WHITEPAPER

Cross Domain Solutions 101

EVERFOX

Cross Domain Solutions solve for being able to safely and securely connect to isolated networks. These networks are often air-gapped, controlled, or secret networks.

For example, these may be networks controlled by the DoD or the intelligence community, such as SIPRnet or Red networks. They could be isolated networks that contain IoT devices such as sensors or controls of critical infrastructure: water treatment facilities, manufacturing control systems, security devices such as cameras or badge/door lock systems. Firewalls are fantastic at defending the perimeter of high threat networks, but they may not provide everything you need to complete the mission.

It helps to put things in the perspective of airport security. Think of the airport as an air gapped, isolated network— something controlled or secret.

Firewalls function like a check-in desk at an airport—they are designed to pass data through them, performing a credential check (identification, as an example). A very baseline inspection is performed, and you can check some items not authorized for carry on.

A Guard is implemented when transferring data into or out of this network. It is designed to verify data at the byte level as it passes through the guard. It is specifically designed to stop data—similar to a security check. It is providing the authority to remove data from the stream, such as an item that is banned,like a flammable liquid. So, where a firewall looks at credentials, a guard looks at everything on your person and in your suitcase and restricts items from passing through.

The restrictions, or filters, are customized based on the requirements of the mission.

Why CDS is like Airport Security:

Data Guard, Next-Gen Firewall, Data Diode Working Together

Firewall

Airport Check-in

- → Verification of ID & proof of travel (show your boarding pass and ID)
- → Basic checks performed
- → Can check items not authorized with carry-on

Guard - Data Transfer

Security Checks

- → Deeper inspection than ID only
- → Fine-grained, detailed inspections of personal belongings, such as a hand swap for residue detection
- → Authorized to remove unauthorized/banned items

Diode

Airport Exit

- → One-way path of exiting the airport terminal security zone
- → No security inspections
- → Cannot reenter without going through security checks

Can leverage multiple solutions for defenses in depth

In some cases, requirements call for Data Diodes. They act like a turnstile exit at the airport—it's a one-way path for data to go through that does not allow data to re-enter, and it must go through a Guard (the Security check) to pass back into the airport. Think of high threat networks (like NIPRnet or the general internet)—it can prevent activities and threats such as malicious code from communicating back out to the original network.

Lastly, attaching to these isolated networks was completed traditionally by creating separate edge devices (desktops, laptops) properly configured with the security infrastructure to guarantee proper connections into each network—and housed within the four walls of a controlled building or space. However, with increased field and remote work, driven by the pandemic, the costs to do this can skyrocket. So, the ability to connect to multiple isolated networks with proper assurances from a single device can provide the fourth leg to the table that meet many organizations' needs on flexibility.

These items (edge devices, firewalls, guards, and data diodes) in conjunction provide a deeper level of security than a firewall alone. However, the complex requirements and intricacy of these system becomes clear when relating it to the type of data being accessed or transferred within an isolated network.

A great example is large satellite pictures/weather information. Those images are terabytes in file size–and ensuring that the content being transferred doesn't have any malicious code embedded into them is key to secure operations. That security check point must be efficient to be effective. Another example is video files often the mission requires people in different areas of the world to examine video data, created by a drone or a camera. Transcoding video (compressing it for faster transfer) as well as filtering that data for safety and security is often a requirement. Transcoding changes the file type, which can limit a virus ability to stay within a file. However, those video streams need to be transcoded and filtered in real time or near real time, because it could impact various missions.

If you are dealing with new or complex requirements based on the nature of the data you need to access or transfer, or the nature of the security of the mission at hand, a Cross Domain Solution can provide the security needed. Let's expand on scoping a cross-domain solution space, assessment of vendors and services providers, migration of Cross Domain Solutions.

Fundamental Considerations when Evaluating Your Approach to Cross Domain Solutions:

There are many considerations for implementing a new Cross Domain Solution, evaluating solutions based on U.S. NCDSMO Raise-The-Bar requirements, or potentially migrating from your current solution to a new one.

Many organizations are shoring up security in the wake of remote work or work from anywhere requirements and this has increased attack surfaces and the complexity in which security is delivered. Empowering organizations to perform in today's global environment demands a shift in how you consider security around isolated, controlled, and classified networks. In the constant state of change that has become our new normal, government off-the-shelf solutions and one-size- fits-all approaches to access and transfer solutions may not keep your environments secure, provide the support required, or enable you to complete your mission. Let's explore how to take a proactive stance on evaluating a Cross Domain Solution now and for the future.

