07.03.2022

Hornetsecurity Managed Security Services

Vertragsbedingungen und Leistungsbeschreibung

1 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 der Hornetsecurity Archiv Service 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.

2 Leistungsbeschreibung Advanced Threat Protection (ATP)

1. Hornetsecurity ATP schützt den E-Mail-Verkehr von Unternehmen vor gezielten und individuellen Angriffen,

wie Spearphishing, Blended Attacks, Advanced Persistent Threats, Ransomware und CEO-Fraud.

2. Zur Erkennung von Angriffen werden als verdächtig eingestufte E-Mails des Auftraggebers durch folgende Filtertechniken untersucht:
    a. Sandboxing: Verdächtige E-Mail-Anhänge werden in mehreren separaten, geschützten Umgebungen geöffnet oder ausgeführt und ihr Verhalten auf mögliche Schadwirkung untersucht. Als verdächtig werden insbesondere Anhänge eingestuft, in denen ausführbarer Code gefunden wird.
    b. Link Scanning: In E-Mails oder in E-Mail-Anhängen enthaltende URLs werden aktiviert und das resultierende Verhalten analysiert.
    c. Link Rewriting: URLs in E-Mails werden durch andere URLs ersetzt, die die entsprechenden Inhalte bei Aktivierung über Hornetsecurity Web Filter abrufen. Ggf. werden heruntergeladene Daten per Sandboxing auf ihr Verhalten untersucht. Durch den Web Filter als potentiell gefährliche erkannte Inhalte werden gesperrt.
    d. Targeted Fraud Forensics: Heuristische Filter zur Erkennung gezielter Angriffe, mit Prüfung von Authentizität und Integrität von Metadaten und E-Mail-Inhalten, Erkennung und Blockierung gefälschter Absender-Identitäten, Erkennung gefälschter Inhalte, Erkennung von Angriffen auf besonders schützenswerte Daten, insbesondere Daten die Zahlungsflüsse betreffen (z.B. Kreditkartendaten, Rechnungen, Zahlungsanweisungen), Erkennung gezielter Angriffe auf besonders exponierte Personen des Auftraggebers (z.B. Buchhaltung, CFO, CEO, Controlling).
    e. Freezing: Zeitweiliges "Einfrieren" verdächtiger E-Mails. Eingefrorene E-Mails werden nach einigen Minuten erneut mit aktualisierten Filtern verarbeitet.
    f. Malicious Document Decryption: Verschlüsselte E-Mail-Anhänge in Form von Office-Dateien, Archiven und PDF-Dateien werden vor dem Eintreffen beim Empfänger entschlüsselt, sofern das Passwort aus der E-Mail rekonstruiert werden kann, und die Inhalte nach einer möglicher Schadsoftware untersucht.
    g. Ex-Post-Alarmierung: Stellt sich im Nachhinein heraus, dass eine bereits zugestellte E-Mail doch als potentiell schädlich eingestuft werden muss, erhält das IT-Sicherheitsteam eines Unternehmens nach Bekanntwerden eine Alarmierung.
3. E-Mails können durch die zusätzliche aufwändige Filterung zeitlich verzögert zugestellt werden. Die Verzögerung beträgt im Einzelfall maximal 15 Minuten.
4. Als potenziell schädlich identifizierte E-Mails werden von Hornetsecurity in Quarantäne gestellt.
5. Auf quarantinierte E-Mails kann der Auftraggeber über das Hornetsecurity Control Panel zugreifen.
6. E-Mails in der Quarantäne können von Administratoren des Auftraggebers aus dem Control Panel heraus per Sandboxing geprüft werden. Detaillierte Ergebnisse der Prüfung werden über das Control Panel zur Verfügung gestellt.

7. Sicherheitsverantwortliche des Auftraggebers werden bei erkannten Bedrohungen unmittelbar per E-Mail über die Bedrohung informiert (Real-Time Alerts).
8. Für den ATP-Dienst wird eine Verfügbarkeit von 99,9% garantiert, ausgenommen sind angekündigte Wartungszeiten.

3 Leistungsbeschreibung Archiving

1. Hornetsecurity Archiving ist eine Erweiterung der Hornetsecurity Spam and Malware Protection und setzt dessen Nutzung voraus.
2. Hornetsecurity archiviert E-Mails des Auftraggebers revisionssicher auf seinen eigenen IT-Systemen.
3. Auf die archivierten E-Mails können autorisierte Benutzer aus dem Internet zugreifen. Archivierte E-Mails können nach bestimmten Kriterien und Inhalten durchsucht werden, um bestimmte E-Mails im Archiv ausfindig zu machen. Autorisierte Benutzer können interaktiv die erneute Zustellung archivierter E-Mails auf die Systeme des Auftraggebers veranlassen.
4. Der Zugriff durch autorisierte Nutzer erfolgt über ein webbasiertes Frontend (Control Panel) oder die Progressive Web App für iOS und Android.
5. Die Archivierungsdauer und Archivierungsausnahmen können auf Domain, Gruppen oder Nutzer Ebene festgelegt werden.
6. Hornetsecurity garantiert die Verfügbarkeit der archivierten E-Mails für den Auftraggeber, für die vorab durch den Auftraggeber konfigurierte Dauer in vollständigen Jahren ab Ende eines Kalenderjahres, in dem die jeweilige archivierte E-Mail versandt bzw. erhalten wurde.
7. Die Standardeinstellung für die Archivierung beträgt 10 Jahre. Der Auftragnehmer kann per Control Panel oder API abweichende Einstellungen setzen, die ab dem Zeitpunkt der Einstellung für neu eingegangene E-Mails, jedoch nicht rückwirkend, gelten.

   Voraussetzung ist die Fortdauer des Vertrags und die Erfüllung der vertraglichen Pflichten durch den Auftraggeber. Für den Fall der Beendigung dieses Vertrags setzt die fortdauernde Verfügbarkeit den Abschluss eines Anschlussvertrags über die kostenpflichte Aufrechterhaltung der Datenspeicherung voraus. Hornetsecurity behält sich vor, die archivierten Mails auch bei vorzeitiger Vertragsbeendigung für den vorab festgelegten Zeitraum zu archivieren. Eine explizit gewünschte Löschung vor Erreichen der Archivierungsdauer muss gesondert beantragt werden mittels Löschersuchen nach DSGVO.
8. Autorisierte Benutzer können E-Mails als „privat" markieren. Auf als „privat" markierte E-Mails ist anschließend kein Zugriff aus dem Archiv mehr möglich.
9. Hornetsecurity garantiert die Zugriffsmöglichkeit autorisierter Benutzer auf die archivierten E-Mails im Normalfall 24 Stunden am Tag an allen Tagen im Jahr. Ausgenommen sind Wartungszeiten.
10. Speziell autorisierte Nutzer können einen speziellen Zugang einrichten, der den Zugriff auf alle archivierten E-Mails eines bestimmten Zeitraums erlaubt (Prüfzugang, z.B. zum Zweck einer Betriebsprüfung). Einrichtung und Nutzung des Prüfzugangs werden geloggt.
11. Archiviert werden solche E-Mails, die
    a) durch den Auftraggeber über die Server von Hornetsecurity an Dritte verschickt werden (ausgehende externe E-Mails),
    b) dem Auftraggeber durch Dritte über die Server von Hornetsecurity zugeschickt werden (eingehende externe E-Mails),
    c) der Auftraggeber zur Archivierung durch Hornetsecurity über vereinbarte Schnittstellen an Hornetsecurity zur Verfügung stellt (interne E-Mails, optional).
12. Die Archivierung genügt den derzeitigen gesetzlichen Auflagen in Deutschland bezüglich der elektronischen Archivierung

von E-Mails. Hornetsecurity wird alles in seiner Macht stehende veranlassen, um die Erfüllung dieser gesetzlichen Auflagen auch im Fall der Änderung dieser Auflagen sicher zu stellen.

13. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.
14. Hornetsecurity stellt die Geheimhaltung der archivierten Daten und sonstiger im Rahmen dieses Vertrags bekannt gewordenen geschäftlichen Geheimnissen des Auftraggebers gegenüber Dritten sicher. Die Pflicht zur Geheimhaltung besteht auch nach Ende dieses Vertrags fort.
15. Im Preis ist die Bereitstellung von unlimitiertem Speicherplatz für alle lizenzierten Postfächer enthalten.
16. Hornetsecurity bietet optional den Nachimport bestehender Archivdaten an. Die Archivdaten müssen in einem festgelegten Format angeliefert werden. Die technischen Voraussetzungen und Rahmenbedingungen können bei Hornetsecurity erfragt werden. Der Nachimport bestehender Archivdaten ist kostenpflichtig.
17. Auf Wunsch exportiert Hornetsecurity die bestehenden Archivdaten auf einen externen Datenträger. Der Export erfolgt im EML Format auf einem verschlüsselten Datenträger, der anschließend an den Auftraggeber gesendet wird. Der Export von Archivdaten ist kostenpflichtig.
18. Mit dem Aeternum Export Manager ist es zudem möglich, archivierte E-Mails auf Postfachbasis im Selfservice zu exportieren und anschließend herunterzuladen. Für den Export stehen die Formate PST, EML und MBOX zur Verfügung. Der Export von Archivdaten mit dem Aeternum Export Manager ist kostenpflichtig.

4 Leistungsbeschreibung Email Encryption

1. Der Hornetsecurity Email Encryption ist eine Erweiterung des Hornetsecurity Spam and Malware Protection und setzt die Nutzung des Spamfilterservice voraus.
2. Hornetsecurity verschlüsselt und signiert ausgehende E-Mails und entschlüsselt eingehende E-Mails des Auftraggebers auf seinen eigenen IT-Systemen entsprechend den eingestellten Richtlinien.
3. Ausgehende E-Mails werden per S/MIME signiert, sofern die dazu nötigen privaten Schlüssel im Zertifikatsspeicher vorliegen.
4. Die Richtlinien zur Verschlüsselung ausgehender E-Mails können von dazu autorisierten Benutzern des Auftraggebers im Hornetsecurity Control Panel eingestellt werden.
5. Je nach Einstellung der Richtlinien werden ausgehende E-Mails:
   a) mit dem öffentlichen Schlüssel des Empfängers per S/MIME oder PGP verschlüsselt übertragen,
   b) nicht verschlüsselt aber über einen per TLS verschlüsselten Kanal übertragen,
   c) im geschützten Hornetsecurity Websafe für den Empfänger bereitgestellt,
   d) unverschlüsselt übertragen.
6. Die Policies können durch autorisierte Benutzer z.B. im Hornetsecurity Control Panel gesetzt werden. Die Verschlüsselung einer Mail kann zusätzlich durch den Benutzer beim Versand über einen Betreff-Zusatz („Tag") oder das Hornetsecurity Outlook Add-In sichergestellt werden.
7. Sofern die Richtlinie zwingend die verschlüsselte Übertragung vorsieht, aber der dazu nötige öffentliche Schlüssel des Empfängers nicht im Zertifikatsspeicher vorliegt und die ggf. eingestellte Übertragung per TLS vom empfangenden Server nicht unterstützt wird, werden ausgehende E-Mails an diesen Empfänger zurückgewiesen und nicht übertragen.
8. Eingehende, per S/MIME oder PGP verschlüsselte E-Mails werden automatisch entschlüsselt, sofern der dazu nötige private Schlüssel des Empfängers im Zertifikatsspeicher vorliegt.
9. Öffentliche Schlüssel werden automatisch aus Signaturen eingehender E-Mails

extrahiert und im Zertifikatsspeicher hinterlegt.

