EVERFOX

Implementing the UK National Cyber Security Centre Principles for Cross Domain Solutions

Brochure

What's inside:

This is a detailed overview of how Everfox Cross Domain Solution products implement the principles set out by the UK's National Cyber Security Centre (NCSC) in their Security Principles for Cross Domain Solutions advice.

Challenge:
Valued ('trusted') IT systems which handle sensitive information or control highly critical operations are separated from other less trusted IT systems ('untrusted'), to protect them from either deliberate or accidental misuse. Typically, business processes must flow between the trusted and untrusted systems. Whilst just connecting the two systems would make it easy to implement the business flow, generally the internal security controls that would then be needed to protect the system would be too expensive, too risky and impractical.

Solution:
The answer is to provide a Cross Domain Solution, a way for information to safely cross between untrusted and trusted IT systems allowing business processes to flow whilst protecting the confidentiality, integrity, and availability of the trusted system.

Best Practice Guidance:
The UK NCSC provides important cyber security guidance to organisations across the UK. This guidance includes a set of principles which can be used to guide the design, development, assessment, and deployment of Cross Domain Solutions.

Connecting The Unconnectable

For over 25+ years, Everfox have provided Cross Domain Solutions to government, defence and commercial organisations worldwide, enabling information to flow safely between trusted and untrusted systems.

To assist organisations, we have provided detailed analysis on how Everfox Cross Domain Solutions will achieve the guidance outlines by the NCSC.

Everfox Cross Domain Solution Portfolio

In the context of the NCSC principles, they can provide suitable controls when exporting data.

Information eXchange (iX) Appliance: Everfox iX Appliance is designed to be the bridge between a network of lower trust and one of high value in a Cross Domain Solution. The iX Appliance is comprised of both software and hardware components and implements Content Disarm & Reconstruction (CDR).

CDR works by extracting the valid business information from content, verifying the extracted information is well-structured, and then building new, fully functional content to carry the information to its destination. Delivering threat-free, fully editable content and in near-real time.

Policy Engine Guard: Everfox Policy Engine Guard is used by organisations that need to tightly control business content passing across an external boundary or between separate internal zones over email, web or file transfer. It defends against known malware and accidental data loss by focusing on business content.

High Speed Verifier (HSV): Everfox HSV is a hardsec device that connects two networks together. Implementing a protocol and data break entirely in hardware logic. Meaning no software vulnerabilities can undermine the control it imposes.

Data Guard: Everfox Data Guard is a highly customisable platform for moving data between networks that are otherwise kept separate. It can be used to build Cross Domain Solutions and other high assurance defences for critical networks, meeting information sharing and remote access requirements.

File eXchange (PX): File eXchange (PX) enables users with a footprint on two separate networks to send files from one network to themselves on the other network. It has built-in features which are relevant to the NCSC principles for Cross Domain.

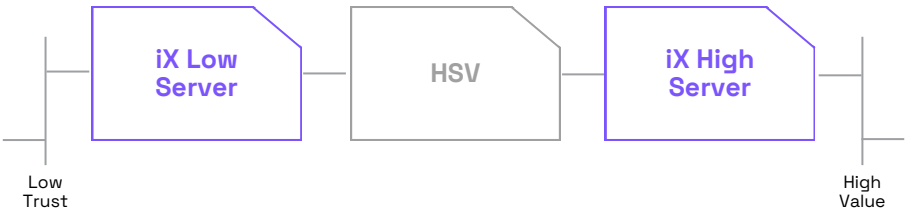


Figure 1: iX Appliance bridges two networks

Principle 1

- **Import and export flows should be separate**
- **Hardware enforced one way flow for export**
- **Hardware enforced one way flow for import with protocol break**
- **Protocol break should be robust and use a simple transport mechanism**

The above principles help ensure that the connection to untrusted external networks provides protection from attacks that attempt to use the Cross Domain Solution as a route to compromise a protected network.

Figure 2: The iX Appliance High Speed Verifier (HSV) providing separate import and export flows

The iX Appliance is a bi-directional device that bridges two networks. Import and export flows can be enabled and are treated separately. Within the iX Appliance, the HSV component provides hardware-enforced flows using two independent one-way paths, implemented on two independent hardware boards. Meaning that the iX Appliance can be used for flows that are just one-way (e.g., importing raw internet feeds) and those that are naturally two-way such as email and web services.

