ViON MLS-e System Implementation

White Paper

November 2015

196 Van Buren Street | Herndon, Virginia 20170 | (571) 353-6000 | (800) 761-9691 | vion.com

ViON MLS-e System Implementation

MLS-e (Multi Level Security-ecosystem) is a centralized storage and compute solution that can properly store and process data from multiple security levels on one combined system. This simplifies the process of segmenting unclassified, secret and top-secret information allowing users to share this data quickly and securely for improved decision making. ViON Corporation, in collaboration with Seagate, and engineers from the CSCF have implemented an MLS-e capability for demonstration purposes in ViON's Herndon lab that demonstrates this powerful capability, particularly tailored for the DoD intelligence community.
The purpose of this white paper is to:

- Demonstrate the impact that MLS-e can have in transforming storage capability for classified environments
- Highlight how storing and processing multi-tenant data can be simplified and delivered more efficiently with MLS-e
- Illustrate how MLS-e is handling multi-level datasets
- Provide supporting documentation of the superior capability of the ViON MLS-e solution

Why is MLS-e Important?

The need for multi-tenancy is an ever growing problem for storage of classified information, particularly for the larger intelligence agencies. Data is processed from multiple sources and at various classification levels and compartments; and thus distributing and storing it requires a large outlay of redundant equipment. This results in increased cost, maintenance, and complexity for operators, and due to the networking restrictions between security levels, can present challenges for gaining timely access to vital Intel data. This is particularly troublesome for imagery applications that require low-latency to function optimally. MLS-e can help solve this problem, or greatly diminish the impact by securely allowing multiple classification levels and compartments to be unified on a single storage and compute architecture.

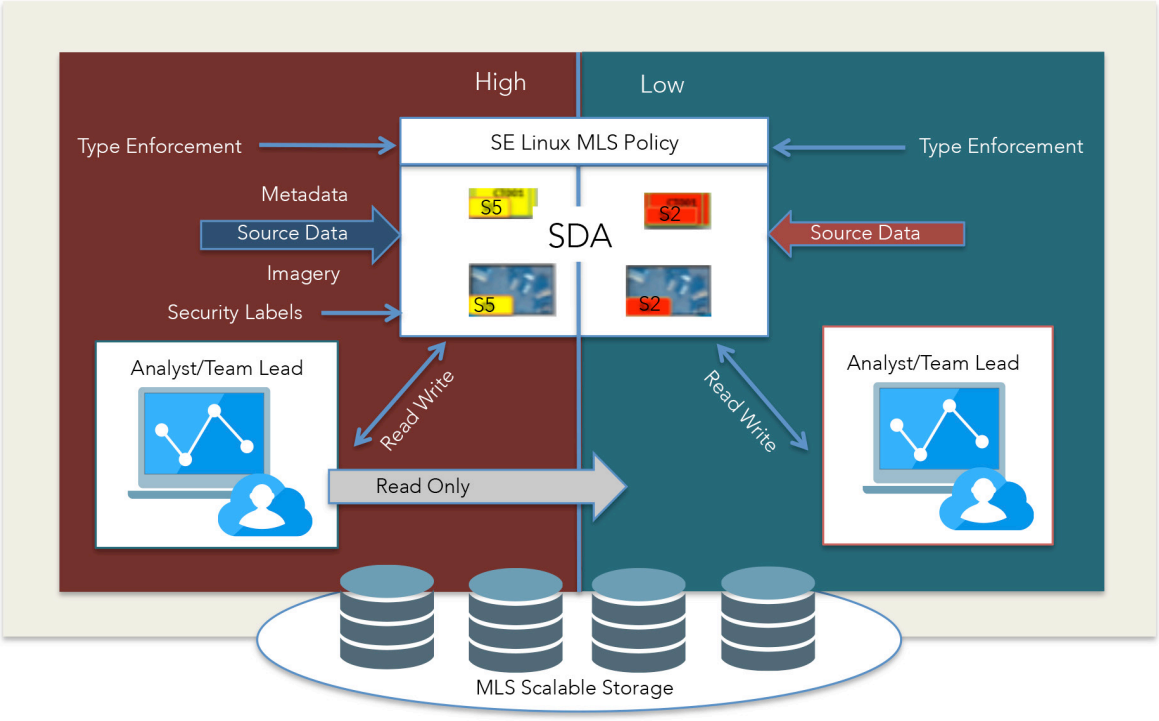

Figure 1. ViON MLS-e Demo Overview

What is ViON doing with MLS-e?