10. S/MIME-Zertifikate für Benutzer des Auftraggebers können im Rahmen der S/MIME User Subscription per Control Panel bestellt werden. Alternativ können PGP Keys für die Benutzer des Auftraggebers generiert oder vorhandene S/MIME Zertifikate und PGP Keys vom Hornetsecurity Support im Zertifikatsspeicher abgelegt werden. Für die Nutzung von Zertifikaten und Keys erhebt Hornetsecurity eine jährliche Gebühr pro Zertifikat und Key des Benutzer gemäß der aktuellen Preisliste. Diese Subscription verlängert sich automatisch sofern sie nicht 3 Monate vor Ablauf deaktiviert wird und inkludiert die automatische Neubestellung von Zertifikaten und Keys bei Bedarf.
11. Hornetsecurity stellt die Geheimhaltung der im Zertifikatsspeicher gespeicherten privaten Schlüssel des Auftraggebers sicher. Die Pflicht zur Geheimhaltung besteht auch nach Ende dieses Vertrags fort.
12. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.
13. Hornetsecurity ermöglicht optional eine Anbindung der E-Mail-Infrastruktur des Kunden an den E-Mail made in Germany (EmiG) – Verbund und realisiert hierfür die Mailserver-seitige Umsetzung, die für die Erfüllung der Anforderungen an eine durchgehende Transportverschlüsselung von E-Mails im EmiG-Verbund notwendig sind.
    a. Hornetsecurity stellt sicher, dass eine als EmiG gekennzeichnete Nachricht nicht über andere, potenziell unsichere Kanäle zugestellt wird.
    b. Die durchgängig verschlüsselte Datenübertragung zwischen den Mail Transfer Agents (MTAs) hierfür wird sichergestellt mittels STARTTLS-Erweiterung gemäß RFC 3207.
    c. Die TLS1.2-Verbindung wird durch Hornetsecurity eingehend (TLS-Client) wie ausgehend (TLS-Server) realisiert.
    d. Hornetsecurity stellt sicher, dass EmiG-Kommunikation nur unter Verwendung Perfect Forward Secrecy (PFS)-fähiger Schlüsselaustauschverfahren basierend auf dem Diffie-Hellmann-Verfahren aufgebaut wird.
    e. Bei Schlüsselneuverhandlungen für Mailkommunikation innerhalb des EmiG-Verbundes verwendet Hornetsecurity secure renegotiation gemäß RFC 5746.
    f. Jeder Zertifikats- / Verschlüsselungsfehler beim STARTTLS-Aufbau wird genauso behandelt, als sei gar keine SMTP-Verbindung aufgebaut worden: Die Mail wird in eine Mail-Queue zurückgestellt, aus der weitere Zustellversuche unternommen werden. Bei dauerhaftem Fehlschlagen der Zustellung wird eine Bounce-Nachricht an den Sender geschickt.
    g. Hornetsecurity überprüft anhand der innerhalb des EmiG-Verbunds annoncierten Zertifikatsfingerprints die Identität und EmiG-Verbund-Zugehörigkeit der Kommunikationspartner der Nutzer des Kunden:
    h. Der per MX-Lookup ermittelte Hostname eines Mailservers wird mit dem im Host-Zertifikat hinterlegten Namen abgeglichen.
    i. Es wird überprüft, ob der Fingerprint des vom Mailserver des Kommunikationspartners verwendeten Zertifikats dem über EmiG annoncierten Fingerprints entspricht.
    j. Schlägt diese Validierung fehl, wird die E-Mail-Kommunikation mit diesem Mailserver unterbrochen, die Mail wird nicht weitergeleitet.
    k. Die Zertifikatsprüfung wird gemäß PKIX einschließlich der Sperrprüfung der Server- und Sub-CA-Zertifikate durchgeführt.

l. Die per https vom EmiG-Verbund bidirektional zur Verfügung zu stellenden JSON-MX-Infrastrukturlisten werden durch Hornetsecurity gemäß der EmiG-Vorgaben für den Kunden vollautomatisch generiert und gepflegt.
m. Hornetsecurity annonciert die notwendigen Informationen, die der Kunde dem EmiG-Verbund mitzuteilen hat, über die von EmiG vorgegebenen Verfahren (MX-Infrastruktur-Listen).
n. Die Authentifikation des sendenden Mailservers als Server eines EmiG-Teilnehmers wird mittels dynamischem Abgleich mit den bei EmiG registrierten IPs durchgeführt.
o. Hornetsecurity bietet dem Kunden verschiedene Möglichkeiten der Darstellung, ob eine Nachricht gemäß den Vorgaben des EmiG-Verbunds versendet oder empfangen wurde.
    i. Im Control Panel wird dem Nutzer dargestellt, ob eine Mailkommunikation gesichert über den EmiG-Verbund stattfand.
    ii. Unter Verwendung eines Outlook-Addins kann der Nutzer den EmiG-Status seiner Nachrichten und Kommunikationspartner in Outlook einsehen (Feature ist in Vorbereitung).

5 Leistungsbeschreibung Continuity Service

1. Der Hornetsecurity Continuity Service ist eine Erweiterung der Hornetsecurity Spam and Malware Protection Service und setzt die Nutzung der Spam and Malware Protection Service voraus.
2. Hornetsecurity speichert eingehende und ausgehende E-Mails des Auftraggebers für einen Zeitraum von 3 Monaten auf seinen eigenen IT-Systemen unter der Voraussetzung, dass diese E-Mails über die Server von Hornetsecurity geleitet werden.
3. Auf die gespeicherten E-Mails können autorisierte Benutzer aus dem Internet zugreifen. Gespeicherte E-Mails können nach bestimmten Kriterien und Inhalten durchsucht werden, um bestimmte E-Mails im Speicher ausfindig zu machen. Autorisierte Benutzer können interaktiv die erneute Zustellung gespeicherter E-Mails auf die Systeme des Auftraggebers veranlassen.
4. Für den Fall des Ausfalls des E-Mail-Servers des Auftraggebers stellt Hornetsecurity einen eigenen E-Mail-Server (Backup-Server) im Rechenzentrum von Hornetsecurity zur Verfügung, auf den eingehende E-Mails umgeleitet und von dem ausgehende E-Mails verschickt werden können.
5. Die Umleitung eingehender E-Mails auf den Backup-Server erfolgt wahlweise auf Anforderung oder automatisch. Die entsprechende Einstellung (manuell oder automatisch) wird auf Anforderung des Auftraggebers vom Hornetsecurity Support aktiviert.
6. Auf E-Mails im Backup-Server können autorisierte Benutzer des Auftraggebers während des Ausfalls des E-Mail-Servers des Auftraggebers per POP3, IMAP oder Webmail-Interface zugreifen.
7. E-Mails im Backup-Server werden automatisch an den E-Mail-Server des Auftraggebers übertragen, sobald dieser wieder verfügbar ist und die E-Mails nicht zuvor per POP3, IMAP oder Webinterface in andere Ordner verschoben oder gelöscht wurden. E-Mails werden nach Übertragung an den E-Mail-Server des Auftraggebers aus dem Backup-Server gelöscht.
8. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.

6 Leistungsbeschreibung Signature and Disclaimer

1. Der Service Signature and Disclaimer ist eine Erweiterung des Hornetsecurity Spam and Malware Protection und setzt dessen Nutzung voraus. Zusätzlich muss der

Versand von E-Mails über Hornetsecurity aktiviert sein.

2. Die Nutzung von Signature and Disclaimer kann auf zwei unterschiedliche Arten erfolgen – über das LDAP-Protokoll oder über die statische Version ohne LDAP-Anbindung. Abhängig von der Nutzungsart gelten unterschiedliche Voraussetzungen und inbegriffene Serviceleistungen:
    a. Für die Nutzung über das LDAP-Protokoll wird der Einsatz eines Verzeichnisdienstes vorausgesetzt. Zusätzlich müssen die Gruppen aus dem Benutzerverzeichnis im Control Panel organisiert sein.
    b. Für die Nutzung der statischen Version muss der Service über den Support aktiviert sein. In der statischen Version sind die Funktionen 4b, 4c, 4d und 5 nicht im Service inbegriffen.
3. Mit Signature and Disclaimer kann der Auftraggeber Signaturen und Disclaimer für Benutzergruppen erstellen. Diese werden beim Versand von E-Mails über Hornetsecurity automatisch angehängt. Pro Benutzergruppe ist es möglich eine Vorlage für eine Signatur und einen Disclaimer auszuwählen.
4. Der Zugriff durch autorisierte Benutzer erfolgt über ein Webinterface, in dem mit Hilfe eines WYSIWYG-Editors mit auswählbaren Attributen aus dem Verzeichnisdienst Vorlagen für Signaturen und Disclaimer erstellt werden können. Zusätzlich bietet der WYSIWYG-Editor folgende Funktionen an, um individuelle Signaturen und Disclaimer erstellen zu können:
    a. Einfügen einer Signatur oder eines Disclaimers aus HTML-Quellcode,
    b. Einbinden vordefinierter AD-Variablen, *
    c. Einbinden zuvor erstellter Signaturen als Subsignaturen, *
    d. Ausblenden von unbenutzten AD-Variablen in Signaturen und Disclaimern bei Benutzern mit der Funktion „If Not Empty", *
    e. Einbinden eigener Grafiken, Werbebanner oder Social-Media-Buttons über die Drag & Drop-Funktion oder über die direkte Einbettung einer URL.
5. Eine Vorschaufunktion ermöglicht eine mit Daten gefüllte Vorschau der Vorlage für Benutzer der ausgewählten Gruppe. *
6. Erstellte Vorlagen werden vom Kunden gespeichert und können für unterschiedliche Benutzergruppen ausgewählt werden. Alle Benutzer, die keiner Gruppe zugeordnet sind und Gruppen, denen keine eigene Vorlage zugewiesen wurde, werden unter einer Standardgruppe zusammengefasst.
7. Nach Einrichtung werden die Signatur und der Disclaimer bei dem Versand über Hornetsecurity an ausgehende E-Mails, unabhängig vom eingesetzten Endgerätetyp angehängt. Dies gilt sowohl für extern, als auch für intern verschickte E-Mails, sofern deren Routing über die Hornetsecurity Cloud eingerichtet ist.

