GARRISON

Garrison SAVI® use cases

How Garrison SAVI® can deliver security with usability

Introduction

Garrison SAVI® is a revolutionary technology that is promoted primarily as a tool for secure web browsing. But the potential uses for Garrison SAVI® extend far beyond web browsing. This document provides a high level overview of use cases where Garrison SAVI® can help.

Garrison SAVI® 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 Garrison is our patented Silicon Assured Video Isolation (Garrison SAVI®) technology.

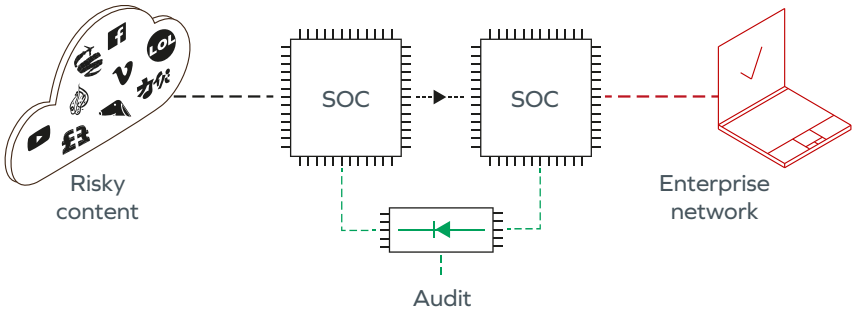

Figure 1 – Garrison SAVI® technology

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:

- The ARM® SoC device on the left hand side in the diagram above 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. 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.

Garrison SAVI® Isolation Appliances come in a range of sizes, supporting up to 280 concurrent sessions (with 280 pairs of ARM® devices) per appliance.

Re-enabling blocked web pages

Regular commercial IT environments typically have existing technology such as a proxy or an endpoint agent which restricts access to web pages which are considered too dangerous.

In some cases however, users need a way of accessing these blocked web pages. There are a number of reasons why this might be the case:

- Because their job function specifically requires them to access dangerous websites – for example security or fraud investigators
- Because the organisation 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
- Because the organisation 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
- Because the user's job function is so sensitive that the organisation 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 re-enable these blocked pages. And of course, with Garrison SAVI® in place, organisations can consider being much more aggressive with their blocking policies.

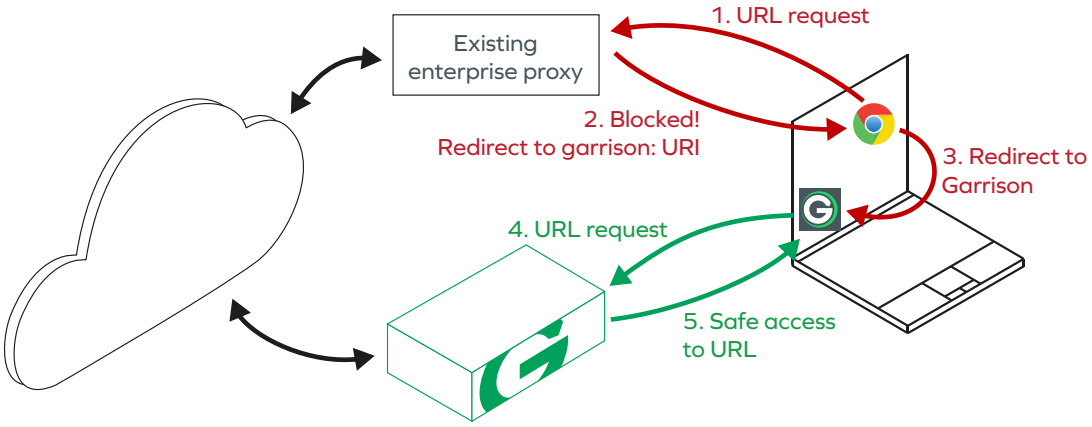

Figure 2 – example deployment for re-enabling pages blocked by an enterprise proxy

Web access from high-security air-gapped networks

In some cases, organisations are so security sensitive that they provide no access to the Internet at all – their networks are fully "air-gapped".

Garrison SAVI® is being used today to provide web browsing for users of such 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.

In these cases Garrison can supply extensive materials to national authorities to assist with security assurance. For many potential customers, further information may also be available from the UK's National Cyber Security Centre (part of GCHQ).

