Leistungsspezifikation

365 Multi-Tenant Manager for MSPs

365 Multi-Tenant Manager for MSPs (das „Produkt“) ist eine Software-as-a-Service-Lösung (SaaS), die es Managed Service Providern (den „MSPs“, auch als „Service Provider“ bezeichnet) ermöglicht, die Governance zu optimieren und zu standardisieren sowie die Behebung von Problemen im Zusammenhang mit der Einhaltung von Vorschriften und der Risikominderung für M365-Tenants zu automatisieren – alles von einer zentralen Plattform aus.

Um den 365 Multi-Tenant Manager for MSPs zu nutzen, müssen Sie ein Microsoft Partner Center mit dem Hornetsecurity Control Panel verbinden.

Alle aktivierten M365-Tenants von Kunden unterliegen der Lizenzierung des 365 Multi-Tenant Manager for MSPs, unabhängig von den aktiven Einstellungen oder der implementierten Richtlinien. Die Kundengröße wird durch die Anzahl der Microsoft Cloud-Lizenzen mit aktiver Exchange-Funktionalität definiert, unabhängig von der tatsächlichen Nutzung (gesamter Microsoft-Tenant).

Die höchste Nutzung des Monats wird in Rechnung gestellt.

1. 365 Multi-Tenant Manager for MSPs ermöglicht es dem Service Provider, mehrere Tenants zu verwalten und auf vordefinierte sowie benutzerdefinierte Einstellungen, Richtlinien und Vorlagen zuzugreifen, um M365-Tenants zu verwalten. Die folgenden Funktionen sind enthalten:
    a. **Automatische Dienstaktivierung:** Während des Verbindungsassistenten des Microsoft Partner Centers wird der Benutzer aufgefordert, auszuwählen, ob alle M365-Tenants in der „Partner“-Hierarchie im Control Panel ihre 365 Multi-Tenant Manager for MSPs-Dienste automatisch aktivieren sollen oder ob diese später manuell aktiviert werden.
    b. **Automatische M365-Tenant-Integration**: M365-Tenants, die so konfiguriert sind, dass sie während der Verbindung des Microsoft Partner Centers automatisch in den 365 Multi-Tenant Manager for MSPs integriert werden, werden automatisch in das Produkt aufgenommen. Dies nutzt die Granular Delegated Admin Privileges (GDAP)-Beziehung zwischen dem Partnerkonto und den M365-Tenants (sofern vorhanden). Tenants, die über diesen Mechanismus integriert werden, können ohne zusätzliche Anmeldeinformationen oder Autorisierungen verwaltet werden.
    c. **Manuelle M365-Tenant-Integration:** M365-Tenants, die die GDAP-Beziehung mit dem Service Provider nicht nutzen können, können manuell integriert werden. Der Service Provider kann:
        i. Administrationsanmeldeinformationen für den zu integrierenden Tenant direkt im Produkt bereitstellen.
        ii. Einen Autorisierungslink generieren, der an einen Kunden gesendet werden kann, um die Anmeldeinformationen des M365-Tenants extern bereitzustellen und die Integration des Tenants zu ermöglichen.

iii. Einen Autorisierungslink generieren und ihn bequem über eine Vorlage per E-Mail senden, die der 365 Multi-Tenant Manager for MSPs im Namen des Service Providers an den Kunden sendet. Die Anmeldeinformationen des M365-Tenants werden dann extern vom Administrator des M365-Tenants bereitgestellt, um die Integration des Tenants zu ermöglichen.