* nicht in der statischen Version des Signature and Disclaimer enthalten

7 Leistungsbeschreibung Web Filter

1. Ausgehende http/https- und ftp-Aufrufe des Auftraggebers werden über Proxy-Server von Hornetsecurity geleitet. Dies erfolgt durch Umstellung der Proxyeinstellungen im Browser des zu filternden Internetzugangs des Partners oder des Kunden.
2. Der Web Filter arbeitet unabhängig von der Netzwerkstruktur des Partners / Kunden und ist in Rechenzentren von Hornetsecurity redundant ausgelegt. Garantiert wird eine Verfügbarkeit von 99,9%.
3. 99,9% aller aufgerufenen Webseiten werden in unter 1 Sekunde kategorisiert.
4. Die Authentifizierung gegen den Hornetsecurity Proxy-Server kann über folgende Mechanismen erfolgen:
    a. IP Adresse

   b. Eingabe von Benutzername und Passwort
   c. Hornetsecurity Web Filter Add-In
   d. Im Proxy-Server werden:
   e. Datenverbindungen auf Viren, Trojaner, Phishing, gehackte Server und Kategorien untersucht,
   f. Datenverbindungen mittels einer Schnellerkennung nach gefährlichen Links durchsucht,
   g. https-Verbindungen aufgeschlüsselt und Datenströme in den Verbindungen analysiert,
   h. verbotene Dateidownloads geblockt,
   i. Webseiten nach Kategorien erfasst, analysiert und gefiltert.
5. Der Zugang zu unerwünschten und gefährlichen Inhalten wird geblockt.
6. Bei Verwendung des Hornetsecurity Web Filter Add-Ins können zusätzlich lokale Applikationen der überwachten Endgeräte gesperrt werden.
7. Eine Nachkategorisierung ggf. bisher nicht erfasster Webseiten erfolgt vollautomatisch ohne Eingriffe des Benutzers.
8. Die Nachkategorisierungszeiten betragen im maximalen Durchschnitt 2 Stunden. Falschkategorisierungen können auf Anfrage nachgearbeitet werden. Die Rate der falsch kategorisierten Seiten im Verhältnis zu den richtig kategorisierten Seiten beträgt maximal 1:100.000.
9. Die ggf. vorgenommene Ablehnung von Webzugriffen und Inhalten (Blocken) geschieht in Übereinstimmung mit über das Hornetsecurity Control Panel vorgenommenen Policy-Einstellungen des Auftraggebers oder des beauftragten Dienstleisters.
10. Nicht kategorisierte Seiten werden optional durch Eintrag in eine Blacklist geblockt.
11. Der Hornetsecurity Web Filter ermöglicht zudem die Verwendung abweichender Policies zur Nutzung in vorher festgelegten Zeiträumen (Pausenzeiten Regelung).
12. Die Einstellung individueller Policies ist für Benutzer und Gruppen von Benutzern möglich.
13. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.

8 Leistungsbeschreibung Managed Internet Security für KMU

1. Hornetsecurity stellt je Benutzer ein E-Mail Postfach mit 10 GB Speicherplatz zur Verfügung.
2. Auf E-Mails im Postfach können autorisierte Benutzer über ein Webmail-Interface oder per IMAP und POP3 zugreifen.
3. Der E-Mail-Versand aus dem Postfach erfolgt ebenfalls über das Webmail-Interface oder per SMTP.
4. Die Verfügbarkeit von Webmail-Interface und Mailbox beträgt 99,9% im Jahresmittel.
5. Alle Postfächer sind über die Hornetsecurity Spam and Malware Protection geschützt; die für die Spam and Malware Protection angegebene Leistungsbeschreibung gilt auch für Managed Internet Security für KMU.
6. Eingehende und ausgehende E-Mails werden zusätzlich für 3 Monate gespeichert und können aus dem Archiv erneut abgerufen werden.
7. Optional und gegen Aufpreis können Nutzer die Leistungen der Hornetsecurity Archivierung und des Hornetsecurity Web Filter nutzen.
8. Die Garantien für die Spam and Malware Protection gelten analog, wie auch die Garantien für das optionale Archiving und den Web Filter.
9. Geplante Wartungsarbeiten werden nicht berücksichtigt, diese werden soweit es möglich ist am Wochenende nachts ausgeführt (MEZ).

9 Leistungsbeschreibung Hornet.email

1. Hornetsecurity stellt mit Hornet.email eine Kombination aus Mailbox, Kalender, Adressbuch und direkt integrierter Spam and Malware Protection zur Verfügung.
2. Die Hornet.email Mailbox umfasst wahlweise 2GB oder 25 GB Datenspeicherung für Emails, Kalender, Adressbuch sowie Aufgaben.
3. Der Zugriff auf Hornet.email Mailboxen ist per Webinterface und nativen Clients sowie Outlook Clients von allen gängigen aktuellen PCs (Windows, Mac, Linux) sowie mobilen Endgeräten (iOS, Android) möglich. Zudem werden je nach Fähigkeiten des Endgeräts die Protokolle Exchange ActiveSync, IMAPS, SMTPS, CalDAV sowie Autodiscover und Autoconfig zur beidseitigen Synchronisation der Hornet.email Mailbox mit beliebig vielen Geräten und Clients pro Benutzer zur Verfügung gestellt.
4. Hornetsecurity sichert einmal täglich die E-Mails der Mailbox. Diese Sicherung wird 14 Tage lang aufbewahrt. Hornetsecurity kann bei Bedarf und nach schriftlicher Auftragserteilung des Auftraggebers die Mailbox auf einen Sicherungsstand zurücksetzen (kostenpflichtiger Service).
5. 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.
6. 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.
7. 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.
8. 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.
9. 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).
10. Die Verfügbarkeit von Hornet.email-Schnittstellen sowie Webinterface beträgt 99,5% in Jahresmittel.
11. Soweit der Auftraggeber es wünscht werden auch ausgehende E-Mails gefiltert.
12. Empfangene E-Mails werden:
    e. Geblockt (zurückgewiesen), soweit sie noch während der Aufnahme der Datenverbindung mit den Servern von Hornetsecurity mit hoher Sicherheit als unerwünscht erkannt werden,
    f. 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,

g. Zugestellt oder zur Abholung bereitgestellt, sofern sie als erwünschte E-Mail erkannt werden.
h. Die Zustellzeiten liegen typisch im Durchschnitt bei unter 30 Sekunden, der maximale durchschnittliche Wert liegt bei 3 Minuten.

13. 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).
14. 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.
15. 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.
16. 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.
17. 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.
18. 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:
    d. mit einer entsprechenden Fehlermeldung zurückgewiesen (eingehend),
    e. ohne Anhang zugestellt und mit Anhang in eine Quarantäne gestellt, aus der sie von Administratoren dem Empfänger zugestellt werden können (eingehend),
    f. mit einer entsprechenden Fehlermeldung zurückgewiesen (ausgehend).
19. Die Richtlinien zur Content- und Compliance- Filterung können von dazu autorisierten Benutzern des Auftraggebers im Hornetsecurity Control Panel eingestellt werden.
20. 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.
21. Hornetsecurity kann neben den bereits bestehenden Methoden und Verfahren zur Erkennung von Viren weitere AV-Engines von Antivirus Spezialisten optional hinzuschalten.
22. 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.

10 Leistungsbeschreibung Hornetsecurity Altaro VM Backup

Hornetsecurity Altaro VM Backup ist eine zuverlässige, intuitive und einfach zu verwaltende Backup- und Wiederherstellungslösung für virtualisierte Server in Hyper-V und VMware-Umgebungen sowie physische Microsoft Server.

Die aktuellen Voraussetzungen für die Nutzung des Services sind https://www.hornetsecurity.com/de/vm-backup-information/ zu entnehmen.

Die Nutzung des Services unterliegt der vorherigen Zustimmung zum Endbenutzer-Lizenzvertrag („Standard EULA"), bereitgestellt unter https://www.hornetsecurity.com/de/vm-backup-information/.

1. Hornetsecurity Altaro VM Backup ermöglicht die Durchführung von Backups auf die vom Kunden festgelegten Orte in den vom Kunden festgelegten Zeitintervallen. Dies inkludiert die folgenden Funktionalitäten:
    a. Augmented Inline Deduplication: Daten werden bereits vor dem Transfer zum Speicherort dedupliziert, um Transportkosten und -zeiten zu minimieren.
    b. WAN-optimierte Replikation: VMs können kontinuierlich auf einen Remotestandort repliziert werden Somit kann die RPO (Recovery Point Objective) deutlich verbessert werden.
    c. Continuous Data Protection (CDP) & Flexible backup scheduling – Backups werden in frei wählbaren Zeitabständen, bis auf 5 Minuten Zeitabstand, vollautomatisiert durchgeführt.
    d. Concurrency –durch gleichzeitige Sicherung mehrerer VMs sind die Sicherungsvorgänge besonders effizient.
    e. Mehrere externe Sicherungsstandorte sind durch den Kunden frei wählbar:
        i. NTFS, SMB Shares in der Kundeninfrastruktur
        ii. Offline Kopien: Hornetsecurity Altaro Offsite server, hier ist ggf. mit Zusatzkosten zu rechnen.
        iii. Azure, Wasabi Amazon S3. Hier ist ggf. mit Zusatzkosten zu rechnen.
    f. Durch den Backup Health Monitor kann der Kunde Integritätsprobleme mit Backup-Daten aufgrund von Datenträgerproblemen erkennen. Sollten Probleme gefunden werden, versucht Hornetsecurity Altaro VM Backup, die Probleme automatisch zu beheben, indem die betroffenen Daten beim nächsten Backup erneut gesichert werden.
    g. Hot / Live Backups: Backups können unabhängig vom Scheduling auch jederzeit per Knopfdruck durch den Administrator aktiv ausgeführt werden, ohne dass eine Ausfallzeit der VM auftritt.
    h. Microsoft Hyper-V-Cluster (CSV) und VMware vCenter (grafische Verwaltungskonsole) werden wie folgt unterstützt:
        - Hyper-V
            - Standalone Host
            - Hyper-V Cluster
            - Azure Stack HCI
        - VMWare
            - Standalone ESXi Host
            - vCenter server / Cluster
    i. Die Verschlüsselung der Backups wird durch vom Kunden konfigurierte AES-256-Verschlüsselungsschlüssel (Passwort) sichergestellt. Alle Offsite-Kopien sind AES-265-verschlüsselt. Für Onsite-Backups (primär) ist die Verschlüsselung optional und wird ebenfalls unterstützt.
    j. Retention policies: Der Kunde kann die Aufbewahrungszeiten selbständig definieren und ändern.
    k. Grandfather-Father-Son-Archiving (GFS): hierarchische Backupintervalle für Jahre, Monate, Wochen können vom Kunden definiert werden.

