

Securing Artificial Intelligence (AI)

Innovation in Classified Environments with Hardsec

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

Securing Artificial Intelligence (AI)

Innovation in Classified Environments with Hardsec

Problem

Historically, access to classified data has been limited to Sensitive Compartmented Information Facilities (SCIFs) to guard against electronic surveillance and data leakage. At the same time, utilization of innovative and disruptive technologies in those secure environments has been delayed due to the evaluation and implementation processes required to maintain both control and security.

As Artificial Intelligence (AI) accelerates both deep insight and battlefield decisions across the world, secure, agile, and efficient implementation of AI utilizing sensitive data is now critical to mission success.

Solution

The Garrison Platform, powered by Everfox, unlocks new possibilities. Instead of multiple workstations and locations, personnel can utilize a single device to access sensitive systems and infrastructure. The Garrison Platform provides access through a “browse down” model to multiple sensitive systems while using hardware-enforced security (Hardsec) to provide a rigorous, hardware-level isolation between those systems as is generally required for information assurance purposes.

The Garrison Platform empowers secure development of AI systems by enabling subject matter experts and contractor staff operating from multiple secure facilities and networks to collaborate on AI development and implementation in a single controlled environment.

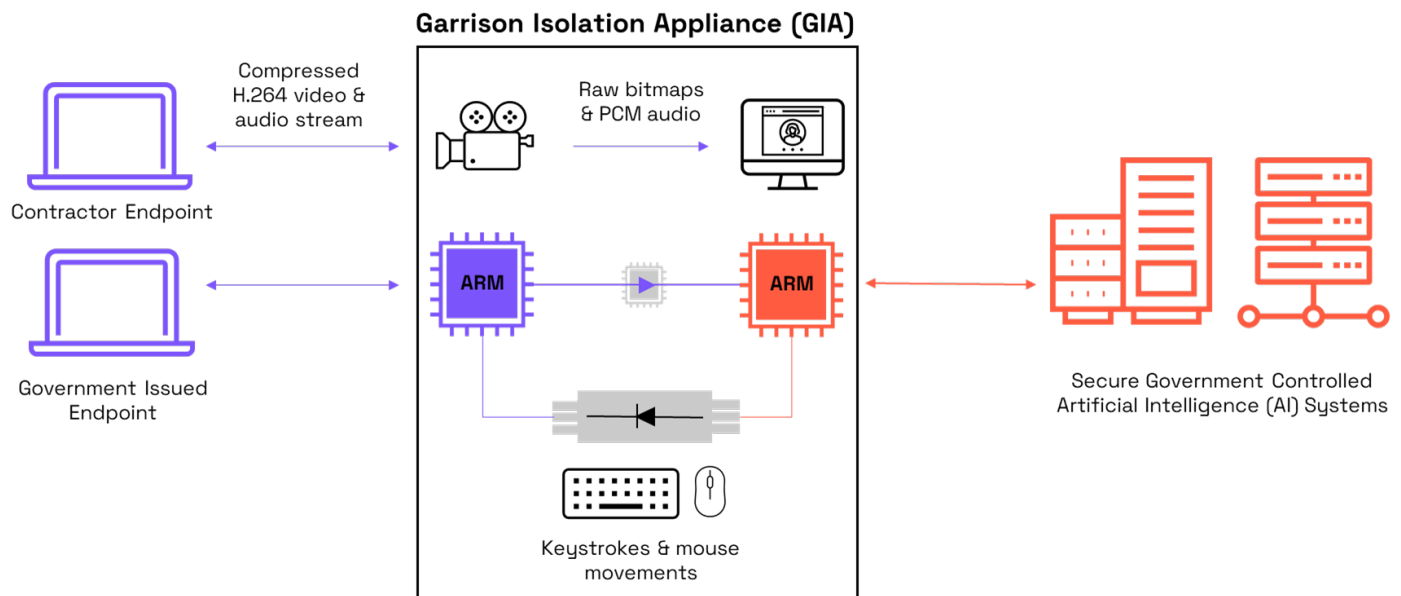
Benefits

- Mitigates the risk of data persistence
- Designed to prevent data exfiltration
- Securely enables Access to third-party devices and networks

No Data Left Behind

Hardsec Secure Access Model

The Garrison Platform's Hardsec Secure Access model enables locked-down workstations or mobile devices to act as the ultimate thin clients: devices that users can rely on to interact with classified data sets and systems, but without introducing the risks of data persistence. By converting data in the remote environment to a transient video stream, the Garrison Platform aims to remove the risk that even inadvertently cached data is left behind.