d. **Multi-Tenant-Übersicht**: Eine zentrale Ansicht, die den aktuellen sowie historischen Compliance-Status der verwalteten M365-Tenants übersichtlich darstellt und maximale Sichtbarkeit für den gesamten Kundenstamm bietet. Aktive Vorgänge sowie eine gekürzte Historie von Vorgängen stehen dem Service Provider als Ausgangspunkt zur Überwachung der allgemeinen Servicefunktionen zur Verfügung. Tenant-spezifische Verknüpfungen sind verfügbar, um die Fehlerbehebung oder detaillierte Untersuchungen einzelner M365-Tenants zu erleichtern.
e. **Vordefinierte Einstellungen:** Mehrere vordefinierte Einstellungen sind Teil der Einstellungen-Bibliothek und unterstützen den Service Provider dabei, schnellstmöglich einen Basisservice anzubieten. Diese Einstellungen decken eine Reihe von kritischen M365-Tenant-Funktionen ab, darunter Entra (ehemals Azure AD), Exchange Online, SharePoint Online sowie andere allgemeine M365-Einstellungen. Jede Einstellung hat einen Standardwert für jeden Parameter, den sie enthält. Diese Werte können nur geändert werden, wenn die Einstellung den M365-Tenants zugewiesen wird, sowohl als Teil der vordefinierten Vorlage als auch im eigenständigen Format. Zusätzlich können vordefinierte Einstellungen, die zugewiesen wurden, zu einem späteren Zeitpunkt für einen spezifischen Kunden überschrieben werden.
f. **Vordefinierte Richtlinien:** Mehrere Richtlinien, die Intune (ehemals Endpoint Manager), bedingten Zugriff, Gerätekonformität, Gruppenrichtlinienkonfiguration und Gerätemanagement abdecken, stehen in der Richtlinien-Bibliothek des Produkts zur Verfügung. Jede Richtlinie hat vordefinierte Standardwerte, die von Hornetsecurity empfohlen werden. Diese Richtlinienwerte können nur geändert werden, wenn die Richtlinie einem M365-Tenant zugewiesen wird, sowohl als Teil der vordefinierten Vorlage als auch im eigenständigen Format. Darüber hinaus können vordefinierte Richtlinien, die zugewiesen wurden, nach ihrer Zuweisung für einen spezifischen Kunden überschrieben werden.
g. **Vordefinierte Vorlagen**: Der 365 Multi-Tenant Manager for MSPs ist mit vordefinierten Vorlagen ausgestattet, die es dem Service Provider ermöglichen, M365-Einstellungen für verwaltete M365-Tenants in wenigen Minuten über einen leistungsstarken und intuitiven Assistenten bereitzustellen. Der Inhalt der vordefinierten Vorlagen umfasst wesentliche Sicherheitseinstellungen für M365-Tenants, die Hornetsecurity empfiehlt. Neue benutzerdefinierte Vorlagen können von Grund auf neu erstellt oder basierend auf einer bestehenden Vorlage für einen schnellen Einstieg erstellt werden. Jede Vorlage kann auch geklont und separat als benutzerdefinierte Vorlage bearbeitet werden.

h. **Leistungsstarke Personalisierung:**
    i. **Benutzerdefinierte Einstellungen**: Fügen Sie beliebige benutzerdefinierte Automatisierungsskripte ein, indem Sie eine benutzerdefinierte Einstellung in der Einstellungen-Bibliothek erstellen. Das Produkt enthält einen leistungsstarken Einstellungs-Builder, der es dem Service Provider ermöglicht, Parameter und PowerShell-Skripte zu definieren. Benutzerdefinierte Einstellungen können einem M365-Tenant ähnlich wie vordefinierte Einstellungen zugewiesen werden, jedoch werden sie auf der vom Benutzer bereitgestellten Azure Function App ausgeführt.
    ii. **Importierte Richtlinien**: Verwaltete M365-Tenants werden gescannt, und alle entdeckten Richtlinien können in die Richtlinien-Bibliothek importiert werden. Sobald sie importiert sind, werden sie als benutzerdefinierte Richtlinie gespeichert und können über einen integrierten Richtlinien-Editor bearbeitet werden. Wenn eine Richtlinie von einem Quell-Tenant importiert wird, werden alle Änderungen, die an der Richtlinie im Quell-Tenant vorgenommen werden, vom 365 Multi-Tenant Manager for MSPs erkannt, und der Service Provider kann die beiden Versionen vergleichen und Änderungen problemlos übernehmen. Benutzerdefinierte Richtlinien können einem M365-Tenant ähnlich wie vordefinierte Richtlinien zugewiesen werden.