2. Hornetsecurity Altaro VM Backup ermöglicht die Wiederherstellung von Backups. Dies inkludiert folgende Funktionen:

a. Boot from Backup – Booten kann direkt aus der Backup Location erfolgen.
b. Instant Business Continuity – Der Zeitraum bis zur Wiederherstellung der replizierten VM wird durch diverse technische Maßnahmen für ein schnellstmögliches Weiterverarbeiten der replizierten VM optimiert.
c. Wiederherstellung als Klon: Die Wiederherstellung einer VM kann auf dem gleichen Hypervisor unter einem anderen Namen erfolgen.
d. Exchange item-level-restore – Wiederherstellung einzelner Mailboxen oder E-Mails einer gesicherten Exchange VM.
e. Die Wiederherstellung kann auf abweichenden Host erfolgen.
f. Sandbox Restoring & Backup Verification: der Aufbau eines Wiederherstellungsplans und eines Testszenarios sind für den Kunden möglich.
g. Granular restore: Dateibasierte Wiederherstellung von einzelnen Dateien oder Ordnern der VM.
h. Fast onepass restore: Ermöglicht einen effizienten und optimierten Wiederherstellungsprozess von deduplizierten Daten, die auf der Festplatte gespeichert sind.

3. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.

11 Leistungsbeschreibung 365 Total Protection

11.1 365 Total Protection Business

Hornetsecurity 365 Total Protection Business erweitert durch die Managed Security Services von Hornetsecurity die E-Mail Services von Microsoft 365.
Voraussetzung für die Nutzung des Produktes 365 Total Protection Business ist die Verwendung von Microsoft Cloud Lizenzen mit durch Microsoft aktivierter Exchange Funktionalität.
Folgende Leistungen sind in 365 Total Protection Business enthalten:

1. **Einfaches Onboarding:**
   Die Einrichtung von 365 Total Protection Business funktioniert automatisiert. Alle Domains, Postfächer und Gruppen des Auftraggebers werden direkt aus Microsoft 365 in das Hornetsecurity Control Panel übertragen.
   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 Kunden. Dies geschieht einmalig im Onboarding-Prozess.
   E-Mails an den Auftraggeber werden zur Erbringung des Services durch Umstellung der MX-Records für die zu filternden Domains des Auftraggebers auf die Server von Hornetsecurity geleitet. Für die Umstellung der MX-Records ist Hornetsecurity nicht verantwortlich. Soweit der Auftraggeber es wünscht, werden auch ausgehende E-Mails gefiltert.
2. **Single Sign-on:**
   Alle Benutzer des Auftraggebers mit einer gültigen Lizenz von Microsoft 365 können sich mit Ihren Benutzerdaten für Microsoft 365 bei Hornetsecurity authentifizieren.
   Sind die Benutzer bereits bei Microsoft 365 angemeldet, müssen sie sich nicht erneut bei Hornetsecurity authentifizieren.
3. **E-Mail-Live-Tracking:**
   Dem Auftraggeber werden alle ein- und ausgehenden E-Mails in einer individuell einstell- und filterbaren Übersicht angezeigt. Zudem werden ausführliche

Informationen zu jeder E-Mail angezeigt wie z. B. die Verschlüsselungsart.
Je nach Klassifizierung der E-Mail (Gültig, Infomail, Spam, Content, Virus, ATP, Abgewiesen) können E-Mails von dazu autorisierten Benutzern aus der Anzeige ausgelöst und an den Empfänger zugestellt werden. Aktionen wie Black- oder Whitelisten können ebenfalls durchgeführt werden.

4. Infomail-Handling:
   Die Zustellung von Newslettern und werblichen E-Mails wird durch individuell einstellbare Richtlinien verhindert, die der Auftraggeber festlegen kann.
5. Content-Control:
   Ein- und ausgehende E-Mails werden nach eingestellten Richtlinien zu ihren Dateianhängen gefiltert. 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) und/oder
   c. mit einer entsprechenden Fehlermeldung zurückgewiesen (ausgehend).

   Die Richtlinien zur Content-Filterung können im Hornetsecurity Control Panel von dazu autorisierten Benutzern des Auftraggebers eingestellt werden.
6. Compliance-Filter:
   Ein- und ausgehende E-Mails werden entsprechend eingestellter Richtlinien gefiltert. Je nach Einstellung werden E-Mails, die den Richtlinien entsprechen:
   a. an das Empfängerpostfach zugestellt (eingehend),
   b. mit einer entsprechenden Fehlermeldung zurückgewiesen (eingehend),
   c. als Spam oder Virus markiert (eingehend),
   d. ein oder mehrere BCC-Empfänger hinzugefügt (ein- und ausgehend),
   e. auf eine oder mehrere E-Mail-Adressen umgeleitet (ein- und ausgehend),
   f. über eine andere Route geschickt (ein- und ausgehend) und/oder
   g. zugestellt und der Absender benachrichtigt (ausgehend).

   Die Richtlinien zur Compliance-Filterung können im Hornetsecurity Control Panel von dazu autorisierten Benutzern des Auftraggebers eingestellt werden.
7. Spam and Malware Protection:
   Hornetsecurity filtert eingehende E-Mails des Auftraggebers auf schädlichen Inhalt (z. B. Viren) und unerwünschte Werbung (z. B. Spam) auf seinen eigenen IT-Systemen.
   Empfangene E-Mails werden:
   a. geblockt (zurückgewiesen), sofern 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 und/oder
   c. zugestellt oder zur Abholung bereitgestellt, sofern sie als erwünschte E-Mail erkannt werden.

   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).

8. Outlook-based Black- und Whitelisting:
   Hornetsecurity stellt dem Auftraggeber ein Add-In für Outlook zur Verfügung, mit dem der Auftraggeber die Möglichkeit erhält, das Black- und Whitelisten von Absendern direkt in Outlook vorzunehmen.
9. Individual User Signatures:
   a. Die Verwendung von Userbased Individual Signatures setzt voraus, dass der Auftraggeber den Versand von E-Mails über Hornetsecurity aktiviert.
   b. Mit Userbased Individual Signatures kann der Auftraggeber Signaturen für Benutzergruppen erstellen. Diese werden beim Versand von E-Mails über Hornetsecurity automatisch angehängt.
   c. Pro Benutzergruppe ist es möglich, eine Vorlage für eine Signatur auszuwählen.
   d. Der Zugriff durch autorisierte Benutzer erfolgt über ein Webinterface, in dem mit Hilfe eines WYSIWYG-Editors mit auswählbaren Attributen aus dem Verzeichnisdienst Vorlagen für Signaturen erstellt werden können. Zusätzlich ist es möglich, direkt HTML-Quellcode einzufügen.
   e. Eine Vorschaufunktion ermöglicht eine mit Daten gefüllte Vorschau der Vorlage für Benutzer der ausgewählten Gruppe.
   f. Erstellte Vorlagen werden vom Kunden gespeichert und können für unterschiedliche Benutzergruppen ausgewählt werden. Alle Benutzer, die keiner Gruppe zugeordnet sind und Gruppen denen keine eigene Vorlage zugewiesen wurde, werden unter einer Standardgruppe zusammengefasst.
   g. Nach der Einrichtung wird die Signatur bei dem Versand über Hornetsecurity an ausgehende E-Mails angehängt. Dies gilt sowohl für extern als auch für intern verschickte E-Mails, sofern deren Routing über den Auftragnehmer eingerichtet ist.
10. 1-Click-Intelligent-Ads:
    1-Click-Intelligent-Ads erweitert die Userbased Individual Signatures um die Einblendung von Werbeanzeigen in den Signaturen auf Gruppen- oder Unternehmensebene.
    Autorisierte Benutzer des Auftraggebers können an zentraler Stelle Subsignaturen erstellen und in vorhandene Signaturen einbetten. Diese können mit einem Klick für Gruppen oder die gesamte Domain aktiviert oder deaktiviert werden.
11. Company Disclaimer:
    Zusätzlich zu Userbased Individual Signatures erhält der Auftraggeber die Möglichkeit, unternehmensweite oder gruppenbasierte Pflichtabgaben zu erstellen.
    a. Die Pflichtangaben werden beim Versand von E-Mails über Hornetsecurity automatisch angehängt.
    b. Vorhandene Pflichtangaben können importiert werden.
12. Global S/MIME/PGP-Encryption:
    a. Hornetsecurity verschlüsselt und signiert ausgehende E-Mails und entschlüsselt eingehende E-Mails des Auftraggebers auf seinen eigenen IT-Systemen entsprechend den eingestellten Richtlinien.
    b. Ausgehende E-Mails werden per S/MIME signiert, sofern die dazu nötigen privaten Schlüssel im Zertifikatsspeicher vorliegen.
    c. Die Richtlinien zur Verschlüsselung ausgehender

E-Mails können von dazu autorisierten Benutzern des Auftraggebers im Hornetsecurity Control Panel eingestellt werden.

d. Je nach Einstellung der Richtlinien werden ausgehende E-Mails:
   i. mit dem öffentlichen Schlüssel des Empfängers per S/MIME oder PGP verschlüsselt übertragen,
   ii. nicht verschlüsselt, aber über einen per TLS verschlüsselten Kanal übertragen,
   iii. über einen mit DANE geprüften und verschlüsselten Kanal übertragen,
   iv. im geschützten Hornetsecurity Websafe für den Empfänger bereitgestellt und/oder
   v. unverschlüsselt übertragen.

e. Die Richtlinien können durch autorisierte Benutzer im Hornetsecurity Control Panel gesetzt werden. Die Verschlüsselung einer E-Mail kann zusätzlich durch den Benutzer beim Versand über einen Betreff-Zusatz („Tag“) sichergestellt werden.

f. Sofern die Richtlinie zwingend die verschlüsselte Übertragung vorsieht, aber der dazu nötige öffentliche Schlüssel des Empfängers nicht im Zertifikatsspeicher vorliegt und die ggf. eingestellte Übertragung per TLS vom empfangenden Server nicht unterstützt wird, werden ausgehende E-Mails an diesen Empfänger zurückgewiesen und nicht übertragen.

g. Eingehende, per S/MIME oder PGP verschlüsselte E-Mails werden automatisch entschlüsselt, sofern der dazu nötige private Schlüssel des Empfängers im Zertifikatsspeicher vorliegt.

h. Öffentliche Schlüssel werden automatisch aus Signaturen eingehender E-Mails extrahiert und im Zertifikatsspeicher hinterlegt.

i. S/MIME-Zertifikate für Benutzer des Auftraggebers können im Control Panel bestellt werden und werden dann automatisch im Zertifikatsspeicher abgelegt. Alternativ können vorhandene private Schlüssel durch autorisierte Benutzer des Auftraggebers im Zertifikatsspeicher abgelegt werden.

j. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.