The ViON demonstration applies MLS-e to an imagery workflow process. ViON has expertise in this area, as our engineers understand the system processing requirements needed to fulfill these demanding mission profiles. Often analysts are working with high-resolution still or motion imagery data at various classification levels, and must go through a cumbersome process to move data between these levels. In the ViON MLS-e Demo, we process imagery data in real-time to the MLS-e system on both classification levels, and demonstrate how analysts connecting to the imagery catalog at each level can view only data appropriate to their access. More importantly, the demo illustrates how analysts at the higher-classification level can "read-down" to the data on the lower level. ViON is also designing new scenarios where an MLS-e aware workflow can be employed to help system security administrators to more easily move data down appropriately--while still enforcing 2-man review—and/or rapidly create new compartments.

SELinux Security Enforcement:The Heart of MLS-e!

The heart of the MLS-e system is inherent in its strong security controls. The nature of the SELinux operating system requires that type enforcement and access to file system objects be validated through a mandatory MLS security policy. Therefore any software (eg. process/daemon) that will interact with SDA shared files must be authorized against these access controls. In the case of a file or web crawler (see more on crawlers and MLS-e in a later section of this paper), this means that the user account used to run the crawler is validated against the normal Linux discretionary access control, as well as the mandatory controls imposed by SELinux MLS. To perform user authorized indexing of data therein (i.e. row/cell-level security), it would be optimal that the crawler application and index store also be MLS or context aware.

