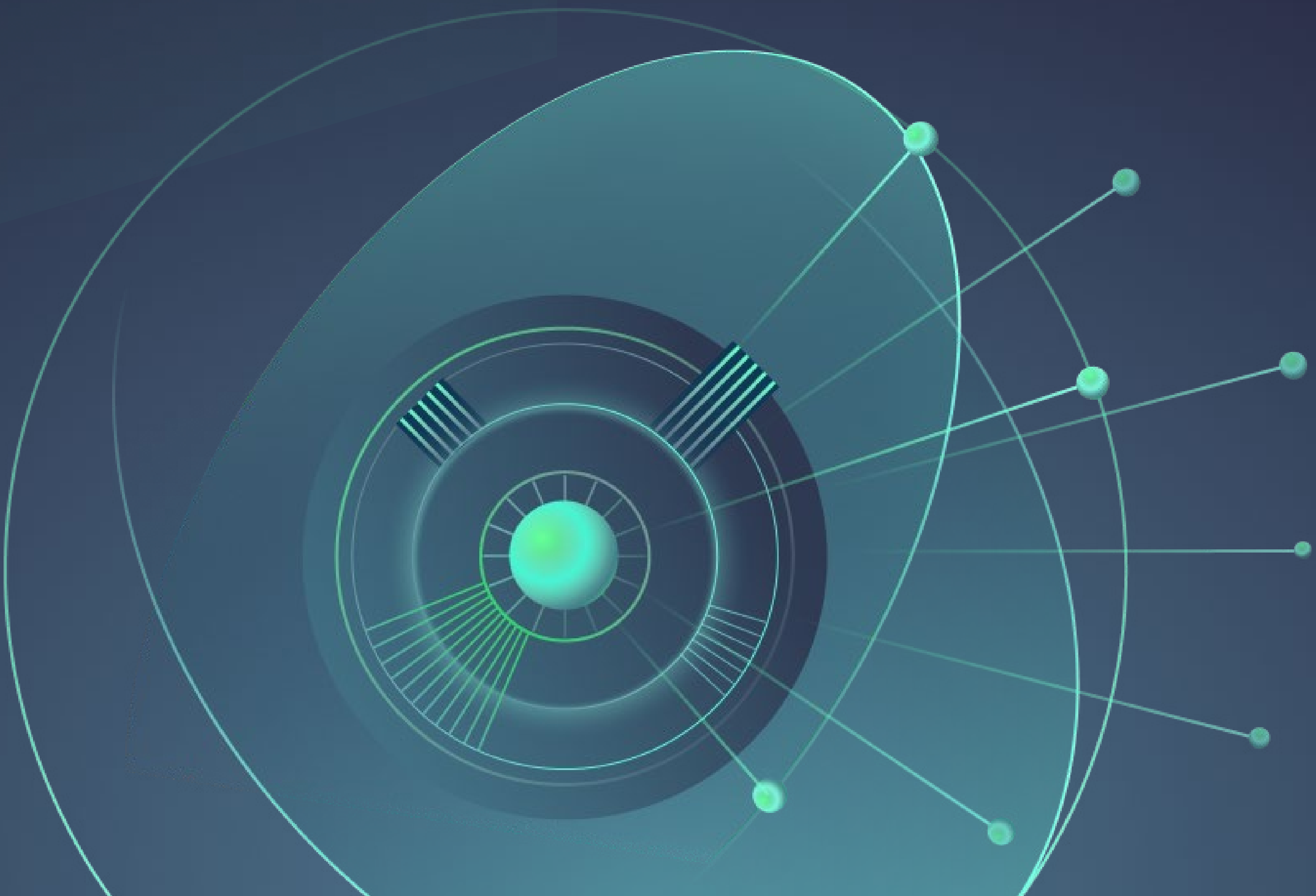
GARRISON

Garrison SAVI® Use Cases

How Garrison SAVI® can deliver security with enablement



Garrison is revolutionizing ways of working for classified and unclassified government, by delivering innovative hardsec (FPGA-based) Cross-Domain Solutions (CDS) to enable mission critical activities. Garrison's solution is a Commercial Off the Shelf (COTS) product that was developed to provide ultra-secure isolated browsing solutions to commercial enterprises, however the use cases for Garrison's technology extend far beyond web browsing, addressing myriad use cases to help deliver new ways of working to government organizations.