13. Hornetsecurity stellt die Geheimhaltung der im Zertifikatsspeicher gespeicherten privaten Schlüssel des Auftraggebers sicher. Die Pflicht zur Geheimhaltung besteht auch nach Ende dieses Vertrags fort.

14. **Secure Cipher Policy Control:**
    Mit der Secure Cipher Policy Control kann der Auftraggeber die Vertrauenseinstellungen von Zertifizierungsstellen selbstständig steuern.
    Autorisierte Benutzer des Auftraggebers können:
    a. Vertrauenseinstellungen für Zertifizierungsstellen und Cipher Suites feingranular auf

Benutzer- und Domainsbasis definieren.
   b. selbstsignierte Zertifikate inklusive der gesamten Trust Chain importieren

15. **Websafe:**
Hornetsecurity ermöglicht dem Auftraggeber, E-Mails verschlüsselt zu übertragen, selbst wenn der Kommunikationspartner keine Möglichkeit besitzt, seinerseits Verschlüsselungsmechanismen einzusetzen.
   a. E-Mails an Kommunikationspartner ohne Verschlüsselungsmöglichkeit werden einem https- und passwortgeschützten Websafe-Postfach zugestellt.
   b. Der Kommunikationspartner erhält eine Nachricht mit der Einladung zu seinem persönlichen Websafe-Postfach.
   c. Die sichere Auslieferung des Zugangspassworts an den Kommunikationspartner obliegt dem Benutzer des Auftraggebers.
   d. Zukünftige E-Mails an den Kommunikationspartner werden verschlüsselt an das Websafe-Postfach zugestellt.

<u>11.2 365 Total Protection Enterprise</u>

Voraussetzung für die Nutzung des Produktes 365 Total Protection Enterprise ist die Verwendung von Microsoft Cloud Lizenzen mit durch Microsoft aktivierter Exchange Funktionalität.
Hornetsecurity 365 Total Protection Enterprise beinhaltet alle Leistungen von 365 Total Protection Business; die für 365 Total Protection Business angegeben Leistungsbeschreibung gilt auch für 365 Total Protection Enterprise.
Folgende weitere Leistungen sind enthalten:

1. **E-Mail-Archivierung:**
   a. Hornetsecurity archiviert E-Mails des Auftraggebers revisionssicher auf seinen eigenen IT-Systemen. Die Archivierungsdauer und Archivierungsausnahmen können auf Domain-, Gruppen- oder Nutzerebene festgelegt werden.
   b. Autorisierte Benutzer können E-Mails als „privat" markieren. Auf als „privat" markierte E-Mails ist anschließend kein Zugriff aus dem Archiv mehr möglich.
   c. Speziell autorisierte Nutzer können einen speziellen Zugang einrichten, der den Zugriff auf alle archivierten E-Mails eines bestimmten Zeitraums erlaubt (Prüfzugang, z. B. zum Zweck einer Betriebsprüfung). Einrichtung und Nutzung des Prüfzugangs werden geloggt.
   d. Archiviert werden solche E-Mails, die
      i. durch den Auftraggeber über die Server von Hornetsecurity an Dritte verschickt werden (ausgehende externe E-Mails),
      ii. dem Auftraggeber durch Dritte über die Server von Hornetsecurity zugeschickt werden (eingehende externe E-Mails) und/oder
      iii. der Auftraggeber zur Archivierung durch Hornetsecurity über vereinbarte Schnittstellen an Hornetsecurity zur Verfügung stellt (interne E-Mails, optional).

e. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.
f. Die Bereitstellung eines Inklusiv-Volumens von bis zu 25 GB je Postfach ist enthalten. Der Speicherplatz wird über alle Postfächer eines Kunden gemittelt berechnet. Die über das Inklusiv-Volumen hinausgehende Nutzung wird separat berechnet.
g. Hornetsecurity bietet optional den Nachimport bestehender Archivdaten an. Die Archivdaten müssen in einem festgelegten Format angeliefert werden. Die technischen Voraussetzungen und Rahmenbedingungen können bei Hornetsecurity erfragt werden. Der Nachimport bestehender Archivdaten ist kostenpflichtig.
h. Auf Wunsch exportiert Hornetsecurity die bestehenden Archivdaten auf einen externen Datenträger. Der Export erfolgt im EML-Format auf einem verschlüsselten Datenträger, der anschließend an den Auftraggeber gesendet wird. Der Export von Archivdaten ist kostenpflichtig.
i. Mit dem Aeternum Export Manager ist es zudem möglich, archivierte E-Mails auf Postfachbasis im Selfservice zu exportieren und anschließend herunterzuladen. Für den Export stehen die Formate PST, EML und MBOX zur Verfügung. Der Export von Archivdaten mit dem Aeternum Export Manager ist kostenpflichtig.

2. Die Archivierung genügt den derzeitigen gesetzlichen Auflagen in Deutschland bezüglich der elektronischen Archivierung von E-Mails. Hornetsecurity wird alles in seiner Macht stehende veranlassen, um die Erfüllung dieser gesetzlichen Auflagen auch im Fall der Änderung dieser Auflagen sicher zu stellen.
3. Hornetsecurity stellt die Geheimhaltung der archivierten Daten und sonstiger im Rahmen dieses Vertrags bekannt gewordenen geschäftlichen Geheimnissen des Auftraggebers gegenüber Dritten sicher. Die Pflicht zur Geheimhaltung besteht auch nach Ende dieses Vertrags fort.
4. 10-Years-E-Mail-Retention:
   Autorisierte Benutzer des Auftraggebers können:
   a. auf das E-Mail-Archiv zugreifen und
   b. interaktiv die erneute Zustellung archivierter E-Mails auf die Systeme des Auftraggebers veranlassen.
5. Hornetsecurity garantiert die Verfügbarkeit der archivierten E-Mails für den Auftraggeber für die Dauer von 10 Jahren ab Ende des Jahres, in dem die jeweilige archivierte E-Mail versandt bzw. erhalten wurde. Voraussetzung ist die Fortdauer des Vertrags und die Erfüllung der vertraglichen Pflichten durch den Auftraggeber. Für den Fall der Beendigung dieses Vertrags setzt die fortdauernde Verfügbarkeit den Abschluss eines Anschlussvertrags über die Aufrechterhaltung der Datenspeicherung voraus.
6. eDiscovery:
   Archivierte E-Mails können nach bestimmten Kriterien und Inhalten durchsucht werden, um bestimmte E-Mails im Archiv ausfindig zu machen.
7. Hornetsecurity garantiert die Zugriffsmöglichkeit autorisierter Benutzer auf die archivierten E-Mails im Normalfall 24 Stunden am Tag an allen Tagen im Jahr. Ausgenommen sind Wartungszeiten.

8. Forensic analyses:
   Heuristische Filter zur Erkennung gezielter Angriffe, mit Prüfung von Authentizität und Integrität von Metadaten und E-Mail-Inhalten, Erkennung und Blockierung gefälschter Absender-Identitäten, Erkennung gefälschter Inhalte, Erkennung von Angriffen auf besonders schützenswerte Daten, insbesondere Daten die Zahlungsflüsse betreffen (z. B. Kreditkartendaten, Rechnungen, Zahlungsanweisungen), Erkennung gezielter Angriffe auf besonders exponierte Personen des Auftraggebers (z. B. Buchhaltung, CFO, CEO, Controlling).
   a. Als potentiell schädlich identifizierte E-Mails werden von Hornetsecurity in Quarantäne gestellt.
   b. Auf E-Mails in der Quarantäne kann der Auftraggeber über das Hornetsecurity Control Panel zugreifen.
9. ATP-Sandbox:
   Verdächtige E-Mail-Anhänge werden in mehreren separaten, geschützten Umgebungen geöffnet oder ausgeführt und ihr Verhalten auf mögliche Schadwirkung untersucht. Als verdächtig werden insbesondere Anhänge eingestuft, in denen ausführbarer Code gefunden wird.
   a. Als potentiell schädlich identifizierte E-Mails werden von Hornetsecurity in Quarantäne gestellt.
   b. E-Mails in der Quarantäne können von Administratoren des Auftraggebers aus dem Control Panel heraus in der ATP-Sandbox geprüft werden. Detaillierte Ergebnisse der Prüfung werden über das Control Panel zur Verfügung gestellt.
   c. Sicherheitsverantwortliche des Auftraggebers werden bei erkannten Bedrohungen unmittelbar per E-Mail über die Bedrohung informiert (Real-Time Alerts).
   d. E-Mails können durch die zusätzliche aufwändige Filterung zeitlich verzögert zugestellt werden. Die Verzögerung beträgt im Einzelfall maximal 15 Minuten.
10. URL-Malware-Control:
    a. Link Scanning: In E-Mails oder in E-Mail-Anhängen enthaltene URLs werden aktiviert und das resultierende Verhalten analysiert.
    b. Link Rewriting: URLs in E-Mails werden durch andere URLs ersetzt, die die entsprechenden Inhalte bei Aktivierung über Hornetsecurity Web Filter abrufen. Ggf. werden heruntergeladene Daten in der ATP-Sandbox auf ihr Verhalten untersucht. Durch den Web Filter als potentiell gefährliche erkannte Inhalte werden gesperrt.
11. Realtime Threat Report:
    Der Auftraggeber erhält einen Überblick über alle gebuchten Services von Hornetsecurity sowie weitreichende Informationen und Statistiken zu seinem aktuellen Sicherheitsstatus.
12. Malware-Ex-Post-Alert:
    Sicherheitsverantwortliche des Auftraggebers werden im Fall bereits zugestellter potentieller Schadmails unmittelbar nach Erkennung des Vorfalls (z. B. durch Filter-Updates) automatisch per E-Mail informiert.
13. Malware Ex Post Deletion:
    Erkennen Hornetsecurity Artificial Intelligence Algorithmen verschleierte Schadmails nach erfolgter Zustellung, können berechtigte Sicherheitsverantwortliche und Administratoren die betreffenden Mails über das Control Panel suchen und direkt aus der Mailbox Ihrer Benutzer löschen.

