GARRISON

Garrison SAVI® - between physical and virtual isolation

The importance of isolation

To protect sensitive systems, it is critical to protect the endpoints that can access them: if endpoints are compromised by malware, the attacker can manipulate other systems that the endpoints can access in order to steal sensitive data or carry out undesirable actions.

In the face of today's threats, traditional endpoint protection measures such as antivirus are no longer enough: it is necessary to isolate sensitive endpoints from risky systems (for example, the Internet) that *might* be the source of malware. Two techniques are commonly used:

- **Physical isolation.** The use of physically separate endpoint devices to access sensitive systems and risky systems
- **Virtual isolation.** The use of VDI or remote-desktop technologies to provide isolation, by giving remote access to risky systems from a sensitive endpoint. (The reverse – giving remote access to sensitive systems from a risky endpoint – is not advised because an attacker in control of the risky endpoint can also gain remote access to the sensitive system).

Issues with physical isolation

At a purely technical level, physical isolation provides extremely strong security. However, in the presence of human factors, security can be significantly reduced. Physical isolation is extremely inconvenient for human users and this leads to unwanted behaviours.

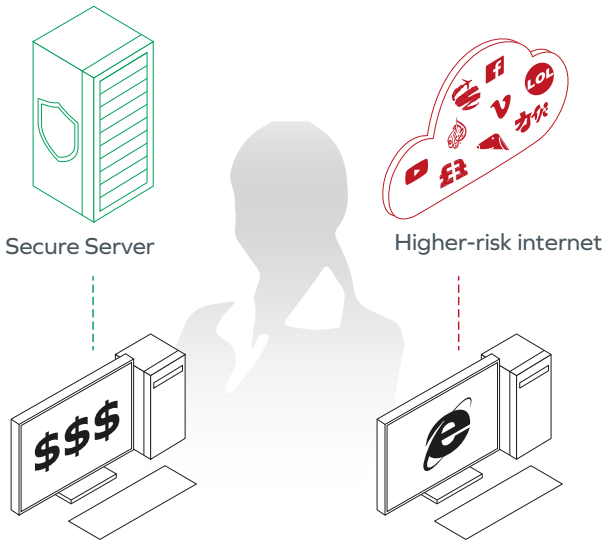

Figure 1 - Physical isolation

Firstly, users will make strenuous efforts to avoid the imposition of physical isolation. But if physical isolation is imposed, users will often find workarounds that reduce the level of inconvenience but also reduce security. These workarounds usually involve using unauthorised, risky, systems to carry out sensitive work – for example, working using a personal machine and communicating with colleagues using Gmail rather than using secure machines and the secure

organisational email system. More extreme workarounds may involve installing unauthorised connections to physically isolated endpoints: these are typically even worse than non-isolated architectures because these connections are uncontrolled.

In addition, complete isolation is almost never truly possible: it is always necessary to move files from the risky environment to the sensitive environment. This introduces risk, because these files may be vectors for malware. Inconvenient physical separation will often lead to the need to transfer large volumes of files to the sensitive environment.

In addition to potential security issues, inconvenient physical isolation also of course leads to business inefficiency and unhappy users.

Virtual isolation

Virtual isolation provides improved convenience over physical isolation, because users can gain access to all required information from a single physical device. Virtual isolation is even possible with mobile computing (where it is often impractical to carry multiple physical endpoints around).

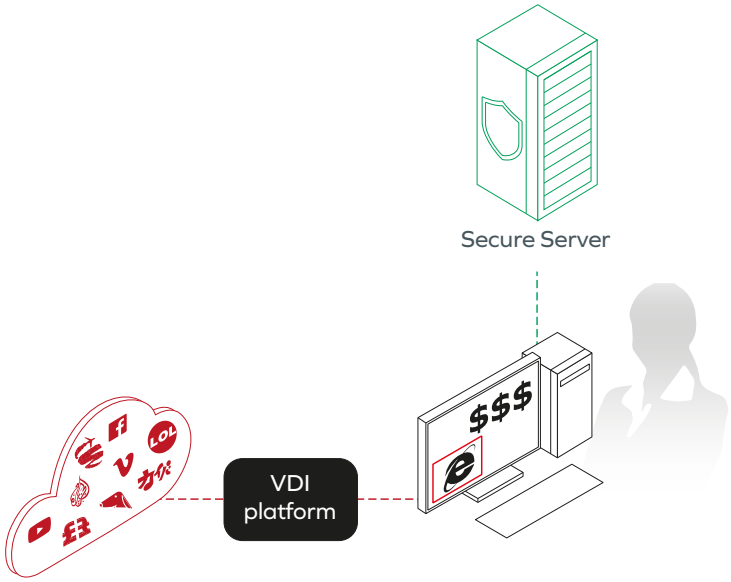

Figure 2 – Virtual isolation

Virtual isolation can improve security in two ways:

- By reducing the incentive for user workarounds
- By reducing the number of files that need to be transferred from the risky to the sensitive environment.