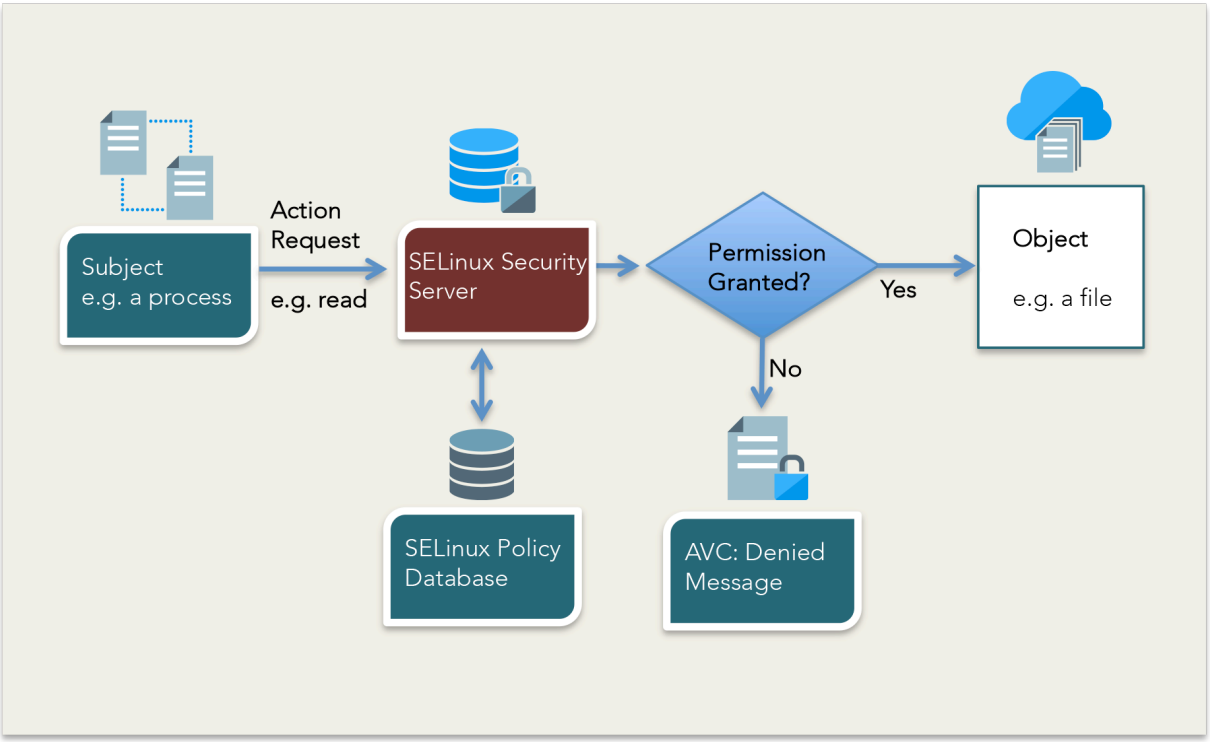

Figure 2. SELinux Type Enforcement Overview

This presents a challenge for software that is not readily portable to the SELinux OS, but can be overcome in other ways, as we will demonstrate in this White Paper. The basic function of an MLS capable system is to ensure that each user is validated for a specific level of access. The model employed is called Bell-LaPadula, which allows for a user to have access at or below their level of security authorization, and exclusive access to compartments to which they have been assigned. Users below that level are not authorized to access anything above their approved access level, and have no access to compartments to which they have not been specifically granted rights. Access is assured through the use of labels that are applied, controlled and verified on all data processed by the operating system.

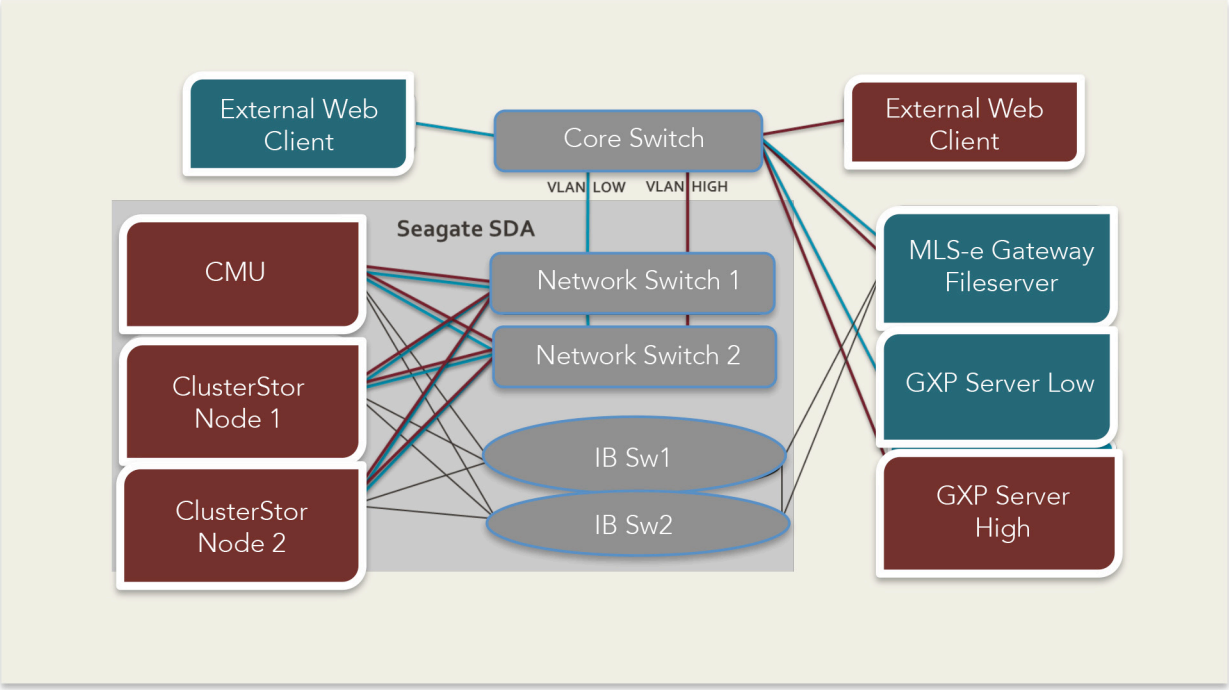

Figure 3. MLS-e Network connections

System Configuration:

The ViON MLS-e configuration includes 2 application servers to simulate both a high side and low-side processing system--"high" or "low" used as generic terms for higher or lower classification levels (see drawings below). VLAN access on the network is used to separate the 2 simulated security enclaves. The role of the GXP Xplorer application servers is to crawl and index the file system presented through the SDA (at the appropriate level). The SDA itself is not directly accessible to these servers. The secure file system that the SDA presents is shared through a Gateway server also running the SELinux operating system. The Gateway server is connected to both the internal storage network as well as high/low side Ethernet networks, and enforces access controls and network policy restrictions to the shared data stored on the SDA. The gateway server runs Samba in an MLS-e aware configuration. This provides controlled Windows file sharing access to GXP at each level, allowing only properly verified users on a specific network to gain access to the classified or compartmented information allowed to them.

