FORCEPOINT
POWERED BY Raytheon

Datasheet

FORCEPOINT Data Guard

As more enterprises focus on the two-pronged problem of effective data protection and data sharing, the need for secure data transfer is becoming more and more apparent. Data from a wide variety of sources is commonly transferred to protected enclaves for processing and analysis; sharing this data is essential to the rapid, accurate and precise execution of our customers' sensitive missions. The persistent threat of a cyberattack and the resulting penetration and data loss necessitates only the most secure methods for data sharing and transfer.

Forcepoint Data Guard, the latest addition to the Forcepoint Cross Domain Solutions (CDS) portfolio, addresses the secure data transfer needs of customers looking for the highest degree of sensitive data protection. Built to address specific high-assurance security requirements found predominately in government and critical infrastructure environments, Forcepoint Data Guard is a bi-directional, automated data transfer guard that enables the secure movement of structured data between separate domains or networks.

A Flexible Approach

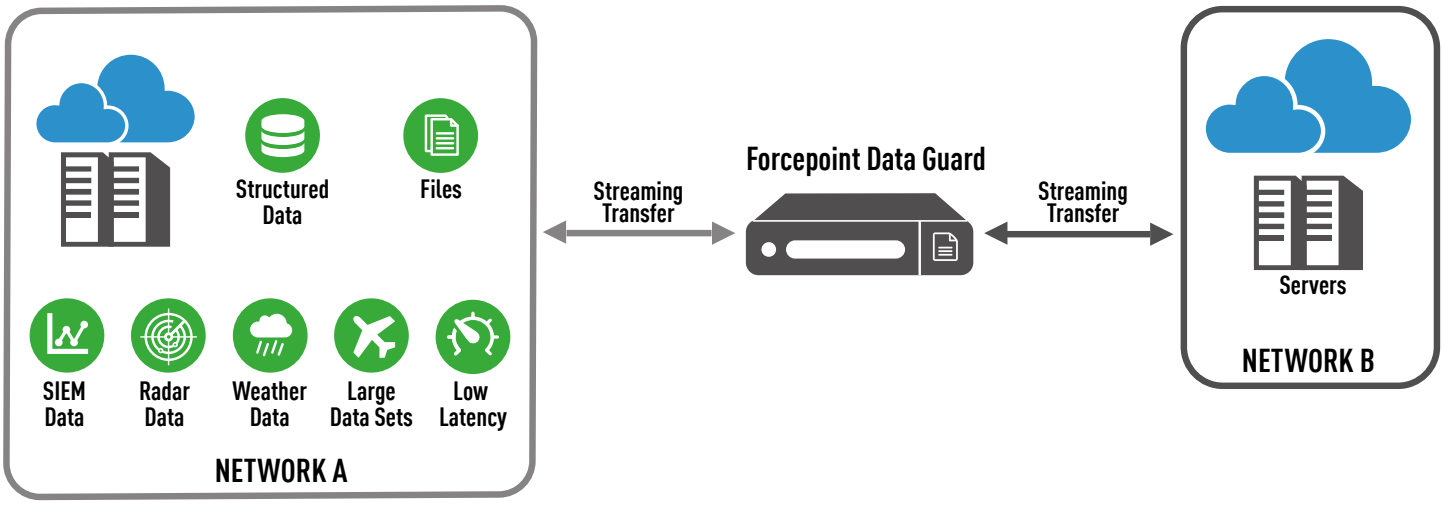
Forcepoint Data Guard is built on a multilevel-capable operating system that enables high assurance network separation and flow control. Delivering byte-level deep content inspection, data validation and filtering, Forcepoint Data Guard can be tailored to meet customer-specific security policies, requirements and risks.

Derived from the Red Hat Enterprise Linux 7 secure operating system with Security Enhanced Linux (SELinux) modules, the operating system is Common Criteria certified at Evaluation Assurance Level (EAL) 4+ under the Operating System Protection Profile (OSPP).

Forcepoint Data Guard provides a flexible yet exhaustive capability to inspect data streams down to the byte level as required by customer security policy. Forcepoint's professional services team works with you to assess your data transfer requirements and build specific policies and rules to ensure project success.