Garrison works closely with a number of national authorities including US NCDSMO (Raise the Bar compliance – testing commenced January 2022) and UK NCSC (CAPS and the Cross-Domain Industry Pilot) to deliver assurance.

THE TECHNOLOGY

The Garrison SAVI® Isolation Appliance is a unique hardware appliance engineered from the ground up to deliver security and performance at an affordable cost. At the heart of the solution is our patented Silicon Assured Video Isolation (Garrison SAVI®) technology combined with hardsec security principles.

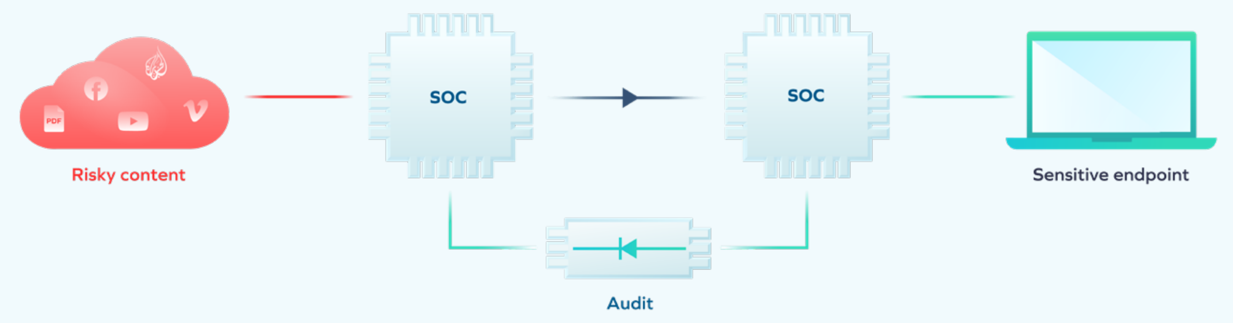


Figure 1-
Garrison SAVI® node

Garrison SAVI® technology

Garrison SAVI® technology relies on the use of the ARM® System-on-Chip (SoC) devices found in mobile phones and tablet devices. Two ARM® SoC devices are used as a pair to create a SAVI Node (see figure 1):

- The ARM® SoC device on the left hand side of figure 1 acts as a tablet – consuming and rendering Internet content. With on-board hardware graphics acceleration and video decoding, it delivers an excellent price/performance profile.
- The video output from this ARM® SoC device which would normally be transmitted to a screen for display is instead transmitted to the camera input of a second ARM® SoC device, on the right-hand side of Figure 1. This device takes the camera input, compresses it – using the on-board video compression hardware found in every smartphone – and transmits it for display at the user's endpoint.
- In the reverse direction, keyboard and mouse commands are transmitted via Garrison's Hardware Security Enforcement Fabric which ensures that this channel is unidirectional and bandwidth-limited – and that an audit copy of every interaction is available for monitoring.

The Garrison SAVI® security design means that even if the ARM® device on the left of the diagram gets compromised, the worst it can do is to show bad pictures to the user. And as soon as the user's session is complete, the device will be fully wiped down at the hardware level to ensure that no malware can persist.

Built on hardsec principles

Hardsec security principles, described fully at https://hardsec.org, use lower-complexity (non-Turing-machine) digital logic to implement security, avoiding software's weak point. By making use of FPGA silicon, hardsec can deliver incredibly strong security while maintaining the flexibility to address real-world cybersecurity problems.

The GIA (Garrison Isolation Appliance)

The Garrison SAVI® Isolation Appliance is a rackable appliance that comes in three form factors: Enterprise (3U chassis supporting 280 concurrent sessions with 280 Garrison SAVI® nodes), Reduced Form Factor (1U chassis supporting 28 concurrent sessions with 28 Garrison SAVI® nodes) and Tactical (top of rack chassis supporting 4 concurrent sessions with 4 Garrison SAVI® nodes) to match scaling needs.

