EVERFOX

DATASHEET

Data Guard

Providing defense-grade control over data transfers.

Challenge

Globally, organizations and Governments are grappling with the challenge of protecting sensitive data from both internal and external threats, including unauthorized access, espionage, and cyberattacks.

Solution

Implementing robust protocols,restricting access based on user roles, and employing advanced threat detection systems,organizations can fortify their defenses against potential security breaches and safeguard critical information assets.

Key Benefits

- Data validation rules are highly customizable for maximum flexibility
- Flexible software implementation for all environments
- Enables real-time video streaming
- Integrated with Everfox Content Disarm and Reconstruction (CDR)
- Customer maintainable for simplified configuration and management
- Common Criteria certified forEAL4+
- Full protocol break using common criteria-evaluated platform

Connecting the ”unconnectable”

The persistent threat of cyberattacks, penetration and data loss require that only the most secure methods are used to maintain the highest standards of security, particularly in highly regulated industries. Many organizations struggle with how to balance protecting sensitive data.

The common approach many organizations take is to separate sensitive data and networks from information technology systems and the internet. This is a good security practice, but on its own can leave systems vulnerable and prevent adoption of automation and cloud-based technologies.

Everfox Data Guard

The Everfox Data Guard delivers this balance by enabling highly complex, bi-directional, automated data and file transfers between physically separated networks.

Providing defense-grade data control at scale

Data Guard leverages a trusted operating system and security policies that enforce role and process separation and isolation for automated, byte-level content inspection and sanitization. With customizable rules to handle even the most specialized data types and protocols.

Supporting Current Security Paradigms

The Data Guard is built on a trusted operating system – Red Hat Enterprise Linux with enhanced SELinux modules – which is used to enforce network separation and ensure data constraints are always applied, allowing it to be used in highly regulated environments.

Ready for tomorrow’s challenges

Data Guard is designed to evolve as the demands on your environment change. Thanks to its highly flexible and customizable rule- and policy-based structure, Data Guard ensures an organization’s ability to monitor and control any future data types and devices.

Data Guard was designed for highly regulated environments such as government, military, law enforcement,and any other environment that must:

- Move sensitive data between separated networks.
- Adhere to strict regulations for devices that move data between networks.
- Utilize non-standard or non-typical data types and formats.

A flexible approach

Everfox Data Guard enables secure data and file transfers between otherwise disconnected networks. Supporting both structured (e.g. JSON and XML/SOAP) and unstructured data (imagery, Office, and PDF etc), as well as streaming data formats such as video. Different constraints can be applied depending on the direction of travel. The guard can connect multiple networks, and flow scan be made strictly one-way.

Filtering process

The Data Guard filtering process consists of built-in filtering capabilities: Rule Engine (plugins) and the Filtering Rules. Each capability provides consistent policy enforcement across all adaptors. Instead of pre-packaged point-and-click policies, the filtering process supports full customization of inspection capabilities that enable the creation of complex security policies. This allows specific inspections and constraints for each deployment rather than generic controls based on file type. Almost any security policy can be expressed through the user-configurable LUA interface language.

Everfox Professional Services works with each customer to determine which adaptor(s) and plugins best support use case requirements. Any combination of adaptors and plugins can be used to secure a flow. Data Guard supports multiple flows, with each flow managed independently without affecting other operational flows.

