Leistungsbeschreibung
365 Permission Manager

365 Permission Manager ist ein Governance, Risk & Compliance (GRC)-Service, der es Benutzern ermöglicht, einen vollständigen Überblick über ihre Microsoft 365-Dateiberechtigungen in SharePoint, OneDrive, Microsoft Teams und Microsoft 365 Groups zu erhalten und deren Einhaltung durchzusetzen.

Um den 365 Permission Manager Service nutzen zu können, müssen Sie über Microsoft Cloud-Lizenzen mit SharePoint-, OneDrive- und/oder Teams-Funktionalität verfügen, die von Microsoft aktiviert wurden.

Alle Entitäten innerhalb des gesamten Microsoft-Tenants, denen eine Microsoft 365-Lizenz zugewiesen ist, die Funktionalitäten für SharePoint, OneDrive oder Teams gewährt, unterliegen unabhängig von ihrer aktiven Nutzung der 365 Permission Manager-Lizenzierung.

Es wird der höchste Nutzungsumfang des Monats berechnet.

1. 365 Permission Manager ermöglicht Ihnen das Management, Monitoring und Audit der Compliance von Berechtigungen für die vom Kunden angegebenen Daten. Die folgenden Funktionalitäten sind enthalten:

    a. Auto-Provisioning: 365 Permission Manager erkennt automatisch neu erstellte Benutzerinhalte, Gruppeninhalte, SharePoint Sites und OneDrive-Accounts und kann sie automatisch ohne Eingreifen des Administrators scannen.
    b. Mit 365 Permission Manager können Sie Compliance-Richtlinien für SharePoint Sites erstellen und zuweisen. Falls das Verhalten der Benutzer in Bezug auf eine Site, ihre Ordner und/oder Dateien gegen die Kriterien der zugewiesenen Compliance-Richtlinie verstößt, kann der Site Besitzer und/oder Administrator alarmiert werden.
        i. Eine Reihe von Best-Practice-Compliance-Richtlinien wird standardmäßig bereitgestellt, aus denen der Benutzer einfach auswählen kann, um sie SharePoint Sites zuzuweisen und zu monitoren.
        ii. Benutzerdefinierte Compliance-Richtlinien können während des Tenant-Onboardings und zu jedem späteren Zeitpunkt erstellt und zugewiesen werden.
        iii. Eine Compliance-Richtlinie kann als Standard konfiguriert werden, wodurch die Durchsetzung der Compliance für jede neu erstellte SharePoint-Site oder jedes neu erstellte OneDrive-Konto erleichtert wird.
        iv. Site-Konfigurationen können bei der Zuweisung einer Policy optional für eine Site erzwungen werden. Wenn diese Option aktiviert ist, werden die Site-Konfiguration und die Link-Sharing-Einstellungen automatisch auf Grundlage der Policy-Parameter konfiguriert.
    c. ToDo-Liste: Eine konsolidierte Liste aller Richtlinienverstöße, mit der Benutzer bequem mehrere Prüfungen auf einmal durchführen können.

d. Delegation an Site-Besitzer - Benutzer innerhalb einer Organisation, die SharePoint-Sites oder OneDrive-Konten besitzen, können selbständig die Compliance-Verstöße gegen ihre Sites überprüfen.
    i. Automatische Warnungen vor Verstößen werden in Übereinstimmung mit der den jeweiligen Sites zugewiesenen Compliance-Richtlinien generiert und versendet.
    ii. Site-Besitzer erhalten durch die Warnmeldungen direkten Zugriff auf 365 Permission Manager, mit dem sie Verstöße genehmigen oder beheben können.
e. Audit: ein Wizard zum Genehmigen oder Beheben von Verstößen:
    i. Mit dem Audit können Benutzer und CISOs neue und bestehende Verstöße gegen Element- oder Site-Einstellungen leicht erkennen, indem sie alle Richtlinienverstöße in einem geführten Assistenten im Detail auflisten und so die Möglichkeit bekommen, Änderungen entweder zu genehmigen oder zu beheben.
    ii. Ein vollständiger Audit kann geplant werden, um Verstöße, die in der Vergangenheit genehmigt wurden, zu überprüfen und zu aktualisieren.
f. Automatische Korrektur: Verstöße gegen die Freigabeeinstellungen von Elementen und die Site-Konfiguration können nach Ablauf einer konfigurierten Zeitspanne auf Grundlage der Policy-Parameter automatisch korrigiert (behoben) werden.
g. Im Explorer Elemente und deren Berechtigungen überprüfen:
    i. Es ist möglich, die SharePoint- und OneDrive-Elementhierarchie zu durchsuchen, Elementberechtigungen anzuzeigen, nach mehreren Kriterien wie Berechtigungsattributen (z. B. "Extern freigegebene Elemente"), Compliance-Richtlinien und dem Status der Compliance-Richtlinie zu filtern und auffällige Berechtigungen zu identifizieren.
    ii. Die Funktion "Anzeigen als" ermöglicht es dem Benutzer, SharePoint aus der Sicht eines anderen ausgewählten Benutzers zu sehen, während er die SharePoint- und OneDrive-Elementhierarchie durchsucht, um auf einfache Weise Elemente zu identifizieren, auf die die ausgewählte Entität Zugriff hat.
    iii. Die Berechtigungsleiste im Explorer:
        1. Zeigt eine vereinfachte Ansicht aller Benutzer und Gruppen, die Zugriff auf die jeweilige Site-, Ordner- oder Dateiebene haben, sowie deren Berechtigungen, d. h. "Eigentümer", "Bearbeiten" und "Anzeigen".
        2. Es ist auch eine detaillierte Ansicht verfügbar, in der Gruppen innerhalb der Berechtigungsleiste für einzelne Berechtigungen erweitert werden, um Gruppenmitglieder einschließlich verschachtelter Gruppen und deren Mitglieder anzuzeigen. Mit einem Klick kann der Benutzer die Verschachtelung von Gruppen auflösen und alle Benutzer anzeigen, die Zugriff haben.
h. Management von Berechtigungen - Mit 365 Permission Manager können Sie die folgenden Management-Aktionen durchführen:
    i. Auf der Organisationsebene:
        1. Berechtigungen eines Benutzers oder einer Gruppe über ausgewählte Share-Point Sites und OneDrive-Konten in einer Organisation entziehen.
        2. Auffinden und Entfernen von Gruppenzugriff auf Unternehmensebene, wie z. B. die Gruppe "Jeder" oder "Alle Benutzer".
        3. Auffinden und Entfernen von Berechtigungen, die Benutzern zugewiesen wurden, die nicht mehr in einer Organisation existieren (auch bekannt als verwaiste Benutzer).
        4. Identifizieren und konfigurieren Sie "Externe Freigabeebenen", die einschränken, welche Arten von Benutzern auf Elemente auf SharePoint-Sites und OneDrive-Konten zugreifen können.