14. Email Continuity Service:
    a. Hornetsecurity speichert eingehende und ausgehende E-Mails des Auftraggebers für einen Zeitraum von drei Monaten auf seinen eigenen IT-Systemen unter der Voraussetzung, dass diese E-Mails über die Server von Hornetsecurity geleitet werden.
    b. Auf die gespeicherten E-Mails können autorisierte Benutzer aus dem Internet zugreifen. Gespeicherte E-Mails können nach bestimmten Kriterien und Inhalten durchsucht werden, um bestimmte E-Mails im Speicher ausfindig zu machen. Autorisierte Benutzer können interaktiv die erneute Zustellung gespeicherter E-Mails auf die Systeme des Auftraggebers veranlassen.
    c. Für den Fall des Ausfalls der E-Mail-Server von Microsoft 365 stellt Hornetsecurity einen eigenen E-Mail-Server (Backup-Server) im Rechenzentrum von Hornetsecurity zur Verfügung, auf den eingehende E-Mails umgeleitet und von dem ausgehende E-Mails verschickt werden können.
    d. Die Umleitung eingehender E-Mails auf den Backup-Server erfolgt wahlweise auf Anforderung oder automatisch. Die entsprechende Einstellung (manuell oder automatisch) wird auf Anforderung des Auftraggebers vom Hornetsecurity Support aktiviert.
    e. Auf E-Mails im Backup-Server können autorisierte Benutzer des Auftraggebers während des Ausfalls des E-Mail-Servers des Auftraggebers per POP3, IMAP oder Webmail-Interface zugreifen.
    f. E-Mails im Backup-Server werden automatisch an den E-Mail-Server des Auftraggebers übertragen, sobald dieser wieder verfügbar ist und die E-Mails nicht zuvor per POP3, IMAP oder Webinterface in andere Ordner verschoben oder gelöscht wurden. E-Mails werden nach Übertragung an den E-Mail-Server des Auftraggebers aus dem Backup-Server gelöscht.
    g. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.
15. Content-Preview:
    Autorisierte Benutzer des Auftraggebers können Anhänge von E-Mails, die durch Richtlinien von Content Control blockiert wurden, in einer statischen Vorschau innerhalb einer gesicherten Umgebung betrachten. Dies erleichtert Administratoren die Freigabe der entsprechenden E-Mail-Anhänge, da Benutzer nicht bösartige Anhänge selbständig über die Outlook Web-App anfordern können. Die Content Preview wird angewandt auf für eine Sandboxanalyse geeignete Dateiformate, sofern für diese eine Regel zur Entfernung des Anhangs in den Content Control Security Settings gesetzt wurde.
16. Für Forensic Analyses, ATP-Sandbox, URL-Malware-Control und Malware-Ex-Post-Alerts wird eine Verfügbarkeit von 99,9% garantiert, ausgenommen sind angekündigte Wartungszeiten.

12 Leistungsbeschreibung 365 Total Encryption

1. Hornetsecurity 365 Total Encryption, ein Hornetsecurity Service für Microsoft 365 Kunden, erweitert die Leistungen von

Hornetsecurity 365 Total Protection Enterprise.

2. Voraussetzung für die Nutzung von Hornetsecurity 365 Total Encryption ist die Aktivierung und Verwendung von Hornetsecurity 365 Total Protection Enterprise.
3. Hornetsecurity 365 Total Encryption bietet einen zusätzlichen Service zur Verschlüsselung von in der Microsoft 365 Cloud gespeicherten E-Mails. Der Service dient dazu, dass
   a. Inhalte der in Microsoft 365 gespeicherten Unternehmenskommunikation per E-Mail durch Verschlüsselung gegen unbefugte Einsichtnahme geschützt werden können,
   b. Unternehmensdaten, die in der Microsoft 365 Cloud abgelegt sind, auch dann vor unbefugter Einsichtnahme geschützt sind, wenn der Microsoft 365 Account durch einen Angreifer übernommen wurde,
   c. die in der Microsoft 365 Cloud gespeicherten E-Mails entsprechend gesetzlichen Anforderungen, wie z.B. der Datenschutz-Grundverordnung (DSGVO), vor Einsichtnahme Dritter geschützt sind.
4. Folgende Leistungen sind in 365 Total Encryption enthalten:
   a. Verschlüsselung aller neu in Microsoft 365 gespeicherten E-Mails bei Erreichen der Microsoft 365 Cloud für die Postfächer, für die die Option aktiviert wurde,
   b. nachträgliche Verschlüsselung aller in der Microsoft 365 Cloud gespeicherten E-Mails nach der Aktivierung von 365 Total Encryption für die entsprechenden Postfächer,
   c. Entschlüsselung der E-Mails mittels eines nur für autorisierte Benutzer hinterlegten privaten Schlüssels.
5. In der Microsoft 365 Cloud gespeicherte E-Mails werden nur dann verschlüsselt, wenn die Größe der verschlüsselten E-Mail die von Microsoft vorgegebene Dateigrößenbegrenzung nicht überschreitet. Anderenfalls wird die E-Mail nicht verändert, d.h. sie bleibt unverschlüsselt gespeichert.
6. Das Produkt Hornetsecurity 365 Total Encryption wird mit dem Produkt Hornetsecurity 365 Total Protection Enterprise zur Aktivierung bereitgestellt.
7. Die Aktivierung der Verschlüsselung für ein bestimmtes Postfach findet über eine Zwei-Faktor-Authentisierung im Hornetsecurity Control Panel statt. Nur autorisierte und authentisierte Benutzer können private Schlüssel zur Entschlüsselung herunterladen.
8. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers oder Drittanbietern wie Microsoft ist nicht Vertragsbestandteil.

13 Leistungsbeschreibung 365 Total Backup

Hornetsecurity 365 Total Backup ist eine zuverlässige, intuitive und einfach zu verwaltende Backup- und Recovery-Lösung für Microsoft 365-Mailboxen, OneDrive-Konten für Unternehmen, SharePoint-Dokumentenbibliotheken, Teams-Konversationen und Endpoints.

Die aktuellen Voraussetzungen für die Nutzung des Services finden Sie unter https://www.hornetsecurity.com/de/365-total-backup-information/.

Um den 365 Total Backup Service nutzen zu können, benötigen Sie Microsoft Cloud-Lizenzen mit entweder Exchange-, Teams-, SharePoint- und/oder OneDrive-Funktionalität, die von Microsoft aktiviert wurden.
Alle Objekte innerhalb des gesamten Microsoft-Tenants, denen eine Microsoft 365-Lizenz zugewiesen ist, die entweder Exchange-, Team-, SharePoint- oder OneDrive-Funktionalität gewährt, unterliegen unabhängig von ihrer

aktiven Nutzung der 365 Total Backup-Lizenzierung.
Die höchste Nutzungsmenge des Monats wird gemeldet und in Rechnung gestellt.

1. Mit Hornetsecurity 365 Total Backup können Backups der vom Kunden angegebenen Daten durchgeführt werden. Hornetsecurity 365 Total Backup beinhaltet folgende Funktionen:

(b) Multi-Tenancy: Über eine webbasierte Multi-Tenant-Konsole kann der Kunde alle Microsoft 365 Unternehmens- und Windows-Endpoint-Backups überwachen und verwalten. Pro Organisation können unterschiedliche Einstellungen festgelegt werden.
(c) Benutzerfreundliches Backup-Dashboard: Mithilfe von Widgets können alle Sicherungs- und Wiederherstellungsaktivitäten, Backup-Status sowie den Verlauf der letzten Wiederherstellungen überblickt werden.
(d) Wird eine Organisation hinzugefügt, kann der Kunde auswählen, welche Benutzer und M365-Elemente gesichert werden sollen. Dabei kann auch konfiguriert werden, welche Verzeichnisse von User-Endpoints gesichert werden sollen, die sich entweder vor Ort oder im Roaming befinden, ohne dass eine VPN-Verbindung erforderlich ist.
(e) Automatische Bereitstellung: Hornetsecurity 365 Total Backup erkennt automatisch neu erstellte Benutzer, Gruppen und SharePoints, die ohne Eingreifen des Administrators automatisch gesichert werden können.
(f) Planen & Organisieren: Microsoft 365 Backups sind vollständig automatisiert und können bis zu mehrmals täglich durchgeführt werden, so dass keine manuelle Konfiguration erforderlich ist. Für Endpoints kann der Kunde die Sicherungshäufigkeit für bestimmte Maschinen wählen.
(g) Endpoint Backup Policies: Der Kunde kann (individuelle) Einstellungen für große Gruppen von Windows-Endpoints konfigurieren. Dabei werden Richtlinien für Backup-Verzeichnisse, Cloud-Speicher, Häufigkeit und Aufbewahrung definiert.
(h) Der Kunde kann jederzeit bestimmte User, Gruppen, SharePoint-Dokumentenbibliotheken und Endpoints manuell sichern.
(i) Bulk User Management: Das De- und Aktivieren von Backups und das Löschen von Backup-Daten kann für mehrere Benutzer parallel durchgeführt werden.
(j) Backup Mailbox: Backups für E-Mail-Benutzer enthalten E-Mails, Kalendereinträge und Kontaktadressen.
(k) Backup OneDrive Accounts: Alle in OneDrive for Business gespeicherten Dateien werden gesichert.
(l) Teams Chats Backup: Der Kunde kann auch Teams Chats für Benutzer und Gruppen innerhalb der eigenen Organisation, einschließlich aller Dateien, die während der Unterhaltungen geteilt werden, sichern.
(m) Sharepoint Backup: Dateien und Kommunikation in Sharepoint-Dokumentenbibliotheken werden gesichert, einschließlich der Zugriffsberechtigungen.
(n) Endpoint Backup: Richtliniengesteuertes File-Level-Backup für Windows-Desktops und -Laptops. Endpoint Backup besteht aus:
    i. Endpoint Manager - ist eine Serversoftware, die ein MSP in seinen Räumlichkeiten oder auf einer virtuellen Maschine (VM) in der Cloud installieren muss,

die ein MSP verwaltet und mit einem vom MSP verwalteten Azure Storage-Konto verbunden ist. Der Endpoint Manager muss in Verbindung mit Endpoint Agent(s) (die eine Verbindung zu ihm herstellen) verwendet werden, um Backup-Vorgänge zu verwalten und Endpoints zu konfigurieren

ii. Endpoint Agent - wird auf Endpoints installiert, die ein MSP sichern muss. Der Endpoint Agent stellt eine Verbindung zum Endpoint Manager her, den ein MSP hostet, und sichert Dateien und Ordner entsprechend der eingerichteten Backup-Richtlinie.

