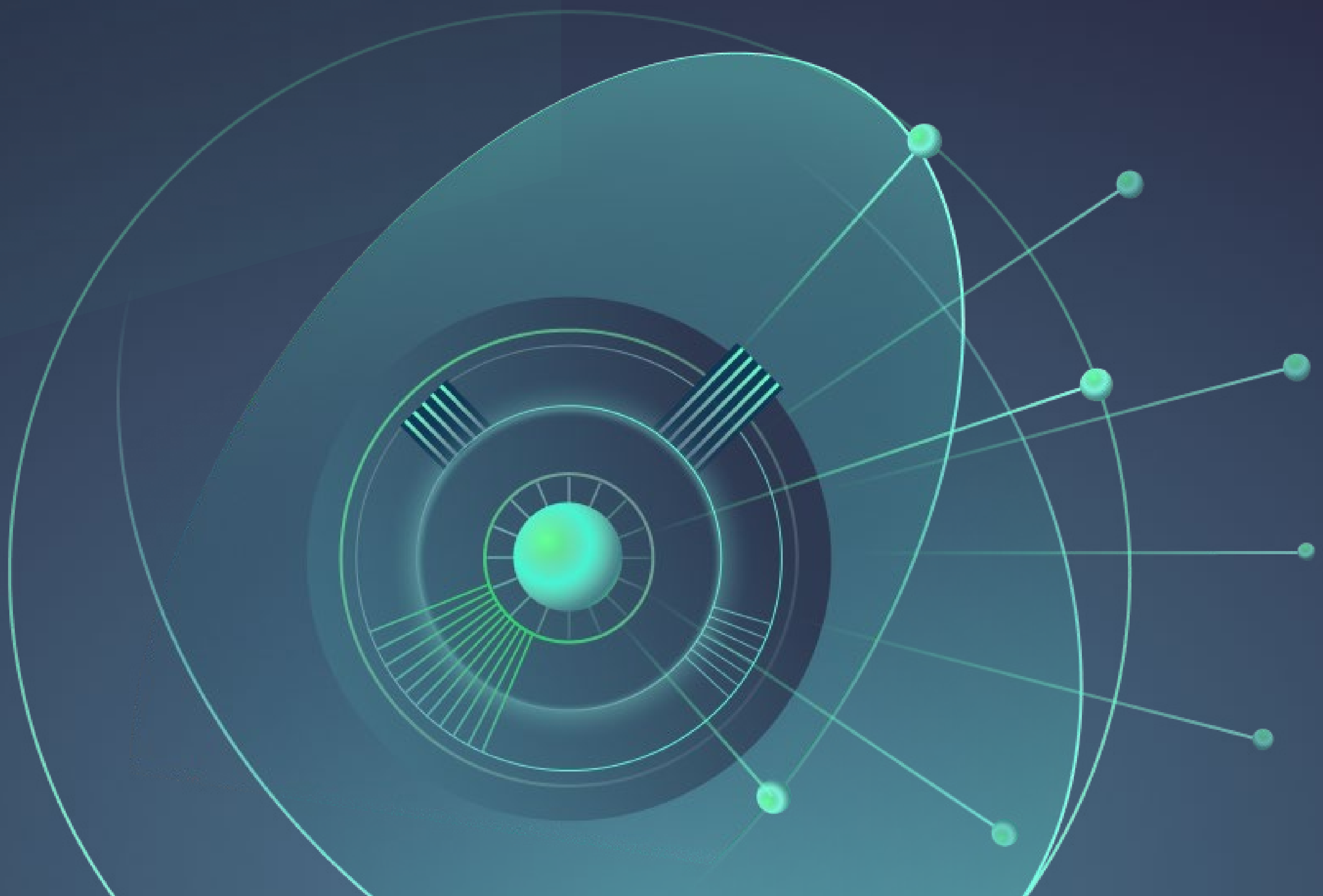
GARRISON

Multi-Domain Operations

Hardware-based Cross-Domain Access
Whitepaper



Today’s operational forces require access to the right information from the right source in real-time.

Historically there have been a number of cross-domain access and cross-domain transfer solutions that have been used to attempt to meet this requirement. However, the currently available access solutions have to date not been robust enough to connect to High Threat Networks (HTN), while the existing transfer solutions have been unable to cope with the complexity of the new and emerging data sets.

