

Secure Connectivity for Critical Infrastructure

Centralized Management of Critical Infrastructure.

Bringing Secure Visibility to Isolated OT Environments

Critical infrastructure operators are increasingly trying to bring together monitoring, management and analysis across sites that have traditionally been kept isolated for safety and security. This shift creates a need for trusted ways to move information in and out of OT environments without weakening the boundaries that protect essential systems.

Everfox addresses this challenge by combining hardware-enforced separation, policy-driven control, and deep content inspection to enable trusted connectivity while maintaining strong security boundaries between sites.



Challenges

- Gaining central visibility without introducing risk when connecting to isolated sites
- Moving data safely out of OT and updates safely back in
- Supporting modern data flows
- Providing secure remote access without adding software risk

Solution

- Hardware-enforced separation between OT and management
- Deep inspection on every transfer
- Controlled bi-directional data flows
- Secure, isolated remote access with audit

Benefits

- Strong defence against lateral movement
- Assured separation using hardware controls
- Safe, central visibility across sites

Centralizing Management Across Isolated Sites

Centralized management of critical infrastructure replaces the individual management of systems, often spread across physically isolated sites, with a “single pane of glass.” This typically involves a dedicated management network and associated technologies to improve visibility, compliance, and threat response; capabilities that are essential in the face of increasingly sophisticated cyber threats.

However, preserving site isolation while enabling trusted connectivity introduces a significant Cross Domain challenge; the risk of lateral movement between isolated sites, where the compromise of a single site could propagate across the wider environment and result in physical harm, environmental impact or the disruption of essential services at scale. There is therefore a requirement for strict, policy-driven control over how data moves between environments, and robust protection of the information exchanged.

Safe Remote Management and Data Transfer

Remote management depends on dedicated, secure access to each site such that no compromise at the site level can traverse back into the management network. Additionally, remotely monitoring and managing each isolated site will depend on the controlled transfer of operational data such as logs and alerts from Operational Technology (OT) environments into the central management network, alongside the secure delivery of updates and configurations back into those sites. These interactions increasingly follow publish/subscribe patterns, where OT systems publish data outward and central platforms subscribe to it for aggregation and analysis.

Limitations of Traditional One-Way Technologies

Implementing these workflows in OT environments is non-trivial. Traditional one-way technologies, such as optical data diodes, enforce unidirectional flows but do not verify that the data being sent is safe. They can also make it difficult to support bi-directional communications without introducing additional complexity.

Deploying Everfox CDS for Secure, Controlled Connectivity

Deploy Everfox Cross Domain Solutions (CDS) between the central management network and each isolated site to enable secure, controlled connectivity. This approach allows organizations to meet operational and business requirements such as centralized monitoring, data aggregation, and remote management while maintaining assured security boundaries between environments.

A tailored combination of Everfox CDS technologies can be deployed to balance capability, security, and flexibility. The specific solution design will depend on each customer’s operational needs, risk profile, and existing infrastructure, ensuring the right fit for both current requirements and future scalability.

Everfox Cross Domain Transfer

Everfox Data Guard

Everfox Data Guard enables the bi-directional, automated transfer of highly complex data. With deep content inspection and highly granular policy based control over source, destination, and content, Data Guard is ideally suited to Cross Domain data transfer and targets specific security requirements.

Everfox High Speed Verifier (HSV)

The HSV is designed to verify that protocols and, optionally, the data being carried by those protocols are safe to pass on to a software guard and / or on to destination systems. It achieves this using hardware logic implemented in Field Programmable Gate Arrays (FPGAs)

Everfox Cross Domain Access

Garrison Isolation Appliance (GIA)

The GIA uses FPGA technology to help ensure only a valid video stream view of the remote network is transferred to the protected network. It enables users to browse remote web servers, perform management functions using RDP, SSH etc., and connect to remote Virtual Desktop Infrastructure (VDI) environments.

