carahsoft

EVERFOX

Trusted Access for Secure Environments

Supporting Mission Operations Without Expanding Risk

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA Schedule 70, CMAS, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Everfox, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/EverfoxResources

Join Events & Webinars:
carah.io/EverfoxEvents

Discover Technology Solutions:
carah.io/Everfox

Learn About Procurement:
carah.io/EverfoxContracts

Connect With Our Team:
Everfox@Carahsoft.com
(888) 662-2724

SOLUTION BRIEF

EVERFOX

Trusted Access for Secure Environments

Supporting Mission Operations Without Expanding Risk

Beyond Secure Boundaries

Government, defence, and high-assurance organisations increasingly depend on access to the open web, SaaS applications, collaboration platforms, and external data sources to support mission operations. Intelligence gathering, operational coordination, infrastructure management, and remote mission support all require interaction beyond the traditional security boundary.

However, enabling external access from classified and sensitive environments introduces significant risk. Traditional security architectures rely on complex software stacks, continuous patching cycles, and layered controls that increase operational burden while expanding the attack surface.

Security leaders must enable trusted access to external resources without compromising the integrity of sensitive systems or slowing mission execution.

Mission Outcomes Enabled by the GIA

The Garrison Isolation Appliance (GIA) enables organisations to securely connect sensitive environments to the modern digital world while maintaining the assurance required for mission-critical operations.

GIA is not ITAR-controlled, but it does fall under UK export controls, which are managed through the usual authorisation steps during deployment. This gives organisations a clearer and more predictable procurement path, making it easier to plan, approve, and deploy GIA where missions require it.

Outcomes

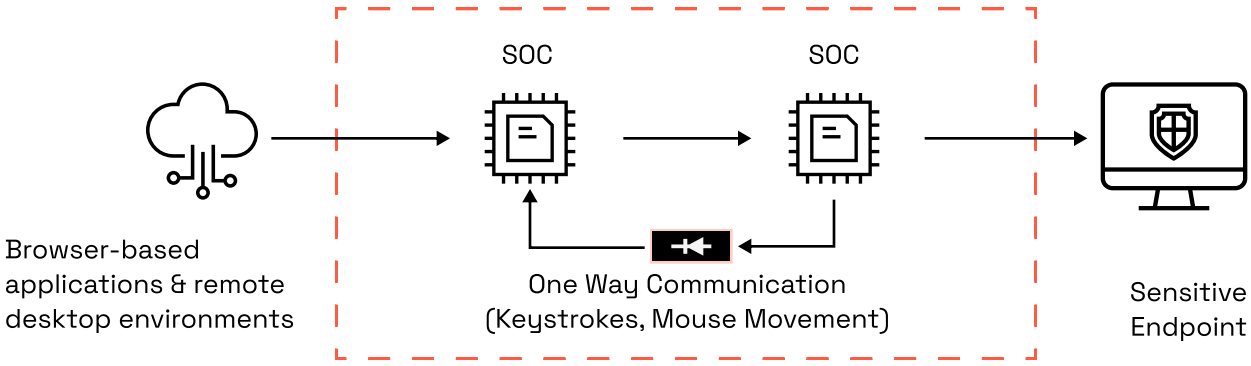
- → **Trusted Internet Access from Secure Environments** – Enable personnel to securely access the open web and web-based applications without exposing sensitive environments to active content or web-borne threats.
- → **Secure Collaboration Across Security Boundaries** – Allow mission teams to interact with external collaboration platforms and shared workspaces while preserving the integrity of classified and high-assurance domains.
- → **Controlled Browse-Down from Classified Networks** – Support secure access from classified environments to lower-classification or public resources without increasing operational or cyber risk.
- → **Secure Administration of Critical Infrastructure** – Enable administrators to safely access external tools, services, and resources required to manage secure infrastructure and operational environments.
- → **Trusted Remote Access for Cleared Workforces** – Extend secure access capabilities to distributed and remote personnel while maintaining the assurance of sensitive environments and CSfC-aligned deployments.
- → **Mission-Critical Communications and Identity Access** – Support capabilities such as bi-directional voice and CAC-enabled workflows (Series B-VX), ensuring secure identity-enabled operations remain available across connected environments.

A Different Approach: Hardware-Enforced Threat Elimination

Traditional cybersecurity approaches rely heavily on detecting and blocking threats after they interact with software-based systems. As threats become increasingly automated and sophisticated, maintaining confidence in complex software-centric architectures becomes more difficult. GIA applies a different model.

Rather than relying solely on software-based threat detection, GIA eliminates web-borne threats at the boundary before they reach sensitive systems. Using Everfox's hardware-enforced isolation approach, active content and malicious code are prevented from entering the secure environment entirely.

This creates a highly trusted access path between trusted and untrusted environments while significantly reducing attack surface exposure and operational complexity.



Secure Access Architecture

The Garrison Isolation Appliance sits between sensitive networks and external resources such as the internet, SaaS applications, collaboration platforms, and external services.

All active content and potential threats are eliminated at the boundary before information reaches the secure environment. Only safe, rendered content is delivered to the user, preventing malicious code from interacting with sensitive systems.

GIA can operate as a standalone capability or integrate with Everfox Trusted Thin Client (TTC) deployments where required. The solution is exportable and deployable globally, supporting secure access requirements across fixed, distributed, and mission-deployed environments.

Trusted Security for High-Assurance Environments

Strong security starts with a trusted access path. GIA uses hardware-enforced isolation to help high-assurance organisations enable external connectivity while maintaining confidence in sensitive systems. It provides a secure way to connect mission-critical environments to the modern digital ecosystem without compromising assurance.