

EVERFOX

A woman with dark hair pulled back, wearing black-rimmed glasses and a light blue button-down shirt, is looking down at a laptop screen. The background is a blurred office setting.

WHITEPAPER

Boost your Everfox Data Guard with CDR

Organizations
thrive when a
cohesive security
solution delivers
the right tools for
the job

Connecting the Unconnectable

04

Supported Workflows for Data Guard with Zero Trust
CDR Technology

05

03

Boost your Everfox Data Guard with CDR
www.everfox.com

Whitepaper



Connecting the Unconnectable

Secure data and threat-free file transfer between physically separated networks.

The persistent threat of cyberattacks and data loss require that only the most secure methods are used to maintain the highest standards of security – particularly in highly regulated industries.

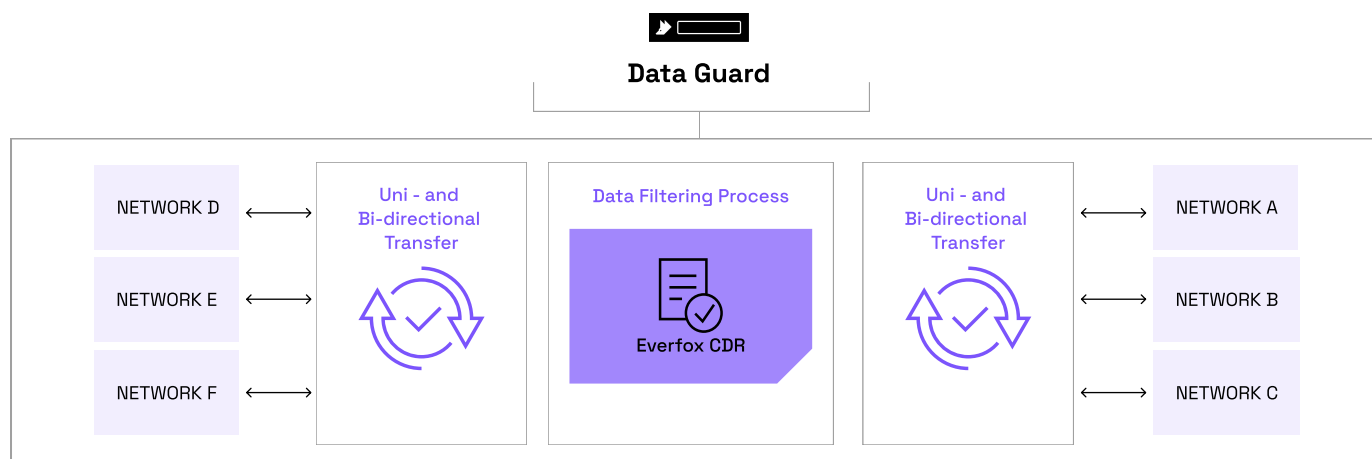
Many organizations struggle with how to balance protecting sensitive data, while at the same time utilizing cutting-edge collaboration and automation technologies. The common approach many organizations take is to separate sensitive data and networks from information technology systems and the internet. This is a good security practice, but on its own can leave systems vulnerable and prevent adoption of automation and cloud-based technologies.

Everfox 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.

Bringing native Content Disarm & Reconstruction (CDR) technology inside the Data Guard itself.

When it comes to securing data and file transfers, the combination of the Everfox Data Guard and Everfox Content Disarm & Reconstruction (CDR) offers unparalleled security with less disruption.

Supported Workflows for Data Guard with CDR Technology



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. The CDR technology can be applied to generic policies within Data Guard, or custom policies can be configured with scripting capabilities in LUA.

Web Services Workflows

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 front-end server talking to a back-end server or two independent systems, Everfox Data Guard can sit in the middle of the traffic flow, running HTTPS decryption and cleaning any applicable data using CDR technology.

Custom Application Workflows

As the CDR technology is natively implemented within the Data Guard, it is also possible to use the 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.

Security Simplified

All the above supported workflows can be implemented independently on the same hardware, meaning that you do not need multiple boxes to achieve multiple use cases.

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.

Built for highly regulated environments 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.

Boost your Data Guard defenses today with Everfox CDR

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.

Schedule your demo now @ [Everfox.com](https://www.everfox.com) »