GARRISON

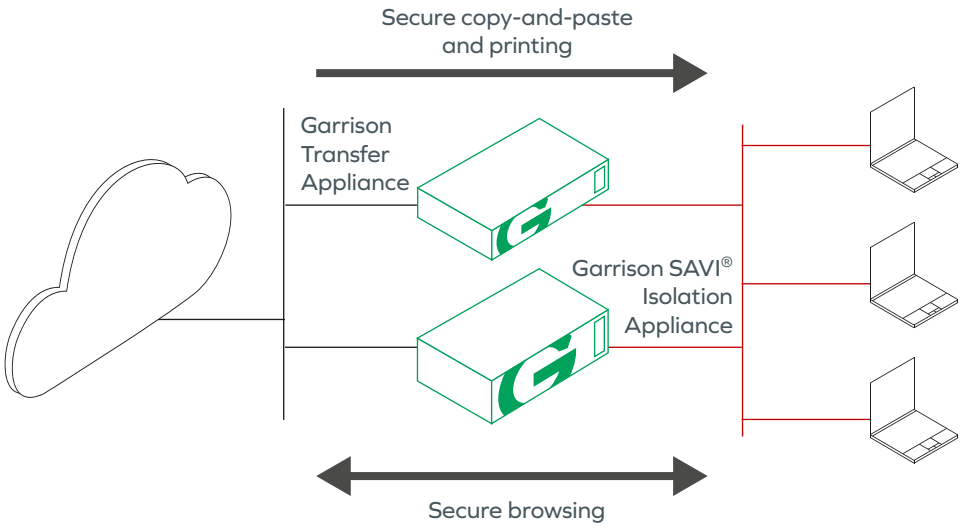
Extending Garrison SAVI® with the Garrison Transfer Appliance

Extending Garrison SAVI® with the Garrison Transfer Appliance

Garrison SAVI® users can safely browse to websites which would otherwise be considered too risky to access. But for security reasons, the base Garrison SAVI® capability provided by the Garrison SAVI® Isolation Appliance (GIA) does not provide the ability for users to copy and paste from web content, or to print it. Great care must be taken when enabling such functionality, because a malformed clipboard entry, or a malicious print job, could be a vector for exploitation and malware.

The Garrison Transfer Appliance (GTA) is an add-on product for Garrison SAVI® which provides sanitisation for text and image copy-and-paste, and for printing. Like the GIA, the GTA exploits the power of hardware-level security to provide import sanitisation in accordance with the UK National Cyber Security Centre's guidance on Safely Importing Data[1].

Note that the GTA does not provide support for importing files or other complex data types. To support file import, contact us to learn how Garrison SAVI® can integrate with a range of 3rd party content security products to enable easy and secured download of web content to a user's endpoint.



Inside the Garrison Transfer Appliance

To deliver text and image sanitisation, the GTA exploits the power of Field Programmable Gate Array (FPGA) silicon – the same silicon that is used to deliver the Hardware Security Enforcement Fabric (HSEF) within the GIA. Like conventional processors, FPGA chips are programmable – but where conventional processors are programmed with software, FPGA chips are programmed with raw (fixed function) digital logic circuits.

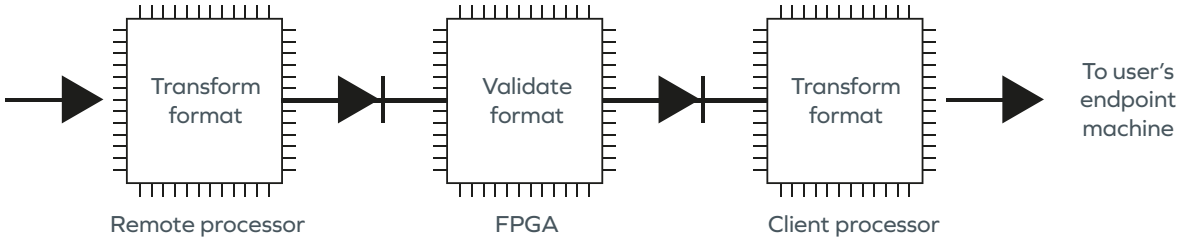
Widely used for prototyping silicon designs, and increasingly finding uses within High Performance Computing, FPGAs are also used to deliver high-assurance security functions. Because FPGAs are programmed with fixed function digital logic rather than software, the range of failure modes – and hence the opportunities for exploitation – are much smaller.

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

For precisely this reason, FPGAs have long been used to construct government-grade cryptography devices for scenarios where software-based cryptography cannot be trusted.

The GTA combines processors and FPGAs to deliver a mixed mode device that combines the flexibility of software with the security of fixed-function digital logic:

- Software running on a conventional "remote" processor chip is used to transform text and images to an easy-to-validate format
- Fixed-function digital logic running on FPGA chips is used to validate the transformed format and ensure it has been sanitised
- The transformed format is transferred from one "remote" physical processor chip to another "client" physical processor chip using fixed-function digital logic in an FPGA, ensuring that there is a complete protocol break with no network connectivity between those two processor chips
- Software running on a "client" physical processor chip converts the format back to the desired format for delivery to the user.



Beyond text and images

Garrison does not have plans to extend use of the GTA to cover complex file types. However, the GTA will be used to support other lower-complexity transfers. These include:

- URLs, for example for link redirection to a secure Intranet site or cloud service that cannot be accessed using Garrison SAVI®. A maliciously formed URL could pose a risk to the user's endpoint machine: the GTA will use FPGA-based validation to ensure that the URL is safe before sending to the endpoint
- SAML AuthnRequest messages, to support SAML2.0 authentication for sites where the web server (SAML SP) is only accessible using Garrison SAVI® but the SAML Identity Provider (IdP) is only accessible from the user's physical endpoint
- Other tokens to support integration with 3rd party content security platforms where a complex file is being downloaded to the user's endpoint. In many cases a token representing the content inspection or transformation "job" needs to be transferred to the user's endpoint so that it can then retrieve the results of the inspection or transformation.

Security assurance

Garrison will be happy to share more detailed design and security testing documents under NDA to support security assurance work. Please contact us for further information.

GARRISON

Email info@garrison.com

UK telephone +44 (0) 203 890 4504

US telephone +1 (646) 690-8824

www.garrison.com

CD00000229v1.1 - November 2018