4 Foundational Cross Domain Solution Criteria

Organizations are experiencing increased scrutiny of implementation of cross domain solutions, due to recent data and security breaches, and the ever-expanding threat landscape. Accreditation, such as Raise-The-Bar, is starting to broaden as a requirement across more systems, networks, and agencies. To update, expand, or create a new Cross Domain Solution, its critical to evaluate your organization's needs, and understand these criteria in detail.

1. Technical Capabilities Required

What does your organization need to do with the data that resides on an isolated, controlled, or an air-gapped network? In other words, does your organization need to view data on a multi-level network, also commonly known as access this data? Or does your organization need to move that data to somewhere else, or merge it with data on another isolated network? What are your requirements? Consider whether you solely require access needs. Are you only viewing data such as satellite images, documents and assessments? Or do you also require transfer capabilities, or moving data, in addition to access.

Examples could include compiling information and research from different networks for analysis or investigation, or for a data scientist to model. You might also need to pull images or video together to centralize an investigation.

Moreover, are, timing and latency needs important for the data? Do you require real-time or near-real–time access and data transfer? Or is a short delay acceptable and will not impact the mission?

2. Current Environment, planning for now and future

What does your current environment look like? Is it all in a traditional enterprise data center? Or are you cloud-enabled, or even multi-cloud enabled? Are your end users typically working within the office, do they need an ability to access controlled or classified networks from their home? Or are they in the field environment that might require a very tactical solution? Evaluating today's needs and looking a few years out at how your environment might shift can help you plan for near-term needs.

Beyond your environment, thinking about costs and funding is key to proper implementation. Historically, government-created solutions (GOTS or government off-the-shelf solutions) for some internal agency needs within cross domain were developed, and the perception is that utilizing this solution in your agency is free.

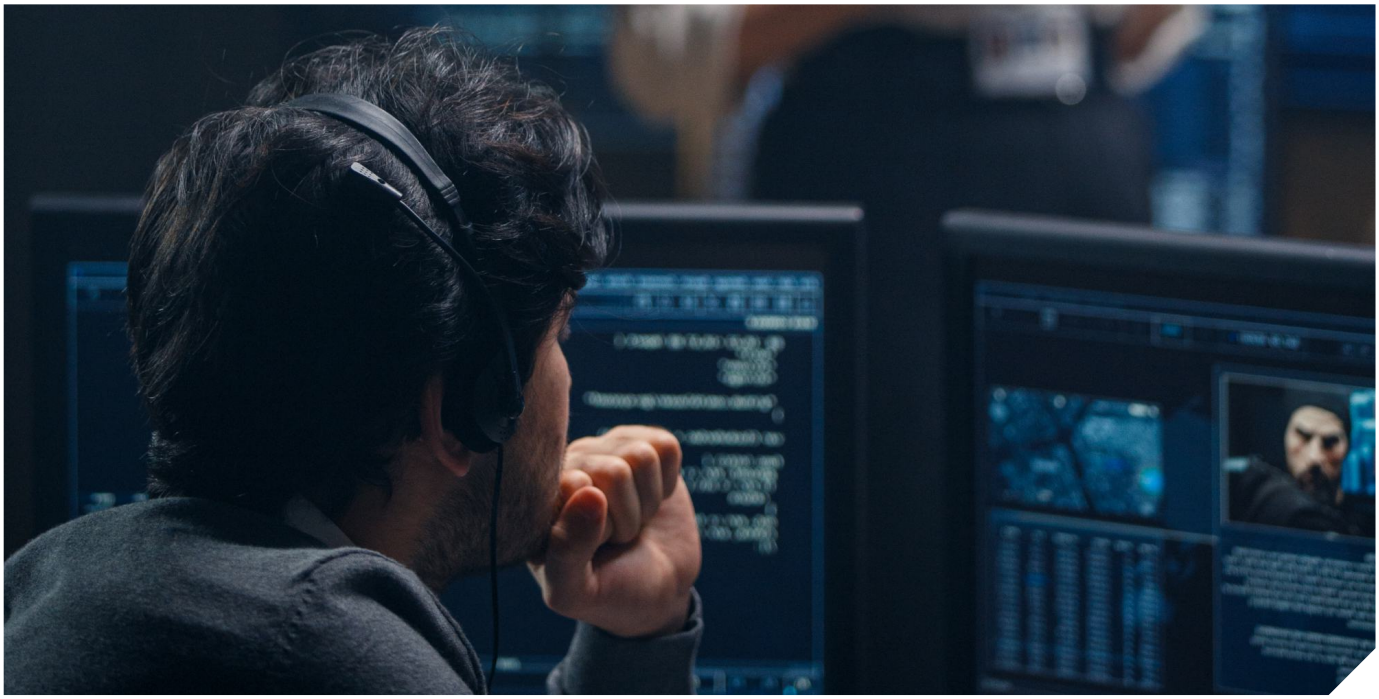
However, the complexity of customization (tailoring to your needs), upgrading, and maintenance, the picture of cost is not straight forward. COTS (commercial off-the-shelf) solutions are by and large the best choice for most solutions.