   ii. Auf der Ebene eines Elements:
      1. Löschen von Freigabelinks auf SharePoint- und OneDrive-Elementen.
      2. Wiederherstellung der Vererbung von Berechtigungen für SharePoint- und OneDrive-Elemente.
      3. Konfigurieren von Eigentümer-, Bearbeiter- und Leserberechtigungen für SharePoint- und OneDrive-Elemente.

i. Management von Dateien, die über private Teams-Chats geteilt wurden:
   Hinweis: Wenn eine Datei in einem privaten Teams-Chat zwischen einem oder mehreren Benutzern freigegeben wird, lädt Microsoft automatisch eine Kopie der Datei in das OneDrive des sendenden Benutzers hoch und erstellt einen Freigabelink für diese Datei. Dies ist nicht der Fall, wenn Dateien in Teams-Gruppen-Chats freigegeben werden.
   i. Freigabelinks, die beim Teilen von Dateien in einem privaten Teams-Chat erstellt werden, können identifiziert werden. Ein Policy-Verstoß kann ausgelöst werden, wenn der Freigabelink nicht innerhalb einer festgelegten Frist gelöscht wird.
   ii. Separat können auch Dateien identifiziert werden, die auf OneDrive hochgeladen wurden, wenn sie in einem privaten Chat von Teams geteilt worden sind. Ein Policy-Verstoß kann ausgelöst werden, wenn diese Dateien nicht innerhalb eines festgelegten Zeitraums gelöscht werden.
   iii. Außerdem können Dateien nach einem in der Policy festgelegten Zeitraum automatisch gelöscht (in den Papierkorb verschoben) werden.

j. Das Dashboard bietet leicht verständliche visuelle Darstellungen des Compliance-Status für alle SharePoint-, Teams-Sites oder OneDrive-Konten des Tenants, mit Links zum vorgefilterten Explorer, um Sites mit nicht konformem Richtlinienstatus zu bearbeiten.

k. Es kann eine tägliche Sammelwarnmeldung eingerichtet werden, um die Empfänger über Sites zu informieren, die neue geteilte Elemente enthalten mit:
   i. Anonymen Benutzern
   ii. Gästekonten, die nicht zur Organisation gehören
   iii. Dem Dienstprinzipal "Jeder", der zur Organisation gehört

l. Generieren Sie Berichte über Berechtigungen mit detaillierten Angaben:
   i. Elemente, auf die anonyme Benutzer von außen zugreifen können, und solche, die mit externen Benutzern der Organisation gemeinsam genutzt werden, einschließlich der Art des Zugriffs auf diese Elemente.
   ii. Elemente, auf die ein bestimmter Benutzer oder eine bestimmte Gruppe Zugriff hat, einschließlich die Art des Berechtigungszugriffes, den sie für jedes Element haben.
   iii. Elemente, die zu einer SharePoint-Site oder einem OneDrive-Konto gehören, einschließlich der Berechtigungen, die den Benutzern und Gruppen zugewiesen wurden, die auf diese Elemente zugreifen dürfen.

m. Aktivitätsprotokoll: Alle Aktivitäten des Benutzerkontos in 365 Permission Manager werden automatisch protokolliert. Dazu gehören grundlegende und sicherheitsrelevante Aktionen sowie datenschutzrelevante Informationen, wie z.B. das Browsen und Anfragen zur Verwaltung von Berechtigungen, die bei der Durchführung von Compliance-Audits gestellt werden.