INTRODUCTION

A plethora of networks, ranging from the very sensitive, to the highest of threats, from the trusted partner to the necessary collaborations, or even the open Internet, causes huge challenges for legacy approaches:

- The right information is hidden in vast quantities of data that changes constantly and is widely distributed;
- The right sources are increasing in numbers, are on higher threat networks/systems and are produced by an increasing range of tools;
- Traditional gateways are unable to safely filter and quickly transfer these wider information sets;
- Traditional network defenses are inadequate to protect against risks from connecting higher threat networks; and
- The speed of operations and volume of information are expanding, while the value of the information diminishes as it ages.

Users need to be able to access, view and search data in real time in its source/native environment. They then need to be able to transfer necessary information. The promise of being able to transfer ALL data to a location for immediate analysis has never been delivered.

In addition, the challenge of transmitting data for the operational force is that much of the data is in a format that cannot be sufficiently filtered according to the standards of the National Cross Domain Strategy Management Office (NCDSMO) and therefore cannot be effectively transferred to sensitive environments. Current software-based technologies cannot pass information assurance requirements as they are simply not secure enough. As a result, the operational force is unable to access mission critical information due to a level of risk that is just too high.

It is also often incredibly challenging to provide analysts and decision makers working in classified environments with essential data collected from multiple untrusted sources. These sources are often acquired from High Threat Networks (HTN), impacting the ability to connect to them and meet mission requirements.

For the maintainer, the need for information and connectivity to HTNs drives a requirement to manage and monitor trusted and untrusted infrastructure in a safe way.

A new approach to multi-domain operations, such as a hardware-based cross-domain access solution, is therefore required to address the following needs:

- Connecting the operational force to the right network, system or sensor;
- Allowing operational forces to reach into and access any data source, in real time, in its native environment using native tools;
- Providing ultra-secure cross-domain access as the main enabler and allowing cross-domain transfer to be used more selectively, reducing the burden on legacy gateways and allowing key information to move faster and more securely;
- Enabling the maintainer to safely manage and control a complex, multi-domain infrastructure.

DEFINING THE NEW APPROACH

Challenges

Several key dimensions must be considered when leveraging data in a multi-domain context:

Access - the center of gravity of data (volume, velocity and location) makes it hard to reach

Integrity - what happens to the data when it is processed in traditional gateways

Timeliness - how much delay does "accessing the data" introduce

Connectivity - the risk associated with joining high threat sources to high value sinks

Edge - the need to deploy and operate AI/ML across the battlespace

Management - how to maintain and operate the underlying infrastructure

Flexibility - the need to quickly connect to and consume new sources

Environment - considering strategic HQ, theatre HQ and forward deployed HQ

Partnering - the need to operate in a flexible coalition environment

Many of these challenges are manifested in today's familiar working environment, requiring multiple endpoint devices and lots of backend cables (see Figure 1).

Figure 1 · Typical Legacy Challenges

In a strategic HQ this adds cost and complexity but is relatively static. In a theatre HQ or other forward environment this cost and complexity is magnified by the need for mobility and flexible deployment. As an example, how do you deliver the required level of access to the range of endpoint devices required to meet the mission need, e.g. mobile computers/pads.

In the background there is also the cost and complexity of delivering adequate cross-domain transfer gateways in support of Multi-Domain Operations (MDO). Furthermore, the hidden cost of not being able to provide the full gamut of necessary access also needs to be accounted for.

The common constraints to implementing solutions within the dimensions described above are:

- The availability of capabilities that meet assurance requirements
- The ability to provide sufficient "speed to value"
- The ability to provide extensible solutions to meet evolving needs

Goals for the operational force

The operational force at the strategic, theatre and tactical edge needs to be able to access data from secure networks without putting those DoD or IC networks at risk.

Situation awareness and decision support needs to be enabled by real-time data from many sources to reduce the time for military resources to be put in harm's way.

The operational force needs a transformational approach to meet the evolving challenges to win in the battlefield of today and tomorrow.

All of these goals and the underlying challenges need to be met in ways that address common issues with high assurance solutions, while being delivered quickly and extensibly to meet the evolving mission need.

