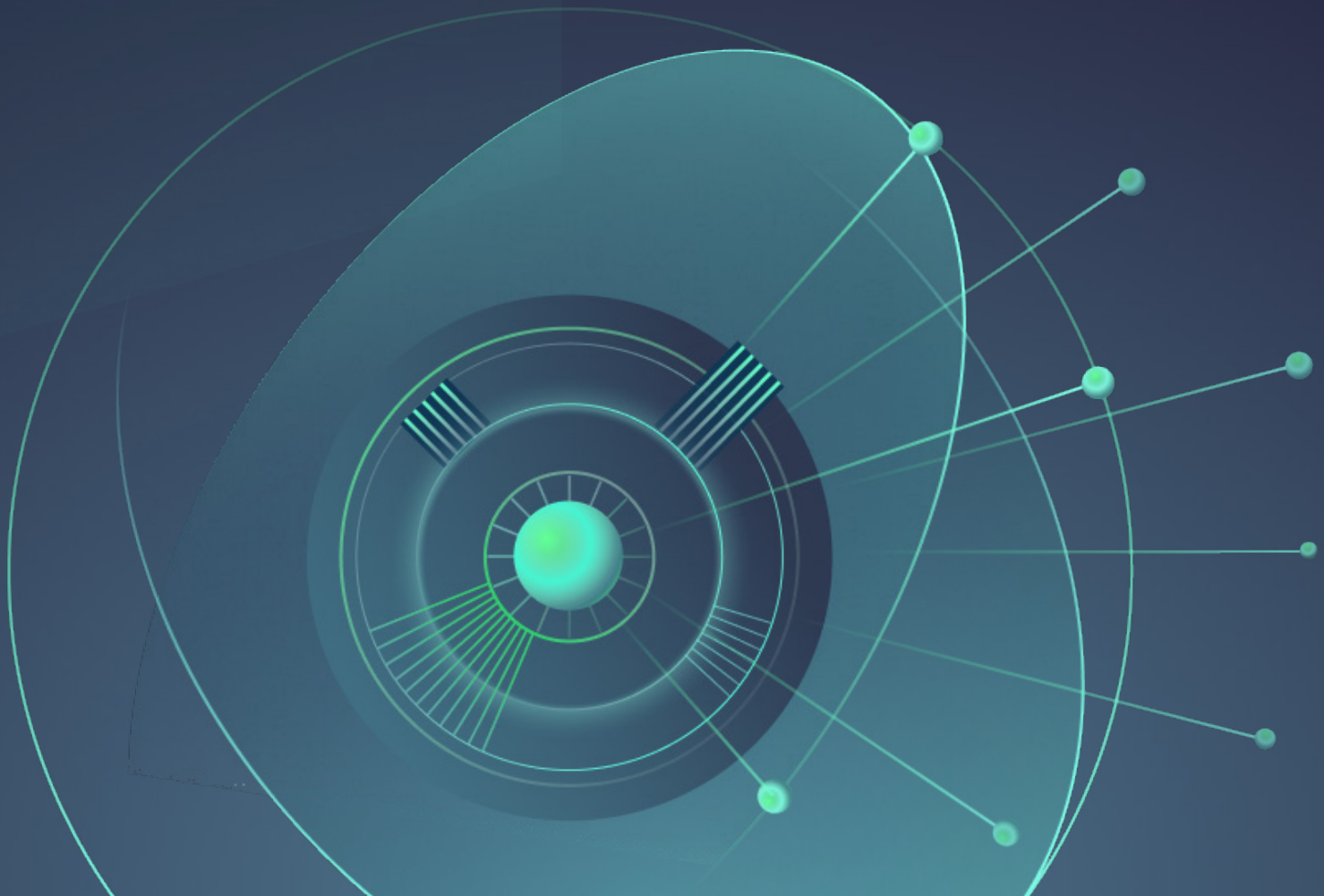