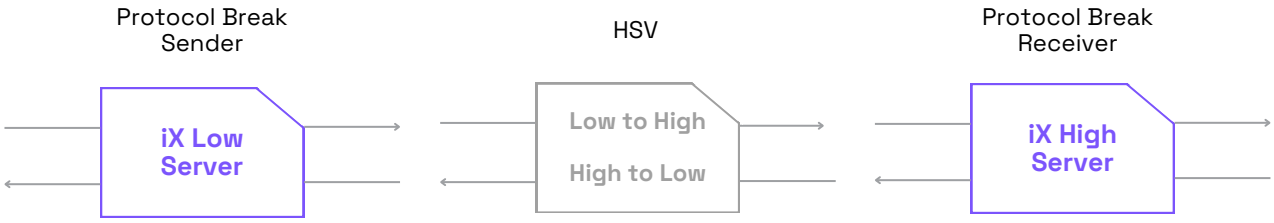


Figure 3: The iX Appliance acting as a Protocol Break Sender and Receive

The iX Appliance acts as a protocol break sender and receiver. All application and network layer protocols are terminated in the source side iX Appliance server. Information about the protocols are extracted and streamed across the HSV in simple data structures along with the information extracted from the content. The data is streamed using a simple protocol that is carried in Ethernet frames.

All data is verified in the HSV using the logic deployed on a Field Programmable Gate Array (FPGA) ensuring the destination-side iX Appliance server can only receive data that has been verified to be correct and so will not be handling malformed data designed to exploit software vulnerabilities. A completely new connection is made to the destination using the information about the content and the protocols that was carried across the HSV.

Principle 2

- **Transform complex data types into simple, verifiable data types**
- **Use a hardware verification engine to ensure data structures are valid in simple data types**
- **Use a hardware or software verification engine to ensure data is valid for the end application**
- **Recursively handle embedded data types**
- **Reliably determine data types where multiple types are processed**

The above principles help defend against attacks using malicious content contained in the data being sent across a Cross Domain Solution.

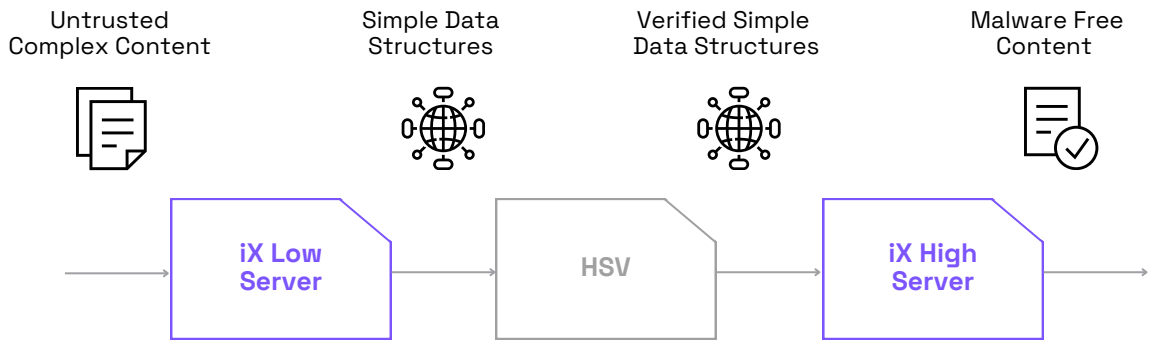
The iX Appliance utilises transformation via Everfox Content Disarm and Reconstruction to all content to ensure it is completely free from malicious content. The iX software component extracts the business information from the content and writes it into an intermediate data structure called XDS. This is a simple structure designed to be verified in the hardware logic of the hardware component (HSV). The HSV verifies the XDS before the software builds brand new content from the extracted information

Both simple (e.g. JSON) and complex (e.g. PDF) data types are handled in the same way using a hardware verification engine. All data types are converted into XDS (simple data structures) and are verified in the HSV using FPGA logic. The logic ensures that the data is structurally correct and valid.

Embedded data is handled in the same way. All data is recursively decomposed, and the information extracted. Any embedded data that cannot be extracted and transformed is removed.

The iX Appliance attempts to process the data using the configured parsers for the designated file type. Parsing extracts the business information from the data and so requires full knowledge of the file format. Successful parsing, therefore, reliably identifies the file type. If data does not parse as any of the configured data types, it does not cross the HSV, and diagnostic and audit log errors are written. The audit logs can be sent off-box using syslog to a SIEM which can notify administrators.