Reduced Form Factor

Enterprise

Tactical

CAPABILITIES

Three core capabilities can be delivered using Garrison's technology, and each of the use cases outlined in this document relies on at least one of these capabilities:

- Browser isolation, providing browser access to HTTP(S) sites
- VDI isolation, providing access to VDI platforms such as Windows Terminal Services
- Isolated system/network management, providing access to tools such as SSH and RDP in addition to the browser

Each of these capabilities can be easily enabled by applying the relevant images to the Remote Environment (the left-hand SoC of Figure 1), ensuring that all the security functions built into the GIA are maintained regardless of the chosen capability.

Note: Custom software options can be used to create new images for the Remote Environment to support other tools.

USE CASES

Browse the web from unclassified environments

In many cases, users need to be able to access the web securely to do their jobs for several reasons:

- Their job function specifically requires them to access dangerous websites – for example security or fraud investigators
- The organization has determined that the risk of permitting access to unusual websites is too high. For most users most of the time that is not a problem – but for some users, some of the time, there is an urgent and important need to visit the site
- The organization has determined that the risk of permitting access to some categories of website is too high. This can have a productivity impact on a significant number of users
- The user's job function is so sensitive that the organization has restricted their web access to only a defined allow-list. While potentially very effective from a security perspective, this will cause significant practical issues for the user.

Garrison SAVI® provides a tool that can be used to safely enable access to the entirety of the web.

Garrison uniquely supports x.509 authentication to web-based resources. This allows browser requests from high side clients to low side domains. Certificates can be installed locally on high side devices or read from CAC / PIV cards.

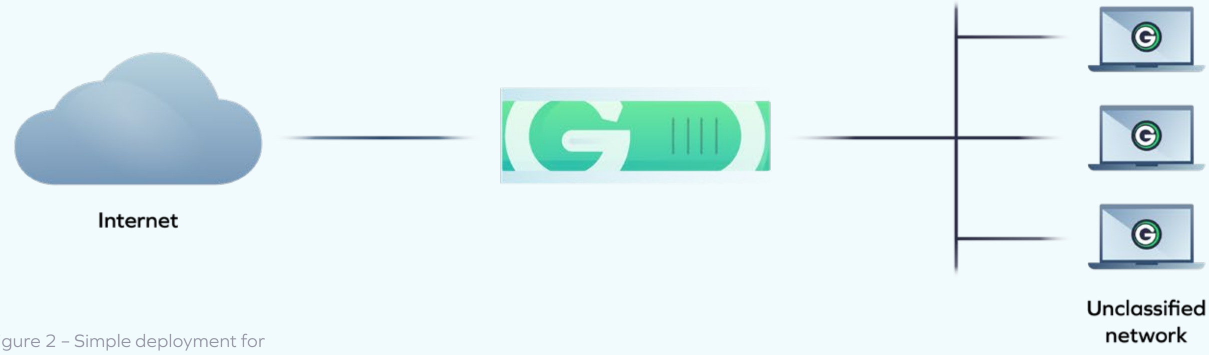


Figure 2 – Simple deployment for web browsing from unclassified environment

Browse the web from secure environments

Even in the most sensitive environments, web access can be critical for providing real-time information as well as enriching knowledge and decision making via key online resources.

Garrison SAVI® is being used today to provide web browsing for users of such sensitive networks: the level of security delivered by Garrison's hardware-level security technology is so high that Garrison SAVI® can be trusted where no other connection is.

Garrison uniquely supports x.509 authentication to web-based resources. This allows browser requests from high side clients to low side domains. Certificates can be installed locally on high side devices or read from CAC / PIV cards.