3. Where does the data you need to access or transfer reside?

Often, having a picture of where critical data currently resides is key to ensuring a mature security posture. High threat networks - such as the internet, the NIPRnet, or green networks may be places where your organization connects or accesses information. Based on the networks your organization needs, would your solution be subject to RTB Guidelines, or would those guidelines be good guidance? Assessing this information in partnership with the larger organization completes the picture on what and where you need to provide protection.

4. Lifecycle and Long-Term Management Picture

Considering the long-term picture of your organization's needs, the resources you have currently can paint the path forward with Cross Domain Solutions. Your organization may be subject to accreditation or auditing post installation. Are you looking for a partner to manage, or does your team want to be trained to manage it long-term? Scoping the resources available and the timing of installation is key to selecting the right technology provider and services partner.



13 Critical Questions to Ask When Evaluating a Cross Domain Solution

After gathering a picture of foundational criteria for a Cross Domain Solution, engaging with vendors to assess options is a natural step forward in your process. Below is a way to frame your approach—with key questions to utilize when engaging with a vendor to assess capabilities and services, so you can identify the key candidates that are right for your organization and the mission at hand.

1. Does the Cross Domain Solution support both Transfer and Access of Data?

It is critical to understand the current CDS solution's capabilities—as there are vendors and solutions that only support accessing data. Today, your organization might need access capabilities, but they might grow into needing transfer capabilities in the future. Understanding the solution capabilities today and tomorrow is important to evaluate working with a long term partner in this space. And timing of these capabilities is critical.

2. Does the Cross Domain Solution support modern email or print needs?

A major driver for CDS for senior leadership may include shifting to a modern work environment—viewing all email on a single device, or simplifying printing of critical, secret, or controlled data. Often, moving to CDS includes a reduction of desktop and printer hardware, simplifying management of devices, and cost savings on future hardware.

3. Does the vendor support your VDI Environment, or does it support more than 1 VDI Environment?

VDI is a critical component to access solutions within Cross Domain. Best-of-breed CDS vendors support both Citrix and VMware VDI solutions, which keeps your organization out of having to lock into a single VDI vendor.

4. Does the vendor support your data and timing needs?

If your organization needs to transfer data, the types of data you are considering, and the acceptable latency expectations are important considerations. Regarding data types, is it structured data such as database files, or video files? Is it unstructured data, such as word, PDFs, or PowerPoint documents? Also, given the mission at hand, what kind of latency is acceptable? Does it have to be real-time or near real-time, or is a longer time frame more acceptable? It is important to pick a vendor that makes purpose-built solutions that transfer different kinds of data efficiently and effectively.

Selecting an all-in-one style solution may not ensure the solution can work in the acceptable time frame, or cause problems in implementation.

5. Does the vendor support your current and future infrastructure environment needs?

Different entities are moving to the cloud at different rates. Ensuring that the vendor can support the enterprise/data center, cloud service provider environments such as AWS and Azure, and tactical environments. is a good indicator that the vendor can support you today and as your organization grows or shifts in the future.

6. Does your vendor provide ROI and help you estimate cost savings if you are consolidating in your current environment?

Key to understanding the total cost picture for a solution, is working with a partner that can showcase costs and cost savings to any consolidation that is enabled through their solution. Understanding if their process for engagement includes consolidation estimates is key to projecting total cost of a project and showcases the experience this vendor has with CDS.

7. Does the vendor solution support proper handling of data that comes from a high-threat network?

If you are transferring data from areas such as the internet or the NIPRnet, it could contain any number of threats. Best practices are to select a vendor that has diode technologies—technologies that enable one-way transfer (OWT) of information. Purchasing a CDS from one vendor and a diode from a different vendor can cost you valuable time to implement and, in some cases, require additional customization services to make the total solution work.

8. Does the vendor have solutions found on the NCDSMO List?

Some vendors have waivers currently or do not carry solutions currently listed by the U.S. NCDSMO. Often times, it's critical to implement with a partner that has gone through independent lab-based assessment testing (LBSA) which produces a body of evidence that can be utilized in your documentation to validate the level of assurance needed for stringent security requirements on multi-level networks.