Figure 4: The iX Appliance transforms complex content into simple data structures that can be verified in hardware



Principle 3

- **Keep exported data to a minimum and ensure exports do not contain superfluous data**
- **Limit exports to authorised uses by authenticated users**
- **Authorise the release of information and bind the data to the authorisation**
- **Correlate requests and responses**

The above principles help to prevent the transfer of unauthorised information via the Cross Domain Solution.

The iX Appliance, Policy Engine Guards, Data Guard and File Exchange products can work together to help protect against the unauthorised export of information.

The process of extracting the business information from content in the iX Appliance means that any redundant data is removed from the data flow. This includes information that may be hidden in the data formats, not visible to a human review or to Data Loss Prevention (DLP) tools, e.g. in hidden areas of a file format.

Everfox Policy Engine Guards and Data Guard can be used in combination with the iX Appliance to provide DLP capabilities to search and block prohibited information or prohibited file types from being exported. The PX Application can be used in combination with the iX Appliance to provide a human review of files exported.

The PX Application requires users to authenticate prior to accessing the application and sending files across the Cross Domain Solution. The Policy Engine Guards apply policy based on the source and destination of the traffic ensuring only authorised exports are made.

All three products support mutual authentication with the other Cross Domain Solution components to ensure they only receive data from and send data to authorised applications.

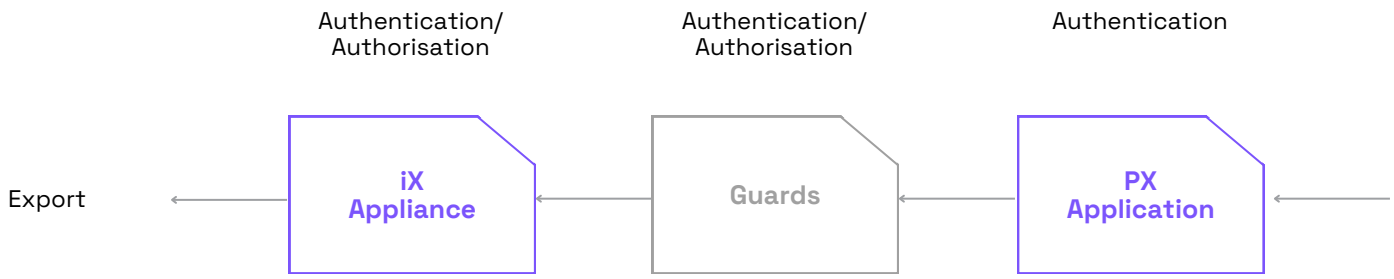


Figure 5: Everfox products authenticating and authorising data export

When exporting emails, the Policy Engine Guards can check and remove signatures on S/MIME email messages prior to release allowing strong binding of the email authorisation with the release. The iX Appliance, the Policy Engine Guards and Data Guard all correlate all requests and responses for bi-directional communications in the proxies.

SESSION ISOLATION

Principle 4

- **Keep complex data handling separate**
- **Reset to a known good state after processing**
- **Use separate paths for different types of data**

The above principles help to ensure an attack on one session in the Cross Domain Solution cannot influence another session.

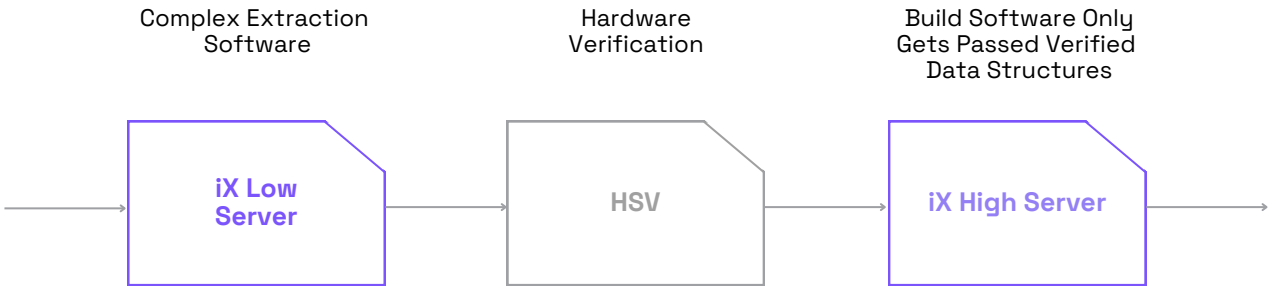
The architecture of the iX Appliance ensures that the complex data handling of the source data is kept separate from the delivery of the data to the destination. Separate physical devices implement extraction of information from the complex data to create XDS, verification of the XDS and building of the data to send on to the destination, and each are connected with simple interfaces.

