Forcepoint

Datasheet

Forcepoint Policy Engine Guard

Protects organizations from accidental data loss and known malware infiltration at the network boundary.

Key Benefits

- Granular policies – by source, destination, user, group, content type, label, phrase, signed and/or encrypted content
- Data type identification – application of policy according to data type
- Labelling – apply policy based on identification of unstructured or structured protective markings/ security labels and user clearances
- Textual analysis – detection of words or phrases wherever they are embedded in content
- Authentication – address validation (email) and NTLM authentication of users (Web)
- Integrity – validation of S/MIME signed messages (email)
- Secrecy – deep content inspection of encrypted messages (email) and HTTP(s) web browsing

Platforms

- Physical: The Forcepoint MRB001 platform is certified for use with Oracle Solaris 10 (16GB RAM, 2 x 120GB hard disk, 2 x 6-core Intel Xeon processors) or any hardware platform on the Oracle Solaris 10 hardware compatibility list

The Policy Engine Guard is used by organizations that need to tightly control business content that needs to pass across an external boundary or between separate internal zones over email, web, or file transfer. It defends against known malware and accidental data loss by focusing on business content. It is ideally suited to systems in government, law enforcement, defense, and critical national infrastructure.

Deep Content Inspection

The Policy Engine Guard intercepts content at the boundary point and uses Deep Content Inspection (DCI) to examine it for the presence of known threats and the possibility of accidental data loss. Embedded content, including archives, are unwrapped to gain a complete picture of the data being carried. Data types contained within the traffic are identified so that those deemed a risk can be prevented from crossing the boundary. Malformed and encrypted data is blocked. In addition, application services traffic can be checked to ensure that the data being carried is constrained and conforms to definitions in pre-loaded schemas.

Consistent Content Security Policies across Multiple Protocols

The Policy Engine Guard can be deployed to check the content being carried across the boundary in SMTP Internet email, X.400 messaging, including military specific versions, file transfers using Forcepoint File Transfer Utilities, and in HTTP and HTTP(s). A graphical management console makes it easy to model and enforce content security policies that can be applied to one or multiple protocols ensuring an organization's content security policy is consistent across all ingress/ egress channels. Highly granular policy rules determine whether content should pass depending on source, destination, user, group, content type, data type, label, phrase, and the presence of signed and/or encrypted content.

Key Benefits (continued)

Platforms (continued)
- Virtual: Minimum specification - VMware ESXi virtual machine with 2 cores, 2GB RAM, 100GB hard disk, 2 network cards

Protocols
- SMTP email
- X.400 email including military specifications
- DSFSP (Forcepoint File Sharing Protocol)
- HTTP(s)

Operating System
- Solaris 10 (optionally with Trusted eXtensions (TX))
- CentOS 6 or 7

Management GUI
- Clearpoint Windows graphical management console
- Key Policy Areas
- Protocol control
- MIME type control
- Source/destination checking
- Size Restriction
- S/MIME Signature and encryption
- Data type checking
- Macro filtering
- Textual analysis
- XML schema validation
- Security labelling

Security Label Checking
- Supports S/MIME ESS, P772, X.411 and ASN.1 encoded labels and Subject, First Line of Text, Meta Data and Header/Footer text encoded labels
- Supports translation / mapping between labelling schemes

(Optional) Anti-Virus Integration
- Sophos
- McAfee

Alerts, Accounting and Auditing
- SNMP and SMTP alerting
- Off-box logging for SIEM integration
- Auditing for compliance and forensic investigation – to individual user level

Market Leading Protection for Protectively Marked Content

The Policy Engine can identify the security labels a sender attaches to a message/attachment in the case of email or the in the content of a web upload/download. The label can be either metadata or visible text that indicates the sensitivity of the information or any special restrictions on how it can be handled. Labels can be extracted from the first line of the message's text, its subject field, from message headers, from digital signatures, from document properties, and document headers/footers.

Integrity and Secrecy

When it comes to email, the Policy Engine Guard enforces address validation rules to ensure the sender's address belongs to the network they come from and can validate message signatures (S/MIME) applying appropriate constraints depending on whether a message is signed/unsigned.

The Policy Engine Guard can validate messages that are encrypted using the S/MIME standard, as long as the sender includes the Guard as a copy recipient. Rules can be set to allow the message to be delivered if its content is acceptable, or to strip the encryption before delivery. This prevents sensitive information leaking out of a system.

Connecting Networks Previously Thought Unconnectable

The Policy Engine Guard can be deployed on Forcepoint's Bastion platform, which connects two (or more) networks using separate network interfaces. It maintains strong separation between the networks while allowing traffic to pass between them, ensuring there is no other potential for attack or leaks and providing a way to connect networks that were previously thought unconnectable. Bastion is specially hardened to withstand direct attacks, using the advanced security mechanisms of Oracle's Solaris 10 Trusted Extensions operating system. These mechanisms ensure the critical content-checking Policy Engine cannot be bypassed and are independently assured with a Common Criteria EAL4 certification.

To request a demo →

forcepoint.com/contact

Forcepoint

[Forcepoint Policy Engine Guard Datasheet] 27Apr2022