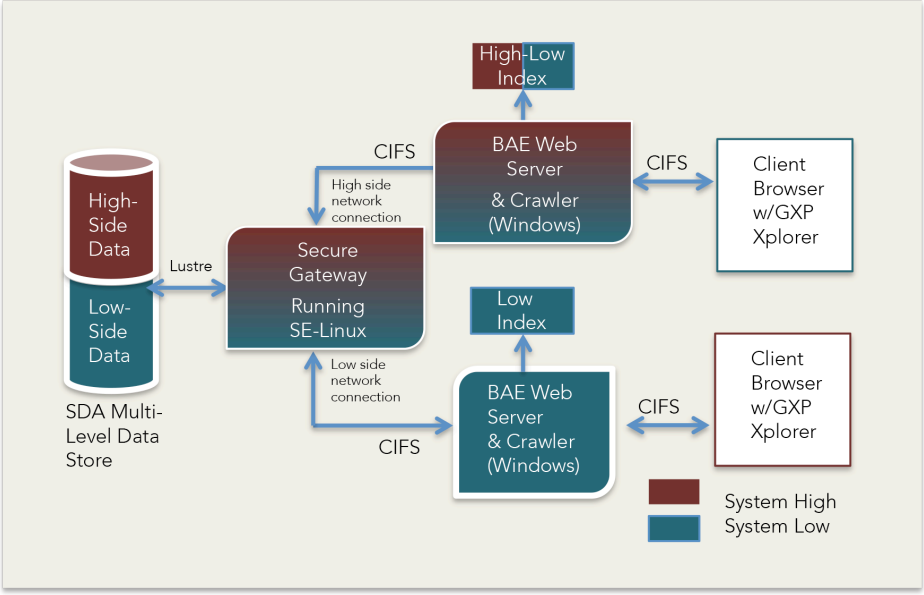

Figure 4. High-level Logical Drawing

Data Crawlers in an MLS-e Environment

It is anticipated that MLS-e system environments will require some form of crawling/indexing software that is able to index and present customer data files to client-side users, preferably through a browser interface. The basic requirement includes the ability to search, view and potentially manipulate relevant information stored on the SDA (Secure Data Appliance), and download and upload data sets (at the appropriate security context). In the case of the ViON demonstration system, we use the GXP Xplorer application to perform this crawling function, but are considering other software options as well.

Crawling/Indexing Software and Third Party Application Integration

A crawler or "web crawler", spider or bot is a software process or service that can traverse a virtual directory structure on a server, the content of which can then be indexed by a search engine. Many open source and commercial products are available that do this (too many to include a full listing in this paper). Web crawling is performed via http or file system request methods and requires a URL (or list of them) endpoint reference of the intended web document directory hierarchy to crawl. At the least, it is expected that file names are included in search index results, but many software products can also index file contents as well. Some web crawler software described below include products like Crawl Anywhere (open source), or SharePoint (Microsoft) which is a full collaborative document sharing environment.

File system search crawlers or indexers are more specialized software in that they are typically built as part of a client/server application or embedded in the OS. They index files/folders on a local or remote device mount and produce results internal to the application. They are often designed only to run inside a LAN environment or on a local computer. There are tools and applications that perform this kind of indexing and also in some cases produce a web view of the results, but are intended to be used within that application workflow (i.e. imagery analysis). They may be too cost prohibitive, resource intensive, or not a good fit for other workflows. Other products provide a developer SDK or framework to create file system-to-web index views (i.e. dtSearch) for these purposes. It is also important to note that many applications will not be MLS-e aware, and may require some integration effort (create the appropriate SELinux policy).

