HORNETSECURITY

FACT SHEET

SPAM AND MALWARE PROTECTION

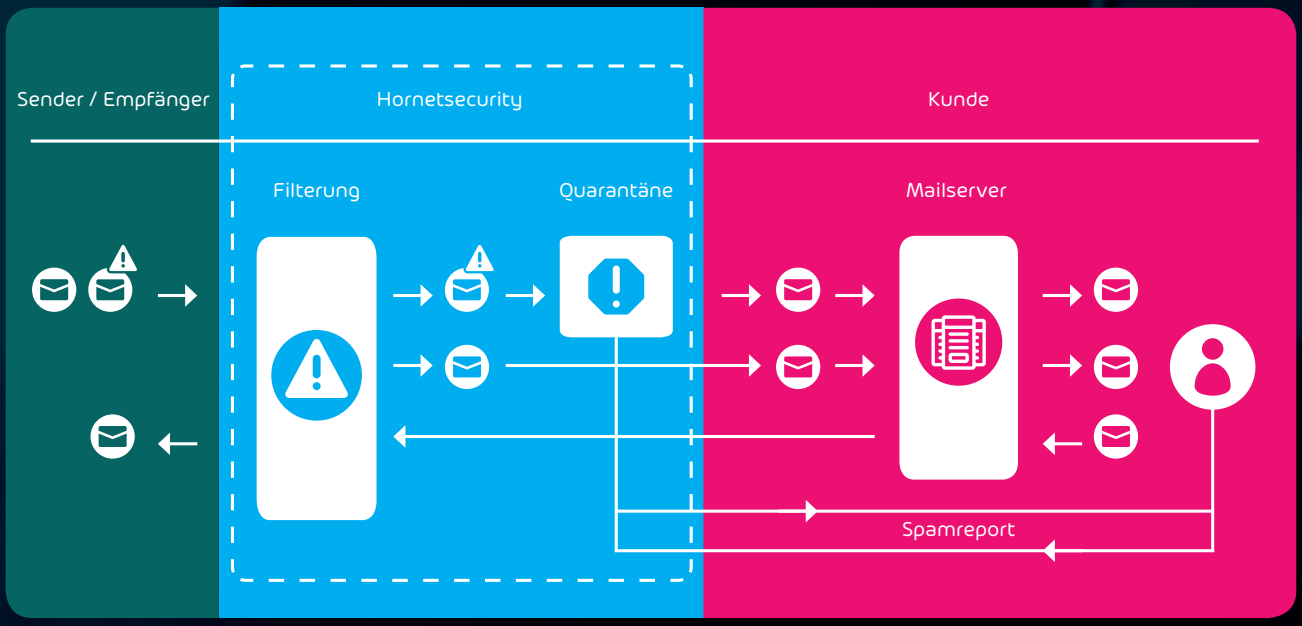
Mit einer garantierten Spamerkennung von 99,9% und einer Virenerkennung von 99,99% bietet Spam and Malware Protection die höchsten Erkennungsraten am Markt.

Mit einem Anteil von über 50% am gesamten E-Mail-Verkehr stellen Spam-E-Mails die aufdringlichste Methode Cyberkrimineller dar, um Malware und Viren ins System von Unternehmen zu schleusen. Die umfassenden Features und gründlichen Filtermechanismen von Spam and Malware Protection halten Ihr E-Mail-Postfach frei von lästigen und schadhaften Spam-E-Mails.

Schutz vor:

- **Viren**
- **DDoS-Attacken**
- **Backscatter**

INTEGRATION VON SPAM AND MALWARE PROTECTION IM E-MAIL MANAGEMENT SYSTEM



Eingehende E-Mails durchlaufen zwei Stufen:
Im Blocking-Stadium wird der Großteil der Spamnachrichten zurückgewiesen, die übrigen E-Mails erreichen die aktive Analyse, wo der E-Mail-Strom durch eine Vielzahl von Filterregeln gereinigt wird.

HORNETSECURITY

FACT SHEET

PRÄZISE ANALYSEMECHANISMEN UND ZUVERLÄSSIGE FILTER:

Phishing-Filter: Link-Tracking und weitere Mechanismen schützen wirksam vor Phishing-E-Mails. Dazu werden u. a. nachladbare schädliche Script-Befehle erkannt. Dies ermöglicht z.B. die Erkennung von gefährlichen Drive-By-Downloads.

Infomail-Filter: Nicht als Spam klassifizierte Newsletter und andere Infomails, die den Arbeitsablauf unnötig unterbrechen, werden aussortiert und zum späteren Abruf vorgehalten. Sie werden im individuellen Spamreport aufgelistet und lassen sich von dort bei Bedarf per Mausklick zustellen und whitelisten.

Link-Tracking: Eingehende und ausgehende E-Mails werden automatisch nach schädlichen URLs gescannt.

Automatische Virus-Signatur-Aktualisierung: Die Malwarefilter werden ständig aktualisiert und sind stets auf dem neuesten Stand. Eingesetzt werden u. a diverse eigene Scanner, der auf per E-Mail verbreitete Malware spezialisiert sind.

Outbound Filtering: Ausgehende E-Mails werden auf Spam und Viren geprüft, um zu vermeiden, dass der Kunde ungewollt Malware und Spam-Mails verschickt bzw. weiterleitet.

Bounce-Management: Im eingehenden Mailverkehr erreichen nur echte Bounces den Empfänger, Bounces als Antwort auf Spam mit gefälschten Absenderadressen werden zuverlässig ausgefiltert.

Content Filter für Dateianhänge: Unerwünschte Anhänge können zurückgewiesen oder in die Quarantäne verschoben werden.

Dynamic Virus Outbreak Detection: Neue und bisher nicht bekannte Viren werden durch das Frühwarnsystem gestoppt. Hornetsecurity analysiert dazu permanent eingehende Mails auf sogenannten Honeypot-Accounts (E-Mail-Adressen, die nur den Zweck haben Spam zu empfangen) auf ungewöhnliche Anhänge, Links, Absender oder Inhalte. Die Ableitung von Signaturen daraus erfolgt innerhalb kürzester Reaktionszeit (i.d.R. < 5 Minuten).

Weniger als 0,00015 False Positives: Die Zahl der versehentlich als Spam klassifizierten, jedoch regulären E-Mails liegt bei weniger als 0,00015.

EINFACHE VERWALTUNG UND EINHALTUNG VON **COMPLIANCE RICHTLINIEN:**

Spamreport in konfigurierbaren Intervallen: Benutzer können die Zustellung ihrer Spamreports an ihre Arbeitsweise anpassen und auf bestimmte Uhrzeiten legen, auch mehrmals am Tag.

One-Click-Release: E-Mails in der Quarantäne lassen sich aus dem Spamreport per Mausklick zustellen, egal, ob vermeintliche Spam-Nachrichten oder Infomails.

Gute Übersicht dank Blocking: Die überwiegende Mehrzahl aller Spam-E-Mails wird direkt geblockt. Der Benutzer erhält dadurch schnell einen Überblick über aktuelle E-Mails in der Quarantäne.

Entlastung des Mailservers: Spam and Malware Protection lässt nur gültige Nachrichten durch, was die Performance des Kunden-Mail-Servers deutlich erhöht.