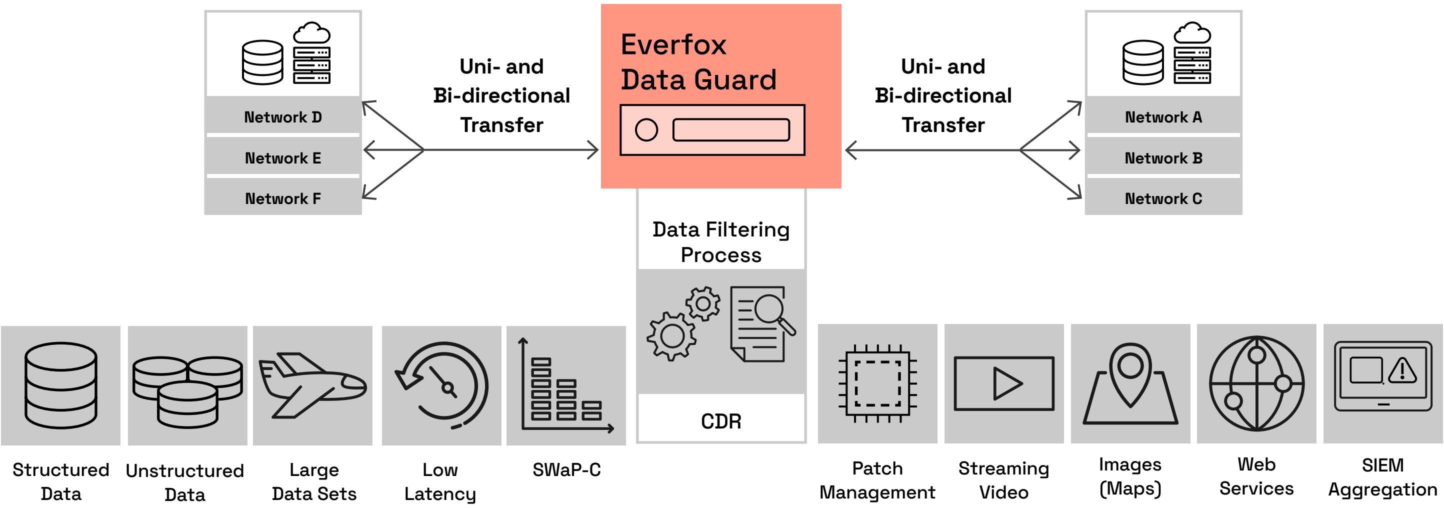


Figure 1: Everfox Data Guard

Adaptors

Data Guard Adaptors are service applications used to receive and transmit data from source and destination networks. When inbound, the adaptors terminate the network protocol. When outbound, they receive filtered data and send it out on to the appropriate network.

Generic TCP and UDP

Data Guard supports the transfer of most TCP and UDP based protocols. These adaptors are also used to create custom protocols to meet specific data requirements. The UDP adaptor can be used with multicast applications to securely bridge multicast domains or to convert multicast to unicast or vice versa.

Video Streaming

KLV checking, decoding, and encoding of various video transport protocols (e.g., MPEG-TS, RTSP/RTP,HLS) and video frames (H.264, H.265)for security inspections.

Adaptors (cont.)

Secure File Drop

The File Drop adaptor monitors directories on source servers and retrieves files for inspection and content filtering prior to dissemination to destination servers. Files that fail transfer due to policy violation can be quarantined on the source system for further analysis and review. The File Drop adaptor uses Secure Copy (SCP) to transfer files between the guard and external servers. The File Drop adaptor requires an optional feature license.

Web Services

Data Guard supports the transfer of most TCP and UDP based protocols. These adaptors are also used to create custom protocols to meet specific data requirements. The UDP adaptor can be used with multicast applications to securely bridge multicast domains or to convert multicast to unicast or vice versa.

Plugins

Data Guard plugins are helper modules that assist with the data filtering process. Plugins simplify the filtering rules (in the LUA language) needed to perform data validation and transformation. All plugins require an optional feature license.

Virus Scanner

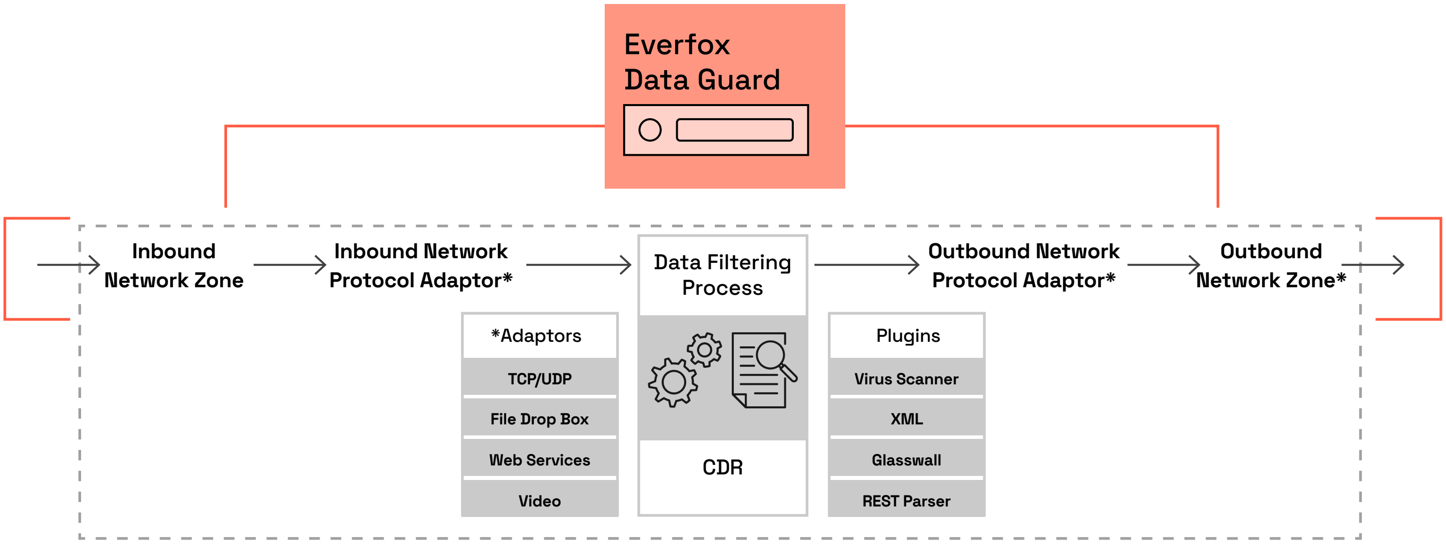
Integrated McAfee® Anti-Malware Engine for scanning block data or files, a top rated product for effectively detecting malware in real time.

XML

Parse, validate (schema and digital signature), and modify standards-compliant XML data types.

Content Disarm & Reconstruction

Data Guard supports the transfer ofmost TCP and UDP based protocols. These adaptors are also used to create custom protocols to meet specific data requirements. The UDP adaptor can be used with multicast applications to securely bridge multicast domains or to convert multicast to unicast or vice versa.



Learn More: www.everfox.com