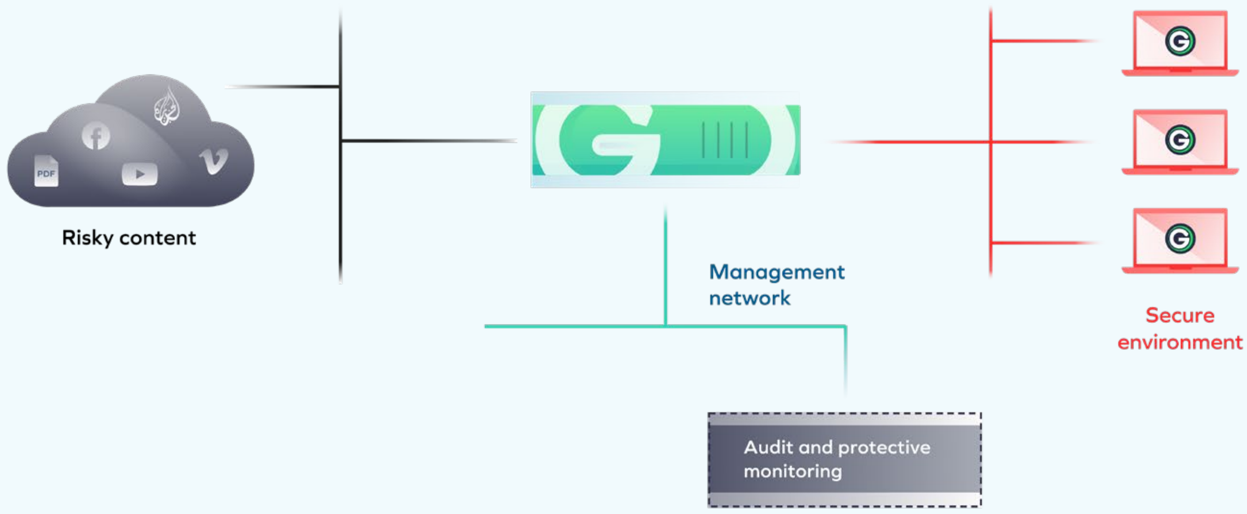


Figure 3 - Accessing the web from secure environments

Browse down and across from classified domains

For some users of high-security networks, it may be desirable to gain rapid access to source data and applications in their native environments, but in multi-domain environments, user workflows can be inefficient and expensive, hindering time-critical mission needs. Garrison SAVI® can be used to provide secure access that overcomes these security concerns, enabling a single environment with access to multiple domains and offering integrated workflows for data transfers, delivering huge efficiency, cost and security improvements.

Garrison uniquely supports x.509 authentication to web-based resources. This allows browser requests from high side clients to low side domains. Certificates can be installed locally on high side devices or read from CAC / PIV cards.

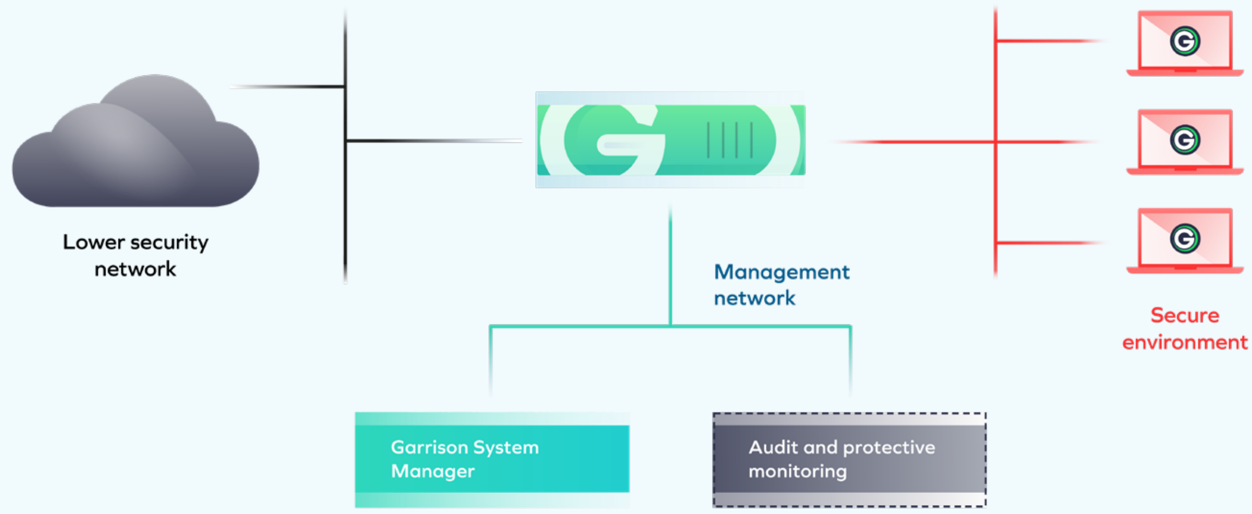


Figure 4 -
Browse down and across from secure environments

Secure access to collaborative workspaces

Working with allies, accessing commercial cloud resources, or even collaborating on 'lower-tier' security environments can all be enabled through Garrison's secure VDI isolation. Garrison's ultra-secure hardsec based isolation platform enables access to collaboration resources for even the most sensitive of environments.

