EVERFOX

SOLUTION BRIEF

Providing Defense-Grade Control over Data Transfer

Everfox Data Guard API
Security Overview

Everfox Data Guard

Everfox Data Guard is a defense-grade Cross Domain Solution (CDS) created to enable best practices and the most resilient architectures in government, regulated industries, and corporate networks. It is designed to meet Cross Domain Security principles of inspect, validate, and transform data, while providing full network isolation / protocol break. Both cybersecurity and data security capabilities are provided by the Everfox Data Guard.

Everfox Data Guard as Part of Web Service Security Best Practices

Utilizing Everfox Data Guard as part of a purposely designed hightly resilient and secure system offers many benefits that enhance the security posture and compliment traditional web service security solutions. This is especially true when connecting to “high risk” networks such as external partners or to the dirty internet. Data Guard is designed to provide complete network isolation, full protocol break, protection against TCP/IP stack vulnerabilities, and sophisticated advanced persistent threats. It is designed to “fail secure” and created using the strictest security and resiliency methodologies in its systems architecture. Through independently controlled granular and customizable inspection and validation mechanisms, all aspects of a web service connection can be validated, controlled, blocked, or modified. By implementing Everfox Data Guard as part of the web services security stack, the following benefits can be realized.

Protocol Break and Network Isolation

The Everfox Data Guard is designed to sit in between two networks of differing trust levels, often connecting sensitive networks to high risk networks. As such, it is vital that the Data Guard ensure that networks are kept isolated, sensitive information about these networks remains secure, and the flow of data is guaranteed to be as intended.

- TCP/IP Stack Protections - Data Guard strips layers 1-6 of the OSI model from a packet to protect against TCP/IP stack vulnerabilities. Once the data is validated and allowed to pass, the packet is rebuilt and transmitted. The packet coming in is not the same as the packet leaving the Data Guard.
- SE Linux provides robust separation and isolation of system data, flows, and networks. Each network’s data is contained in it’s own memory space, and only defined processes can move this data in a well defined path.
- Bi-directional data flows are designed to act as two uni-directional flows with a state maintained in the flow, which is maintained in its own flow dedicated memory space. This ensures proper network isolation/separation.
- Data Guard is designed to have a minimal attack surface, therefore it is completely walled off by default, and configuration consists of opening only the specified ports/protocols along with the relevant validation/filtering rules.
- Data Guard is designed to fail secure if any abnormalities are detected such as integrity check failures.
- Data Guard acts as a reverse proxy, hiding the IP addresses/network topology of a network from any other network.

Resilient Architecture Based on CDS Design Principals

Everfox Data Guard Architecture is based on US Government defined Cross Domain Solution (CDS) design principals providing a greater level system security, data handling, inspection, and validation compared to traditional cybersecurity solutions. CDS technology has been required for US Government organizations needing to share data between different classification levels or with external entities. Everfox CDS products are deployed in some of the most sensitive and high-risk environments in the United States and around the world.

Everfox Data Guard uses a non-bypassable pipeline of independent data handling, validation and modification processes for all data movement between the connected networks. This pipeline ensures that only the specifically approved data and protocols are permitted to transit across the device. Extensive use of SELinux Mandatory Access Controls (MAC) and process isolation ensures there is no single point of failure in the pipeline, meaning a successful compromise of the Data Guard would require multiple unknown zero-day attacks to be executed simultaneously. Additionally, the underlying OS is minimized, hardened, and tailored such that it can only perform the tasks required for the Data Guard function.

- → Fully hardened OS and Data Guard application, with testing conducted in order to receive Common Criteria Certification EAL 4+ of the overall solution.
- → Continuous System integrity Checking on bootup and during operations.
- → No access to root, all functionality is limited to Data Guard provided commands which are logged, audited, and controlled via role based access.

Defense in Depth

The inclusion of the Everfox Data Guard as part of a secure web service architecture ensures independent defense grade, in depth controls of the full web service connection communications.

- → Protect against misconfiguration, insider threat, and provide a strong layer of defense from external attackers.
- → Validation from web service connection down to the values of the payload
  - Ensure that no additional data is included in the HTTPS connections, and that it is in the expected structure.
  - Protect against intentional or accidental data leakage.
- → Protect Parsers/Validation Systems from vulnerabilities or misconfiguration
  - Syntax validation to confirm data is of the expected type.
  - Semantic validation to confirm specified values are included and nothing outside of these are allowed.
  - Structural validation of content.
- → True file typing of information before it reaches the internal network
  - Validate claimed file type against design specifications, such as order, structure, and data types held within the file.
  - Prevents unsafe file types or malformed/false file types from entering the network.
- → Full protocol inspection capabilities versus a typical Firewall which only validates the beginning X number of bytes.

25+Years

Innovators in Cross Domain Solutions

Everfox has been designing and implementing cross domain solutions for over 25+ years, with thousands of deployments in some of the most secure environments in the world.