



---

## Leistungsbeschreibung

### Spam and Malware Protection

1. Hornetsecurity filtert eingehende E-Mails des Auftraggebers auf schädlichen Inhalt (z.B. Viren), unerwünschte Werbung (z.B. Spam) und legitime Werbung (z.B. Newsletter) auf seinen eigenen IT-Systemen. E-Mails an den Auftraggeber werden dazu durch Umstellung der MX-Records für die zu filternden Domains des Auftraggebers auf die Server von Hornetsecurity geleitet. Für die Umstellung des MX-Records ist Hornetsecurity nicht verantwortlich.
2. Die Spamerkennungsrate liegt bei mindestens 99,9% im Monatsdurchschnitt, bezogen auf die Zahl aller E-Mails, die die Systeme von Hornetsecurity für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen. Voraussetzung ist die direkte Zustellung eingehender E-Mails per SMTP auf die Systeme von Hornetsecurity durch Umstellung der MX-Records der Domains des Auftraggebers.
3. Die Virenerkennungsrate liegt im Jahresdurchschnitt bei mind. 99,99%, bezogen auf die Zahl aller E-Mails, die die Systeme von Hornetsecurity für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen.
4. Die Falsch-Positiv-Rate liegt unter 0,00015 im Monatsdurchschnitt, bezogen auf die Zahl aller Clean-E-Mails, die die Systeme von Hornetsecurity für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen. Ausgenommen sind solche E-Mails, die durch falsch konfigurierte Server (nicht RFC-Konform), über verifizierte Open Relays oder mangelhaft eingerichtete Mailclients versendet wurden.
5. Die Verfügbarkeit im Mailverkehr per SMTP beträgt 99,99% im Jahresmittel. Voraussetzung ist die direkte Zustellung eingehender E-Mails per SMTP auf die Systeme von Hornetsecurity durch Umstellung des MX-Records. Geplante Wartungsarbeiten werden nicht berücksichtigt, diese werden soweit es möglich ist am Wochenende nachts ausgeführt (MEZ).
6. Soweit der Auftraggeber es wünscht werden auch ausgehende E-Mails gefiltert.
7. Empfangene E-Mails werden:
  - a. Geblockt (zurückgewiesen), soweit sie noch während der Aufnahme der Datenverbindung mit den Servern von Hornetsecurity mit hoher Sicherheit als unerwünscht erkannt werden,
  - b. Wahlweise In Quarantäne gestellt oder mit einer Markierung im Betreff zugestellt, sofern sie nach vollständiger Annahme der E-Mail durch die Server von Hornetsecurity als unerwünscht erkannt werden,
  - c. Zugestellt oder zur Abholung bereitgestellt, sofern sie als erwünschte E-Mail erkannt werden.
  - d. Die Zustellzeiten liegen typisch im Durchschnitt bei unter 30 Sekunden, der maximale durchschnittliche Wert liegt bei 3 Minuten.
8. E-Mails in Quarantäne werden drei Monate zur Einsicht durch autorisierte Benutzer des Auftraggebers gespeichert. Auf Wunsch des Auftraggebers werden Benutzer über neue E-Mails in der Quarantäne informiert (in der Regel einmal täglich).
9. Auf E-Mails in der Quarantäne können autorisierte Benutzer aus dem Internet zugreifen. Autorisierte Benutzer können interaktiv die Zustellung von E-Mails in Quarantäne auf die Systeme des Auftraggebers veranlassen.
10. Autorisierte Nutzer können persönliche White- und Blacklists pflegen. Die Konfiguration kann über verschiedene Wege erfolgen, z.B. Hornetsecurity Control Panel,