These challenges can be addressed, and the key benefits can be realized today but are affected by these three areas:

- **Assurance** - using Commercial-off-the-Shelf (COTS) solutions that allow connection of sensitive systems to high threat data sources while providing a level of hardware-based assurance that is future proof for the NCDSMO Raise-the-Bar (RTB) initiative.

- **Speed to value** - using COTS products to provide high confidence of rapid movement from proof of concept - to pilot - to operational deployment; delivering capability to the operational force quickly without the high risk associated with development from a speculative, low/medium TRL.

- **Extensible solutions** - using a common, extensible high assurance platform to enable a range of differing workflows with the same level of isolation/separation and trust.

By highlighting these elements as key enablers, users will be better prepared for successful exploitation of MDOs spanning all dimensions of MDO (Land, Sea, Air, Space, Cyber, PSEMII, etc.).

Overcoming the challenges

ACCESS

Operational forces are in general already familiar with the benefits of cross-domain access, but they are also very aware of the risks, limitations, and frustrations of not being able to use this technology to access high threat environments.

Providing a hardware-based high assurance cross-domain access solution that offers a previously unachievable level of access can deliver:

- Improved ways of working that can be readily achieved,
- A reduced need to move data and information across domain boundaries,
- The possibility of establishing persistent/flexible/secure/non-aligned collaboration with a broad range of external entities,
- More efficient cross-domain and complex infrastructure management capability, and
- Optimized setup/teardown capability for expeditionary/deployed forces.

Access solutions are required because ingest of all data is not always possible. Some sources are just too large to ingest into a traditional intelligence processing workflow. One has only to look at the public Internet as an example of a far too large and fast-moving data source.

Operational forces require real time access to web-based resources direct from their sensitive desktops to consume filter and present relevant data sources into native environments, where they can use native tools and the power of Cloud-based processing (see Figure 2).

Taking this a step further, for example, from a counter-terrorism perspective it was once the case that the media were often first on the scene, whether that was CNN, Fox, AP or BBC, so every Operations Room had a television on the wall.

Today that could look more like every analyst having "Tweet Deck" running in a window on their classified desktop - and this can extend to any useful web or Cloud-based resource.

In even the most sensitive environments, direct Web access can provide critical real-time information as well as enriching knowledge and decision-making via key online resources (see Figure 3).

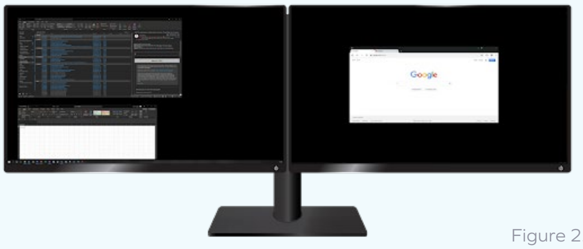


Figure 2.
Web Access on a
Sensitive Desktop

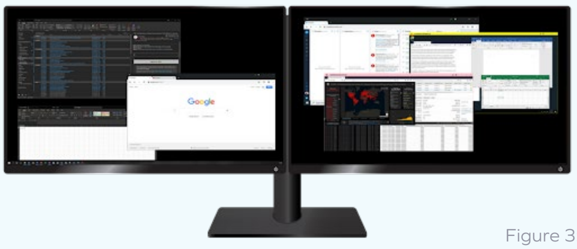


Figure 3:
Multi-Source access
on a Sensitive Desktop

Using ultra-secure web browsing capability to access remote, web-based resources, coupled with powerful search and processing capability provides a way to identify specific, relevant, and necessary information that can then be ingested through appropriate cross-domain transfer pipelines.

INTEGRITY

Cross-domain transfer solutions, by definition, need to process, filter, and manipulate traffic to mitigate the risk of importing malicious content. This very process of sanitization is known to introduce further risk to the integrity of the data as it is processed.

Additionally, moving data from one system to another is known to introduce risk to the integrity of visualizing that information in different applications to those in which it was originally generated, i.e. the semantic meaning of the data is different than intended. This is highlighted in the range of standards associated with data transformation, for example: NATO Standardization Agreements (STANAG 4559, 4545, 4607 & 4609) and Allied Engineering Data Publications (AEDP 17, 18 & 19).