The same hardware security architecture that provides the assurance for web access from high-security networks means that Garrison SAVI® is being used today to provide secure VDI access in scenarios where raw VDI access is not permitted.

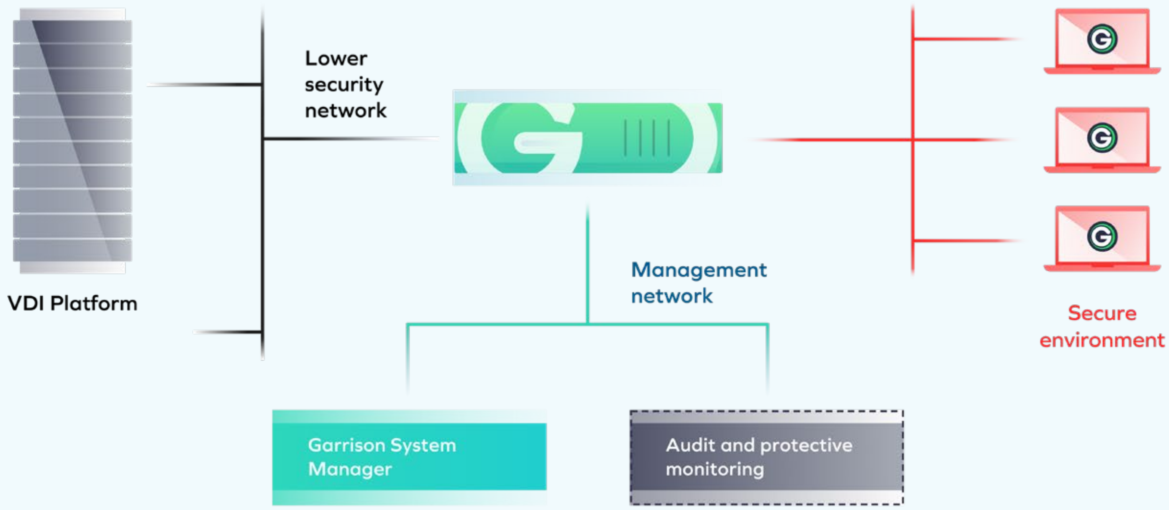


Figure 5 -
Reach down and across to collaborative workspaces

Manage Secure Infrastructure

Managing secure infrastructure for sensitive networks can itself be a huge and expensive security challenge. Garrison's ultra secure hardsec isolation can provide the 'jump box' access required to control network infrastructure without the traditional risks. Hardware enforced security mitigates the traditional issues and cost associated with patching legacy systems – ensuring a long-term, low cost and highly effective approach to network management.