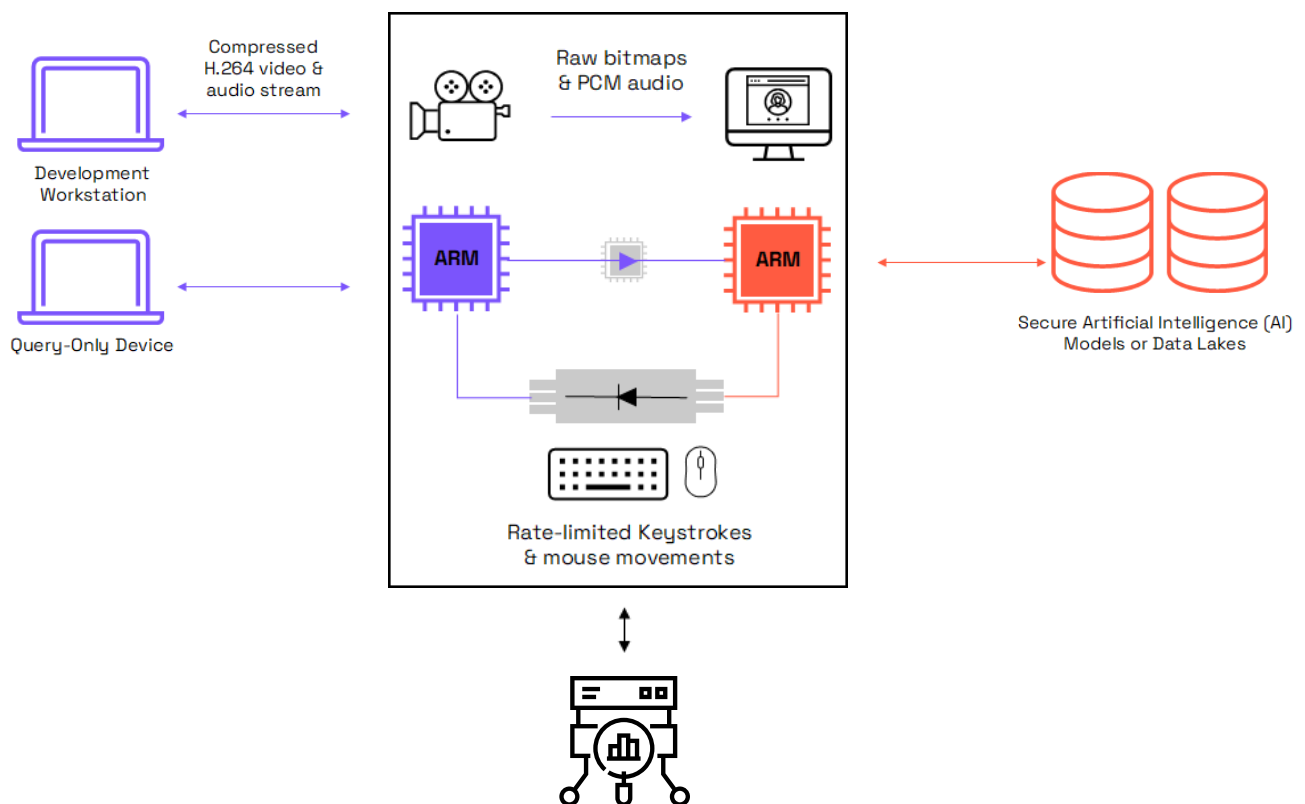


Leveraging Silicon Assured Video Isolation (SAVI®) Technology, the GIA is designed to eliminate the risk of residual sensitive data on endpoints in the event of compromise, loss, or theft.

Designed to Prevent Data Exfiltration

Full-Stack Protocol Break

AI models containing sensitive or classified data can provide a wealth of information for adversaries, creating a significant data exfiltration risk. To address this risk, the Garrison Platform creates a full-stack protocol break between the remote device and the secure system. This protocol break means that, even in the event of a compromise, an adversary would only have access to a video stream of data from the secure AI system, rather than the rights to exfiltrate the underlying raw data.



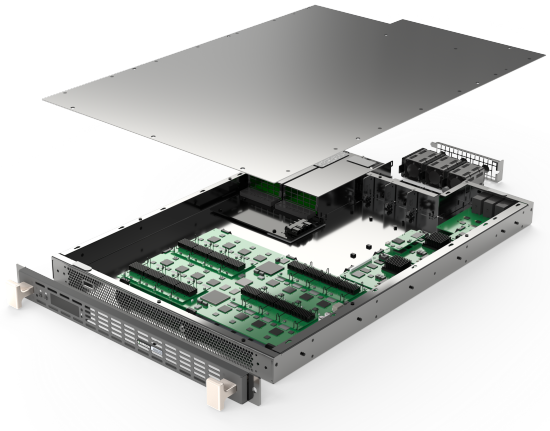
By restricting inputs to rate-limited keystrokes and mouse movements and outputs to a verified video stream, the GIA is designed to prevent data exfiltration, data poisoning, and tampering. Full audit capabilities provide comprehensive logs for high integrity investigations.

Mitigates the Risk of Third-Party Devices and Networks

Secure development access

The Garrison Platform's flexibility enables secure development access from appropriately accredited third-party facilities such as contractor SCIFs while allowing the underlying data and models to remain in USG control, mitigating the risks associated with an attacker or insider who could use third-party sites or systems as an infiltration or exfiltration vector.

The Garrison Platform uses a Secure Access "reach in" approach to permit users to access a VDI or other environment within the development environment to perform a wide variety of development activities on AI and other innovation-focused projects. At the same time, it significantly contracts the Government's attack surface, leveraging the full-stack protocol break to reduce the risk of insider data exfiltration, lateral movement by an attacker present on the contractor system, and software supply chain poisoning of code inputs.



The Garrison Platform Powered by Everfox

Garrison provides industry-leading Hardsec which helps enable access from classified devices to High Threat Networks (HTNs) like the internet, from higher-classification devices to lower-classification systems, and into enclaves within networks of the same classification.

The Garrison Platform enforces – at the hardware level – that all lower-classification data is converted into a stream of raw bitmap data and allows interaction only via keyboard and mouse to prevent attacks on the device. Given the high intelligence value of a Secure AI environment to a near-peer adversary, Hardsec Secure Access architectures like those provided by Garrison provide a high-performance, high-assurance means to increase the pace of innovation and AI adoption in secure government operations.



About Everfox

Everfox, formerly Forcepoint Federal, has been defending the world's most critical data, networks, and personnel against complex cyber threats for more than 25 years. Everfox is proud to help defend global governments, critical infrastructure, and commercial enterprises against known and novel cyber threats. Our unwavering dedication and commitment to our customers and the critical missions they serve are what set us apart. Pioneering a better path forward to a more secure future, Everfox is the trusted high assurance cybersecurity company.