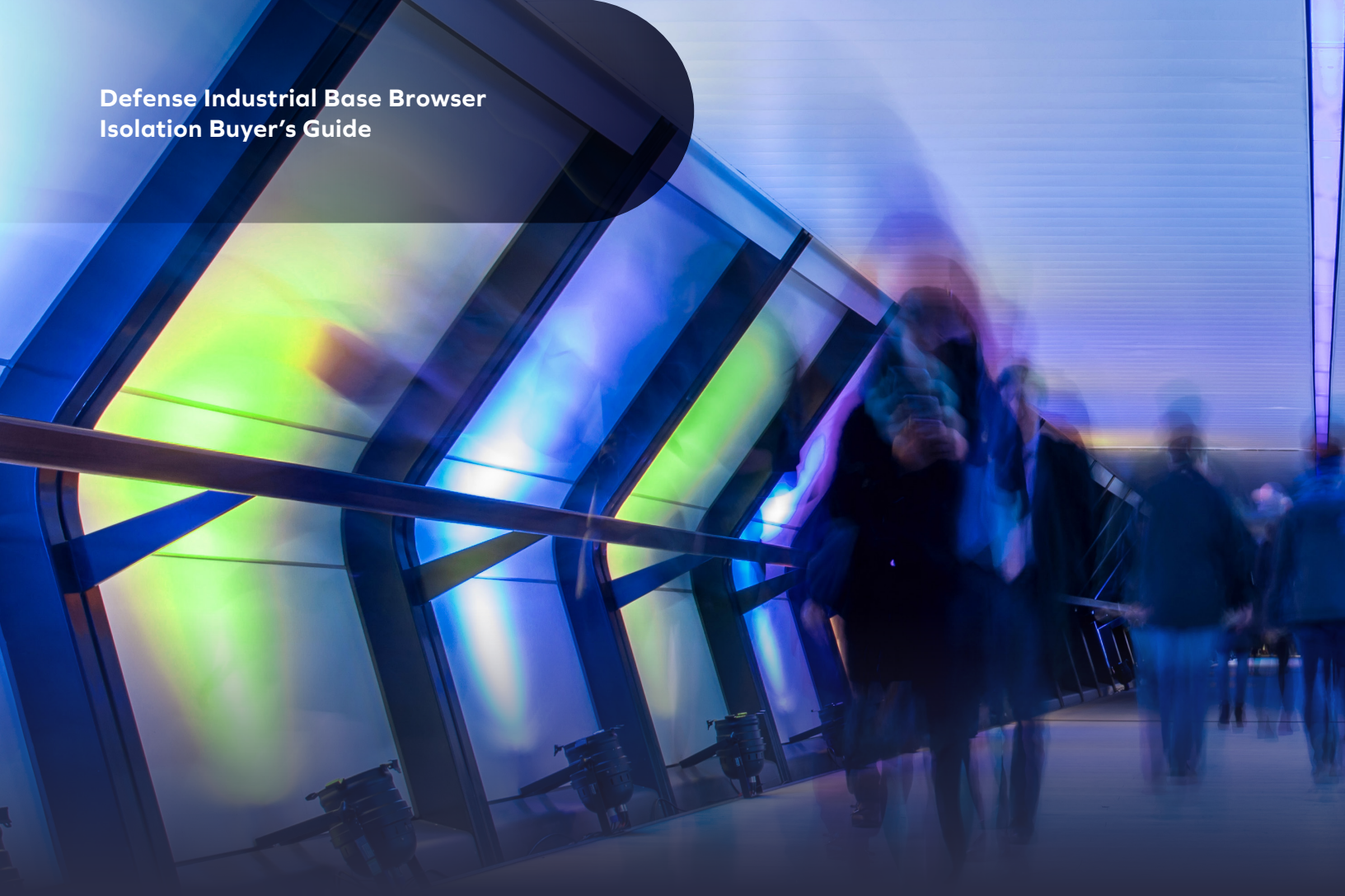
GARRISON

