be able to provide supporting documentation that describes the mechanism and evidence of the ongoing use of that mechanism to address evolving threats
S.10	The solution shall prevent re-use of contaminated sessions/resources between users	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.11	The solution shall prevent MitM attacks between the service and the endpoint	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.12	The solution shall provide remote isolation for file download storage	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.13	The solution shall provide support for secure copy, paste and print from the isolated browser	This must be based on hardsec conversion/transformation of content across the isolation boundary
S.14	The solution shall initiate an isolated browsing session in a clearly separated browsing window	The solution must be able to clearly help a user to identify when they are browsing to untrusted URLs through a distinctly separated browsing window to minimize the risk of user negligence (e.g., susceptibility to phishing attacks)

Cloud Service Requirements

SR#	Service Requirement	Response Consideration
S.15	The browser isolation service should be delivered as a vendor managed cloud service	The vendor must be able to provide this as a cloud service with no on-premises hardware deployment dependency to better scale the scope of large public sector departments and agencies.
S.16	The service shall provide a robust segregated control plane architecture	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.17	The service shall provide robust multi-tenancy separation	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
S.18	The service shall be SOC2 certified	The vendor must be able to provide a valid certificate on demand
S.19	The service shall prevent provider/admin access to tenant/user sessions	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation

Usability

SR#	Usability Requirement	Response Consideration
U.1	The solution shall introduce only an acceptable level of latency	The vendor must be able to demonstrate the impact of latency on the set of required workflows
U.2	The solution shall not introduce unacceptable A/V artefacts	The vendor must be able to demonstrate delivery of at least full HD.
U.3	The solution shall allow the user to normally interact with the isolated environment	The vendor must be able to demonstrate typical user interaction with any isolated web service
U.4	The solution shall provide a consistent user experience with the isolated environment	The vendor must be able to demonstrate a consistent latency, completeness, etc. of rendering for any isolated web service
U.5	The solution shall require minimal or no user training	The vendor must be able to demonstrate the user experience, and, if desired provide suitable user guidance
U.6	The solution shall provide support for basic persistence between sessions	The vendor must be able to demonstrate persistence of history, cookies, bookmarks, auto-complete, and downloads between sessions
U.7	The solution shall provide support for enhanced persistence between sessions	The vendor must be able to demonstrate the persistence of WhatsApp for Web, Facebook, Twitter, etc. login between sessions

Cost Effectiveness

SR#	Cost Effectiveness Requirement	Response Consideration
C.1	The service shall be licensed as a discrete standalone item	The vendor must be able to provide pricing for just the web isolation service
C.2	The service shall provide consumption-based licensing	The vendor must be able to provide licensing related to actual utilization rather than size of user base
C.3	The service shall be able to scale on demand	The vendor must be able to provide verification of the scaling mechanism through inspection of architecture, design and implementation documentation

Ease of Deployment and Maintenance

SR#	Integration Requirement	Response Consideration
I.1	The service shall have an agentless deployment architecture	The vendor must be able to demonstrate support without any endpoint code deployment (no agent, special browser or browser plug-in needed)
I.2	The service shall be complete and independent of other components	The vendor must be able to demonstrate that no additional security solution components are required for it to function (e.g., no SWG, SASE, SSE, EDR, XDR, or email security)
I.3	The service shall be able to integrate with existing web service allow list policy enforcement points (e.g., proxy)	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
I.4	The service shall permit modification of default web service allow list policies	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
I.5	The service shall always invoke full isolation (100% conversion to pixels and PCM audio) for all websites visited	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
I.6	The service shall be able to integrate with existing identity-based policy enforcement points (e.g., proxy)	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
I.7	The service shall support the use of common browsers	The vendor must be able to demonstrate support for at least Chrome, Safari, and Edge
I.8	The service shall be able to integrate with an email gateway for file transfer	The vendor must be able to demonstrate support for at least SMTP email gateways
I.9	The service shall not permit the relaxation of Security Enforcing Functions through policy	The vendor must be able to provide verification through inspection of architecture, design and implementation documentation
I.10	The service shall support web site/service technology changes with minimal or no impact	The vendor must be able to provide verification of independence from web site/service technology evolution through inspection of architecture, design and implementation documentation



Email info@garrison.com

US Telephone +1 (646) 690-8824

UK Telephone +44 (0) 203 890 4504

16 OF 16

www.garrison.com