In addition, virtual isolation can make it easier to monitor for data loss: monitoring the keyboard and mouse channel from the sensitive endpoint to the risky system can be easier than installing keyloggers on risky systems that may be poorly controlled.

However, virtual isolation provides less technically strong isolation than physical isolation. VDI and Remote Desktop

technologies are not designed predominantly for security, and it can be possible for an attacker in control of a risky VDI server to attack the sensitive endpoint via the remote access protocol.

In addition, VDI and Remote Desktop deployments can require significant investments in server hardware and network bandwidth, particularly where they are used to access dynamic content such as rich media on the Web. To reduce these costs, it can be tempting to use techniques provided by the vendor such as "media acceleration". These techniques however reduce further the level of technical security provided by VDI or Remote Desktop (because, for example, media may be forwarded completely unchanged from the Internet to the sensitive endpoint).

Garrison - between physical and virtual isolation

Garrison aims to provide the benefits of virtual isolation with a strong technical security model that is close to physical isolation. As with virtual isolation, Garrison can provide access from a sensitive endpoint to a risky VDI server or to the World Wide Web, but with a technical security model which is provided by:

- A unique, patented hardware design (Silicon Assured Video Isolation – Garrison SAVI®) that uses physically separate processing systems and an information transfer approach in line with the recommended pattern published by the UK's National Cyber Security Centre (part of GCHQ[1])
- A high-assurance approach to development and implementation of critical functionality combined with 3rd party security assurance provided through a set of design documentation and a security testing regime which can be shared with customers or national technical authorities.

This paper provides an initial overview of Garrison's technology. Further details are available under Non Disclosure Agreement.

The Garrison SAVI® Isolation Appliance

The Garrison SAVI® Isolation Appliance (GIA) is a 3U rackable hardware appliance which supports up to 280 concurrent active users. The number of named users supported by one appliance is strongly dependent on activity levels.

The GIA presents three physically separate network interfaces:

- **A Client network interface.** This interface is for connection to the higher trust network, where users' endpoints will be connected
- **A Remote network interface.** This interface is for connection to the lower trust network, where services are located that the user may wish to access
- **A Management network interface.** This interface is for connection to a management network which is used to configure the appliance and which is assumed to have the highest level of trust.

1 https://www.ncsc.gov.uk/guidance/pattern-safely-importing-data

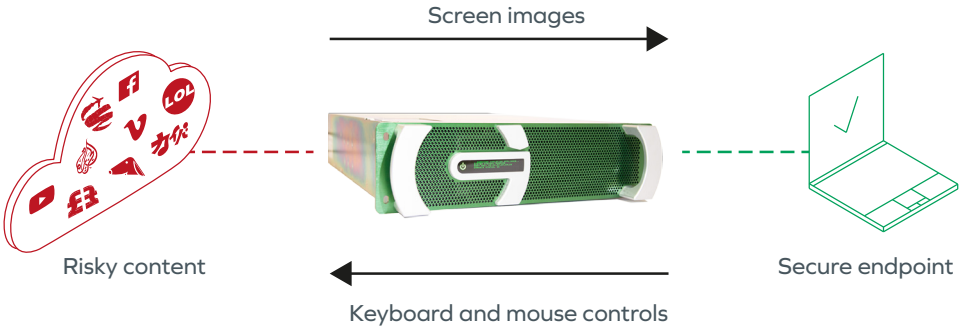

Figure 3 – The Garrison SAVI® Isolation Appliance

Security objectives

The GIA appliance incorporates a wide range of security enforcement functions, but four threats are addressed with the very highest level of security control, implemented in hardware. These four threats are:

- A threat actor on the Remote network seeks to attack the integrity, confidentiality or availability of the Client network
- A threat actor on the Remote network seeks to attack the integrity, confidentiality or availability of the Management network
- A threat actor on the Client network seeks to leak confidential information to the Remote network
- A threat actor on the Client network seeks to attack the integrity, confidentiality or availability of the Management network.