Defense Industrial Base Browser Isolation Buyer's Guide

What you need to know when selecting an appropriate Browser Isolation solution for Defense Industrial Base (DIB) vendors





As great power competition in the cyber domain escalates along with the technical sophistication of our near-peer actors, protecting not only the users, data, and networks of the USG itself, but also of the Defense Industrial Base that supports it is increasingly important – particularly as adversaries like China have specifically identified the DIB and critical infrastructure as potential targets for cyber operations. Legacy software-based solutions have been shown to provide a measure of mitigation against some threats, but the current increasing level of compromise across all industry sectors clearly shows that those mitigations are not keeping pace with cyber criminals, let alone APT actors.

In reaction to digital supply chain threats as demonstrated by Solar Winds and log4shell as well as the value of production and intellectual property of physical supply chain providers, the USG wisely has advanced the Cybersecurity Maturity Model Certification (CMMC) 2.0 into the federal rulemaking process. As small and medium businesses who contract with the USG attempt to meet a new technical security standard, one of the most important points of potential vulnerability common to all vendors will be their interactions with the public Internet via the web browsers on their everyday use computers. Including a strong Browser Isolation platform as a shared service will significantly increase DIB contractors' security and ability to meet the controls set forth in CMMC 2.0 levels 2 and 3.

GARRISON

Contents

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 DIB organizations 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 the DIB needs to secure its critical work while allowing the DIB to benefit from the data, capabilities, and innovation associated with free access to Internet resources.

Why Is Browser Isolation Important to the DIB?

Use of the Internet is part of the day-to-day economic and social fabric of American life and, as such, every member of the DIB, from AI/ML companies developing IMINT algorithms to metalworkers fashioning parts for drones, are exposed to Internet-based threats of which they themselves may not be fully aware.

Less technically-oriented companies, may have neither the time nor capability to understand these threats – nor should they be expected to. Browser Isolation, when implemented correctly, eliminates much of the risk from Internet use while providing a control that answers many of the NIST 800-171 requirements outlined in CMMC 2.0 levels 2 and 3. Some key benefits of Browser Isolation, as grouped by themes within CMMC 2.0, are outlined below:

- **Protection of CUI:** Because Browser Isolation solutions remove a user's ability to transfer files and data from the local filesystem to non-trusted Internet sites, they significantly decrease the risk that CUI will be inadvertently uploaded or maliciously exfiltrated to an unauthorized site. (CMMC 2.0 level 2 requirement 3.1.3, "Control the flow of CUI in accordance with approved authorizations"; 3.1.20, "Verify and control/ limit connections to and use of external systems; level 3 requirement 3.1.3e, "Employ organization-defined secure information transfer solutions to control information flows between security domains on connected systems)
- **Malicious code protection:** Because correctly implemented and architected Browser Isolation ensures that no code is processed on the endpoint, malicious code cannot make its way into DIB members' networks via the Internet. It also rigorously enforces the principle of least privilege by ensuring that Internet code executes with **no** privileges on the endpoint and in the DIB member's network. Remote browser file transfer limitations also restrict users' ability to install non-approved software on DIB member's networks. (CMMC 2.0 level 2 requirement 3.14.2, "Provide protection from malicious code at designated locations within organizational systems"; 3.1.5, "Employ the principle of least privilege, including for specific security functions and privileged accounts"; 3.4.9, "Control and monitor user-installed software")

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.

