



FACT
SHEET



SPAM & MALWARE PROTECTION

Effective protection against spam and malware with a fully automated, multi-level filtering system.

Representing over 50% of all email traffic, spam is the most intrusive method cyber criminals use to introduce malware and viruses into corporate systems. In addition to the danger of infection with ransomware, spyware or a cryptominer, important workflows can also be interrupted by the annoying flood of unwanted spam emails. A multi-level filtering system is a must if you want to stop spam and phishing emails from reaching your inboxes and disrupting the workflow.

Your mailboxes deserve the strongest filters



Multi-level spam detection
and dynamic filter levels



Dynamic Virus
Outbreak Detection



Protection from widescale DOS
and targeted mail bombing attacks

What is affected?



Email
environment



Highest spam
(99.9%) and
virus (99.99%)
detection rates
on the market.



Maximizing
security for
specific tenant
needs via
advanced rule
creation within
the compliance
filter.



Outgoing emails
are checked for
spam and
viruses.



Secure incoming
and outgoing email
communications

PRECISE ANALYSIS MECHANISMS AND RELIABLE FILTERS:

Phishing filter: Link tracking and other mechanisms effectively protect against phishing emails. Among other things, reloadable malicious script commands are detected. This enables, for example, the detection of dangerous drive-by downloads.

Infomail filter: Newsletters not classified as spam and other info emails that interrupt the workflow unnecessarily are filtered out and stored for later retrieval. They are listed in the individual quarantine report and can be delivered and allow listed by mouse click if required.

Link tracking: Incoming and outgoing emails are automatically scanned for malicious URLs.

Automatic virus signature update: The malware filters are constantly updated and are always up to date. Among other things, the company uses its own scanners, which are specialized in malware spread by emails.

Outbound filtering: Outgoing emails are checked for spam and viruses to prevent the customer from unintentionally sending or forwarding malware and spam emails.

Bounce management: Only genuine bounces reach the recipient in incoming mail traffic; bounces in response to spam with fake sender addresses are reliably filtered out.

Content filter for file attachments: Unwanted attachments can be rejected or moved to quarantine.

Dynamic virus outbreak detection: New and previously unknown viruses are stopped by the early warning system. Hornetsecurity permanently analyzes incoming emails on so-called honeypot accounts (email addresses whose sole purpose is to receive spam) for unusual attachments, links, senders or contents. The derivation of signatures from this is carried out within the shortest possible reaction time (usually <5 minutes).

Less than 0.00015 false positives: The number of regular emails inadvertently classified as spam is less than 0.00015.

EASILY MANAGE AND COMPLY WITH COMPLIANCE POLICIES

Quarantine report in configurable intervals: Users can adapt the delivery of their quarantine reports to their working methods and schedule them for specific times, even several times a day.

One-click release: Emails in quarantine can be delivered from the quarantine report with a click of the mouse, regardless of whether they are presumed spam messages or info emails.

Good overview thanks to blocking: The vast majority of all spam emails are blocked directly. This gives the user a quick overview of current emails in quarantine.

Eases the burden on the email server: Spam and Malware Protection only lets valid messages through, which significantly increases the performance of the customer mail server.