High Level Architecture

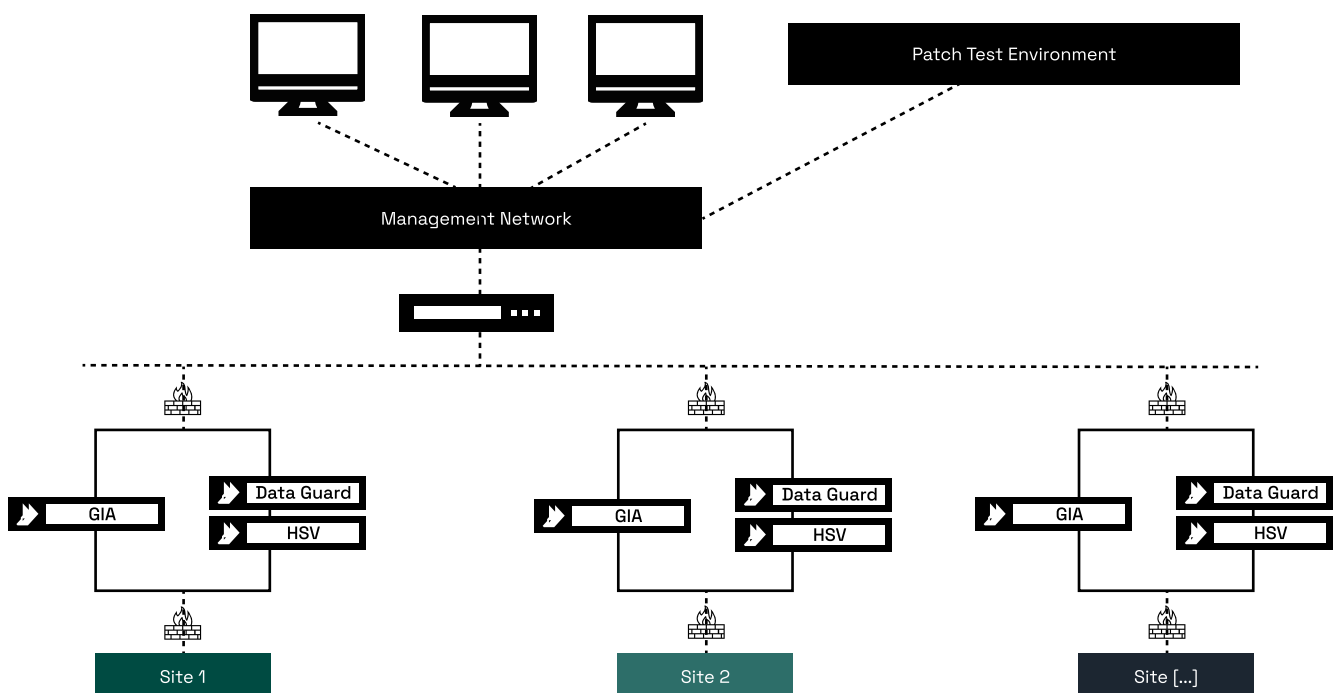
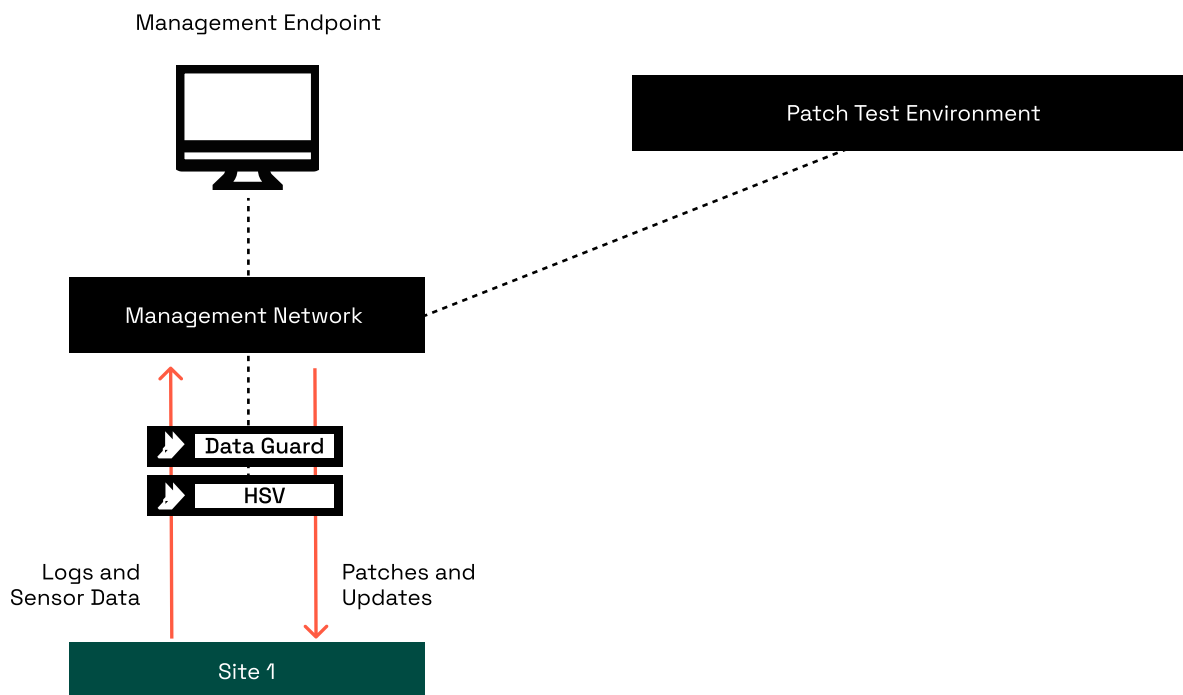


