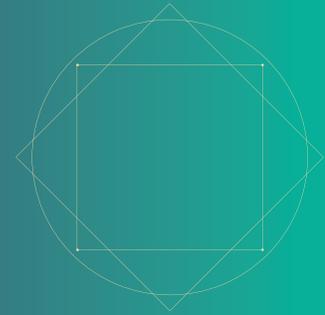# Data Guard

Secure data and file transfer between physically separated networks

Key Benefits

› Provides highly customizable data validation rules for maximum flexibility rather than static, one-size-fits-all policies

› Flexible software implementation for all environments: datacenter to SOC and meets austere, ruggedized SWAP-C requirements

› Enables real-time video streaming while providing unparalleled control and auditing

› Integrated Content Disarm and Reconstruction (CDR) capabilities with Forcepoint Zero Trust CDR

› Customer maintainable for simplified configuration and management

› Common Criteria certified for EAL4+

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 while at the same time utilizing cutting edge collaboration and automation technologies. 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.

Forcepoint Data Guard

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

To provide 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.
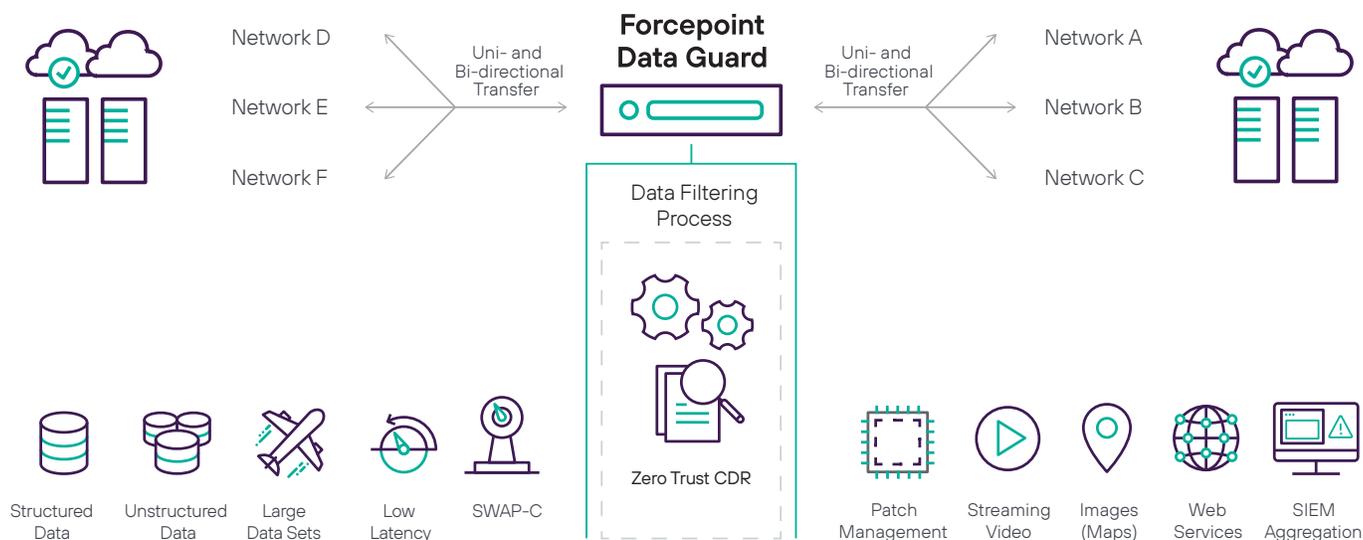
Supporting today's security paradigms

Data Guard enables secure data and file (structured and unstructured data) movement between segmented networks in uni-, bi-, or multi-directional fashion. The trusted operating system foundation derived from Red Hat Enterprise Linux with enhanced SELinux modules allows Data Guard 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 enterprise's ability to monitor and control any future data types and devices.

Data Guard was designed for highly regulated environments such as government, military, critical infrastructure, 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

Forcepoint Data Guard

Network D — Uni- and Bi-directional Transfer — Network A
Network E — Network B
Network F — Uni- and Bi-directional Transfer — Network C

Data Filtering Process

Zero Trust CDR

Structured Data · Unstructured Data · Large Data Sets · Low Latency · SWAP-C · Patch Management · Streaming Video · Images (Maps) · Web Services · SIEM Aggregation

A flexible approach

Data Guard is highly flexible in its secure approach to high assurance data movement through the robust security policies within adaptors, plugins, and the filtering process. The rule engine provides APIs to handle rich data types including: HTTP header, JSON, SOAP, MIME, compression, HTML, XML, file sanitization for Office, PDF, and images, streaming data, and the flexibility to secure most TCP and UDP protocols.