Using ultra-secure virtual desktop capability to directly collaborate in a multi-domain context, in real time, using native applications in their native environments eliminates the risk of transformation and sanitization damaging the integrity of the source data.

TIMELINESS

Trying to bring large volumes of complex, raw data to any sort of aggregation point takes time. Trying to do this across a complex multi-domain environment, through gateways, adds further significant delay, if it is possible at all.

Industry has recognized that it is beneficial and/or necessary to shift the paradigm and instead take the processing to the data to regain the speed-to-value in a distributed enterprise. This is one of the key aspects of edge computing and distributed machine learning. However, shifting complex processing to the edge is not a panacea to the problems.

Using an access-based model to provide analysts with ultra-secure reach into these distributed environments so that they can manage and monitor the deployed tools is essential to the successful delivery of a positive outcome.

Enabling this real-time access from highly sensitive networks into a broad range of high threat environments allows the operational force the freedom of maneuver necessary to overmatch peer and near-peer adversaries.

CONNECTIVITY

MDO requires the operational force to be able to operate across boundaries of classification but also across other boundaries, for example collaborating with Law Enforcement Agencies (LEAs), other government departments, Non-Governmental Organizations (NGO) and directly with the general population either overtly or covertly.

Being able to do this at pace, and without putting the DoD and IC networks at risk requires the ability to connect those secure networks to other high threat networks both in a strategic, proactive, and planned way, but also in a high-tempo, reactive and temporary way.

A model for delivering Internet and therefore Cloud-service connectivity provides a way to work with any Cloud-enabled Organization rapidly and dynamically, on their own terms with potentially little or no need to reconfigure sensitive networks/systems.

Using high assurance, hardware-based, cross-domain access technology allows previously unachievable levels of connectivity between a much wider gamut of systems/networks, enabling the operational force to reach across the boundary and consume essential content in real time.

EDGE

An extension of the Timeliness and Connectivity elements described above is the provision of a mechanism that allows analysts to reach down/forward to the "edge" of the battlespace to control, orchestrate or "nudge" distributed capability (e.g. machine learning) without the need for multiple workstations on their desk, or the need to actually deploy personnel forwards.

A capability that enables the secure access of resources at the edge delivers a direct force multiplier effect, allowing high value resources to operate in a number of different environments near-simultaneously.

MANAGEMENT

Creating the infrastructure necessary to enable MDO results in an additional burden for the J6 function. The increased number of systems, gateways and enhanced segmentation, over and above the traditional complexity of the C4ISR estate requires evermore manpower, skillsets and time to manage.

Securely managing this complexity is also a valid use case for deploying ultra-secure access technology, allowing a maintainer to reach in orthogonally to achieve their mission goals (see Figure 4).