Figure 1

Data Guard and HSV provide the solution's CDS Transfer capability, while the GIA provides a CDS Access capability to enable end users to reach into target environments.

Cross Domain Transfer



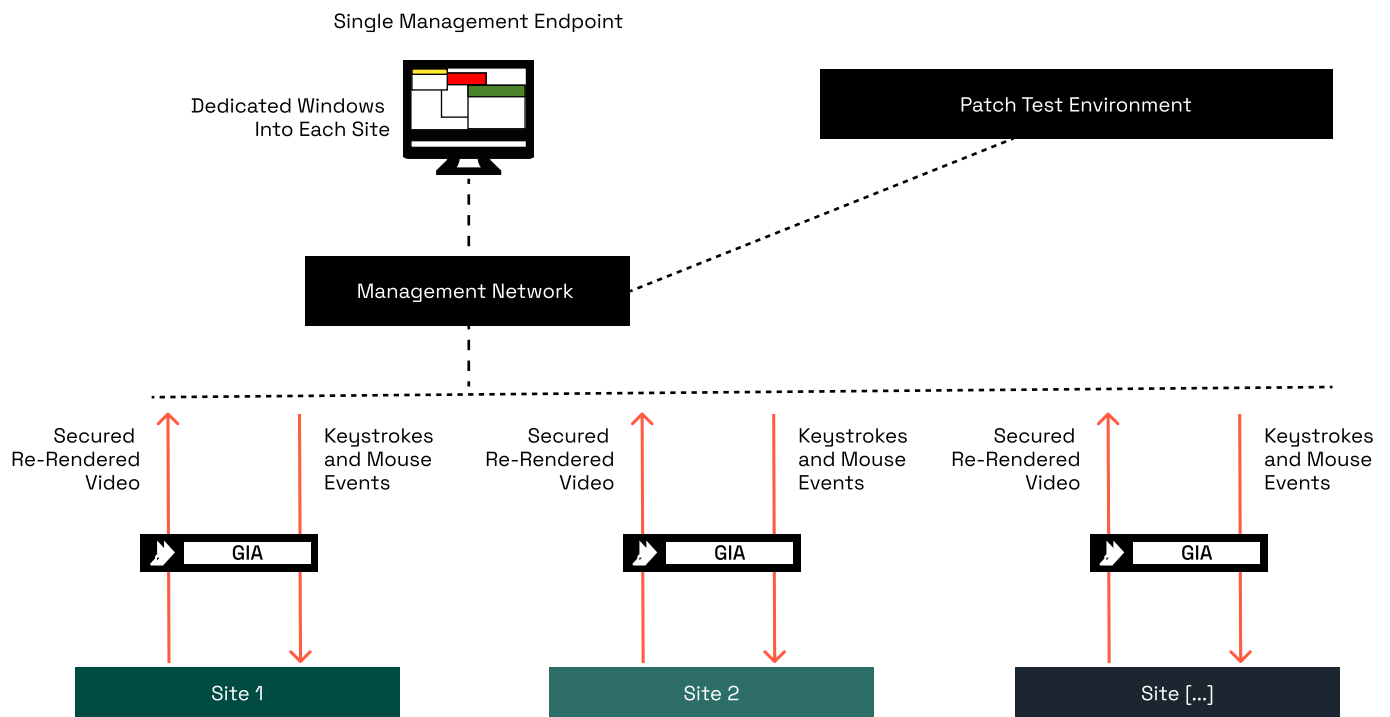
Secure Transfer of Operational/Monitoring Data Out of OT and Patches/Updates Into OT