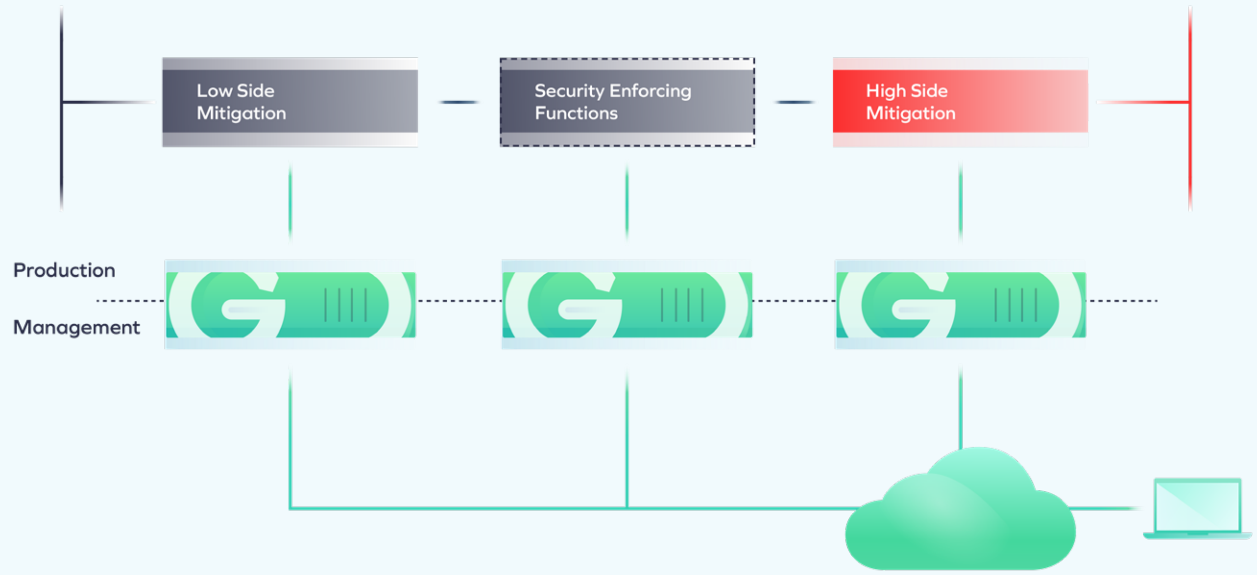


Figure 6 -
Managing secure infrastructure
(e.g. Cross-Domain Solution)

Secure remote working

Remote access models are controversial from a security perspective, but in a world where remote working has rapidly become mission critical and essential to support day-to-day operations, Garrison is working with customers both on hardsec isolation approaches, and key architectural elements to build the confidence that is allowing even the most sensitive organizations to operate with remote workforces.

When used for remote access, Garrison SAVI® can provide a number of risk mitigations:

- Prevents malware upload to the Secure Environment: nothing can pass from the low side to the high side except keypresses and mouse movements.
- Mitigating data loss risks: Only bitmaps are transferred from the secure network to the remote machine. While screen recording could in principle be used to persist this information on the remote machine, there is no structure to the data and an attacker would need to use a further level of processing (for example, Optical Character Recognition) to restore structure to the data.
- Monitoring unexpected behaviour: A complete log of keypresses and mouse movements sent by the remote machine is retained. This can assist with forensic investigations, and can also form the basis of monitoring analytics designed to detect unexpected behaviours by the remote machine.

One remote access model uses Garrison SAVI® to mediate access to a VDI platform in the secure network. In this case, the network owner would typically rely on authentication measures offered by the VDI platform to authorize the remote user.