Only valid data structures pass through to the build server and so any attacks (or failures) in the complex data processing of the source data cannot compromise the delivery of data to the destination.

Further physical separation can be gained, if required, by using multiple physical iX Appliances to handle different types of data. Within a single iX Appliance, data handling is kept separate from the protocol handling and the management traffic.

The iX Appliance implements a process isolation server which can spawn a separate process per data item, ensuring that memory is reset every time or after a configured period of time and that the processing of one data item cannot affect another.

Figure 6: Physical separation of the complex extraction software from the critical build software



PERSISTENT COMPROMISE PROTECTION

Principle 5

- **Return system to a known good state**
- **Reset software execution environment**
- **Monitor integrity of components**

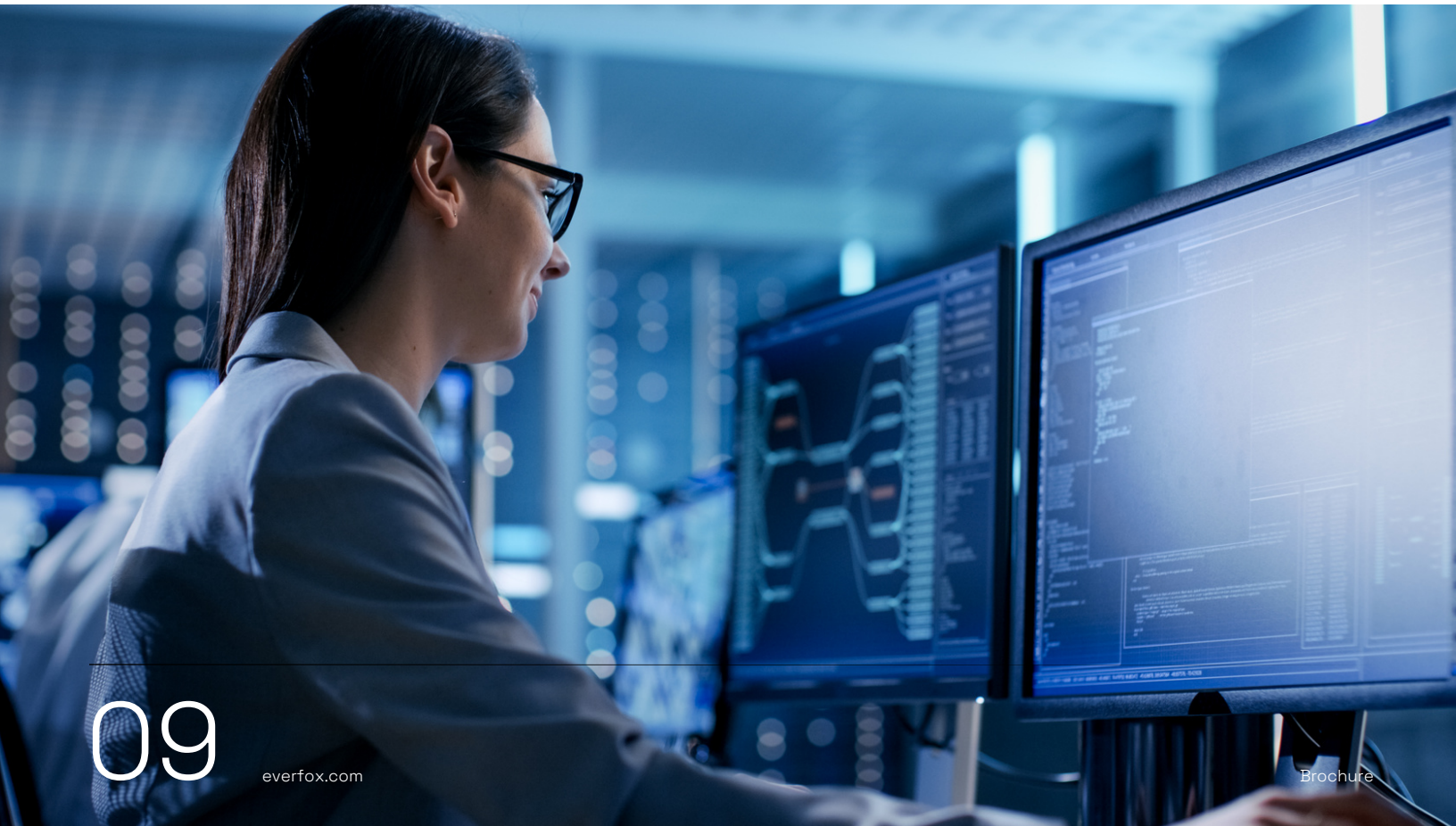
The above principles help to prevent a persistent compromise of the Cross Domain Solution.