Everfox CDS Transfer:

- Everfox Data Guard (EDG)
- High Speed Verifier (HSV)
- Hardware-enforced separation and deep content inspection means only allowed data types are transferred
- HSV provides hardware-enforced (Hardsec) flow controls and protection from protocol-level attacks on the target network and on EDG
- Patches / Updates can be tested outside of isolated sites and digitally signed when checked; Data Guard can then validate signatures before accepting files
- Bi-directional protocols can be used across the gateway, allowing publish/subscribe patterns. Bi-directional communications are treated as independent one-way flows, which are enforced in hardware with the HSV
- The ingest of other file types into either the management network or site can be made safe using Everfox Content Disarm and Reconstruction (CDR)

Cross Domain Access

The Garrison Isolation Appliance delivers CDS Access, giving users secure, hardware-isolated entry into OT environments.



Secure Access to OT Systems In Isolated Sites

Everfox CDS Access:

- Garrison Isolation Appliance (GIA)
 - Managing secure infrastructure for critical networks can itself be a huge and expensive security challenge, as well as an administrative burden. The Garrison Isolation Appliance (GIA) provides a Hardsec-enforced capability required to access and manage infrastructure that exists in isolated sites at source, without the risks of software-based remote access tooling or costs associated with physical OT site access
 - Unlike traditional airgap methods or software-based access or Remote Browser Isolation (RBI) technologies, the GIA provides a full hardware-enforced protocol break. This ensures that only raw bitmaps (at 1080p, 60fps) and raw uncompressed digital audio are transferred from the resources being accessed to the end user device
 - The GIA provides a syslog feed which captures user keyboard and mouse activity, providing an audit stream of user activity that can be fed into end user monitoring tooling
- The solution can be configured to control user access to each GIA, ensuring that only authorised users are able to access and manage specific remote sites

Benefits

Secure Transfer of Operational/Monitoring Data Out of OT and Patches/Updates Into OT

The Benefits:

- Using CDS Access alongside CDS Transfer enables both real-time, controlled interaction with isolated sites and secure, policy-enforced data movement, delivering a complete solution without compromising isolation
- Unlike a firewall, which filters network traffic at a protocol level, a CDS provides deterministic, policy-driven control over exactly what data is allowed to cross boundaries, with enforced directionality and deep inspection that significantly reduces the risk of bypass or lateral movement
- Hardware-enforced (Hardsec) separation and flow control that ensures high-assurance protection of access and transfer across the OT/management boundary. The UK NCSC's [Secure connectivity principles for operational technology \(OT\)](#) discusses the importance of hardening this boundary, including the use of hardware-based Cross Domain Solutions
- Everfox CDS can be configured to ensure all users, including non-human system user accounts, are authenticated and authorised to access the CDS and related security functions, i.e. can granularly define who can do what from both the management network and each isolated site. For example, information will not be transferred between respective networks, except where expressly nominated and authorized for transfer





About Everfox

Everfox delivers trusted connectivity to protect the world's most critical environments and safeguard the sensitive data powering decision advantage.

Built for mission - critical operations, Everfox protects what matters most by securing how data moves, how users access it, and how threats are neutralized across every domain. We enable mission speed and secure collaboration across networks, domains, and allies, while ensuring the data powering AI and advanced analytics remains trusted and protected.

We don't just defend systems; we deliver decision dominance.

Learn More

www.everfox.com

© Everfox 2026

About the Author

Marina West

Senior Sales Engineer, Everfox

Marina specializes in Cross Domain Solutions and Insider Risk, designing and delivering capabilities that safeguard critical systems.

Marina works with government agencies, the Defence Industrial Base, and critical infrastructure organisations across the UK, Europe, and Asia-Pacific, helping them enhance their operational effectiveness while maintaining the highest levels of security.