23.06.2023

Leistungsbeschreibung
365 Total Protection

1.1 365 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, Threat, AdvThreat, 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 SMIME/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 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 Benutzers 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.

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.

1.2 365 Total Protection Enterprise

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 mit geeigneten Anhängen 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.
   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. Secure Links: In E-Mails oder in E-Mail-Anhängen enthaltene URLs werden aktiviert und das resultierende Verhalten analysiert.
    b. Secure Links 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. URLs ohne erkennbare Bedrohung nach einem Scan und URL Einträge auf einer Whitelist werden nicht ersetzt.

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.

17. **Fair Use Limits (Einschränkungen zur angemessenen Nutzung)**
a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Software erforderlich sind und die wir in diesem Zusammenhang zur Verfügung stellen, werden von allen unseren Kunden gemeinsam genutzt. Daher haben wir das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösung angemessen und fair nutzen, so dass eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.
b. Wir haben uns dazu entschlossen, keine Richtwerte vorab festzulegen, die eine exzessive oder unangemessene Nutzung bestimmen, da wir nach unserem Ermessen entscheiden können, unsere normalen Service-Levels aufrechtzuerhalten, indem wir anderen Nutzern reservierte Ressourcen, die zu diesem Zeitpunkt nicht genutzt werden, neu zuweisen oder Ressourcen anderweitig skalieren. Sie verstehen, dass wir, wenn wir uns entscheiden, unsere Richtlinie zur angemessenen Nutzung nicht aktiv durchsetzen, nicht davon ausgehen, dass wir auf unser Recht, dies zu tun, verzichtet haben, noch haben wir zugestimmt, dass Sie unsere Dienste weiterhin auf demselben Niveau nutzen, wie Sie es zu einem bestimmten Zeitpunkt tun.
c. Um unsere Dienste nutzen zu können, müssen Sie abrechenbare Einheiten erwerben. Die Anzahl der abrechenbaren Einheiten, die Sie benötigen, hängt von einer Reihe von Kriterien ab, wie z. B. der Größe Ihres Unternehmens, der Anzahl der Nutzer und der Speichergröße der jeweiligen

Datenquellen. Sie können die Anzahl der abrechenbaren Einheiten, die Sie benötigen, anhand unserer Leitfäden, die wir auf unserer Webseite für Gebühren und Abrechnungen hochgeladen haben, oder durch die Unterstützung unseres Vertriebsteams ermitteln.

d. Unabhängig von der Anzahl der abrechenbaren Einheiten, die Sie erworben haben, müssen Sie unsere Dienstleistungen zweckmäßig nutzen, und zwar in einer Weise, die es nicht erforderlich macht, dass wir unverhältnismäßig viele Ressourcen zuweisen müssen. Um dies festzustellen, werden wir Ihre Nutzung unserer Ressourcen und Ihren Speicherbedarf mit dem eines durchschnittlichen Kunden vergleichen. Den Durchschnittskunden ermitteln wir, indem wir die 5% höchsten und die 5% niedrigsten Kunden der jeweiligen Ressource unberücksichtigt lassen und den Mittelwert über alle unsere aktiven Kunden bilden.

e. Spezifische Merkmale, die sich auf die Branche beziehen, in der Sie tätig sind, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.

f. Wenn wir nach vernünftigem Ermessen und in gutem Glauben davon ausgehen, dass die Nutzung unserer Lösung durch Sie nicht sinnvoll ist oder gegen diese Richtlinie verstößt, werden wir nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen

    i. Ihnen erlauben, unsere Lösungen weiterhin zu nutzen, jedoch vorbehaltlich unter der Bezahlung zusätzlicher Gebühren und der Einhaltung von Bedingungen, die wir unter den gegebenen Umständen für angemessen halten.

    ii. Sie zu informieren, dass Ihr Konto innerhalb eines nach unserem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieses Zeitraums werden die Backups ausgesetzt.

g. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:

    i. werden Ihre Sicherungsdaten am Ende des von uns in der diesbezüglichen Benachrichtigung festgelegten Zeitrahmens gelöscht, ungeachtet anderslautender Bestimmungen in den Allgemeinen Geschäftsbedingungen.

    ii. erhalten Sie eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage Ihres Abonnementzeitraums.