2. Hornetsecurity 365 Total Backup ermöglicht die Wiederherstellung von Backups. Dies umfasst die folgenden Funktionen:

a. M365 Versionierung und Wiederherstellung: Sicherungsdaten werden auf unbestimmte Zeit gespeichert, bis sie vom Benutzer gelöscht werden. Jede im Backup vorhandene Version der Datei, Konversation oder Mailbox kann jederzeit wiederhergestellt werden.
b. Endpoint-Recovery: Endpoint-Backup-Daten werden für den vom Benutzer konfigurierten Zeitraum gespeichert und können jederzeit wiederhergestellt werden - zum ursprünglichen Endpoint zurück oder zu einem Management-Server des Partners.
c. Microsoft 365-Postfächer, OneDrive-Konten und SharePoints können:
   - Auf das ursprüngliche Konto wiederhergestellt
   - Auf ein anderes Konto innerhalb derselben oder einer anderen Organisation, die demselben Kunden gehört, übertragen
   - als .ZIP-Archiv heruntergeladen oder
   - im Falle von Postfach-Wiederherstellung als PST exportiert werden.
   - Microsoft 365 Teams Chats können:
     - Zu einem neuen Teams Chat wiederhergestellt werden
     - Als HTML-Dateien heruntergeladen werden
d. Herunterladen und Wiederherstellen mit Microsoft 365 kann:
   i. die Backup-Daten oder einen Teil davon ("granulare Wiederherstellung") aus einem bestimmten Zeitpunkt direkt in der ursprünglichen Backup-Quelle oder einer anderen Backup-Quelle innerhalb der Microsoft 365-Organisation wiederherstellen und/oder
   ii. die Backup-Daten (kennwortgeschützt) oder einen Teil davon, die zu einem bestimmten Zeitpunkt erstellt wurden, herunterladen. Falls gewünscht, wird ein Download-Link zu den neu gespeicherten Inhalten per E-Mail gesendet.
e. Schnelle und erweiterte Suchfunktion: Kunden können Mailboxen, OneDrive-, SharePoint- und Teams-Backups nach mehreren Kriterien durchsuchen.
f. Granulare Wiederherstellung von Dateien oder E-Mail-Elementen: Durch die erweiterte Suchfunktion können einzelne Dateien für die Wiederherstellung für OneDrive-Konten,

SharePoint-Dokumentenbibliotheken und Endpoints ausgewählt werden.

g. Einfach zu bedienende Diagramme zeigen die monatliche Nutzung bequem an.

h. Für erfolgreiche, fehlgeschlagene oder alarmierende Backup-Zustände können E-Mail-Benachrichtigungen oder eine tägliche Übersichtsbenachrichtigung eingestellt werden.

i. Account Activity Audit: Alle Aktivitäten des Benutzerkontos in 365 Total Backup werden auditiert. Dies umfasst sowohl grundlegende und sicherheitsrelevante als auch datenschutzrelevante Informationen wie Browsing und Wiederherstellungsanfragen.

3. Pflichten des Auftraggebers: Der Kunde ist verpflichtet,

a. Den Dienst in Übereinstimmung mit der Nutzungsrichtlinie zu nutzen und auf ihn zuzugreifen und sich an die Fair Use Limits zu halten.

b. Die Backup-Daten in regelmäßigen Abständen auf Vollständigkeit, Korrektheit und Wiederherstellbarkeit zu prüfen.

4. Limitierungen und Anforderungen

a. Hornetsecurity leistet Support für berechtigte Nutzer, soweit es sich um Hornetsecurity-Systeme handelt. Der Support der Systeme des Auftraggebers ist nicht Bestandteil des Vertrages. Limitierungen und Anforderungen für 365 Total Backup finden Sie hier: https://www.hornetsecurity.com/de/365-total-backup-information/

5. Haftungsausschluss

a. Wir sind möglicherweise nicht in der Lage, unseren Dienst anzubieten, wenn die Funktionen von Microsoft (Office) 365, die Struktur der zu sichernden Daten oder andere technische Spezifikationen von Microsoft oder einem anderen Dritten geändert werden. In diesem Fall sind wir berechtigt, Ihr Abonnement zu kündigen; allerdings werden wir Ihnen in diesem Fall den nicht genutzten Zeitraum Ihres Abonnements anteilig erstatten.

b. Darüber hinaus dürfen wir keine Sicherungskopie einer Backup-Quelle erstellen, wenn diese beschädigt ist, Fehler enthält oder anderweitig unlesbar ist, oder wenn wir aus anderen Gründen von Microsoft oder einer anderen Partei, auf die wir uns bei der Erbringung der Dienste verlassen, daran gehindert werden, dies zu tun.

14 Leistungsbeschreibung HORNETDRIVE

1. Hornetdrive ermöglicht sichere Speicherung, Austausch und gemeinsame Bearbeitung von Dateien in der Cloud. Dafür kann der Benutzer Dokumente und Dateien in sogenannte Drives speichern, oder vorhandene Ordner in Drives umwandeln.
2. Der Benutzer kann eine unbegrenzte Zahl eigener Drives in der Hornetdrive Cloud einrichten.
3. Der Benutzer und vom ihm eingeladene andere Benutzer können Dateien in den vom Benutzer eingerichteten Drives ablegen, sofern sie dazu nach den vom Benutzer eingestellten Berechtigungen für den jeweiligen Drive berechtigt sind.
4. Dem Benutzer wird dazu Speicher in der Hornetdrive Cloud zur Verfügung gestellt Der maximale Umfang des genutzten Speichers richtet sich nach der für den Benutzer geltenden Nutzungslizenz.
5. Je nach vom Benutzer für den Drive vorgenommenen Einstellungen werden bei der Speicherung von Dateien im Drive ältere Versionen der gleichen Datei gelöscht oder weiterhin gespeichert. Die einstellbare maximale Zahl gespeicherter Versionen richtet sich auch nach der Art der Lizenz des Benutzers.

6. Alle in Drives eines Benutzers gespeicherten Daten zusammengenommen, inklusive weiterhin gespeicherter älterer Versionen, ergeben den Gesamtumfang des vom Benutzer genutzten Speichers in der Hornetdrive Cloud. Sofern der tatsächlich genutzte Speicher den lizenzierten und zur Verfügung gestellten Speicher erreicht oder überschreitet, können keine weiteren Daten mehr in Drives des Benutzers gespeichert werden.
7. Auf die in der Hornetdrive Cloud gespeicherten Daten können der Benutzer und von ihm eingeladene andere Benutzer zugreifen, sofern sie dazu nach den vom Benutzer eingestellten Berechtigungen für den jeweiligen Drive berechtigt sind.
8. Der Auftraggeber erhält das nicht ausschließliche Recht zur Nutzung der vom Anbieter bereitgestellten Hornetdrive Software-Clients auf einer unbegrenzten Zahl von Geräten. Das Recht ist nicht übertragbar. Alle weitergehenden Rechte an der Software verbleiben beim Anbieter.
9. Speicherung und Zugriffe auf die Daten in der Hornetdrive Cloud sind ausschließlich über Hornetdrive Software-Clients möglich. Je nach Software-Version werden Daten in den vom Benutzer genutzten Drives automatisch oder manuell mit dem Client-System des Benutzers synchronisiert. Die Lizenz zur Nutzung der entsprechenden Hornetdrive Client-Software ist in der Lizenz zur Nutzung des Hornetdrive Service enthalten.
10. Daten werden vor der Übertragung in die Hornetdrive Cloud im Software-Client verschlüsselt bzw. nach dem Herunterladen aus der Cloud im Software-Client entschlüsselt. Jeder Drive hat einen eigenen Schlüssel. Hornetsecurity hat keinen Zugriff auf die zur Verschlüsselung der Daten genutzten Schlüssel und die in der Cloud gespeicherten Daten. Gehen die zur Verschlüsselung der Daten im Software-Client genutzten Schlüssel verloren, ist kein Zugriff auf im jeweiligen Drive gespeicherten Daten mehr möglich.
11. Hornetdrive speichert Backups der zur Verschlüsselung genutzten Schlüssel in verschlüsselter Form in der Hornetdrive Cloud (konfigurierbar). Zusätzlich speichern Hornetdrive Software-Clients Backups der zur Verschlüsselung genutzten Schlüssel lokal. Eine regelmäßige Sicherung der Schlüssel durch den Benutzer wird dringend empfohlen.
12. Die Speicherung von Daten in der Hornetdrive Cloud erfolgt ausschließlich in gesicherten Rechenzentren in Deutschland, sofern nicht ausdrücklich und auf Wunsch des Auftraggebers ein Speicherort in einem anderen Land eingerichtet ist.
13. Benutzer können in bestimmten Versionen des Software-Clients einzelne Dateien per Weblink zum Download freigeben. Diese Dateien werden nach Freigabe unverschlüsselt in der Hornetdrive Cloud gespeichert.
14. Der Anbieter stellt in unregelmäßigen Abständen neue Versionen der Software über Internet-Server bereit, die ggf. Fehlerbehebungen und neue Funktionen enthalten. Über die Bereitstellung neuer Versionen wird der Anbieter den Auftraggeber auf geeignete Weise (per E-Mail, über App-Shops) informieren. Der Auftraggeber ist selber dafür verantwortlich, die jeweils aktuellen Versionen der Software zu nutzen. Die Gewährleistung einer einwandfreien Funktion des Hornetdrive Service bezieht sich nur auf die jeweils aktuellen, bereitgestellten Versionen der Software.
15. Die Verfügbarkeit der Hornetdrive Cloud beträgt 99,9% im Jahresmittel. Geplante Wartungsarbeiten werden nicht berücksichtigt, diese werden soweit es möglich ist am Wochenende nachts ausgeführt (MEZ).
16. Daten werden auf zwei Speichern redundant gespeichert. Bei Ausfall eines Datenspeichers wird die Redundanz innerhalb von vier Stunden wiederhergestellt.

17. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es Systeme und Software von Hornetsecurity betrifft. Der Support von Systemen des Benutzers und von Software anderer Hersteller ist nicht Bestandteil des Hornetdrive Services.
18. Daten in der Hornetdrive Cloud werden ausschließlich verschlüsselt abgelegt, es sei denn, der Benutzer gibt einzelne Daten ausdrücklich für den Zugriff per Weblink frei. Hornetsecurity hat keinen Zugriff auf von Benutzern in der Hornetdrive Cloud gespeicherte verschlüsselte Daten.