Security Policy Enforcement

The Policy Implementation Engine within Forcepoint Data Guard provides the solution's policy enforcement capability. The Policy Implementation Engine supports full customization of inspection capabilities, enabling the creation of complex security policies; this allows specific inspections and constraints for each deployment.



Transfer Mechanisms

Forcepoint Data Guard supports the following secure transfer methods that can be adjusted or expanded to meet specific mission requirements: TCP and UDP over IP, file drop box, and XML filtering and schema validation.

TCP and UDP Over IP

Forcepoint Data Guard supports the transfer of most TCP and UDP based protocols. This transfer mechanism is also used to create custom protocols to meet specific data requirements.

File Drop Box

The File Drop Box transfer mechanism allows Forcepoint Data Guard to monitor external file servers for files ready to transfer. The guard 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 Box mechanism uses Secure Copy (SCP) to transfer files between the guard and the external servers. *Use of File Drop Box requires an optional feature license.*

XML Filtering & Schema Validation

When transferring XML content through the guard, the XML Filter API is required to write the corresponding rules. The XML rules allow for full inspection and modification of XML content as it moves through the guard. XML document content can be accessed and manipulated with the filter engine. The associated XML Schema Validation API validates XML documents against one or more schema files. *Use of XML Filtering and Schema Validation requires an optional feature license.*

Logging and Auditing

Forcepoint Data Guard is deployed with a standard audit configuration which can be tailored for each deployment. This unique audit capability is driven by the Policy Implementation Engine, permitting the security policy to send any data deemed appropriate to the audit trail at any time. Forcepoint Data Guard supports local log consolidation of the standard operating system syslog, binary auditing and data transfer logging. System and guard log files can be accessed through the Log Viewer.

Use Cases

Forcepoint Data Guard provides defense-in-depth protections for your most critical data and ensures the strongest possible security controls. This is often a mandatory part of regulatory or policy directives for securing national security data and networks.

Sharing Aircraft Tracking Data

Air Operations Centers (AOCs) must coordinate between government- or military- controlled air-traffic management systems and those that are under Civilian control, in order to maintain commercial airspace safety and to manage the opening and closing of military airspace for commercial use. The ASTERIX data collected from radar system sensors must be transferred between these systems in a highly controlled and secure fashion.

Due to the critical nature of this data and the defined structure of the data type, Forcepoint Data Guard is uniquely suited to effectively facilitate this multilevel coordination.

Consolidation of Enterprise SIEM Data

Government agency network environments are frequently built (often mandated) using a physically-separated, multilevel network architecture to maintain a boundary between different classification/sensitivity levels or networks. This model is ideal for data and network protection but can be cumbersome when it comes to administration. This is true for Security Operations Centers (SOCs) and Defensive Cyber Operations Centers (DCOCs), and the tools they use to monitor and address system auditing and alerts.

Administrators commonly utilize a Security Information & Event Management (SIEM) solution to identify threats, manage risk and provide a holistic view of their security posture. Data residing on the individual networks must be kept separate; often times its administration must even be performed by separate individuals, due to the sensitive — and often classified — nature of this data. This results in a large number of separate monitoring tools, which makes it difficult to capture a common operational picture of what is happening across the enterprise.

The inclusion of Forcepoint Data Guard in the SIEM architecture supports the ability to transfer data from multiple, lower-level networks to a single, higher-level network. The result is one location to monitor the entire enterprise, providing administrators a comprehensive view across individual network boundaries.

Automating Communication between Meters and SCADA Systems

Power substations for manufacturing facilities are typically isolated from the SCADA IP network – making them secure but not very efficient. Manual processes are required to access and adjust power usage information, generation/distribution settings, and meter feedback.

With the inclusion of Forcepoint Data Guard in the architecture they can achieve secure automated, machine-to-machine communication between meters and substation. The guard validates all data transfers at the application/data layer. Only valid commands and data sets required for operations are allowed. Any data transaction that does not explicitly meet the Forcepoint Data Guard security policy is audited and rejected (e.g., writes to the meters are blocked). With Forcepoint Data Guard in place, automated bi-directional communications are securely enabled allowing for the elimination of manual processes and increased data security and reliability.

CONTACT
www.forcepoint.com/contact

[DATASHEET_FORCEPOINT_DATA_GUARD] 100072.020818