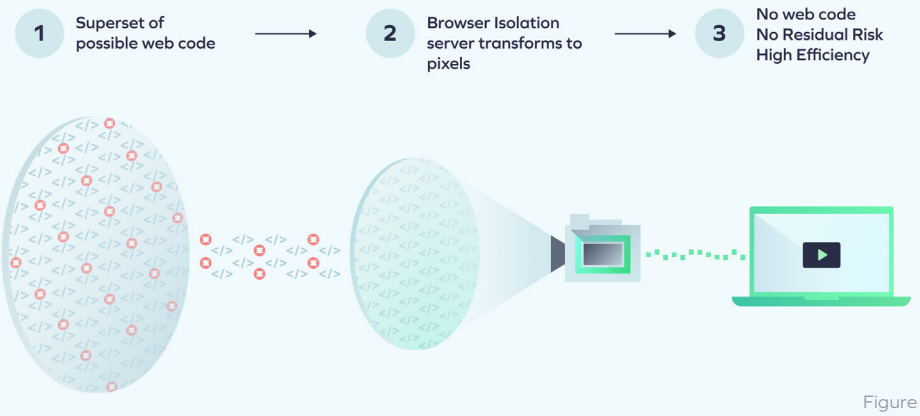


Figure 1 – Full Browser Isolation

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.

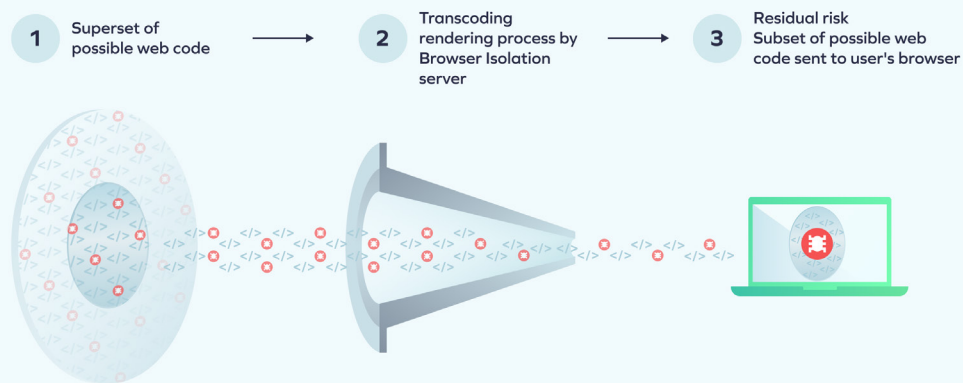


Figure 2 – Partial Browser Isolation

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 the DIB ecosystem.

Such an approach can also result in excessive complexity, duplication of functions and ultimately excessive spend on components within such suites that are irrelevant to many members of the DIB.

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 small and medium-sized DIB entities. It also mitigates the risk of a vendor-homogenous solution facilitating an APT's penetration of the network through exploitation of the common framework.

CMMC 2.0 recognizes the concentration risk of using single-vendor solutions and common technological frameworks. Use of a "best-in-breed" Browser Isolation with a differentiated technology such as *hardsec* architecture creates a strong control to answer level 3 requirement 3.13.1e, "Create diversity in organization-defined system components to reduce the extent of malicious code propagation."

GARRISON

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

As mentioned, robust Browser Isolation can play a key role in fulfilling CMMC requirements by effectively isolating DIB vendors from the riskiest and most ubiquitous information system: the public Internet.