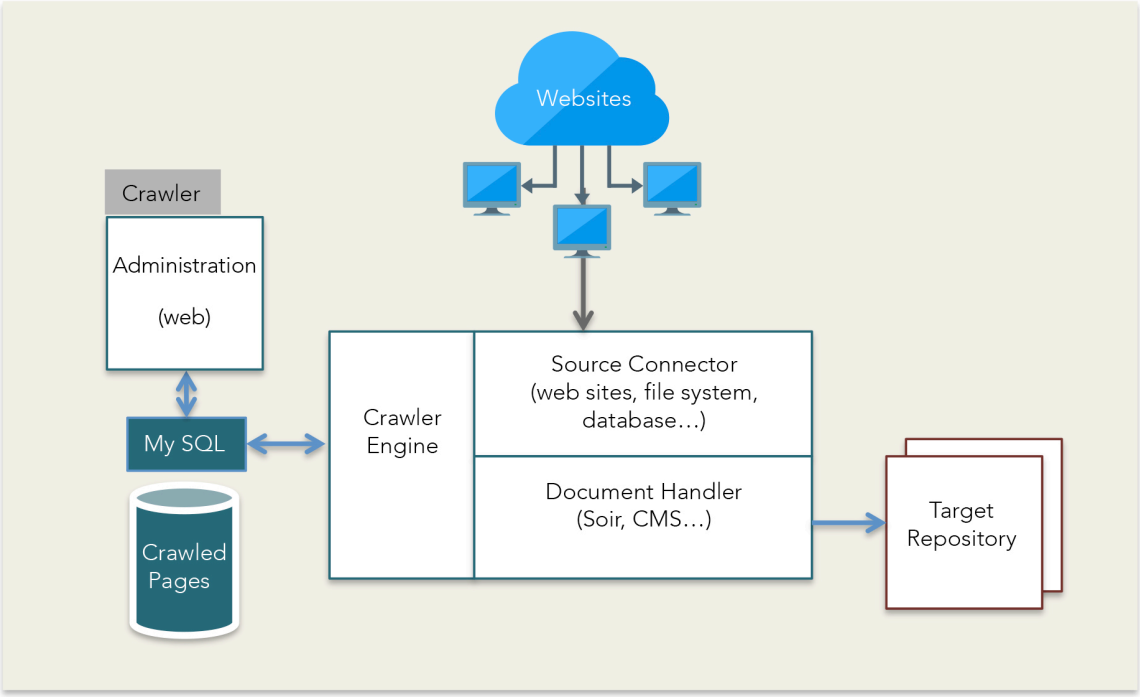

Figure 5. Web Crawler architecture (i.e. Crawl Anywhere)

In the ViON demonstration, we utilize a crawling function of the GXP Xplorer application running at each security level. Xplorer can monitor the network storage mounts to be able to crawl, index and present the data at that appropriate level. This demonstrates secure data consolidation and multi-tenancy in a real-world application environment: A user connected via a web browser at the high-side level can view the imagery products on both the high-side network (read/write) as well as products on the low-side (no write down); while users on the low-side can only view the low-side products to which they are granted access.

Intelligence Exploitation Applications with File Indexing/Crawling Features:

The following is a list of several software products made specifically for the indexing and exploitation of imagery data ingested or stored on a local/remote mount. They also include a web component that can index and present file system data in a web view. In future test iterations, it is ViON's intention to test and verify these solutions with our MLS-e capability, particularly with motion imagery applications.

- GXP Xplorer (http://www.geospatialexploitationproducts.com/content/products/gxp-xplorer)-Windows-based imagery application suite
- Pixia HiPER STARE (http://www.pixia.com/solutions/hiper-stare/)-Windows-based wide area imagery application suite
- Textron Systems Remote View (GeoCatalog-http://www.textronsystems.com/products/geospatial/elt-extensions/geocatalog)-Windows-based imagery applications suite
- 2D3 Catalina Media Server (http://www.2d3sensing.com/catalina#sthash.nkHBXfwf.dpbs)-Motion imagery media server
- MAAS (Multi-Int Analysis and Archive System-http://www.gd-ais.com/Products/ISR-Imagery-Analysis/MAAS)-End-to-end full motion video application suite

Open Source Web Crawlers:

In the case where only a simple web crawler is required, an open source solution may be a better fit. The Apache web server has been integrated in an MLS-e aware configuration.

