Cross Domain Security.
Data Guard.

Ștefan Scânteie
Sales Engineer, SEE

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

Data Guard: Enables Connection of the “Unconnectable”

To deliver defense-grade data control, at scale, Data Guard leverages a trusted operating system and security policies that enforce role and process separation and isolation to perform, automated, byte-level content inspection and sanitization with customizable rules to handle even the most specialized data types and protocols.

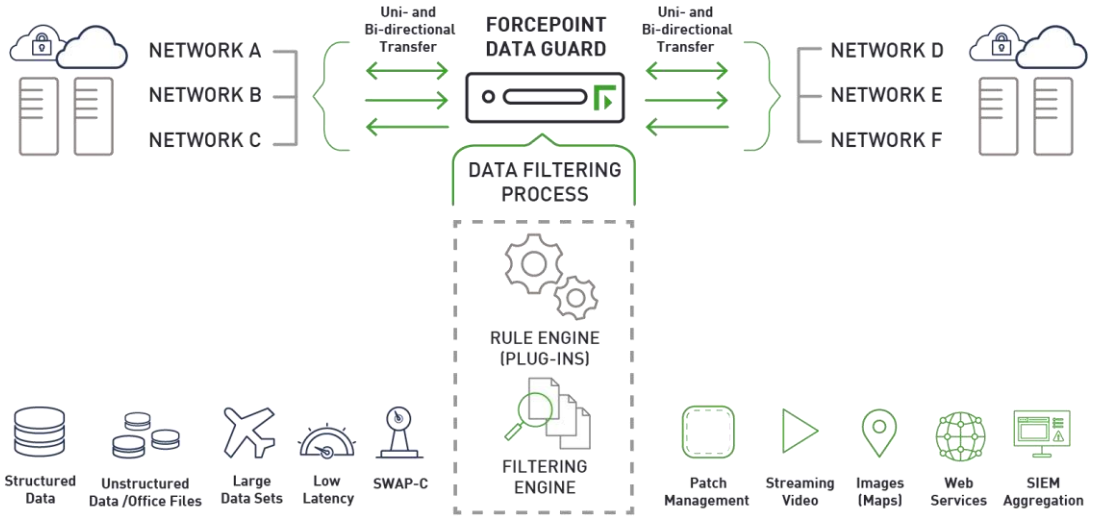
Environments: Typically for use in highly regulated environments such as: government, military, critical infrastructure, law enforcement; and any other environment that must:

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

- ***Today****:* Data Guard enables secure data and file (structured and unstructured data) movement between segmented networks. This movement can be configured for uni- or bi-directional communications between the networks. The trusted operating system foundation of Red Hat Enterprise Linux with SELinux allows Data Guard to be used in highly regulated environments.

- ***Tomorrow****:* Data Guard is designed to evolve as the demands on your environment change. Due to the highly flexible and customizable rule and policy-based structure of Data Guard, your enterprise is ready for the next new data types and devices that need to be monitored and controlled. **Forcepoint Professional Services** can assist you with understanding new data types and protocols and crafting the appropriate rules and policies for your enterprise.

DATA GUARD MARKETECTURE



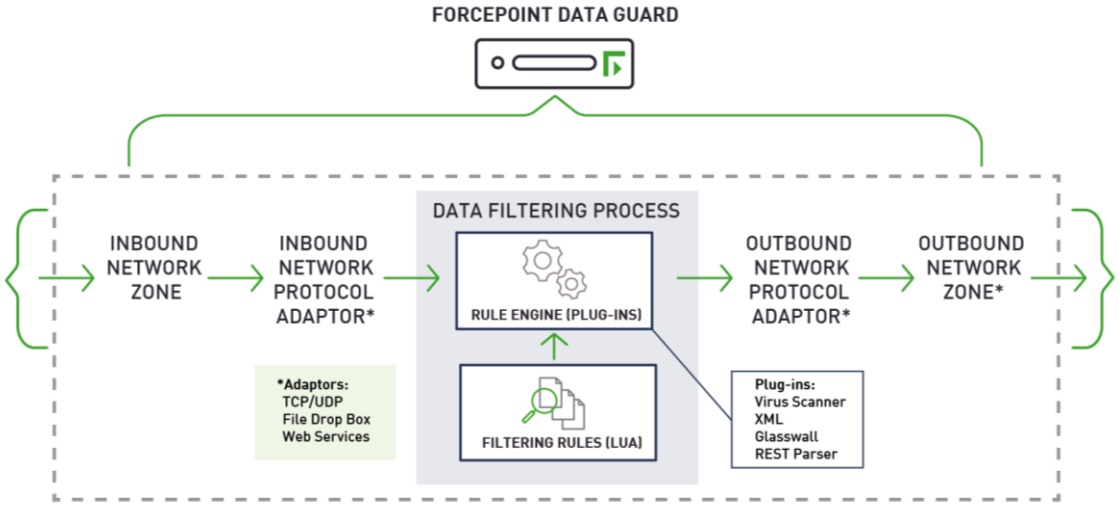
KEY POINTS:

- Multiple Air Gapped Networks:
  - 6 are shown
- Supports multiple transfer flows:
  - Bi-directional
  - Uni-directional
- Data filtering process inside the Guard consists of:
  - Rule Engine: plugins for pre-built rules
  - Filtering Engine
- *Icons on the left:* Broad data descriptions and specialized environments
- *Icons on the right:* Snap shot of common types of data frequently moved with a Guard

DATA GUARD: GOING DEEPER INTO THE ENGINE

KEY POINTS:

- Uni-directional flow through the Guard shown
- Adaptors =
  - **Service applications used to receive and transmit data from source and destination networks**. INBOUND, they terminate the network protocol and pass the data to the filter pipeline. OUTBOUND, they receive filtered data and send it out on to the network
- Plugins =
  - **Helper modules to the assist in the data filter process.** Plugins simplify the filtering rules (in the LUA language) needed to perform data validation and transformation



How Are Guards and Firewalls Different/Similar?

Firewalls/NGFWs

- Built with standard operating systems and open system management and updating procedures
- Built to support the most common environments, protocols and data out-of-the-box
- Excellent to detect and protect organizations from threats as a first layer of defense
- Inspection is performed at the protocol level
- Can be complemented by a Guard when deep inspection, validation, filtering and sanitization are required for file/data transfer

Guards

- Built on a trusted operating system that locks down and divides roles and processes in a compartmented manner
- Built to support, and meet the requirements of, highly sensitive, regulated, and air gapped/segmented environments and data
- Use rules and policies:
  - Provides flexibility to easily tailor each system to customer requirements and environments (Professional Services)
  - Specific to data types and flows and determine the inspection (byte-level), validation, remediation (allow/disallow), and sanitization actions
- Once configured, on-going rules/policy management is not typically necessary (set and forget)

Illustration of Firewalls and Guards

Enter the airport
Front doors, no direct security

FIREWALL

Check In –

- Verification of identity & proof of travel (show your boarding pass & identification)
- You match basic checks

Verified = Pass

NGFW

Security Check All –

- Luggage & body machine inspection for prohibited & hidden materials
- Deeper inspection
- Most people, standard procedures

Verified = Pass

GUARD (Transfer)

Security Check Special –

- Fine-grained, content-aware detailed inspections
- Filtering & sanitization
- Tailored to individual with personnel with specific roles & policies

Verified = Pass

Can Leverage Multiple Solutions for Defense-in-Depth

ELIMINATE THE NEED FOR:

- Manual Processes
- External Media
- Sneakernet

CONNECT THE UNCONNECTABLE

Thank you!

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain