Leistungsbeschreibung
365 Permission Manager

365 Permission Manager ist ein Governance, Risk & Compliance (GRC) dienst, der es Kunden 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-Dienst nutzen zu können, müssen Sie über Microsoft Cloud-Lizenzen mit SharePoint-, OneDrive- und/oder Teams-Funktionen verfügen, die von Microsoft aktiviert wurden.

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

Die höchste Nutzung des Monats wird in Rechnung gestellt.

1. 365 Permission Manager ermöglicht dem Kunden die Verwaltung, Überwachung und Prüfung der Einhaltung von Berechtigungen für die von ihm angegebenen Daten. Die folgenden Funktionen sind enthalten:
    a. Automatische Bereitstellung: 365 Permission Manager erkennt automatisch neu erstellte Benutzerinhalte, Gruppeninhalte, SharePoint-Websites und OneDrive-Konten und kann diese automatisch scannen, ohne dass der Administrator des Kunden eingreifen muss.
    b. 365 Permission Manager ermöglicht es dem Kunden, Compliance-Richtlinien für SharePoint-Sites und OneDrive-Konten zu erstellen und zuzuweisen. Wenn das Verhalten eines Benutzers in Bezug auf eine Website, ihre Ordner und/oder Dateien gegen ein Kriterium der zugewiesenen Compliance-Richtlinie verstößt, wird ein Verstoß festgestellt, und der Eigentümer und/oder Administrator der Website kann entsprechend benachrichtigt werden.
        i. Hornetsecurity stellt eine Reihe von Vorlagen für Compliance-Richtlinien zur Verfügung, aus denen der Kunde bei der Erstellung von Compliance-Richtlinien für die Zuweisung und Überwachung von SharePoint-Sites und OneDrive-Konten einfach auswählen kann
        ii. Benutzerdefinierte Richtlinien können zu jedem beliebigen Zeitpunkt erstellt und zugewiesen werden.
        iii. Eine Compliance-Richtlinie kann vom Kunden als Standard konfiguriert werden, was die Durchsetzung der Compliance für alle bestehenden und neuen SharePoint-Websites oder OneDrive-Konten erleichtert, die in Zukunft erstellt werden.
        iv. Die Standorteinstellungen werden immer durchgesetzt und automatisch korrigiert, so dass das Produkt die gewünschten Richtlinien automatisch anwendet, während sich die CISOs auf strategische Prioritäten konzentrieren können.
    c. ToDo-Liste - Eine konsolidierte Liste, die bequem alle Verstöße enthält, um die Prüfung in großem Umfang zu erleichtern.

d. Delegierung von Website-Eigentümern - Benutzer innerhalb einer Organisation, die Eigentümer von SharePoint-Websites oder OneDrive-Konten sind, können ihre eigenen Compliance-Verstöße unabhängig überprüfen.
    i. Automatische Warnungen vor Verstößen werden gemäß der den jeweiligen Standorten zugewiesenen Compliance-Richtlinie erstellt und versandt.
    ii. Website-Besitzer, die diese Warnungen erhalten, erhalten direkten Zugang zu 365 Permission Manager, wo Verstöße genehmigt oder behoben werden können.
e. Automatische Behebung - Verstöße gegen die gemeinsame Nutzung von Elementen können automatisch behoben werden, nachdem eine konfigurierte Zeitspanne auf der Grundlage der Richtlinienparameter verstrichen ist.
f. Erkundung von Gegenständen und deren Berechtigungen:
    i. Es ist möglich, die SharePoint & 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 anomale Berechtigungen zu identifizieren.
    ii. die Funktion "Anzeigen als" ermöglicht dem Kundenadministrator das Durchsuchen SharePoint- und OneDrive-Elementhierarchie zu durchsuchen, wie sie von dem ausgewählten Benutzer oder der Gruppe wahrgenommen wird, um auf einfache Weise Elemente zu identifizieren, die die ausgewählte entität zugriff hat.
    iii. Die Berechtigungstafel im Explorer:
        1. Zeigt eine vereinfachte Ansicht aller Benutzer und Gruppen, die Zugriff auf den jeweiligen Standort, Ordner oder die Datei haben.
        2. Es ist auch eine Detailansicht verfügbar, in der die Gruppen im Berechtigungsbereich erweitert werden, um die Gruppenmitglieder einschließlich verschachtelter Gruppen und deren Mitglieder anzuzeigen. Mit einem Klick kann der Benutzer die Gruppenverschachtelung auflösen und alle Benutzer anzeigen, die Zugriff haben.
g. Verwaltung von Berechtigungen - Mit 365 Permission Manager können Sie die folgenden Verwaltungsaktionen durchführen:
    i. Auf der Ebene der Organisation:
        1. Entzug von Berechtigungen für einen Benutzer oder eine Gruppe auf ausgewählten SharePoint-Sites & OneDrive-Konten in einer Organisation.
        2. Entdeckung und Entfernung von Gruppenzugängen auf Unternehmensebene, z.B. gruppe "Alle" 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 & OneDrive for Business-Konten zugreifen können.
        5. Kopieren von Berechtigungen von einem Benutzer zu einem oder mehreren Benutzern
    ii. Auf der Ebene eines Gegenstands:
        1. Entfernen von Freigabelinks auf SharePoint & OneDrive-Elementen.
        2. Wiederherstellung der Berechtigungsvererbung auf SharePoint & OneDrive-Elementen.

