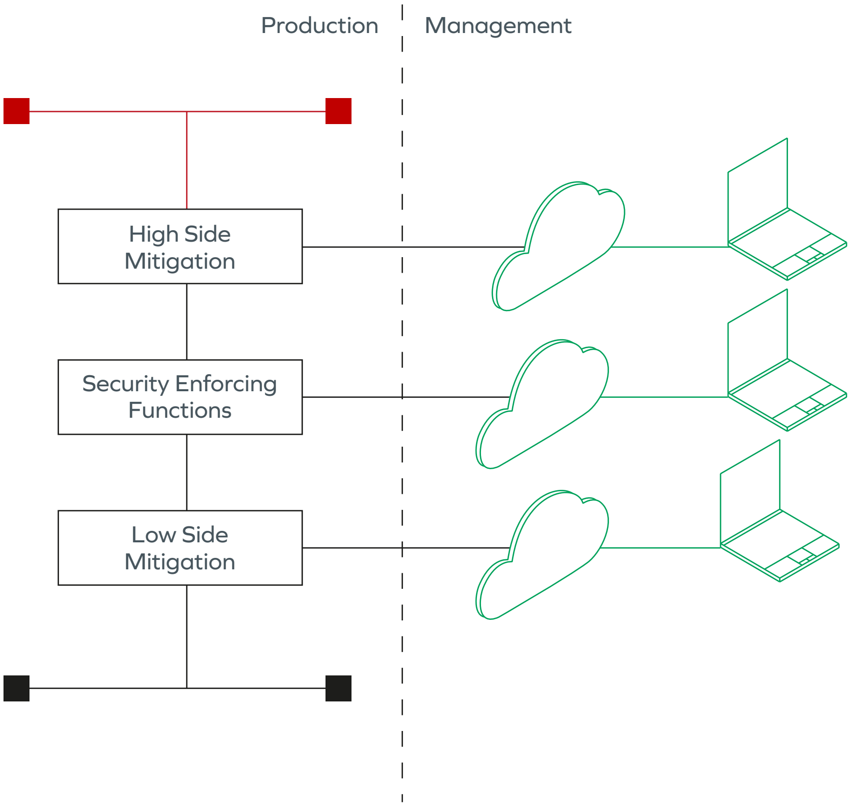
GARRISON

Garrison SAVI®

CDS Gateway Management

Introduction

Cross Domain Solutions (CDS) include a range of architectural approaches and associated technologies for realizing them. However, all the architectures do share some common features, i.e. a trusted/high side, an untrusted/low side, one or more security enforcing or risk mitigating components and an associated number of supporting components. All the physical and virtual components of the solution need to be managed and the cross-domain nature of the environment traditionally means that the management infrastructure also needs to be kept separate. This model is inherent in the need to maintain the integrity and therefore the security of the end to end solution.