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.**

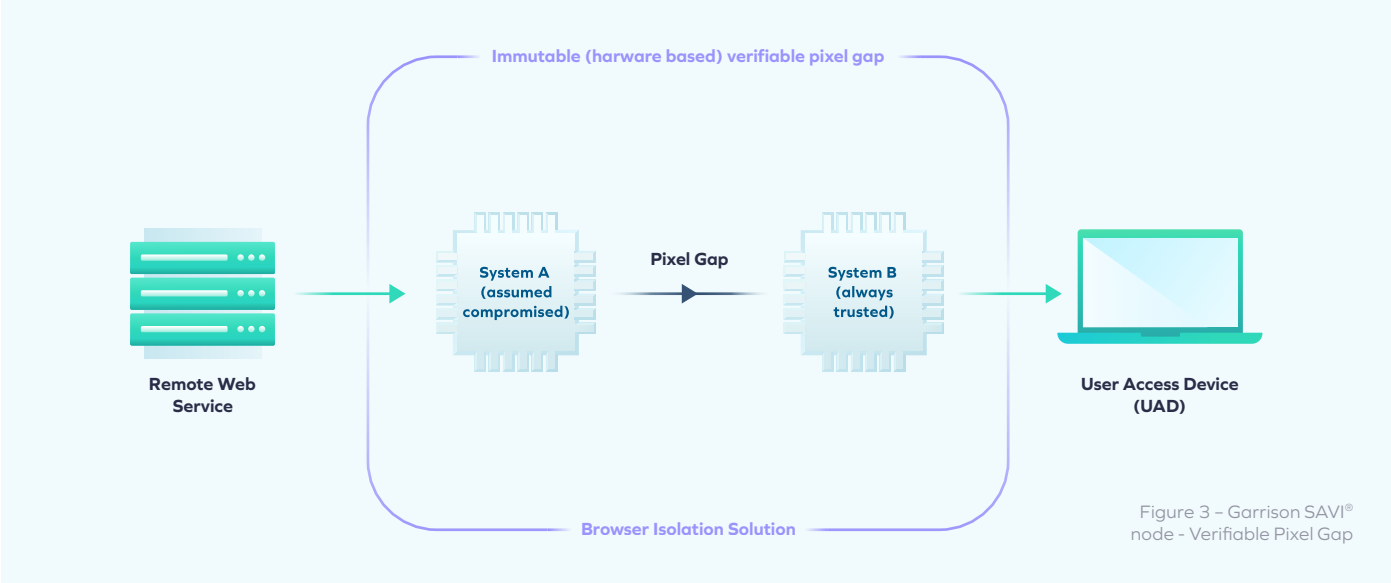
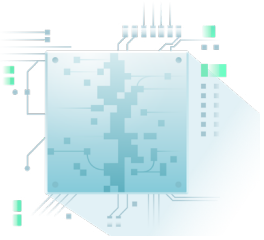


Figure 3 – Garrison SAVI® node - Verifiable Pixel Gap

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 per-seat basis. 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 non-technical DIB vendors, who may spend only a minimal amount of their day using the Internet.

A more cost-effective model to license for a heterogeneous group such as the DIB is on a consumption basis, where concurrent sessions, rather than individual users, are licensed. This will allow the DIB CC to purchase only the license capacity needed to service DIB vendors 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 either on a per-user or capacity-based models, depending on what is most effective for specific organizations. For less-frequent browser users, a capacity-based model allows for users to share capacity across a smaller number of concurrent connections; for organizations whose work involves frequent browsing, a per-user licensing model can decrease complexity.

Ease of Deployment and Maintenance

The small and medium sized businesses in the DIB often lack a dedicated cybersecurity team or even a dedicated cybersecurity individual, so ease of deployment and a low-to-no maintenance approach is paramount, particularly when IT resources for the DIB vendors are focused on other mission essential tasks.

Effectively implemented Browser Isolation also reduces the maintenance load for the individuals responsible for IT and cybersecurity within individual DIB vendors. 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. It also eliminates the need for the DIB CC to continuously evaluate the software being used for Browser Isolation solutions for potentially vulnerable software in their software bills of materials and the threat intelligence being used to ensure that the thresholds for risky content are within USG standards.

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.

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 DIB CC's remote Browser Isolation search and evaluation.

Security

SR#	Security Requirement	Response Consideration
S.1	The solution shall implement hardware-based full isolation using hardsec architectural principles	If it is not a hardware-based full isolation solution, it does not provide robust enough enforcement of CMMC 2.0 level 2 requirement 3.14.2 and level 3 requirement 3.1.3e
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 to the nation-wide distribution of DIB contractors
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

www.garrison.com

CD00000997v1.0 - January 2024