- 
- Quarantäne Bericht, oder das Hornetsecurity Outlook Add-In.
11. Soweit Eingriffe durch den Auftraggeber in die Filterstufen erfolgen (z.B. Einrichten von speziellen White- oder Blacklists), können Qualität und Erkennungsraten der Filterstufen nicht gewährleistet werden.
  12. Autorisierte Nutzer des Auftraggebers (z.B. Support-Mitarbeiter und Administratoren) können über das Hornetsecurity Control Panel den kompletten Mailverlauf des Auftraggebers überblicken. Im Live-Monitor können zusätzlich auch alle geblockten (abgewiesenen) E-Mails der vergangenen 7 Tage nachverfolgt werden.
  13. Optional werden ein- und ausgehende E-Mails entsprechend eingestellter Richtlinien gefiltert (Content und Compliance-Filter). Je nach Einstellung werden E-Mails, die den Richtlinien nicht entsprechen:
    - a. mit einer entsprechenden Fehlermeldung zurückgewiesen (eingehend),
    - b. ohne Anhang zugestellt und mit Anhang in eine Quarantäne gestellt, aus der sie von Administratoren dem Empfänger zugestellt werden können (eingehend),
    - c. mit einer entsprechenden Fehlermeldung zurückgewiesen (ausgehend).
  14. Die Richtlinien zur Content- und Compliance- Filterung können von dazu autorisierten Benutzern des Auftraggebers im Hornetsecurity Control Panel eingestellt werden.
  15. E-Mails werden über einen per TLS verschlüsselten Kanal übertragen, soweit die Gegenseite die Übertragung per TLS unterstützt. Weitere Verschlüsselungsverfahren können optional über den Hornetsecurity Encryption Service genutzt werden.
  16. Der Inhalt zugestellter E-Mails wird nur gespeichert, wenn der optionale Hornetsecurity Continuity Service oder das Hornetsecurity Archiving zusätzlich genutzt wird.
  17. Hornetsecurity kann neben den bereits bestehenden Methoden und Verfahren zur Erkennung von Viren weitere AV-Engines von Antivirus Spezialisten optional hinzuschalten.
  18. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Bestandteil dieses Vertrags.
  19. Auf Wunsch kann der Kunde Weiterleitungspostfächer definieren, über die der E-Mail-Verkehr an einen oder mehrere, bis zu 100, interne oder externe Postfächer weitergeleitet werden kann. Die maximale Größe für die Weiterleitung von E-Mails über Weiterleitungspostfächer richtet sich nach der Anzahl der Weiterleitungsempfängern:
    - a. Bei einem Weiterleitungsempfänger greifen die Standardeinstellungen des Kunden.
    - b. Bei bis zu 9 Empfängern darf die Größe der E-Mail bis zu 50MB betragen.
    - c. Bei 10 bis 24 Empfängern darf die Größe der E-Mail bis zu 30MB betragen.
    - d. Bei 25 bis 49 Empfängern darf die Größe der E-Mail bis zu 15 MB betragen.
    - e. Bei 50 bis 100 Empfängern darf die Größe der E-Mail bis zu 10 MB betragen.
  20. Fair Use Limits (Einschränkungen zur angemessenen Nutzung)
    - a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Soft-ware erforderlich sind und die wir in diesem Zusammenhang zur Verfügung stellen, werden von allen unseren Kunden gemeinsam genutzt. Daher haben wir das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösung angemessen und fair nutzen, so dass eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.
-



- 
- b. Wir haben uns dazu entschlossen, keine Richtwerte vorab festzulegen, die eine exzessive oder unangemessene Nutzung bestimmen, da wir nach unserem Ermessen entscheiden können, unsere normalen Service-Levels aufrechtzuerhalten, indem wir anderen Nutzern reservierte Ressourcen, die zu diesem Zeitpunkt nicht genutzt werden, neu zuweisen oder Ressourcen anderweitig skalieren. Sie verstehen, dass wir, wenn wir uns entscheiden, unsere Richtlinie zur angemessenen Nutzung nicht aktiv durchsetzen, nicht davon ausgehen, dass wir auf unser Recht, dies zu tun, verzichtet haben, noch haben wir zugestimmt, dass Sie unsere Dienste weiterhin auf demselben Niveau nutzen, wie Sie es zu einem bestimmten Zeitpunkt tun.
- c. Um unsere Dienste nutzen zu können, müssen Sie abrechenbare Einheiten erwerben. Die Anzahl der abrechenbaren Einheiten, die Sie benötigen, hängt von einer Reihe von Kriterien ab, wie z. B. der Größe Ihres Unternehmens, der Anzahl der Nutzer und der Speichergröße der jeweiligen Datenquellen. Sie können die Anzahl der abrechenbaren Einheiten, die Sie benötigen, anhand unserer Leitfäden, die wir auf unserer Webseite für Gebühren und Abrechnungen hochgeladen haben, oder durch die Unterstützung unseres Vertriebsteams ermitteln.
- d. Unabhängig von der Anzahl der abrechenbaren Einheiten, die Sie erworben haben, müssen Sie unsere Dienstleistungen zweckmäßig nutzen, und zwar in einer Weise, die es nicht erforderlich macht, dass wir unverhältnismäßig viele Ressourcen zuweisen müssen. Um dies festzustellen, werden wir Ihre Nutzung unserer Ressourcen und Ihren Speicherbedarf mit dem eines durchschnittlichen Kunden vergleichen.
- Den Durchschnittskunden ermitteln wir, indem wir die 5% höchsten und die 5% niedrigsten Kunden der jeweiligen Ressource unberücksichtigt lassen und den Mittelwert über alle unsere aktiven Kunden bilden.
- e. Spezifische Merkmale, die sich auf die Branche beziehen, in der Sie tätig sind, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.
- f. Wenn wir nach vernünftigem Ermessen und in gutem Glauben davon ausgehen, dass die Nutzung unserer Lösung durch Sie nicht sinnvoll ist oder gegen diese Richtlinie verstößt, werden wir nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen:
- i. Ihnen erlauben, unsere Lösungen weiterhin zu nutzen, jedoch vorbehaltlich unter der Bezahlung zusätzlicher Gebühren und der Einhaltung von Bedingungen, die wir unter den gegebenen Umständen für angemessen halten.
  - ii. Sie zu informieren, dass Ihr Konto innerhalb eines nach unserem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieses Zeitraums werden die Backups ausgesetzt.
- g. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:
- i. werden Ihre Sicherungsdaten am Ende des von uns in der diesbezüglichen Benachrichtigung fest-gelegten Zeitrahmens gelöscht, ungeachtet anderslautender Bestimmungen in den Allgemeinen Geschäftsbedingungen.
  - ii. erhalten Sie eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage Ihres Abonnementzeitraums.
-