The GIA is designed to mitigate these four threats while providing an excellent user experience.

Security design

The core hardware architecture of the GIA is shown in Figure 4. Three top-level blocks are shown:

- On the left hand side, the system contains 280 SAVI Nodes. Each SAVI Node contains two (physically separate) ARM System on Chip devices – a Remote Environment Processor (REP) and a Client Connection Processor (CCP)
- On the right hand side, the system contains three (physically separate) system-level processors, one connected to each of the three network interfaces
- In the middle, multiple interconnected Field Programmable Gate Array (FPGA) devices are used to provide network routing to and from the REP and CCP, and to provide a Hardware Security Enforcement Fabric (HSEF) which applies critical security controls to address the key threats identified in the security objectives above. The use of FPGAs to create the HSEF means that security controls are implemented using dedicated digital logic rather than software. This hugely reduces the risk that the security controls could become compromised.

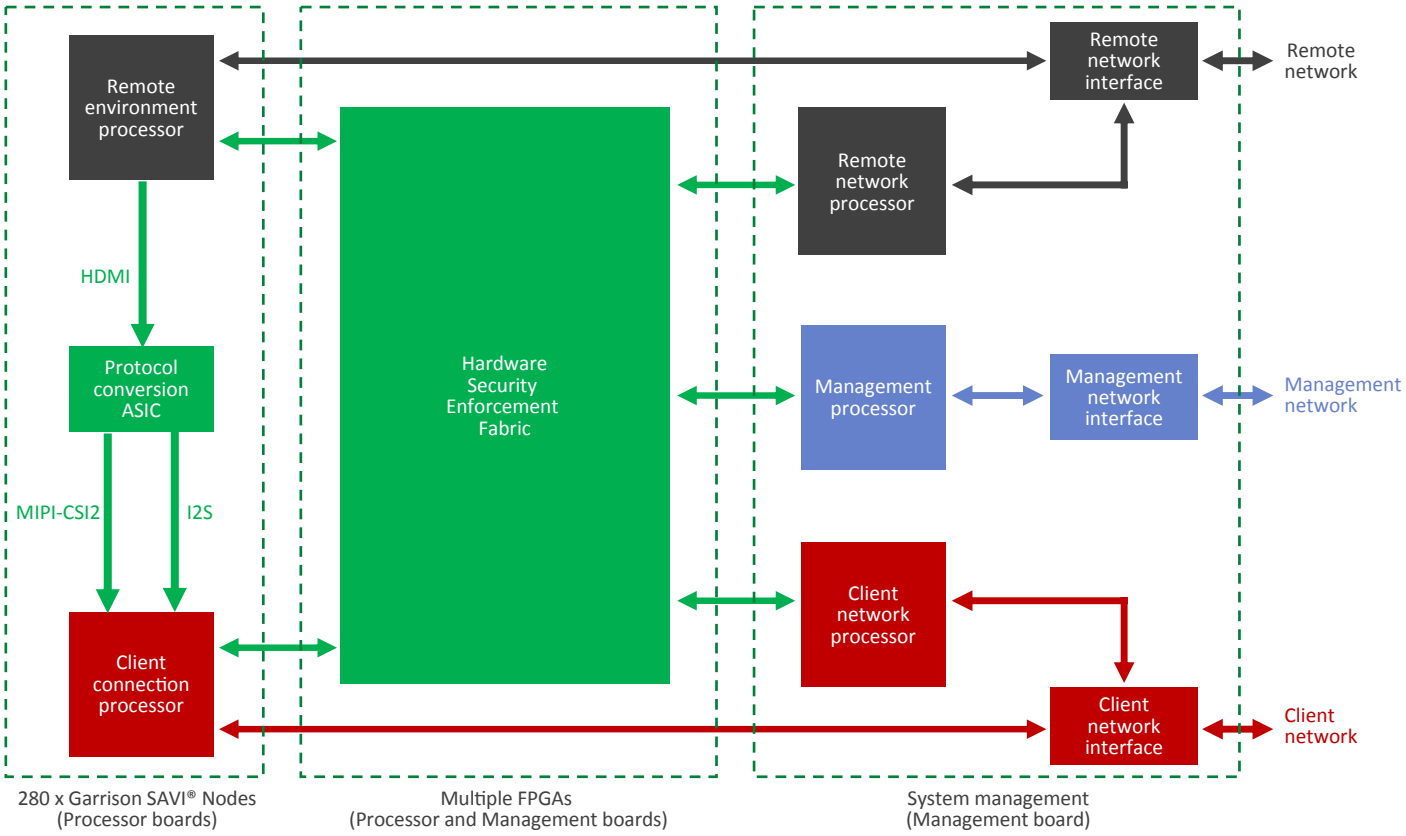

Figure 4 – GIA security architecture

The REP chip runs software to connect to the risky (Remote) network. This software could be either a web browser (for access to the World Wide Web) or a VDI client (for access to a risky VDI platform). The CCP chip runs software to connect to the user's sensitive endpoint, over the Client network. The Security Enforcing Functions of the GIA allow the CCP to control and view the (physically separate) REP while keeping the CCP safe even if the REP is running malware. The core concept is shown in Figure 5.

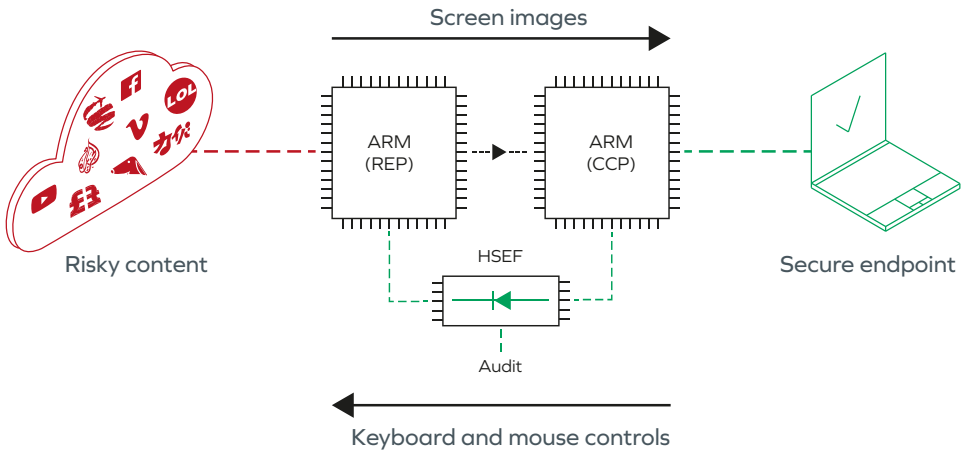

Figure 5 – Garrison SAVI® core concept

Security enforcing functionality

Due to the way the physical electronics of the GIA has been constructed, the REP and the CCP can only communicate in two ways:

- Via the protocol conversion ASIC
- Via the Hardware Security Enforcement Fabric (a number of interconnected Field Programmable Gate Arrays – FPGAs).

Communication via the protocol conversion ASIC allows the screen image and any audio output from the REP to flow to the CCP. The CCP can compress the received signal and deliver it over the network to the user's endpoint for display and playback. This communication flow follows the "transform+flow control+verify" pattern recommended by the UK's National Cyber Security Centre[2]:

- A fixed-function hardware subsystem in the REP device transforms information from the Remote network into HDMI audio+video output
- The protocol conversion ASIC verifies the HDMI data and further converts the information to new protocols (MIPI-CSI2 and I2S)
- Fixed-function hardware subsystems in the CCP further verify the MIPI-CSI2 and I2S data
- Wiring between the REP, protocol conversion ASIC and CCP enforces unidirectionality (for example, HDMI signal lines such as EDID or CEC that incorporate a reverse data flow channel are not connected).

The other means by which the CCP and REP can communicate is the Hardware Security Enforcement Fabric (HSEF). The HSEF implements a secure messaging system (the Garrison Internal Messaging Protocol, or GIMP) using digital logic in FPGAs implemented using high-assurance FPGAs. The HSEF implements three key security enforcing functions:

- SEF_GIMP_VAL – GIMP messages are validated to ensure that they are permissible and correctly formed
- SEF_GIMP_RATE – GIMP messages are rate limited
- SEF_GIMP_AUD – GIMP messages are audited for forensics and analysis via the GIA Management Interface.

In addition, the HSEF implements a patented Hardware Secure Reboot function that ensures SAVI Nodes are returned to a known good state before any new user session.

