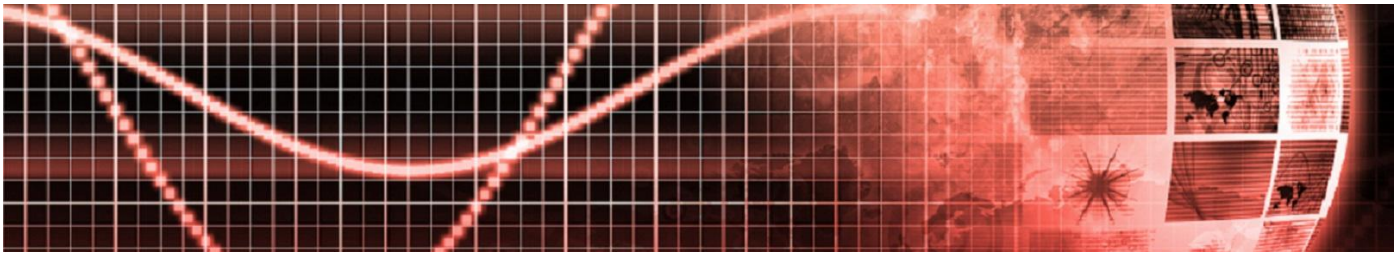
DEEP SECURE



Mail Guard

Email is indispensable for organisations intent on sharing information easily, collaborating across teams and driving business processes quickly and cost-effectively. But email is also a potent attack vector and an easy means of leaking sensitive information, both deliberately and accidentally.

- ✓ Block the spread of malware
- ✓ Data loss prevention
- ✓ Stop social engineering attacks
- ✓ Holds users accountable
- ✓ Ensure messages are authentic
- ✓ Preserve secrecy of messages
- ✓ Effective defence against cyber attacks

The Deep-Secure Mail Guard helps businesses control email traffic entering and leaving the organisation, and effectively defends against advanced attacks and misuse by focusing on the content.

The Guard is used by organisations that need to tightly control Internet email traffic or need to pass email between separate internal zones, without disrupting business processes. It is ideal for systems in Government, law enforcement, defence, pharmaceuticals, finance and utilities.

The Guard terminates email connections and performs deep content inspection of the messages and data they carry before re-establishing new connections for delivery. It also offers the firewalling and end point authentication functionality typically found in next generation firewalls, so it can hide internal services and limit communication to trusted mail servers internally and externally.

Malware and Data Loss Prevention

The Mail Guard performs deep content inspection of both the message and attachments, looking for hidden malware and sensitive information. Embedded content is unwrapped to gain a complete picture of the data.

Deep-Secure's powerful policy enforcement Engine applies rules that enforce constraints on the content and determines how the message is treated. Not only can these rules be conditional on the message sender and recipients, but also on features of the content itself.

Rule actions can be configured to match the security posture of the business, for example, silently discarding messages, putting them into quarantine or rejecting them with a non-delivery report. For more details see the Deep-Secure Policy Engine overview leaflet.

Message Authentication and Integrity

Address validation rules check messages to ensure the sender's address belongs to the network they come from. This prevents spoof messages entering a system as part of a social engineering attack.

The sender of a message can sign it so the recipient can be sure it is authentic and unaltered. The Guard can validate message signatures (S/MIME) and configured policy rules apply appropriate constraints to unsigned and signed messages. This mechanism can be used to block outgoing unsigned messages as a way of preventing unauthorised leaks and to block incoming spoof messages. The Guard can also be given a digital identity with which to sign, or countersign, outgoing messages.

Message Secrecy

The sender of a message can encrypt it so only the intended recipients can read it. The 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

Avoid Accidental Leaks

Messages can be reconstructed to remove meta-data that might reveal sensitive information about the organisation's internal infrastructure, from both message headers and the structures used to encode messages.

The Mail Guard can identify security labels the sender attaches to the message and its attachments. The security labels are meta-data or visible text that indicates the sensitivity of the information or any special restrictions on how it can be handled.

Security labels can be extracted from the first line of the message's text, its subject field, from message headers, from digital signatures, from attached document properties and document headers/footers.

Policy rules can govern how messages with different labels are treated, based on the identity of the sender and recipients or clearances assigned to them. For example, company sensitive documents can be blocked from being emailed to the Internet, unless they are encrypted and sent to trusted partners, preventing accidental leaks.

Quarantine Suspect Data for Closer Inspection

In some cases the checks cannot be certain that data is safe or not. For example, a message might have an attachment that contains a phrase that suggests the content is sensitive and so should be blocked, but the check cannot be certain that the phrase is not being used in some other context. To handle such cases, rules can be configured to place the message into a quarantine area. Here they can be inspected by an administrator and, if their content is acceptable, released to be delivered to their destination.

Keep Informed

Audit logs record activity to give administrators a view of the email traffic passing in and out of the system. Policy rules dictate the level of detail, up to full message content, that is retained and this can be selected on the basis of originator/recipient identity and message content.

The policy rules can identify critical circumstances that must be brought to the administrator's attention and deliver notifications by email. For example, the administrator might be sent an alert if a message is placed into quarantine, or if a virus is detected in an incoming message.

Protocols

The Mail Guard supports both Internet standard (SMTP/MIME) email and X.400 messaging, including the military specific versions. A single server running the Mail Guard can support both protocols.

The Mail Guard supports mail passing in both directions between two networks. However it can be configured to allow mail to pass in only one direction and can support the interconnection of multiple networks.

Platforms

The Mail Guard can run on a single computer placed within an existing Internet or internal gateway. In this configuration it uses Oracle's Solaris 10 operating system running on a commodity server.

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

The Mail Guard's rules and its quarantine area are configured and managed using a Windows application called ClearPoint. Administrators can use this application to configure and manage multiple Guards. Role based access controls determine the functions that each administrator can perform. Administrators are identified using strong certificate based authentication and the operations they perform are monitored, so even the administrators can be held to account for their actions.