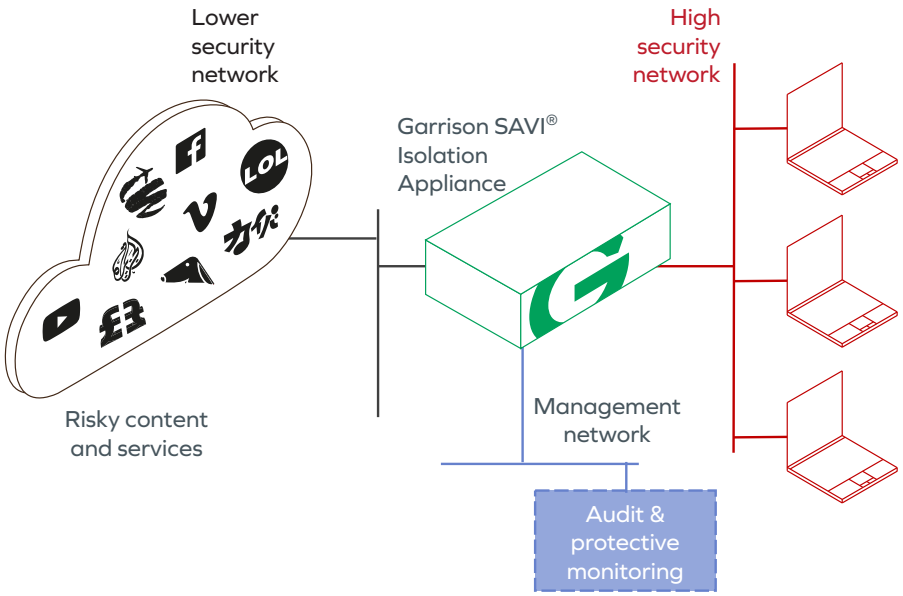

Figure 3 – providing web access from air-gapped high security networks

VDI access from high-security air-gapped networks

For some users of high-security air-gapped networks, it may be desirable to access Virtual Desktop (VDI) platforms within lower-security networks in order to interact with files and other systems. Under normal circumstances, this would not be permitted because of the risk that the lower-security VDI platform might attack the endpoint on the high-security network.

Garrison SAVI® can be used (with an optional VDI software pack) to provide secure VDI access that overcomes these security concerns. 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.

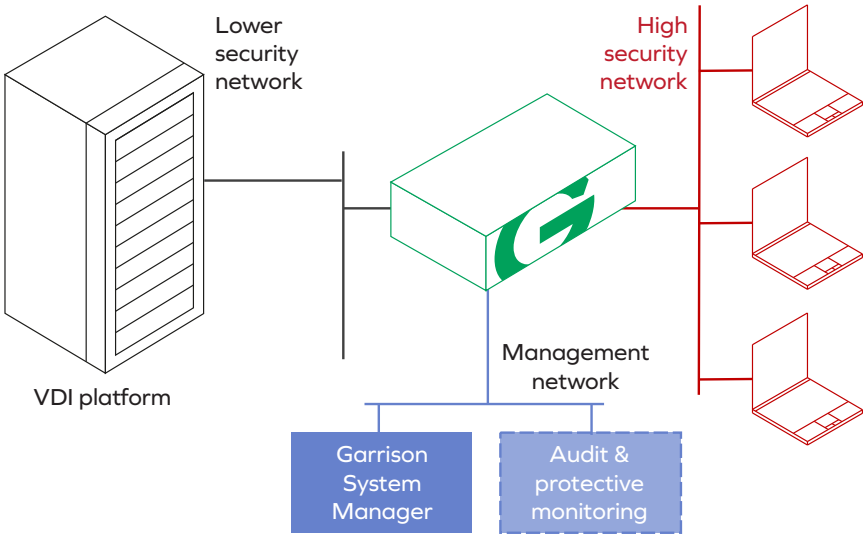

Figure 4 – access to VDI platforms from high-security networks

Remote VDI access to secure networks

Remote access models are controversial from a security perspective: if a lower-security endpoint is used to access (even remotely) sensitive information or systems, then there is a risk that that endpoint could have been compromised by a malicious attacker. In that situation, anything which a legitimate user can do, the malicious attacker can do also: for example, they can take screenshots of sensitive information, or click buttons or enter commands as if they were the valid user.

Nonetheless, in some cases remote access is a business requirement and measures must be taken to mitigate the risks. When used for remote access, Garrison SAVI® can provide a number of risk mitigations:

- The owner of the secure network can be confident that only bitmaps are transferred from the secure network to the remote machine. While screen recording can in principle be used to persist this information on the remote machine, there is no structure to the data: an attacker would need to use a further level of processing (for example, Optical Character Recognition) to restore structure to the data. This can help to mitigate data loss risks
- The owner of the secure network can retain a complete log of keypresses and mouse movements sent by the remote machine. This can hugely 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® (with the optional VDI software pack) 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 authorise the remote user.