Filtering process

The Forcepoint 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.

Forcepoint 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.

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.
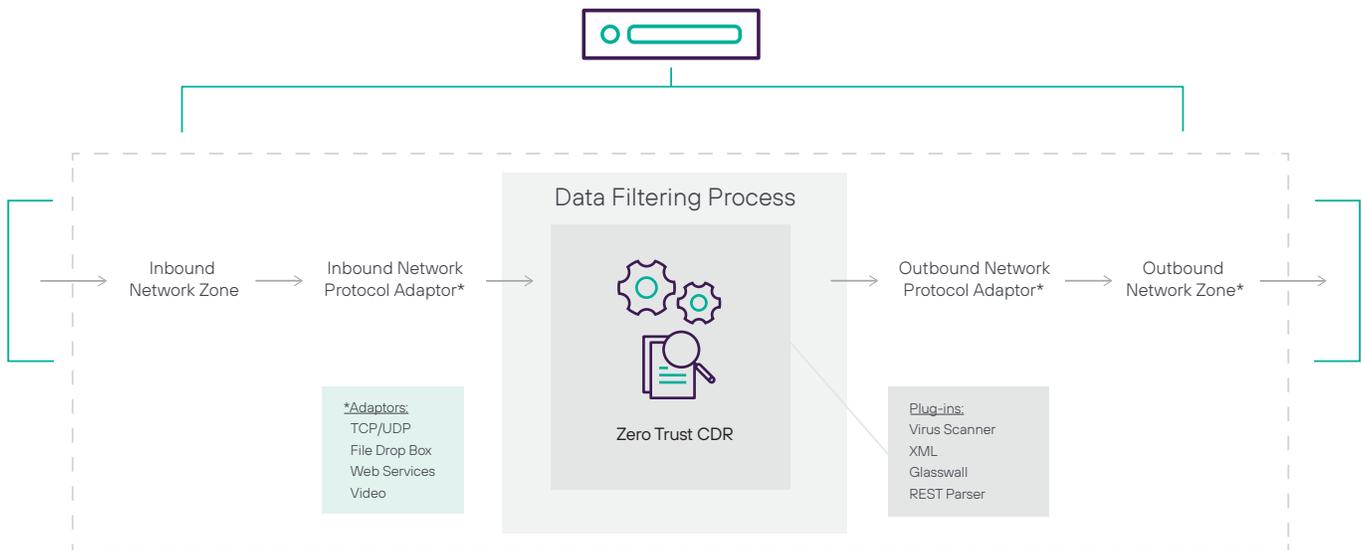
→ **Secure File Drop**
The File Drop adaptor monitors directories on source servers and retrieves files for inspection and content filtering prior to dissemination to destination servers. Files that fail transfer due to policy violation can be quarantined on the source system for further analysis and 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.

→ **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.

Forcepoint
Data Guard

Data Filtering Process

Inbound Network Zone → Inbound Network Protocol Adaptor* → Zero Trust CDR → Outbound Network Protocol Adaptor* → Outbound Network Zone*

*Adaptors:
TCP/UDP
File Drop Box
Web Services
Video

Plug-ins:
Virus Scanner
XML
Glasswall
REST Parser

→ **Web Services**
The Web Services flow within Data Guard allows for workflow creation to inspect and secure REST-based network communications. This is typically used with Server to Server communications, whether that is a frontend server talking to a backend server or two independent systems, Forcepoint Data Guard can sit in the middle of the traffic flow, doing HTTPS decryption and cleaning any applicable data with Zero Trust CDR technology.

→ **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.

→ **Zero Trust CDR**
When it comes to securing data and file transfers, the combination of Forcepoint's Data Guard (FDG) and Zero Trust Content Disarm & Reconstruction (CDR) eliminates malicious threats in real time with less disruption.

→ **REST Parser**
Parse and modify REST (JSON or SOAP) data. Allows for workflow creation to inspect and secure REST-based network communications. Widely used with modern microservices and web services.

→ **Utility Plugins**
Regex search, PKI and cryptography, file typing, file compression/decompression, HTML and MIME handling, JAR file validation, and more.

→ **Custom Application Workflows**
As the Zero Trust CDR technology is natively implemented within the Forcepoint Data Guard, it is possible to use the unique file cleaning capabilities within custom applications. Almost any security policy can be expressed through the user-configurable LUA interface language. This allows for fine grained controls that can be built for specific application workflows.

Forcepoint