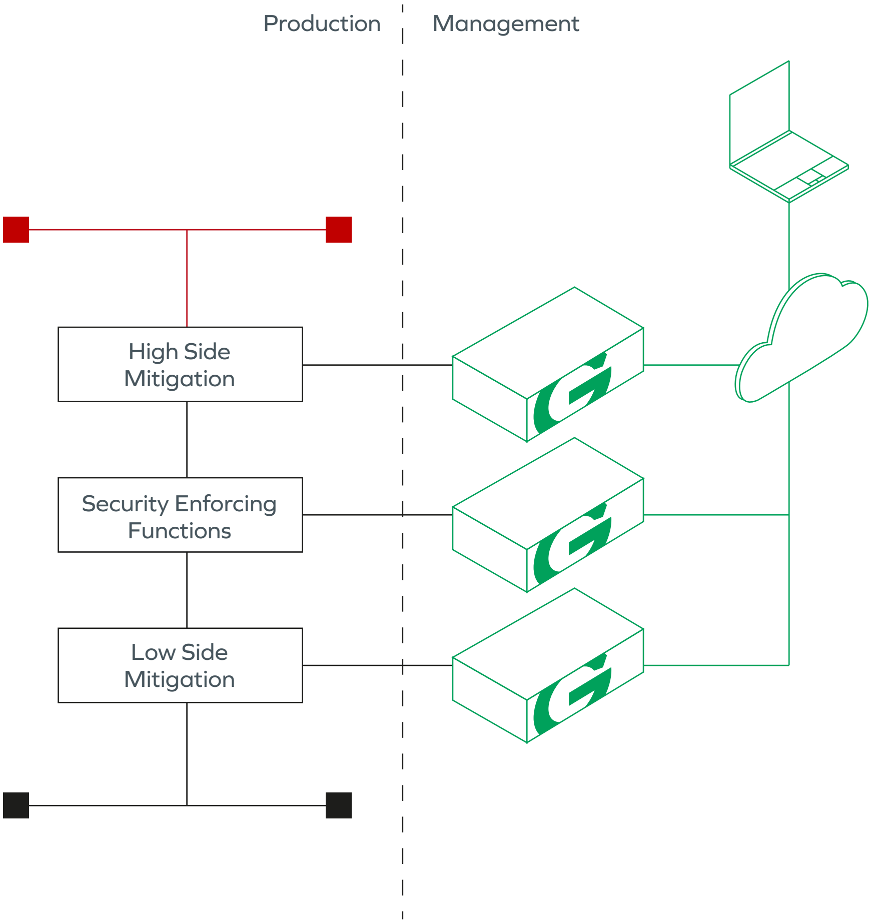


Creating the management environment for a CDS gateway that meets security requirements has always been technically inefficient, generally expensive and invariably sub-optimal for the system manager/operator. The inefficiency comes from the need to deploy completely separate physical infrastructures for each tier of the CDS (three or more), as does the expense. The challenges for the manager/operator are having the desk space to house the multiple terminals and moving between the separate instances in order to perform their tasks.

GARRISON

A Different approach to Management

Using robust isolation technology allows a central management workstation to safely reach across and into all aspects of a CDS gateway. This allows you to collapse a minimum of three separate tiers of management infrastructures down to one within the data centre and coming out from the data centre.



Reliable isolation technology has to use hardware rather than software for the security enforcing functions in order to ensure maximum strength of mechanism as well as providing suitable performance and value for money. Garrison provide the only commercially available, hardware-enforced isolation technology.