i. **Vereinfachter Einsatz:** Vorlagen, sowohl vordefiniert als auch benutzerdefiniert, können einem Tenant oder mehreren Tenants gleichzeitig über einen optimierten mehrstufigen Assistenten zugewiesen werden. Der Service Provider kann die Zuweisung von Einstellungen und Richtlinien an den relevanten Bereich (ganzer Tenant, alle Benutzer oder ausgewählte Benutzer/Gruppen) verwalten und gegebenenfalls Ausschlüsse vornehmen. Für jede Einstellung und Richtlinie wählt der Service Provider den Durchsetzungsmodus („Benachrichtigen“ oder „Erzwingen“). Sobald der Assistent abgeschlossen ist, werden die Einstellungen und Richtlinien auf den M365-Tenant übertragen und wie konfiguriert sofort ausgeführt. Die Compliance-Status der Tenants werden sofort in den Übersichtsbildschirmen des Produkts angezeigt. Die geplante Überwachung beginnt automatisch.

j. **Durchsetzungsmodi**:
    i. **Erzwingen**: Jede Einstellung/Richtlinie, die auf 'Erzwingen' gesetzt ist, wird automatisch korrigiert und auf die zugewiesene Konfiguration zurückgesetzt, wenn Abweichungen (Änderungen) auf dem M365-Tenant erkannt werden.
    ii. **Benachrichtigen**: Jede Einstellung/Richtlinie, die auf 'Benachrichtigen' gesetzt ist, wird als nicht konform markiert und warnt den MSP, wenn Abweichungen (Änderungen) auf dem M365-Tenant festgestellt werden.

k. **Automatisierung, Überwachung und Behebung**: Der 365 Multi-Tenant Manager for MSPs führt Einstellungen und Richtlinien mehrmals täglich aus und stellt sicher, dass jede Abweichung von der Konfiguration so schnell wie möglich erkannt wird. Abhängig vom ausgewählten Durchsetzungsmodus für jede Einstellung oder Richtlinie wird der Service Provider entweder über einen Nichtkonformitätsstatus über einen Produktindikator benachrichtigt

oder Abweichungen werden automatisch wieder durchgesetzt. Für jede Einstellung oder Richtlinie, die auf Benachrichtigen gesetzt ist, kann der Benutzer nach einer durchgeführten Untersuchung im Produkt manuell entscheiden, Abweichungen zu beheben (zu korrigieren) und die nicht konforme Einstellung oder Richtlinie in einen konformen Zustand zurückzusetzen.

l. **Vorgangshistorie**: Der Service Provider kann die vom 365 Multi-Tenant Manager for MSPs durchgeführten Aktionen problemlos nachverfolgen. Die Einträge in der Vorgangshistorie bieten eine detaillierte Übersicht über die durchgeführten Aktionen und deren Status – ob erfolgreich abgeschlossen, teilweise abgeschlossen oder fehlgeschlagen. Die Service Provider können auf diesen Verlauf entweder für alle verwalteten Tenants gesammelt oder für einen bestimmten M365-Tenant im Detail zugreifen..

2. Der 365 Multi-Tenant Manager for MSPs ermöglicht es dem Service Provider, sich auf die Ebene eines verwalteten Kunden zu fokussieren und die individuelle Konfiguration des jeweiligen M365-Tenants zu überwachen und zu verwalten. Folgende Funktionen sind enthalten:
   a. **Tenant-Übersicht:** Ähnlich der Multi-Tenant-Übersicht visualisiert diese Tenant-Übersicht wichtige Informationen in Bezug auf einen bestimmten M365-Tenant. Die Einhaltung der Vorschriften wird sowohl als Momentaufnahme als auch historisch berichtet. Laufende und abgeschlossene Vorgänge können in praktischen Widgets aufgelistet werden. Sie bietet auch eine Übersicht darüber, wie die Einstellungen und Richtlinien für den M365-Tenant bereitgestellt wurden (ob als Teil einer Vorlage oder als eigenständiger Inhalt).
   b. **Einstellungen:** Eine detaillierte Liste aller für den M365-Tenant bereitgestellten Einstellungen wird angezeigt, die den Compliance-Status in Bezug auf die gewünschten Werte, den Durchsetzungstyp (Erzwingen oder Benachrichtigen), die Kategorie, zu der die Einstellung gehört, und ob die Einstellung als eigenständige Einstellung oder als Teil einer Vorlage zugewiesen wurde, anzeigt. Der Service Provider kann die Compliance der Einstellungen manuell durchsetzen, die auf „Benachrichtigen“ gesetzt und nach einer unabhängigen Untersuchung der Ursache für die Konfigurationsabweichung als nicht konform markiert wurden. Einstellungen können manuell überschrieben werden (auf spezifische Werte oder Aktionen), um eine Ausnahme zu machen, die den spezifischen M365-Tenant betrifft, auch wenn sie über eine Vorlage bereitgestellt werden, die anderen M365-Tenants zugewiesen ist.
   c. **Richtlinien**: Eine detaillierte Liste aller für den M365-Tenant bereitgestellten Richtlinien wird angezeigt, die den Compliance-Status mit den gewünschten Werten, die Durchsetzungsaktion (Erzwingen oder Benachrichtigen), die Kategorie, zu der die Richtlinie gehört, und ob die Richtlinie als eigenständige Richtlinie oder als Teil einer Vorlage zugewiesen wurde, anzeigt. Der Service Provider kann die Compliance der Richtlinien manuell durchsetzen, die mit einer Benachrichtigungsaktion als nicht konform markiert sind, nachdem er eine unabhängige Untersuchung der Ursache für die Konfigurationsabweichung durchgeführt hat. Richtlinien können