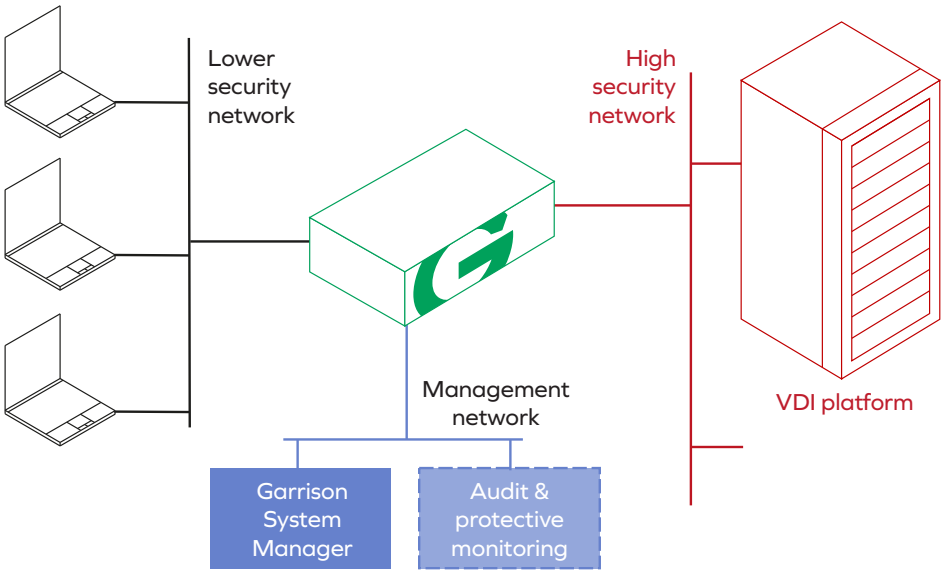

Figure 5 – providing additional security for remote access to a VDI platform

Remote browser access to secure networks

In some cases remote access is required but a full VDI environment is not: the remote user only needs access to Intranet websites on the secure network. In this case, Garrison SAVI® can be used without the need for the optional VDI software pack.

Garrison SAVI® provides built-in authentication when the endpoint connects to the Garrison SAVI® Isolation Appliance. However, in a remote access deployment model, this authentication takes place in the lower-security network and this may be insufficient for the owner of the secure network. In this case, the owner of the secure network would typically use a captive portal within the secure network in order to provide a second layer of authentication.

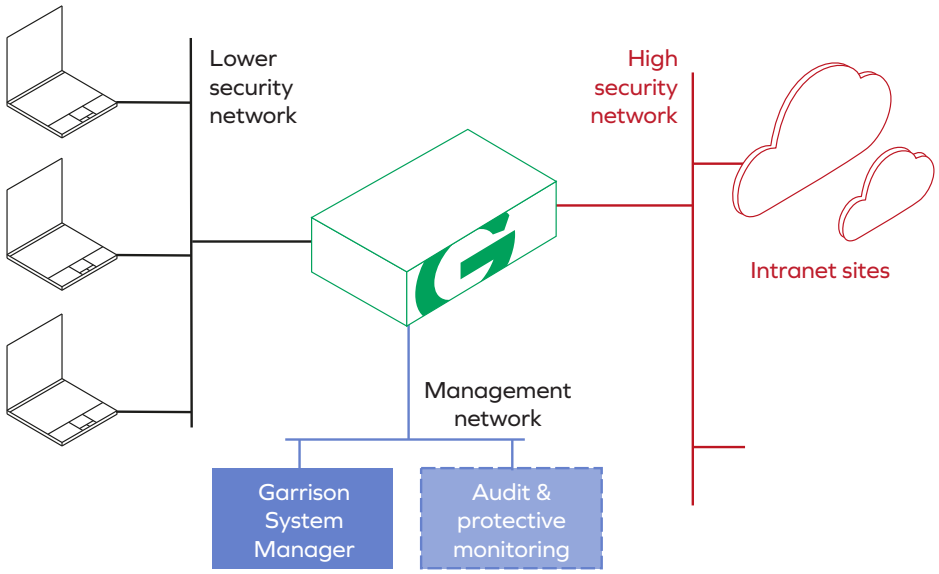

Figure 6 – remote access to intranet sites on a higher security network

Network management

Garrison SAVI® can be used as an ultra-secure jump box for network management.

Where a network administrator is working on a high-security management network, they may need to access lower-security networks using tools such as SSH and RDP in order to perform maintenance. With the optional Network Management software pack, Garrison SAVI® provides administrators with the access they need while maintaining a strong security boundary between the networks.

Custom software options

The use cases described earlier in this document rely on three off-the-shelf software packs:

- The default software, providing browser access to HTTP(S) sites
- The optional VDI software pack, providing access to VDI platforms such as Windows Terminal Services
- The Network Management software pack, providing access for systems administrators using tools such as SSH and RDP.

In addition to these off-the-shelf software packs, Garrison SAVI® can also be used to run custom or 3rd party software applications that are designed for the Android environment. This enables a number of additional potential use cases:

- 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.

Email info@garrison.com

UK telephone +44 (0) 203 890 4504

US telephone +1 (646) 690-8824

www.garrison.com

CD00000228v1.2 - August 2020