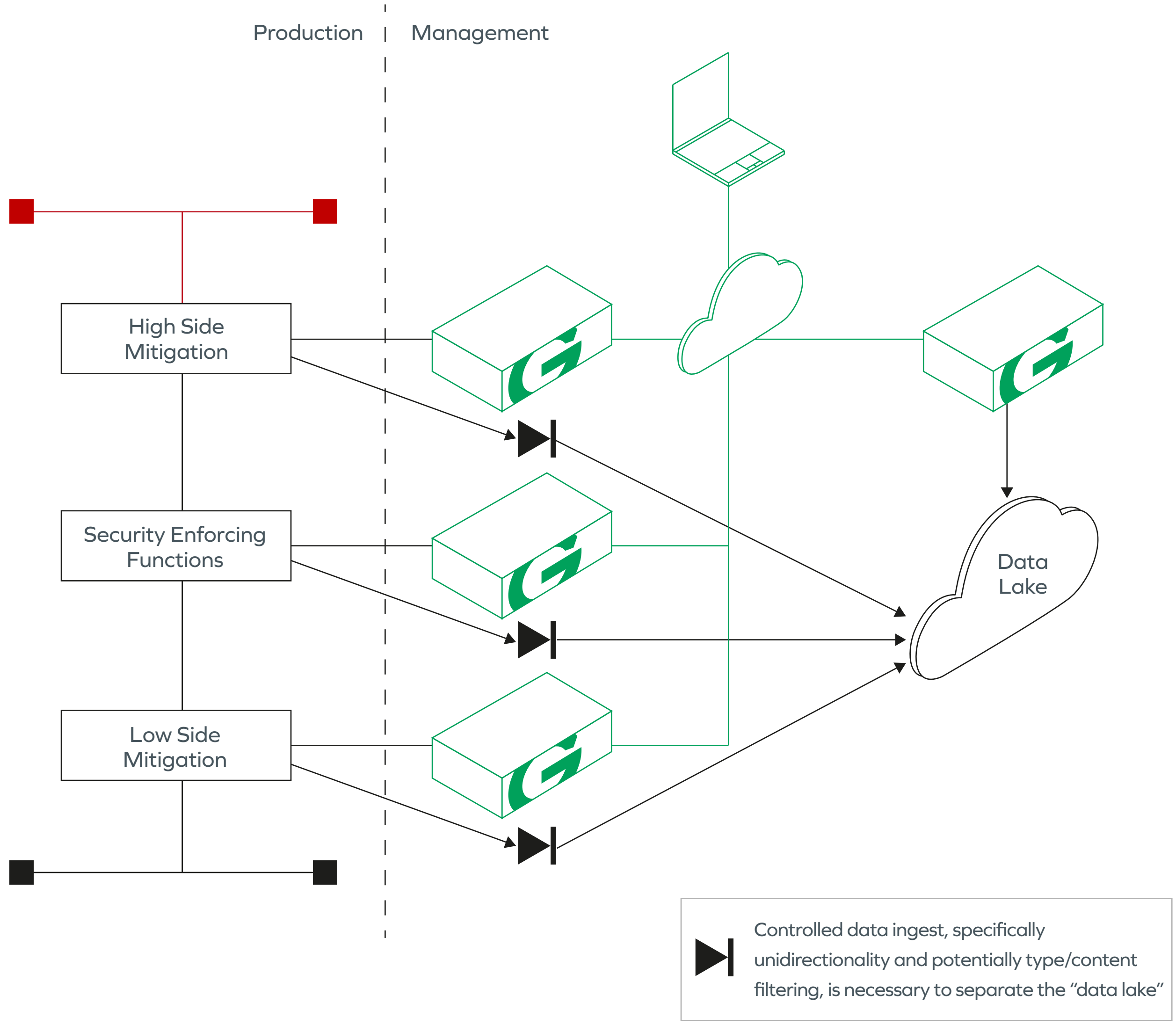
The Garrison appliance delivers support for a range of management functions based on, for example: SSH, RDP, HTTP/S

Garrison provides a robust, hardware enforced protocol break to ensure that there is no way for data or malware to escape any of the differing tiers and get into the management environment. Garrison also ensures that only fully audited keyboard and mouse events can pass from the management environment into the differing tiers – to actually perform the remote management and control. All of this maintains complete separation from any of the production traffic into, out of or through the CDS.

The model is readily extensible if the CDS architecture is more complex, requiring a greater number of management tiers.

Extending the concept to include monitoring

Robust isolation also allows a management workstation to access an aggregated monitoring solution, also without risk to itself or the rest of the infrastructure.



▶| Controlled data ingest, specifically unidirectionality and potentially type/content filtering, is necessary to separate the "data lake"

A fundamental challenge with aggregated monitoring is that the "data lake" tends to be at the highest classification of the combined systems being monitored, the "data lake" is also at risk of being contaminated in accordance with the lowest trust system being monitored. The risk of contamination can be partially mitigated by enforcing type/data controls in series with the unidirectional enforcement (hardware-based data diode).

It is therefore, essential that anybody accessing the "data lake" does so securely to prevent any threat escaping and with full visibility of the actions that they carry out in order to protect the sensitive data.

The Garrison appliance provides a way to reach into the "data lake" from the management infrastructure while keeping both environments isolated. This access may be to the web frontend for an instance of Splunk, or a VDI platform hosting a range of complex tools for all sorts of different analysis and reporting. The Garrison appliance is agnostic of the function and focuses on enabling the analyst to have secured access.

GARRISON

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

www.garrison.com