2. Pflichten des Kunden: Der Kunde ist verpflichtet, den Service in Übereinstimmung mit der *Acceptable Use Policy* (akzeptierbare Benutzungsrichtlinien) zu nutzen und auf ihn zuzugreifen und sich an die *Fair Use Policy* (Richtlinie zur angemessenen Nutzung) zu halten.

3. Einschränkungen und Anforderungen

   a. Hornetsecurity leistet Support für autorisierte Benutzer, soweit es sich um Hornetsecurity-Systeme handelt. Der Support für die Systeme des Kunden ist nicht Bestandteil des Vertrages.

4. Haftungsausschlüsse

   a. Wir sind möglicherweise nicht in der Lage, unseren Service anzubieten, wenn die Funktionen von Microsoft 365, die Struktur der zu scannenden Daten oder andere technische Spezifikationen von Microsoft oder einer anderen dritten Partei geändert werden. Sollte dies der Fall sein, können wir Ihr Abonnement kündigen. In diesem Fall erstatten wir Ihnen den ungenutzten Zeitraum Ihres Abonnements anteilig zurück.
   b. Darüber hinaus ist es uns nicht möglich, Berechtigungsmetadaten zu lesen und zu schreiben, wenn der Quellinhalt 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 Bereitstellung der Dienste verlassen, daran gehindert werden, dies zu tun.

5. Fair Use Policy (Richtlinie zur angemessenen Nutzung)

   a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Software erforderlich sind und die wir in diesem Zusammenhang zur Verfügung stellen, werden von allen unseren Kunden gemeinsam genutzt. Daher haben wir das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösung angemessen und fair nutzen, so dass eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.
   b. Wir haben uns dazu entschlossen, keine Richtwerte vorab festzulegen, die eine exzessive oder unangemessene Nutzung bestimmen, da wir nach unserem Ermessen entscheiden können, unsere normalen Service-Levels aufrechtzuerhalten, indem wir anderen Nutzern reservierte Ressourcen, die zu diesem Zeitpunkt nicht genutzt werden, neu zuweisen oder Ressourcen anderweitig skalieren. Sie verstehen, dass wir, wenn wir uns entscheiden, unsere Fair Use Policy nicht aktiv durchzusetzen, nicht davon ausgehen, dass wir auf unser Recht, dies zu tun, verzichtet haben, noch haben wir zugestimmt, dass Sie unsere Dienste weiterhin auf demselben Niveau nutzen, wie Sie es zu einem bestimmten Zeitpunkt tun.
   c. Um unsere Dienste nutzen zu können, müssen Sie abrechenbare Einheiten erwerben. Die Anzahl der abrechenbaren Einheiten, die Sie benötigen, hängt von einer Reihe von Kriterien ab, z. B. von der Größe Ihres Unternehmens, der Anzahl der Benutzer, der Größe des Datenspeichers der jeweiligen Quelle usw. Sie können die Anzahl der abrechenbaren Einheiten, die Sie benötigen, anhand unserer Leitfäden, die wir auf unserer Webseite für Gebühren und Abrechnungen hochgeladen haben, oder durch die Unterstützung unseres Vertriebsteams ermitteln.
   d. Unabhängig von der Anzahl der abrechenbaren Einheiten, die Sie erworben haben, müssen Sie unsere Dienstleistungen zweckmäßig nutzen, und zwar in einer Weise, die es nicht erforderlich macht, dass wir unverhältnismäßig viele Ressourcen zuweisen müssen. Um dies festzustellen, werden wir Ihre Nutzung unserer Ressourcen (z. B. Speicherbedarf, Anzahl paralleler Verbindungen) mit dem eines durchschnittlichen Kunden vergleichen. Den Durchschnittskunden ermitteln wir, indem wir die 5% höchsten und die 5% niedrigsten Kunden der jeweiligen Ressource unberücksichtigt lassen und den Mittelwert über alle unsere aktiven Kunden bilden.
   e. Spezifische Merkmale, die sich auf die Branche beziehen, in der Sie tätig sind, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.
   f. Wenn wir nach vernünftigem Ermessen und in gutem Glauben davon ausgehen, dass die Nutzung unserer Lösung durch Sie nicht sinnvoll ist oder gegen diese Richtlinie verstößt, werden wir nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen:

i. Ihnen erlauben, unsere Lösungen weiterhin zu nutzen, jedoch vorbehaltlich unter der Bezahlung zusätzlicher Gebühren und der Einhaltung von Bedingungen, die wir unter den gegebenen Umständen für angemessen halten.
ii. Sie zu informieren, dass Ihr Konto innerhalb eines nach unserem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieser Zeit werden alle Services und/oder der Betrieb ausgesetzt.

g. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:
i. werden alle Daten (Metadaten, Sicherungsdaten oder andere) am Ende des von uns in der diesbezüglichen Benachrichtigung 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.