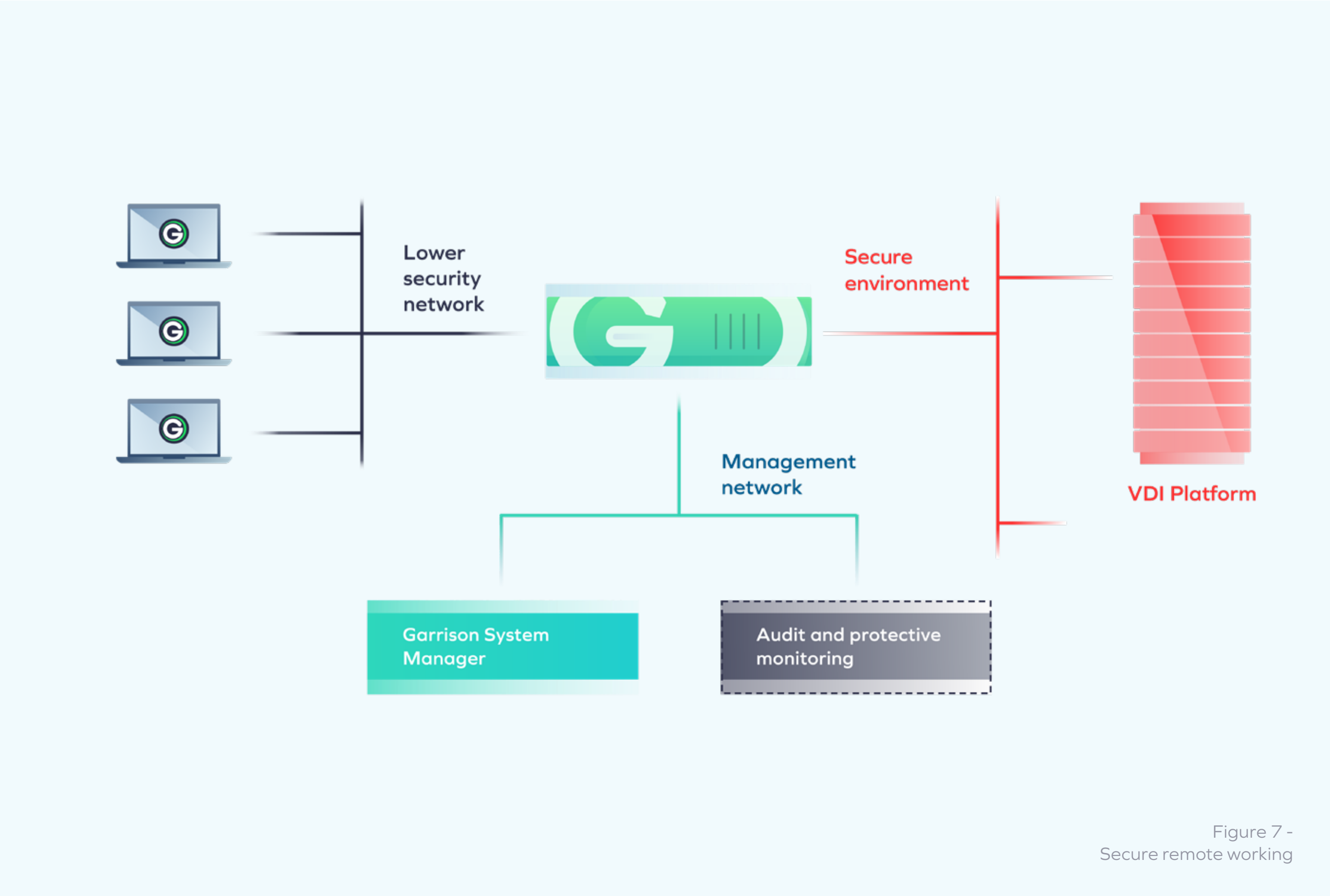


Figure 7 -
Secure remote working

Isolate Third Party Applications

In addition to the off-the-shelf browser and VDI software packs, Garrison SAVI® can also be used to isolate third party applications such as social media, messaging and video tools. Not only does this provide highly trusted access, but it also provides the hardware enforced logging and oversight required to do this in a risk-managed way. Garrison is supporting operations in both fixed and mobile environments for use cases such as:

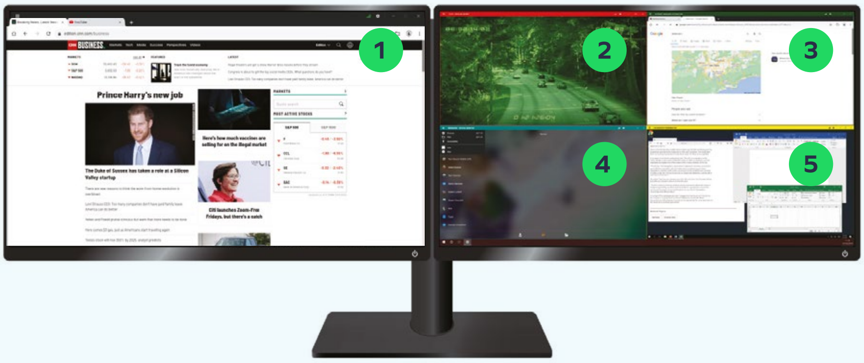
- Access from secure networks to Internet messaging applications such as WhatsApp or Telegram
- Access from secure networks to other native mobile applications such as Facebook
- Remote access to custom business applications without the need for a separate Intranet web server or VDI platform.

Please note that not all applications will be compatible out of the box. In this case, custom software options can be used to create new images for the Remote Environment to support other tools.

Enable a multi-domain workstation

Multiple domains and use-case elements can be combined to create a single-pane-of-glass intelligence desktop with real-time access to critical information sources, revolutionizing ways of working for classified and unclassified government and supporting Multi-Domain Operations.

From a single terminal, users can do all of the following:



1. Web browsing
2. Video feed monitoring
3. Non attributed web browsing
4. Messaging
5. Virtual Desktop Infrastructure

...and many other use cases...

GARRISON

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