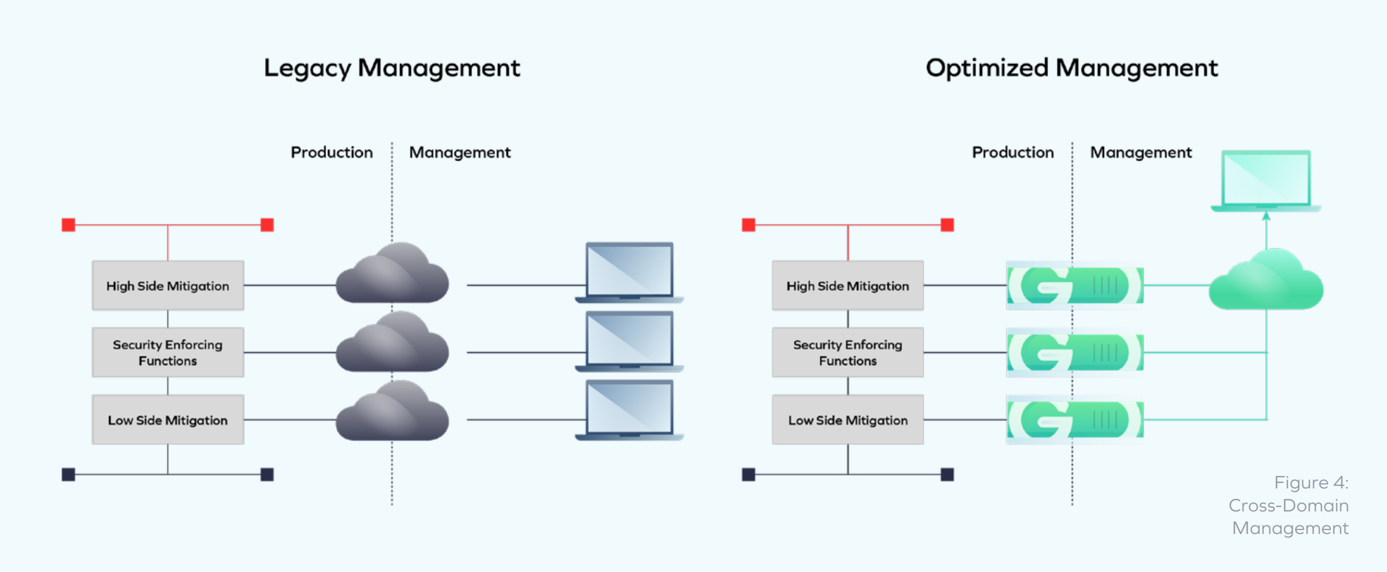


Figure 4: Cross-Domain Management

The maintainer burden is reduced by being able to do this from a single machine, without the risk of this endpoint being a pivot point for a malicious actor to move between layers, segments, or domains within the managed infrastructure.

FLEXIBILITY

Establishing an approach to connectivity that breaks possible connections down into a smaller number of manageable sets, each of the sets having a similar level of risk, allows predefined patterns to be designed, tested, authorized, and held ready to deploy to meet a specific need.

For example, NATO Federated Mission Network (FMN) Civilian Military Information Sharing (CMIS) is a technical challenge, but from an access point of view, any civilian information system for any NGO could be treated as a single high threat environment that is itself a subset of all civilian Cloud-enabled information sources.

Providing a standard pattern for connecting to any Cloud-enabled Organization would also allow on-demand connection to all such Cloud-enabled Organizations on a per-mission basis.

The pattern for such a connection can then be designed, tested, and authorized once, but deployed every time a mission requires connection to such a Cloud-enabled service.

The categorization of such connections could be defined based on the risk of accidental data exfiltration via such a cross-domain access solution. This naturally correlates with the processes and technology employed in the remote organization to control/protect themselves.

This has the additional advantage that the operational force is collaborating with the civilian entity using the native civilian collaboration environment rather than as an explicit interoperability connection between civilians and the military.

ENVIRONMENT

Operational forces are already familiar with the infrastructure rationalization that comes from implementing cross-domain access solutions.

Ultra-secure video-based isolation takes these benefits a step further by ensuring that the only data on the sensitive system that the client is using to access the remote environment is a stream of encrypted, compressed video frame deltas in one direction and encrypted keystrokes and mouse movements in the other direction.

No actual sensitive data is transmitted to or across the client-side network and no residual data is retained at the end of any given cross-domain access session.

PARTNERING

As with the “Flexibility” model above, defining a number of standard connection patterns for the most likely classes of Mission Partner Environment (MPE) that are compliant with the Secret and Below Releasable Environment (SABRE) architecture can provide a technique for rapidly establishing such collaborative connections in a deployed environment as well as within a strategic HQ context.

This concept assumes that any given expeditionary mission will have a defined Community of Interest (CoI) and that the potential partners will fall within one of the predefined sets as constrained by mission parameters (nature of operation, geography, etc.).

DELIVERING THE NEW APPROACH TODAY

Garrison has created a unique, ultra-secure, hardware-based, COTS, cross-domain access solution that is designed from the ground up to meet the new NCDSMO hardware-based RTB requirements and to reach data that previously could not be accessed or transferred (see Figure 5).