manuell überschrieben werden (auf spezifische Werte oder Aktionen), um eine Ausnahme zu machen, die den spezifischen M365-Tenant betrifft, auch wenn sie über eine Vorlage bereitgestellt werden, die anderen M365-Tenants zugewiesen ist. Darüber hinaus erkennt der 365 Multi-Tenant Manager for MSPs andere Richtlinien, die möglicherweise bereits auf dem verwalteten M365-Tenant vorhanden sind, und ermöglicht es dem Benutzer, die Richtlinie in die Richtlinien-Bibliothek zu importieren. Sobald die Richtlinie importiert ist, kann sie angepasst und anderen M365-Tenants als eigenständige Richtlinie oder als Teil einer Vorlage bereitgestellt werden.

3. Verpflichtungen des Service Providers:

   Der Service Provider muss

   a. Den Dienst gemäß dem Abschnitt zu Fair Use Limits verwenden und darauf zugreifen sowie alle geltenden Nutzungsbedingungen und die in dieser Leistungsspezifikation festgelegten Fair Use Limits einhalten.
   b. Den Compliance-Status der verwalteten M365-Tenants in regelmäßigen Abständen überwachen, um festzustellen, ob er mit den festgelegten Basislinien und Compliance-Anforderungen übereinstimmt.

4. Einschränkungen und Anforderungen

   a. Für die Nutzung des 365 Multi-Tenant Manager for MSPs durch einen Service Provider ist eine Verbindung zu einem Microsoft Partner Center zwingend erforderlich.
      i. Auf Partnerebene muss mindestens ein Microsoft Partner Center mit dem Control Panel-Konto verbunden sein. Dies ist eine Mindestvoraussetzung, damit M365-Tenants im 365 Multi-Tenant Manager for MSPs entdeckt und verwaltet werden können.
      ii. Damit sie im 365 Multi-Tenant Manager for MSPs entdeckt und verwaltet werden können, muss die erforderliche Beziehung zwischen dem Microsoft Partner Center und den M365-Tenants die im folgenden Link aufgeführten Kriterien erfüllen:
         - Link zu den Anforderungen hier: https://go.hornetsecurity.com/kb/mpc_m365tenant_relationship
      iii. Basierend auf der oben genannten Beziehung sowie den dokumentierten Anforderungen an die Granular Delegated Admin Privileges (GDAP) können die ausgewählten M365-Tenants automatisch im 365 Multi-Tenant Manager for MSPs integriert und der Benutzer kann sofort mit der Bereitstellung von Vorlagen, Einstellungen und/oder Richtlinien beginnen. Sollte dies aufgrund von nicht erfüllten GDAP-Berechtigungen nicht möglich sein, ist eine manuelle Integration des Tenants (Bereitstellung von administrativen Anmeldeinformationen) erforderlich, bevor der Service Provider mit der Konfiguration der ausgewählten M365-Tenants beginnt.
      iv. Die Granular Delegated Admin Privileges (GDAP) sind nur für die automatische Integration eines M365-Tenants erforderlich. Wenn die GDAP-Beziehung zwischen dem Partner und dem verwalteten M365-Tenant unterbrochen wird, behält der 365 Multi-Tenant Manager for MSPs dennoch alle