The iX Appliance does not store state information about the data being processed. This means that processing of one data item does not affect future data items.

When running multiple iX Appliances in parallel, it is possible to use the Management API to periodically alternately put one appliance into Maintenance Mode and then to reactivate it. This will reset its data handling environment whilst the other iX Appliance is still processing data. In addition, the complete iX Appliance can be reset to a known good state by an administrator, either resetting to factory settings or to a previously saved known good configuration.

The iX Appliance implements a process isolation server which can spawn a separate process per data item, ensuring that memory is reset every time or after a configured period of time and that the processing of one data item cannot affect another.

The integrity of the key components in the iX Appliance is monitored. Changes to these components will prevent the iX Appliance from activating and if modified whilst it is processing, the iX Appliance will deactivate and stop processing traffic.



Principle 6

- **Usability should be evaluated for key users**
- **End users should be aware of the domain they are working in**
- **Users should be informed where transformation has affected content**
- **Feedback should be given on processing**
- **Interfaces should be accessible**
- **Use of the Cross Domain Solution should add little extra complexity for end users**
- **System defaults should ensure reasonable protection**

The above principles help to ensure the Cross Domain Solution is usable by all relevant people.

End users access the Everfox PX Application when transferring files. To gain access they authenticate and for ease of use, they can use single sign-on. Once logged in, the domain that they are working in is clearly labelled and the domain(s) that they are authorised to transfer files to are also clearly marked. The user interface is configurable using the templates provided in order to make it accessible and to fit with the environment in which it is used. When files are transferred, feedback is given as needed whilst keeping the interface as simple as possible.

End users do not see the iX Appliance, Data Guard and Policy Engine Guards, but the use of these products in a Cross Domain Solution is typically transparent to them.

Data is transferred via the iX Appliance, Data Guard and Policy Engine Guards which return results to the calling applications to be able to inform end users of any issues as appropriate.

Configuration of the Policy Engine Guards determines how much information to return to the end users in the result of a policy violation. If data is removed from content during processing by the iX Appliance, the end user is informed.

Administrators access the iX Appliance and Policy Engine Guards, and user interfaces are provided for configuration. For the iX Appliance, the domain in which the administrator is working is marked in the UI. The iX Appliance is installed with a safe default profile and forces the administrator to modify the default password before it can be activated. The Policy Engine Guards can be started with a closed policy, only allowing traffic to flow once further configuration has been made.

MANAGEMENT

Principle 7

- **Management traffic should be separated from business traffic at all network layers**
- **Lower-trust components should not manage or influence a higher-trust component**
- **Higher-trust components should be protected from network/content attacks if managing lower-trust components**
- **Management interfaces should be authenticated and use in-transit encryption**
- **Management actions should be audited**

The above principles aim to secure the management of the Cross Domain Solution throughout its life-cycle.

Everfox iX Appliance is the bridge between lower- and higher-trust networks. iX Appliance comprises a lower-trust server, the HSV and a higher-trust server.

The HSV requires minimal management. The FPGA is pre-loaded with the logic it requires to verify the data. HSV v1 requires physical access to the device to modify the logic. HSV v2 provides a management interface and crypto mechanisms to protect access to the HSV. The lower-trust and higher-trust iX Appliance servers are managed from separate management networks meaning there is no risk of attack on the higher-trust network by the lower-trust management.

Each server has a separate management interface with the business traffic, and HTTPS is used to provide both TLS encryption and mutual authentication for administrators. This allows the server to authenticate the administrator using two-factor authentication, and an administrator can verify that they are connecting to a valid iX Appliance server. The HTTPS server handling the management traffic is separate to the HTTPS proxy which is used for business traffic.

The iX Appliance can restrict the hosts that are allowed to connect to the management interface and audits all management actions taken.