15 Leistungsbeschreibung Hosted Exchange

1. Die für den Hornetsecurity Hosted Exchange Service genutzte Plattform ist Microsoft Exchange 2013.
2. Je Postfach stehen 25 GB Speicherplatz zur Verfügung. Der Speicherplatz kann in Schritten von 1 GB gegen Aufpreis auf bis zu 50 GB vergrößert werden.
3. Zusätzliche stehen Ressourcen-Postfächer zur Verfügung (Kalender, für gemeinsam genutzte Arbeitsmittel wie Besprechungsräume, Beamer etc.) Standardmäßig haben alle Postfach-Benutzer Schreibberechtigungen auf eine Ressourcen-Mailbox. Über das Kundencenter kann einzelnen Benutzern oder Gruppen Vollzugriff auf eine Ressource eingeräumt werden. Diese Benutzer oder Gruppen sind „Manager" der Ressource und können spezifische Ressourcen-Einstellungen über die Outlook® Web App vornehmen.
4. Zum Zugriff auf das Postfach stehen folgende Wege zur Verfügung:
   - Outlook® Web App per Web-Browser
   - IMAP und POP3 Zugang
   - Zugriff mit Outlook® Client (Outlook® Anywhere / RPC over HTTPS, Outlook®-Lizenz muss separat erworben werden)
   - ActiveSync® (für Android, iOS etc.)
   - Entourage / Mac Outlook® 2011 Client mittels Webservices (Entourage- / Outlook®-Lizenz muss separat erworben werden)
5. Zugriff auf Postfächer anderer Benutzer, Gruppenkalender usw. ist per Workgroup-Funktionen möglich.
6. E-Mails werden bis zu maximal 100 MB Bruttogröße verarbeitet (versendete und empfangene E-Mails).
7. Je E-Mail können bis zu 1000 Empfänger angegeben werden.
8. Automatische Maßnahmen gegen Überlauf eines Postfachs:
   - Ablage eines Warnhinweises im Postfach eines Benutzers ab 90% Speicherplatzbelegung
   - E-Mailversand wird ab 95% Speicherplatzbelegung blockiert.
   - Ab 100% Speicherplatzbelegung kann der Endnutzer keine E-Mails mehr empfangen.
9. Alle Postfächer, die Ressource-Mailboxen und Info-Postfächer werden täglich nachts vollständig gesichert. Die Sicherung erfolgt in ein baulich getrenntes Rechenzentrum. Zusätzlich werden alle 60 Minuten inkrementelle Backups erstellt. Die Verfügbarkeit/Restorefähigkeit der stündlichen Backups kann jedoch nicht gewährleistet werden.
10. Die Verfügbarkeit der Exchange Services beträgt 99,9% im Jahresmittel. Die Verfügbarkeit der SMTP-Services (Transport von E-Mails) beträgt 99,99% im Jahresmittel. Geplante Wartungsarbeiten werden nicht berücksichtigt, diese werden soweit es möglich ist am Wochenende nachts ausgeführt (MEZ).
11. Die Restorefähigkeit der Backups wird in regelmäßigen Abständen stichprobenartig durch manuelle Restores einzelner Postfächer bzw. Postfachelemente getestet.
12. Backupdaten werden sieben Kalendertage aufbewahrt.
13. Postfach-Benutzer können eigenständig gelöschte Elemente innerhalb Outlooks® und der Outlook® Web App wiederherstellen, sofern sie nicht durch den Benutzer selbst dauerhaft gelöscht wurden. Gelöschte

Elemente werden dazu 14 Tagen nach Löschung vorgehalten.

14. Hornetsecurity filtert eingehende E-Mails auf schädlichen Inhalt (z.B. Viren) und unerwünschte Werbung (z.B. Spam).
15. 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.
16. 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.
17. 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.
18. Empfangene E-Mails werden:
    a. Geblockt (zurückgewiesen), soweit sie noch während der Aufnahme der Datenverbindung mit des Servern von Hornetsecurity mit hoher Sicherheit als unerwünscht erkannt werden,
    b. In Quarantäne gestellt, 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.
19. 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).
20. Auf E-Mails in der Quarantäne können autorisierte Benutzer aus dem Internet zugreifen. Autorisierte Benutzer können interaktiv die Zustellung von E-Mails in Quarantäne in ihr Postfach veranlassen.
21. Optional werden ein- und ausgehende E-Mails entsprechend eingestellter Richtlinien gefiltert (Content-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).
22. Die Richtlinien zur Content-Filterung können von dazu autorisierten Benutzern des Auftraggebers im Hornetsecurity Control Panel eingestellt werden.
23. Soweit Eingriffe durch den Auftraggeber in die Spam-Filterstufen erfolgen (z.B. Einrichten von speziellen White- oder Blacklists), können Qualität und Erkennungsraten der Filterstufen nicht gewährleistet werden.
24. E-Mails werden über einen per TLS verschlüsselten Kanal übertragen, soweit die Gegenseite die Übertragung per TLS unterstützt.
25. Die Speicherung und Verarbeitung der E-Mails erfolgt ausschließlich in gesicherten Rechenzentren in Deutschland, sofern nicht ausdrücklich und auf Wunsch des Kunden etwas anderes vereinbart ist.
26. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Services von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Bestandteil dieses Vertrags.

16 Leistungsbeschreibung Whitelabeling

Hornetsecurity bietet die Möglichkeit, graphische Oberflächen im Corporate Design des Auftraggebers bereitzustellen. Whitelabeling und Customization sind für folgende Interfaces verfügbar:

1. Control Panel
2. Webmailer
3. E-Mail und HTML-Templates

Control Panel Whitelabeling

1. Über das Hornetsecurity Control Panel kann das Layout des Hornetsecurity Control Panels individualisiert werden. Die Einbindung des erstellten Layouts erfolgt zusammen mit der kostenpflichtigen Auftragserteilung des Auftraggebers durch Hornetsecurity.
2. Der Betrieb des angepassten Control Panels erfolgt durch Hornetsecurity. Spätere Anpassungen des Auftraggebers, sowie alle Updates bestehender und zukünftiger Control Panel Versionen sind in der jährlichen Servicegebühr für das Whitelabeling inkludiert.
3. Hornetsecurity stellt Webservices zur Überwachung des individualisierten Control Panels zur Verfügung.
4. Der Kunde ist für ggf. notwendige DNS Einträge betreffend seiner Domains selbst verantwortlich.
5. Hornetsecurity verwendet SSL Zertifikate zur Sicherung des angepassten Control Panels. Die Bereitstellung und der Austausch der benötigten Zertifikate erfolgt automatisch seitens Hornetsecurity.

Webmailer Whitelabeling

1. Die Anpassung und der Betrieb eines individualisierten Webmailers erfolgt durch Hornetsecurity. Spätere Anpassungen und Aktualisierungen müssen durch den Auftraggeber separat beauftragt werden.
2. Anpassungen werden nach Aufwand abgerechnet.
3. Hornetsecurity stellt Webservices zur Überwachung des individualisierten Webmailers zur Verfügung.
4. Der Kunde ist für ggf. notwendige DNS Einträge betreffend seiner Domains selbst verantwortlich.
5. Hornetsecurity verwendet SSL Zertifikate zur Sicherung des angepassten Webmailers und des Websafe. Die Bereitstellung und der Austausch der benötigten Zertifikate erfolgt automatisch seitens Hornetsecurity.

Customization Templates

1. Der Auftraggeber kann die verwendeten HTML oder E-Mail-Templates basierend auf einem vorgegebenen Grunddesign individualisieren.
2. Hornetsecurity unterstützt die Individualisierung von HTML und E-Mail-Templates durch die Bereitstellung eines Template Builders und einer technischen Dokumentation.
3. Hornetsecurity kann den Auftraggeber bei der Anpassung individueller Templates auf Wunsch unterstützen. Dieser Dienst muss separat bestellt werden und die Abrechnung erfolgt nach Aufwand.

17 Leistungsbeschreibung SIEM Connector

1. Der Hornetsecurity SIEM Connector ermöglicht es dem Auftraggeber, E-Mail-Protokolleinträge automatisiert aus der Hornetsecurity Cloud zu empfangen und in ihrem eigenen SIEM-Dienst zu importieren.
2. Hornetsecurity SIEM Connector liefert detaillierte Informationen (Felder) in jedem Protokolleintrag. Die möglichen Inhalte orientieren sich am Informationsgehalt der E-Mail-Suche im Hornetsecurity Control Panel.
   Folgende Informationen können enthalten sein:

   a. Allgemeine E-Mail-Informationen: E-Mail-Betreff, Dateinamen der Anhänge, Message-ID aus dem Header,

verwendete Verschlüsselungsmethode und Größe der E-Mail.

b. Informationen zum Absender: Quelladresse aus dem SMTP-Dialog und Absender, wie im E-Mail-Header angegeben.

c. Informationen zum Empfänger: Postfach, dem diese E-Mail durch den Hornetsecurity Spam and Malware Protection zugeordnet wurde und Empfänger, wie im E-Mail-Header angegeben.

d. Informationen zur Übertragung: Richtung des E-Mail-Verkehrs, Name des Servers, an den diese E-Mail weitergeleitet wurde, Sender-IP, Name des Remote-Servers und SMTP Reply Code

3. Informationen zur Verarbeitung: Datum und Uhrzeit der ersten Verarbeitung, Klassifizierung und Grund der Klassifizierung sowie Anzahl der Protokolleinträge für diese E-Mail.
4. Voraussetzung für die Nutzung des Hornetsecurity SIEM Connector ist die Buchung von entweder Hornetsecurity Spam and Malware Protection oder Hornetsecurity 365 Total Protection (Business oder Enterprise).
5. Technische Voraussetzung für die Nutzung des Hornetsecurity SIEM Connectors ist ein SIEM-System, das imstande ist, Protokolleinträge über das Syslog-Protokoll zu empfangen oder ein eigenständiger Syslog-Server, der RFC 5424 bzw. RFC 6587 (für Syslog over TCP) vollständig unterstützt. Der Syslog-Server muss über ausreichende Kapazitäten zur Verarbeitung der Protokolleinträge verfügen. Darüber hinaus soll er keine Ratenbegrenzung für den Hornetsecurity SIEM Connector -Verkehr anwenden. Systemspezifische Einstellungen können erforderlich sein. Für die Vollständigkeit der Daten ist eine ständige Erreichbarkeit des SIEMs oder Syslog-Servers für den eingehenden Verkehr aus allen Netzbereichen von Hornetsecurity durch den Auftraggeber sicherzustellen.
6. Der Hornetsecurity SIEM Connector wird pro Domain konfiguriert. Dies bedeutet, dass der Auftraggeber separate Syslog-Server für seine Domains einsetzen und diese Daten empfangen lassen kann.
   Hornetsecurity SIEM Connector unterstützt drei verschiedene Protokolle: TCP mit TLS-verschlüsseltem Kanal (empfohlen), TCP (unverschlüsselt) und UDP (unverschlüsselt).
7. Der Hornetsecurity SIEM Connector unterstützt drei Nutzdatenformate: CEF, LEEF und Schlüssel-Wert-Paare.
8. Der Hornetsecurity SIEM Connector versendet Protokolleinträge innerhalb von Syslog-Paketen. Der Nachrichtenteil des Syslog-Pakets enthält dabei den formatierten Protokolleintrag.
9. Das vom Hornetsecurity SIEM Connector übertragene Syslog-Paketformat entspricht den Anforderungen von RFC 5424 als auch RFC 3164.

Fair Use Limits (Einschränkungen zur angemessenen Nutzung)

1. 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.
2. 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.

3. 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.
4. 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.
5. 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.
6. 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
   a. 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.
   b. Sie zu informieren, dass Ihr Konto innerhalb eines nach unserem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieses Zeitraums werden die Backups ausgesetzt.
7. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:
   a. werden Ihre Sicherungsdaten am Ende des von uns in der diesbezüglichen Benachrichtigung festgelegten Zeitrahmens gelöscht, ungeachtet anderslautender Bestimmungen in den Allgemeinen Geschäftsbedingungen.
   b. erhalten Sie eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage Ihres Abonnementzeitraums.