Verwaltungsfunktionen bei, wenn ein Tenant bereits integriert wurde. Der Zugriff auf die Verwaltung des M365-Tenants kann vollständig entfernt werden, indem der Tenant vom 365 Multi-Tenant Manager for MSPs abgemeldet wird.

b. Hornetsecurity ist nicht verantwortlich für Skripte oder benutzerdefinierte Richtlinien, die außerhalb seiner Infrastruktur ausgeführt werden. Alle benutzerdefinierten Skripte müssen mit einer vom Service Provider bereitgestellten und verwalteten Azure Function App ausgeführt werden, die vollständig unabhängig von der Hosting- und Ausführungsumgebung von Hornetsecurity betrieben wird.
c. Der technische Support von Hornetsecurity beschränkt sich ausschließlich auf Probleme im Zusammenhang mit den eigenen Systemen. Der Support für die Systeme des Service Providers, einschließlich benutzerdefinierter Skripte oder Azure Function Apps, fällt nicht in den Rahmen der vertraglichen Verpflichtungen von Hornetsecurity.

5. Haftungsausschlüsse
   a. Der MSP erkennt an, dass Hornetsecurity möglicherweise nicht in der Lage ist, das Produkt anzubieten, wenn die Funktionen von Microsoft 365, erforderliche API-Endpunkte oder andere technische Spezifikationen von Microsoft oder einem anderen Drittanbieter geändert werden. Sollte dies der Fall sein, kann Hornetsecurity das Abonnement des Service Providers kündigen, Hornetsecurity wird jedoch in diesem Fall dem Service Provider eine anteilige Rückerstattung für den ungenutzten Zeitraum seines Abonnements gewähren.
   b. Der Service Provider versteht und erkennt an, dass keine Handlung oder Unterlassung von Hornetsecurity als Überprüfung, Validierung oder Zustimmung zu einem Skript, Befehl, einer Richtlinie oder anderen Inhalten oder Daten, die vom Service Provider importiert, geschrieben oder ausgeführt wurden, ausgelegt werden darf. Der Service Provider erkennt weiterhin an, dass alle vom Service Provider importierten, geschriebenen oder ausgeführten Skripte, Befehle, Richtlinien oder anderen Inhalte oder Daten in seiner alleinigen Verantwortung liegen.
   c. Der Service Provider darf keine Daten, Informationen oder sonstigen Materialien einreichen, die (i) er als vertraulich oder urheberrechtlich geschützt betrachtet und über 365 Multi-Tenant Manager for MSPs übermittelt; und/oder (ii) schädlich, skandalös, verleumderisch, obszön oder anderweitig rechtswidrig oder unerlaubt sind; und/oder (iii) Computerviren, Zeitbomben, Hintertüren oder andere Programme enthalten, die dazu entwickelt wurden, den normalen Betrieb von 365 Multi-Tenant Manager for MSPs zu stören.
   d. Skripte, Befehle, Richtlinien oder andere Inhalte oder Daten, die im 365 Multi-Tenant Manager for MSPs geschrieben, importiert oder ausgeführt werden (die „Daten“), werden vom Service Provider auf nicht vertraulicher Basis durchgeführt (unabhängig von gegenteiligen Angaben in den übermittelten Informationen oder begleitenden Korrespondenzen), und der Service Provider gewährt Hornetsecurity hiermit ein uneingeschränktes, unbefristetes, unwiderrufliches, nicht exklusives, vollständig bezahltes, lizenzfreies, übertragbares und

unterlizenzierbares Recht, die Daten in jeder Weise, zu jedem Zweck und auf jedem Gebiet zu nutzen, einschließlich der Bereitstellung eines Skripts für andere Kunden, der Verbesserung des 365 Multi-Tenant Manager for MSPs und der Schaffung anderer Produkte und Dienstleistungen.

e. Der Service Provider garantiert, dass er keine Daten bereitstellt, die einer Lizenz unterliegen, die Hornetsecurity verpflichten würde, seine Software, Technologien oder Dokumentationen an Dritte zu lizenzieren, weil Hornetsecurity die Daten des Service Providers in diese integriert.