Name Language Platform
- Heritrix Java Linux
- Nutch Java Cross-platform
- Scrapy Python Cross-platform
- DataparkSearch C++ Cross-platform

OS-Level Indexing and Other Software Options:

- Windows Search-Included as part of the professional operating system, Windows search can be configured to index local and remote shares.
- Linux/Unix Search-Gnome and other desktop environments also include a file search capability similar to that found in Windows, and other search utilities are available in repos for download.
- dtSearch-Software SDK and product solution specifically for automating file system search and access to indexed data through a provided web portal.
- Sharepoint-Windows collaboration environment for group sharing of Microsoft file types.
- Crawl Anywhere-Search Engine/Web crawling software product (Freeware).

MLS-e Challenges and Benefits:

MLS is not a turn-key proposition for every use-case and application, many of which remain to be fully tested. The original design for the SDA is one specifically tailored for super-computing (a large scale out cluster of storage nodes). The severe security restrictions required to implement several levels of classified access for multiple applications, users, networks and storage volumes is not trivial. ViON believes that subject matter experts familiar with both the current ISR environment and with requisite knowledge of SELinux will be required to help customers implement this type of solution properly. ViON is ready to partner and lead these efforts with DoD customers to bring this solution to reality. Some key DoD use cases that could benefit greatly from a consolidated MLS-e architecture are listed below:

- Classified customers who process and store a large amount of imagery data at multiple security levels.
- Customers who have to frequently downgrade or move data between classification levels.
- Customers who need to rapidly create new compartments for storing or segregating data.

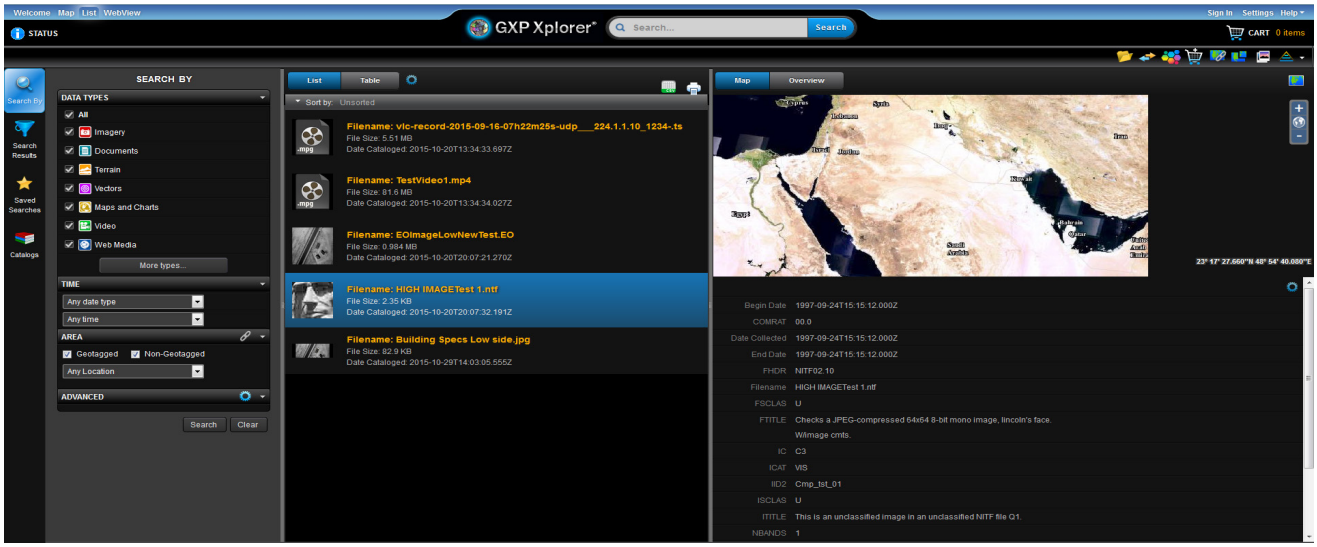

Figure 6. ViON MLS-e Live GXP Application Demo Provided at GEOINT 2015

Conclusion

The ViON MLS-e environment is well suited to help the DoD and U.S. government to meet the demanding requirements of storing a large amount of multi-tenant data in the most secure manner. The MLS-e system can help a customer protect vital data while consolidating and downsizing existing system stove-pipes.

To learn more about how ViON's MLS-e can help you manage you unclassified, secret and top secret information in a single environment or to schedule a demonstration, contact Mike Meister, Director of Motion Imagery Solutions or Nate Adcock, Solution Delivery Consultant at ViON.