Principle 8

- **Monitor configuration changes**
- **Monitor exports for unauthorised exfiltration**
- **Monitor imports for malicious content**
- **Monitor process execution and failures to identify potential attacks**
- **Monitor external boundaries for connections from unknown sources**
- **Monitor internal boundaries for unauthorised outbound connections**

The above principles allow the Cross Domain Solution to be monitored to ensure it is working as expected.

The iX Appliance provides comprehensive audit logging of both management and business traffic. Configurable levels can be separately applied to the audit records for the management traffic, the web user interface and the data. Each can log just failures or both successful and failed operations.

The audit records interface to an external SIEM using syslog and support the different transport and format standards for syslog that may be in operation within a system. SNMP traps can also be sent off box to a configured SNMP manager.

Syslog from the low server of the iX Appliance can be sent through the iX Appliance to the high side allowing all syslog data to be collected from the management network of the high side. The syslog data pushed through the IX Appliance undergoes the same processing as the business data to ensure it is safe to be sent to the high-side management network.

All administrative actions are audited including any changes to the configuration. Configuration of the connections allows specification of a set of allowed peer hosts that can connect to the iX Appliance, and in combination with mutual authentication this ensures that only known and trusted sources can send data across the iX Appliance. Any attempts to bypass these controls is audited.

The extract and build software which handles the information being transferred does not detect malicious content or additional data that may be exfiltrated. This is by design and is how it can prevent zero-day attacks. The software will, however, log when the information cannot be extracted as expected or cannot be built as expected which could be an indication of a potential attack.

The HSV is a hardware only device which does not produce logging, but if it encounters invalid data during processing, the stream is dropped and the software either side of the HSV will log to indicate that there is a problem.

Principle 9

- **Authenticate user sessions**
- **Authenticate system sessions**
- **Support single sign-on**
- **Authenticate with onward components**

The above principles ensure the Cross Domain Solution is only accessed by authorised users or systems.

Users interface with Everfox products when using the File Exchange (PX) Application to transfer files. To use PX, users must first authenticate using either simple username and password or single sign-on using Integrated Windows Authentication (IWA) or Active Directory Federation Services (ADFS).

The iX Appliance, Data Guard and Policy Engine Guards are accessed by other applications and by administrators rather than directly by users. Administrators authenticate to the iX Appliance using two-factor authentication with a username and password supplemented with mutual authentication using certificates.

This both ensures the administrator is authorised to access the iX Appliance and that the administrator is connecting to the expected iX Appliance. Administrators authenticate to the Policy Engine Guards using certificates to ensure they are authorised to access the management user interface. Applications sending business data across the iX Appliance and the Policy Engine Guards can use mutual authentication to ensure that they are both receiving from and sending to authorised components.

Principle 10

- **Support point-to-point protection with encryption**
- **Support certificates with a root of trust**
- **Support certificate pinning and full certificate checking**
- **Support modern cryptographic standards and cypher suites**

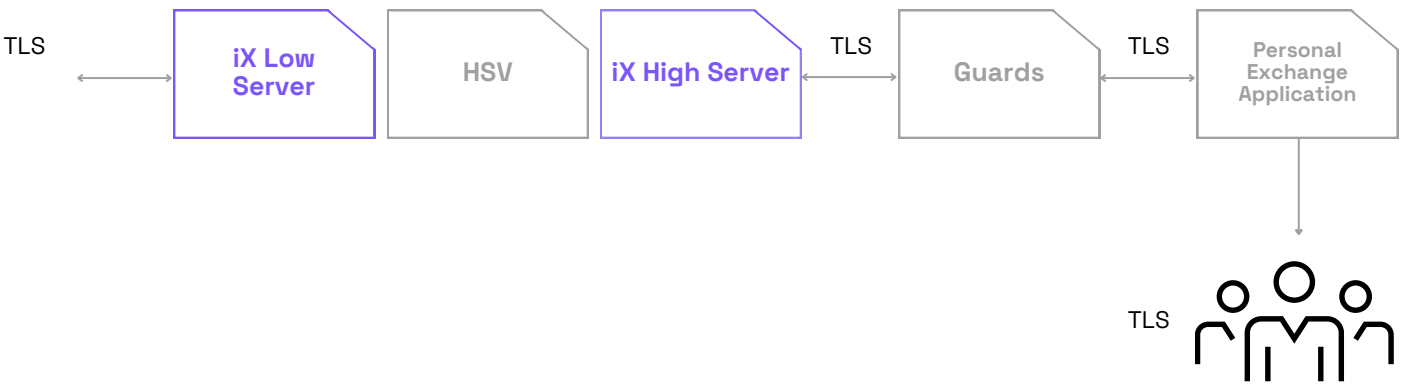
The above principles help to prevent loss of integrity or confidentiality of information being transferred across the CDS.