6. Fair Use Limits

a. Die für die Nutzung der Hornetsecurity 365 Total Protection-Lösungen erforderliche Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die Hornetsecurity in diesem Zusammenhang bereitstellt, werden zwischen allen Service Providern von Hornetsecurity geteilt. Infolgedessen hat Hornetsecurity das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Service Provider die Lösungen in einer angemessenen und fairen Weise nutzen, damit eine solche Nutzung die normale Serviceleistung für andere Service Provider nicht beeinträchtigt oder verhindert.

b. Hornetsecurity hat beschlossen, keine vordefinierten Benchmarks festzulegen, die eine übermäßige oder unangemessene Nutzung bestimmen, da Hornetsecurity nach eigenem Ermessen entscheiden kann, die normalen Servicelevels beizubehalten, indem Ressourcen, die für andere Benutzer reserviert sind und in diesem Moment nicht genutzt werden, umverteilt werden, oder Ressourcen anderweitig skaliert werden. Der Service Provider versteht, dass, wenn Hornetsecurity beschließt, seine Fair-Use-Richtlinie nicht aktiv durchzusetzen, dies nicht als Verzicht auf das Recht von Hornetsecurity ausgelegt wird, dies zu tun, noch dem Service Provider das Recht eingeräumt wird, die Dienste von Hornetsecurity weiterhin zu nutzen.

c. Um von den Diensten von Hornetsecurity zu profitieren, muss der Service Provider fakturierbare Einheiten erwerben. Die Anzahl der erforderlichen fakturierbaren Einheiten hängt von einer Reihe von Kriterien ab, wie der Größe der Organisation des Service Providers, der Anzahl der Benutzer usw.

d. Unabhängig von der Anzahl der erworbenen fakturierbaren Einheiten muss der Service Provider die Dienste von Hornetsecurity sinnvoll nutzen, insbesondere in einer Weise, die nicht erfordert, dass Hornetsecurity unverhältnismäßig viele Ressourcen zuweist. Zur Bestimmung dieses Sachverhalts wird Hornetsecurity die Ressourcennutzung des Service Providers (z. B. Speicheranforderungen, Anzahl der parallelen Verbindungen) mit der eines durchschnittlichen Service Providers vergleichen. Hornetsecurity bestimmt den durchschnittlichen Service Provider, indem die 5 % der höchsten Service Provider und die 5 % der niedrigsten Service Provider bei den jeweiligen Ressourcen außer Acht gelassen und der Wert zwischen allen aktiven Service Providern von Hornetsecurity gemittelt wird.

e. Spezifische Merkmale der Branche, in der der Service Provider tätig ist, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.
f. Wenn Hornetsecurity nach vernünftigem Ermessen und in gutem Glauben der Ansicht ist, dass die Nutzung der Hornetsecurity-Lösungen durch den Service Provider nicht angemessen ist oder gegen diese Richtlinie verstößt, kann Hornetsecurity nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen:
    i. Dem Service Provider die weitere Nutzung der Hornetsecurity-Lösungen erlauben, jedoch unter der Bedingung der Zahlung zusätzlicher Gebühren und der Einhaltung aller Bedingungen, die Hornetsecurity unter den gegebenen Umständen für angemessen hält.
    ii. Den Service Provider darüber informieren, dass sein Konto innerhalb eines von Hornetsecurity festgelegten angemessenen Zeitraums gekündigt wird. In dieser Zeit werden alle Dienste und/oder Vorgänge ausgesetzt.
g. Wenn Hornetsecurity sein Recht zur Kündigung des Kontos des Service Providers wie oben erwähnt ausübt:
    i. Alle Daten (Metadaten oder andere) werden am Ende des von Hornetsecurity in der diesbezüglichen Benachrichtigung festgelegten Zeitraums gelöscht, ungeachtet entgegenstehender Bestimmungen in den Allgemeinen Geschäftsbedingungen.
    ii. Die Service Provider erhalten eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage ihrer Abonnementlaufzeit.