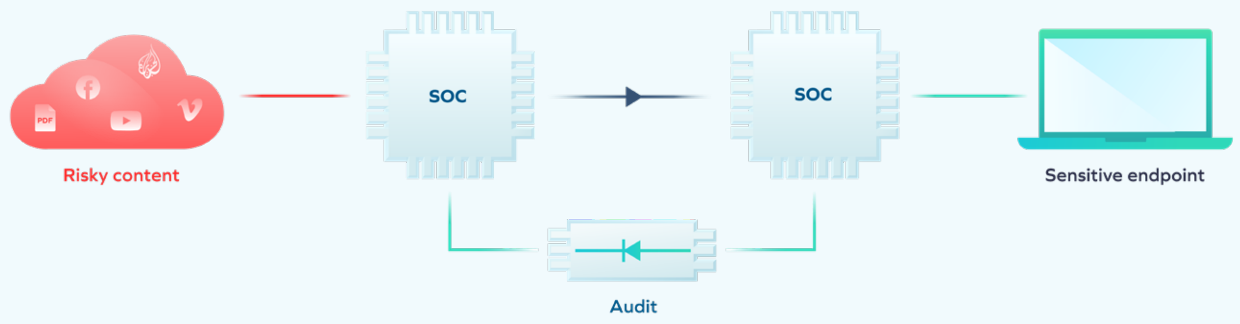


Figure 5: Garrison SAVI - Silicon Assured Video Isolation

To meet the requirements for accessing High Threat Networks (HTN), Garrison leverages two technologies:

- Hardsec (www.hardsec.org) uses Field Programmable Gate Array (FPGA) technology to implement robust Security Enforcing Functions (SEFs)
- Silicon Assured Video Isolation (Garrison SAVI®) uses the dedicated hardware of Arm® system on chip processors to implement a robust isolation pipeline

Garrison SAVI® (Silicon Assured Video Isolation) is a patented hardware-based technology that turns risky content into a known good format, in this case raw pixels. Garrison SAVI® uses two Arm® chips arranged into pairs in a Garrison Isolation Appliance (GIA), as shown in this diagram, to enforce at the hardware level that nothing other than pixels can reach the user's endpoint. The left-hand (low side) chip runs a browser, VDIi client, or other applications designed for consuming web content and turns this risky content into pixels.

The pins of that Arm® chip which would normally be connected to a display are instead connected to the camera input pins of the second (high side) Arm® chip, ensuring at the hardware level that content is transformed and verified before being delivered to the high side.

These pairs of chips are dynamically allocated to users as required and are returned to a guaranteed clean state after each browsing session to ensure no malware persistence across sessions.

In order to enable a fully interactive browsing session, another communications channel between the chips is required to carry keyboard presses and mouse movements. This channel is implemented using FPGA and hardware technology called "hardsec". Among other things, hardsec is used to ensure that two key security controls are applied to this other communications channel, to mitigate the risk of data loss. Firstly, by ensuring that the flow of keyboard and mouse data is rate-limited, so that if data is exfiltrated this way, it is a relatively small amount of data (essentially, what could be typed out at human typing speed). And secondly, by producing a complete audit feed of the data, encrypted for privacy reasons, which can be used for behavioral analysis or for forensic investigation.

What this creates is an interactive session, such as browsing or VDI, between users on a sensitive network and a riskier environment, with only a video representation sent to the users.

In cases where users must pull back mission essential data, Garrison also provides a mechanism so that it can be integrated with cross-domain transfer products.

Where real-time access (across domains) to complex data on High Threat Networks is mission essential, then a hardware-based access solution is the only option.

Garrison is working across the US community to highlight how new, powerful workflows can be enabled using the same ultra-secure platform, with a reduced burden of design rework from use case to use case.

That range of use-cases is based upon:

- Accessing the web from secure environments
- Browsing down from classified domains
- Secure access to collaborative workspaces
- Management of complex secure infrastructures
- Secure remote working
- Isolating third party applications
- Enabling a single workstation for multi-domain operations

RISING TO THE CHALLENGE OF MULTI-DOMAIN OPERATIONS

MDO presents many challenges to the operational force. Meeting these challenges must be done securely, rapidly, and easily for the huge range of data sources that influence awareness and decision making in MDO. Technology, policy, and stakeholder awareness are coming together to provide users routine access to information that was once impossible. Missions require this new and innovative approach, and this solution is available to be evaluated and implemented.

It is time the operational forces take back control of the data they need - ensuring it can be accessed quickly, inexpensively, and securely without relying on movement of the data. This supports expansion of cloud adoption and realizes even greater benefits of cost and flexibility.

Garrison stands ready to support the analysis of your mission needs, to identify relevant use cases, and to work with you to help you build a successful solution to enable MDO.

GARRISON

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

www.garrison.com