2 https://www.ncsc.gov.uk/guidance/pattern-safely-importing-data

Security assurance

Garrison recognises that security-conscious customers will need assurance that the security design is robust and that Garrison's implementation is correct. To support such assurance activities Garrison is able to share (under NDA) various assurance-supporting materials with suitable assurance laboratories or authorities, including:

- GIA Security Target – a formal analysis of the security the GIA is designed to deliver
- High Level Design – how the technology has been designed to deliver the Security Target
- Development Security Plan – how Garrison ensures that the technology developed is consistent with the design
- Assurance Test Plan – how testing is used to support the Development Security Plan
- Manufacturing Security Plan – how Garrison ensures that the hardware which is manufactured is consistent with the design
- Logic definitions for HSEF Security Enforcing Functions – detailed implementations for the critical security functionality.

National authorities may also wish to contact the UK National Cyber Security Centre (via diplomatic channels) for an independent view on Garrison's security assurance.

Enterprise solution

The Garrison SAVI® Isolation Appliance forms part of a sophisticated enterprise solution as shown in Figure 6.

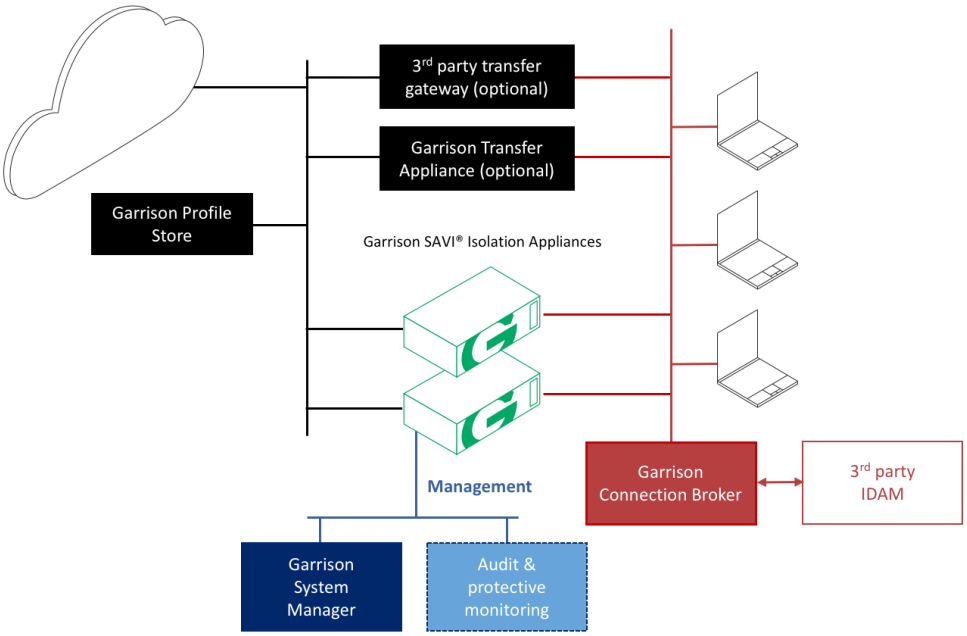

Figure 6 – Garrison SAVI® solution

On the right hand side of the diagram, the Client interface on the GIA is connected to a network where end user devices can connect to it. Optional Garrison Connection Broker software enables load balancing, failover and IDAM integration.

On the left hand side, the Remote interface on the GIA is connected to a lower-trust network where services are located (for example, the Internet). The Remote interface can support an optional Garrison Profile Store (provided either as a virtual appliance or as a physical appliance, called the Garrison Storage Appliance). If used, this appliance provides persistence between sessions – for example cookies and bookmarks in the case of Internet access.

The Management interface on the GIA is used to configure the appliance (via the Garrison System Manager). All software and HSEF images are loaded via the Management interface, allowing for simple updates and upgrades. The root of trust for the appliance is thus the physical security of the Management interface, though this will be supplemented with software controls to ensure that only suitably signed images can be uploaded to the GIA.

The Management interface is also used as the output port for audit messages (including from the remote control channel) which can be fed to 3rd party log management and protective monitoring systems.

Finally, the solution can incorporate the optional Garrison Transfer Appliance (providing Silicon Assured Content Sanitisation technology to support copy-and-paste and printing) and integration with 3rd party content security platforms such as sandboxing or Content Disarm & Reconstruction which can provide a transfer gateway for file import.

GARRISON

Email info@garrison.com

UK telephone +44 (0) 203 890 4504

US telephone +1 (646) 690-8824

www.garrison.com

CD00000213v1.0-UK - September 2018