EVERFOX

DATASHEET

Policy Engine Guard

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

Challenge

Organizations are grappling with the challenge of establishing a secure information-sharing environment that effectively safeguards against malware and data loss.

Solution

Implementing the Policy Engine Guard protects organizations from accidental data loss and known malware infiltration at the network boundary.

The Policy Engine Guard prevents data leakage of files uploaded to web pages and includes measures to stop known malware with an onboard AV engine and some unknown malware by removing active content in Office documents.

Benefits

- Granular policies
- Data type identification
- Labelling – apply policy based on identification of unstructured or structured protective markings/ security labels and user clearances
- Textual analysis
- Validation of S/MIME signed messages (email)
- Deep content inspection of encrypted messages (email) and HTTP(s) web browsing

The Everfox 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 regulated industries.

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, is 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 Everfox File Transfer Utilities, and in HTTP and HTTPs.

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.

Market leading protection for protectively marked content

The Policy Engine Guard 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.

Platforms

Physical

The Everfox 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 onthe Oracle Solaris 10 hardware compatibility list.

Virtual

Minimum specification - VMware ESXi virtual machine with 2 cores, 2GB RAM,100GB hard disk, 2 network cards.

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 labeling

Protocols

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

Operating system

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

Alerts, accounting, & auditing

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

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 labeling schemes

(Optional) Anti-virus integrations

- Sophos
- McAfee

Learn More: www.everfox.com