The iX Appliance, Data Guard and Policy Engine Guards support TLS for management traffic and when communicating via HTTP or DSFSP (file transfer) for business traffic. Authentication of the session uses certificates which are checked to a root of trust. The trusted root certificates are loaded onto the iX Appliance and Policy Engine Guards by an authorised administrator.

The Everfox File Exchange supports TLS when communicating with both the users and the other Cross Domain Solution components (iX Appliance, Data Guard and Policy Engine Guards).

All components implement the latest cryptographic standards and cypher suites using third-party crypto libraries.

Figure 7: Everfox products implement TLS for data in transit protection



DATA-AT-REST-PROTECTION

Principle 11

- **Locate the Cross Domain Solution in a physically secure environment**
- **Encrypt sensitive data when the device is powered off or check integrity prior to use**
- **Limit access to sensitive data**
- **Require authentication to access sensitive data**

The above principles help to protect the confidentiality and integrity of sensitive information stored in the Cross Domain Solution.

The iX Appliance comprises physical hardware which is rack-mountable and typically deployed in a data center inside a physically secure environment. The iX Appliance does not store business traffic but does generate log files and hold configuration files which may be considered sensitive.

Audit logs can be sent off-box as they are created to be protected in a central system. Access to configuration is limited to authenticated administrators via a web user interface.

PATCHING

Principle 12

- **Produce patches and security updates for all components**
- **Identify and patch vulnerabilities in third-party libraries**
- **Allow urgent patching outside of normal patch cycles**
- **Patches should be easy to administer**
- **Patches should be tested**
- **Patches should be cryptographically signed**
- **Ensure only valid and correct patches are applied to the Cross Domain Solution**

The above principles help to maintain the security of the Cross Domain Solution as vulnerabilities are discovered in the underlying code.

Everfox regularly provide patches for their products and monitor the status of third-party libraries used. To minimise the risk, the iX Appliance uses predominantly Everfox code. This makes monitoring third-party libraries simpler and more reliable. If security vulnerabilities are identified in Everfox code, it is immediately patched, and updates are made available to the relevant customers to apply.

Everfox have a stringent testing procedure which covers testing of both updates to software and third-party libraries before a patch is made available to customers. The patches are applied via the management user interface, making them simple to apply.

All Everfox patches are cryptographically signed and can be verified before application to the Cross Domain Solution.

COMPONENT INTEGRITY

Principle 13

- **Ensure supply chain security**
- **Ensure development security**
- **Secure boot for software components**
- **Cryptographically sign bytecode of hardware components**
- **Trusted Boot to remotely attest the state of components**
- **Monitor components state → Anti-tamper solution or system**

The above principles help to ensure the components of a Cross Domain Solutions are not altered in an unauthorised way.

Everfox supply Cross Domain Solution products into multiple organisations worldwide. Our processes include trusted delivery of hardware to its destination and the use of signed packages to validate the integrity of the software. The HSV implements a secure and trusted boot mechanism with cryptographic checks to attest the state of its components.

Everfox use a small number of trusted organisations to supply the hardware that makes up the iX Appliance. These organisations are UK-based and use approved components for the High Speed Verifier.

The Everfox development processes are kept secure using a combination of personnel clearance checks for all development staff, segregated development networks and strong processes for code, build and test.

The use of third party-libraries in the iX Appliance is limited to a very small number that can be monitored and updated as required. The integrity of software components of the iX Appliance is verified prior to activation to ensure they have not been modified, and any changes during processing will cause the appliance to deactivate and stop processing traffic. The HSV implements a secure and trusted boot mechanism with cryptographic checks to attest the state of its components.

Trusted high assurance cyber security

About Everfox
Everfox has been defending the world's most critical data and networks against the most complex cyber threats imaginable for more than 25 years.

Our unwavering dedication and commitment to our customers and the critical missions they serve are what set us apart. We are dynamic, vigilant, and proactive in everything we do.

everfox.com