That documentation and body of evidence contains the critical detail needed for accreditation to connect to multi- level networks.

9. Does the vendor provide centralized management capabilities?

Managing multiple guards is an expectation for a large or complex organization or can become a critical need over time. Some vendors require connecting to guard devices individually to update filters and configurations, which can leave room for errors from device to device and be time consuming. It's important to consider large enterprise management capabilities for your CDS and whether your vendor has these capabilities. Having the tools and people accessible to enable centralized management can drastically impact your time to value on a CDS. Lastly, configuration of CDS can be needed post-installation. You should understand if your vendor can provide expertise on filtering optimization—and if those individuals cleared to be onsite to assist. If not onsite, in what capacity can the vendor support you?

10. How does the vendor enable updating the end user devices that connect to CDS?

This may only be central to your consideration if the end user base is deployed across a large space geographically or a large user base. For example, you may need to provide a single device with multi-level network access for 10,000 to 100,000+ end users. You may have expectations that updates to end devices must be accomplished in days vs. months and deployed from multiple locations or from a single location worldwide. That picture impacts your ability to services your end user base and resources needed to update devices.

11. Does the vendor have an ability to scale out?

Understanding scale of your environment and being able to ascertain if the vendor can meet those needs is key to success. How many simultaneous isolated or controlled networks or how many domains does your environment need to support vs. how many can the vendor support? How many data flows (single or multiple) can the solution support? If you're looking at a mobile endpoint solution to connect with, how large of an installation would you start with? Is it in the hundreds? Would it need to then scale to the hundred thousands?

12. Does the vendor provide training for your team?

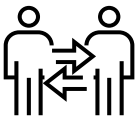
Some organizations build solutions that require an ongoing services contract to manage the technical solution on your behalf. Other organizations offer a choice of providing training to ramp your organization into long-term management of the Cross Domain Solution. You might want to start with a services model, but train and clear your own workforce long-term, which is common. A discussion on training offers can provide a clear picture on options and choices to best suit your needs.

6 Steps to Seamless CDS Migration

As you are assessing your current solution for connecting to isolated networks, it's important to understand where your current provider is with RTB requirements and if their solution is currently listed as approved. Deeper dives into their technology stack, such as assessing the roadmap of new solutions and understanding their approach on the Redundant, Always Invoked, Independent, Non-bypassable principle (RAIN), provides a window into their current and emerging technology capabilities. However, equally important is understanding how the vendor and any partners needed can provide an easy migration path to mitigate risk for your organization.

This is how Everfox provides a seamless migration path for your current CDS solution:

Step 01.



Joint Onsite Assessment

Step 02.

Project Scope & SOW Creation

Step 03.

Deliver SOW

Step 04.

Finalize Project

Step 05.

Execute Project

Step 06.

Post-Installation & Training

Step 01

Joint Onsite Assessment: Level-set on current requirements and goals of the organization, understand the data at the center of the challenge, identify the accrediting authority, and assess the existing environment.

GOAL: Tailor the solution based on the different security risks associated with your CDS requirements and the nature of the mission.

Step 02

Project Scope and SOW Creation: Everfox will complete a detailed design that is customized to the environment and your desired outcomes.

GOAL: The solution will match your objectives and minimize or avoid changes to the environment (or the network).

Step 03

Deliver SOW: Everfox will provide a detailed Statement of Work, including the steps to achieve accreditation. Everfox can provide a wide array of options ranging from an attainable plan to a complete turn-key set of services. This might include capacity or future mission needs, support models, consolidation efforts, and centralizing management to grow with your mission.

GOAL: Clear communication on the scope of the project in detail, creating a clear path to successful completion.

Step 04

Refine SOW/Finalize Project: Everfox will work with you to refine any outstanding open items in SOW before both parties sign off on the project needs.

GOAL: Ensure final details on SOW.

Step 05

Execute Project: For the duration of the project, Everfox will assign a project manager to act as the key point of contact, conduct a site survey, work with the partner to schedule and implement the solution. The project manager will provide support all the way through onsite implementation, training, and onsite accreditation testing.

GOAL: Provide clear communication throughout execution and get the job done.

Step 06

Training & Post Installation: Based on your needs, Everfox can provide services to maintain the solution onsite including: dedicated staff with high security clearance, training your team to manage the solution, or a combination. Everfox can also include semi-annual health checks on an ongoing basis.

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More

www.everfox.com