3. Konfigurieren von Eigentümer-, Bearbeiter- und Leserberechtigungen für SharePoint & OneDrive-Elemente.

h. Verwaltung von über Teams freigegebenen Dateien private Chats

Anmerkung: 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 Groups Chats freigegeben werden.

i. Freigabelinks, die bei der Freigabe von Dateien in einem privaten Chat von Teams erstellt werden, können erkannt werden. Diese werden automatisch behoben, wenn festgestellt wird, dass die Datei über einen bestimmten Zeitraum hinweg nicht verwendet wurde.
ii. Optional können die auf OneDrive hochgeladenen Dateien bei der Freigabe in einem privaten Chat von Teams auch automatisch gelöscht (in den Papierkorb verschoben) werden.

i. Die Dashboards bieten leicht verdauliche visuelle Darstellungen des Konformitätsstatus aller SharePoint-, Teams-Websites oder OneDrive-Konten des Mandanten mit Verknüpfungen zum vorgefilterten Explorer, um Websites mit einem nicht konformen Richtlinienstatus zu bearbeiten.
j. Ein täglicher zusammenfassender Alarm kann eingerichtet werden, um die Empfänger per E-Mail über wichtige Aktivitäten innerhalb des Unternehmens zu informieren.
k. Generieren Sie Berichte über Genehmigungen 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 der Zugriffsberechtigung für diese Elemente.
   ii. Objekte, auf die ein bestimmter Benutzer oder eine bestimmte Gruppe Zugriff hat, einschließlich der Berechtigungsstufe, die sie für jedes Objekt haben.
   iii. Elemente, die zu einer SharePoint-Website oder einem OneDrive-Konto gehören, einschließlich der Berechtigungen, die den Benutzern und Gruppen zugewiesen wurden, die eine Zugriffsberechtigung für diese Elemente haben.
   iv. Änderungen, die an Berechtigungen und Site-Konfigurationen für Elemente innerhalb einer Site vorgenommen wurden.
l. Aktivitätsprotokoll: Alle Aktivitäten des Benutzerkontos innerhalb von 365 Permission Manager werden automatisch protokolliert. Dazu gehören grundlegende und sicherheitsrelevante Aktionen sowie datenschutzrelevante Informationen wie z. B. Browsing und Anfragen zur Verwaltung von Berechtigungen, die im Rahmen der Prüfung der Einhaltung von Vorschriften gestellt werden.

2. Verpflichtungen der Kunden
   a. Der Kunde muss den Dienst in Übereinstimmung mit den folgenden Bestimmungen nutzen und darauf zugreifen Richtlinie zur akzeptablen Nutzung und hält sich an die Grenzen der fairen Nutzung.

3. Einschränkungen und Anforderungen
   a. Hornetsecurity bietet Support für autorisierte Benutzer, soweit es die Systeme von Hornetsecurity betrifft. Die Unterstützung der Systeme des Kunden ist nicht Bestandteil des Vertrags.

4. Haftungsausschlüsse
   a. Wir sind möglicherweise nicht in der Lage, unseren Dienst anzubieten, wenn die Funktionen von Microsoft 365, die Struktur der zu scannenden Daten oder andere technische Spezifikationen von Microsoft oder einem anderen Dritten geändert werden. In diesem Fall können wir Ihr Abonnement kündigen, aber wenn wir dies tun, werden wir erstatten den nicht genutzten Zeitraum Ihres Abonnements anteilig zurück.
   b. Darüber hinaus dürfen wir keine Metadaten zu Berechtigungen lesen und schreiben, wenn der Quellinhalt beschädigt ist, Fehler enthält oder aus anderen Gründen nicht lesbar ist unlesbar 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.

5. Richtlinie zur fairen Nutzung
   a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Lösung 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 vernünftig und fair nutzen, so dass eine solche Nutzung die normale Leistungserbringung 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 Wenn wir uns entscheiden, unsere Fair-Use-Politik nicht aktiv durchzusetzen, so gilt dies nicht als Verzicht auf unser Recht, dies zu tun, und wir haben auch nicht zugestimmt, dass Sie unsere Dienste weiterhin in demselben Umfang 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.
   d. Unabhängig von der Anzahl der abrechenbaren Einheiten, die Sie erworben haben, müssen Sie unsere Dienste sinnvoll nutzen, und zwar so, dass wir keine unverhältnismäßigen Ressourcen zuweisen müssen. Zur Bestimmung dessen werden wir Ihre Ressourcennutzung (z. B. Speicheranforderungen, Anzahl paralleler Verbindungen) mit der eines durchschnittlichen Kunden vergleichen. Wir ermitteln den durchschnittlichen Kunden, indem wir die 5 % der höchsten und die 5 % der niedrigsten Kunden für die jeweilige Ressource außer Acht lassen und den Durchschnittswert aller aktiven Kunden berechnen.
   e. Spezifische Merkmale der Branche, 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 Ihre Nutzung unserer Lösung nicht sinnvoll ist oder gegen diese Richtlinie verstößt, werden wir nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen:
      i. Ihnen die weitere Nutzung unserer Lösungen zu gestatten, allerdings nur gegen Zahlung zusätzlicher Gebühren und unter Einhaltung der Bedingungen, die wir unter den gegebenen Umständen für angemessen halten.
      ii. Sie darüber informieren, dass Ihr Konto innerhalb eines von uns nach eigenem Ermessen festgelegten angemessenen Zeitraums gekündigt wird. In dieser Zeit werden alle Dienste und/oder Vorgänge ausgesetzt.

g. Sollten wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:
   i. Alle Daten (Metadaten, Backupdateien oder andere) werden am Ende des in der diesbezüglichen Benachrichtigung von uns festgelegten Zeitraums gelöscht, ungeachtet entgegenstehender Bestimmungen in den Allgemeinen Geschäftsbedingungen.
   ii. Ihnen wird eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage Ihres Abonnementzeitraums gewährt.