



Leistungsbeschreibung

365 Extended Email Protection

365 Extended Email Protection bietet durch den Integrated Cloud Email Security Ansatz eine zusätzliche Sicherheitsebene zum Schutz des E-Mail-Verkehrs von Microsoft 365-Kunden. Die KI-gestützten Anti-Spam- und Malware-Filter von Hornetsecurity analysieren den eingehenden E-Mail-Verkehr in Echtzeit auf fortschrittliche Cyber-Bedrohungen und entfernen Spam und schadhafte E-Mails zuverlässig und innerhalb weniger Sekunden aus den Postfächern der Benutzer. Die vollautomatische und nahtlose Integration des Services in die Microsoft 365-Plattform ermöglicht eine kontinuierliche Überwachung aller Postfächer und stützt sich auf die 24/7-Threat Intelligence von Hornetsecurity, um den aktuellsten Schutz zu gewährleisten.

Voraussetzung für die Nutzung des Services ist die Verwendung von Microsoft Cloud-Lizenzen mit durch Microsoft aktivierter Exchange-Funktionalität.

Folgende Leistungen sind im Produkt 365 Extended Email Protection enthalten:

1. Einfaches Onboarding

- a. Die Einrichtung von 365 Extended Email Protection erfolgt automatisiert. Alle Domains, Postfächer und Gruppen des Endkunden werden direkt aus Microsoft 365 in das Hornetsecurity Control Panel übertragen.
- b. Voraussetzung für die Nutzung der Hornetsecurity Services für Microsoft 365 ist die Freigabe der Hornetsecurity App-ID für den Microsoft 365 Tenant durch einen administrativen Benutzer des Endkunden. Dies geschieht einmalig im Onboarding-Prozess.
- c. Eine Umstellung der MX-Records ist für die Nutzung des Services nicht erforderlich, denn 365 Extended Email Protection wird per API-Schnittstelle nahtlos mit der 365 Plattform integriert. Alle eingehenden E-Mails des Endkunden werden mittels des E-Mail-Journaling kopiert und durch die erweiterten E-Mail-Filter von Hornetsecurity gefiltert.
- d. Das Onboarding kann entweder direkt im Control Panel oder mittels eines externen Onboarding Links durchgeführt werden.

2. Single Sign-on

- a. Alle Benutzer können sich mit ihren administrativen Benutzerdaten für Microsoft 365 bei Hornetsecurity authentifizieren.
- b. Sind die Benutzer bereits bei Microsoft 365 angemeldet, müssen sie sich nicht erneut bei Hornetsecurity authentifizieren.



3. Erkannte Bedrohungen

- a. Den Benutzern werden alle als Gefahr erkannten und aus den Mailboxen entfernten E-Mails in einer individuellen einstell- und filterbaren Übersicht angezeigt. Zudem werden ausführliche Informationen zu jeder E-Mail angezeigt.
- b. Hornetsecurity analysiert mittels des E-Mail-Journaling eingehende E-Mails des Endkunden auf schädliche Inhalte (z. B. Viren) und unerwünschte Werbung (z. B. Spam). Schadhafte E-Mails und unerwünschte Werbung werden automatisiert aus den Mailboxen des Endkunden entfernt.
- c. E-Mails können durch die Benutzer aus der Übersicht wiederhergestellt und an den Empfänger zugestellt werden.
- d. Entfernte E-Mails werden 3 Monate in Quarantäne zur Einsicht und zur Wiederherstellung durch die Benutzer gespeichert.
- e. Die Spam- und Threat-Erkennungsrate liegt bei mindestens 99,9% im Monatsdurchschnitt, bezogen auf die Zahl aller E-Mails, die die Systeme von Hornetsecurity für Domains des Endkunden im gemessenen Zeitabschnitt erreichen.
- f. 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 Endkunden im gemessenen Zeitabschnitt erreichen.

4. Dashboard

Über das Dashboard erhält der Nutzer eine Übersicht über die gebuchten Services von Hornetsecurity.

5. Reporting & Compliance

- a. Der Endkunde erhält weitreichende Informationen und Statistiken zu seinem aktuellen Sicherheitsstatus.
- b. Darunter fallen E-Mail-Statistiken und erweiterte Gefahrenstatistiken:
 - Gesamtsumme der gescannten E-Mails
 - Gesamtsumme der erkannten Bedrohungen
 - E-Mails klassifiziert nach Gefahr über den Zeitverlauf
 - Top 100 der angegriffenen Mailboxen
 - Angriffe über den Zeitverlauf
 - Gefahren nach Typ und Angriffsvektor
 - Angriffsvektoren über den Zeitverlauf
- c. Die von Benutzern des Control Panels durchgeführten Aktivitäten werden in einem Activity Log protokolliert, z.B. die Wiederherstellung einer E-Mail oder die erfolgreiche Einrichtung eines weiteren Services.



6. Fair Use Policy (Richtlinie zur angemessenen Nutzung)

- a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Software 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 Fair Use Policy nicht aktiv durchzusetzen, 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, z. B. von der Größe Ihres Unternehmens, der Anzahl der Benutzer, der Größe des Datenspeichers der jeweiligen Quelle usw. 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 (z. B. Speicherbedarf, Anzahl paralleler Verbindungen) 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 dieser Zeit werden alle Services und/oder der Betrieb ausgesetzt.
- g. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:
- i. werden alle Daten (Metadaten, Sicherungsdaten oder andere) 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.