AvePoint

Policies & Insights

For Microsoft 365

Erkennen, priorisieren, beheben und setzen Sie Microsoft 365-Sicherheitskontrollen durch.

Sichern Sie die Zusammenarbeit in Microsoft 365

Identifizieren und priorisieren Sie Risiken

Sammeln Sie Nutzungsdaten und sensible Inhalte über Ihren gesamten Tenant. Priorisieren Sie Risiken auf der Grundlage Ihrer Risikodefinition – abgestimmt auf die für Sie relevanten Vorschriften und Sicherheitsrichtlinien. Mit Insights erkennen Sie Ihre größten Risikofaktoren, egal ob es sich dabei um häufig geteilte Inhalte, anonyme Links oder mittlerweile unberechtigte Nutzer handelt!

Überwachen und beheben Sie Risiken

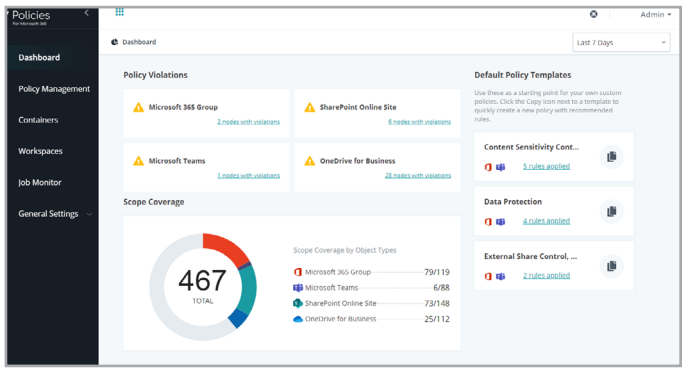
Sicherheits-Dashboards verdeutlichen risikoreiche anonyme Links, hochsensible Inhalte und mehr. Betrachten Sie bekannte und potenzielle Probleme genauer. Beheben Sie Risiken im Laufe der Zeit – Sie haben die Möglichkeit Berechtigungen und Freigabeeinstellungen gebündelt zu bearbeiten.

Setzen Sie Richtlinien durch

Verhindern Sie mithilfe automatisierter Richtlinien Konfigurationsveränderungen. Bei nicht autorisierten Änderungen und riskanten Aktionen werden aufgrund der Richtlinien Warnmeldungen oder ein Roll-Back ausgelöst. Verfolgen Sie den Fortschritt und weisen Sie so nach, dass die Zusammenarbeit gesichert ist.

Entwickeln Sie aufgrund besserer Statistiken stärkere Richtlinien

PI ermöglicht eine einfache Erstellung von tenantweiten Sicherheitsberichten. Doch wie erkennt man, ob es ein Problem gibt? PI geht über gewöhnliche Sicherheitsberichte hinaus, indem auch der Kontext berücksichtigt wird. Über Microsoft Teams, Gruppen, SharePoint und OneDrive zusammengeführte Nutzungsdaten und sensible Inhalte stellen sicher, dass Ihre kritischsten Probleme priorisiert behandelt werden. Anschließend können Sie Berechtigungen und Einstellungen gebündelt bearbeiten und Richtlinien festlegen, die automatisch durchgesetzt werden. So sind all Ihre Arbeitsbereiche vollkommen gesichert.



INSIGHTS

- Führen Sie Microsoft 365-Berechtigungen und Sicherheits-daten mit Nutzungsdaten sowie sensiblen Inhalten zusammen
- Erstellen Sie Berichte über die in Ihrem Tenant vorhandenen Berechtigungen oder betrachten Sie Teams, Gruppen, SharePoint und OneDrive genauer, um bestimmte Services oder Nutzer zu überwachen
- Basierend darauf, wie Sie Risiko definieren, werden kritische Anliegen priorisiert - abhängig von der Art der sensiblen Informationen und der Risikodefinition
- Verwenden Sie die an Ihrer Branche oder Region ange-passten Microsoft-Vorlagen für vertrauliche Informationen oder erstellen Sie in den Microsoft 365 Sicherheits- und Compliance-Centern Ihre eigenen Vorlagen
- Verwenden Sie die von uns empfohlene Risikodefinition oder passen Sie die Einstellungen für große Gruppen und externe Nutzer an
- Die Risikobewertung hebt zu priorisierende Risiken hervor, wie z.B. hochsensible Inhalte oder anonyme Links, die nicht ablaufen
- Gehen Sie bei bekannten oder potenziellen Problemen ins Detail und nehmen Sie direkt in den Berichten Änderungen vor – beachten Sie dabei den Kontext der Inhaltsnutzung sowie die Sensibilität des Inhalts
- Sie können gezielt oder gebündelt Berechtigungen, die für externe, mittlerweile unberechtigte Nutzer oder per anonyme Links erteilt wurden, verfallen lassen, entfernen oder bearbeiten
- Sicherheits-Dashboards zeigen verringerte Risiken und Fortschritte im Laufe der Zeit für anonyme Links, den Zugriff externer Nutzer und mittlerweile unberechtigte Nutzer

POLICIES

- Setzen Sie Richtlinien gemäß Ihren Erkenntnissen oder den Unternehmensvorgaben, sodass diese automatisch durchgesetzt werden
- Wenden Sie für eine sichere Zusammenarbeit Richtlinien auf Microsoft Teams, Microsoft 365 Groups, SharePoint und OneDrive an
- Alle 15 Minuten werden nicht richtlinienkonforme Änderungen gemeldet oder rückgängig gemacht
- Richtlinien werden auf der Grundlage von Microsoft-Nutzungsdaten ausgelöst
- Mehr als 20 Out-of-the-Box-Richtlinien können durch einige Klicks konfiguriert werden, sodass Sie gezielt und kontextabhängig Regeln auf Arbeitsbereiche anwenden können, z. B. basierend auf Metadaten oder der Art sensibler Informationen:

  - Durchsetzung der Klassifikation
  - Einschränkungen bei der Erstellung
  - Einstellungen für die externe Freigabe
  - Einschränkung beim Löschen
  - Einschränkung für die Anzahl der in der Library aufgelisteten Objekte
  - Schutz für Berechtigungsvererbung

  - Mitgliedschafts-/Besitzbeschränkung
  - Gruppensichtbarkeit in Outlook
  - Einschränkung der Besitzeranzahl
  - Vordefinierte Gruppenmitglieder (über die Integration von Cloud Governance)
  - Scannen externer Nutzer

  - Einschränkung bezüglich der Anzahl der Site Collection-Administratoren
  - Einschränkung der Privatsphäre
  - Einstellungen für Zugriffsanfragen
  - Einschränkung der Inhaltserstellung und des Uploads
  - Einschränkung für Site Collection-Administratoren/-Besitzer
  - Einstellungen für die externe Freigabe von Site-Inhalten
  - Einschränkung für Nutzer/Gruppen

Eine umfassende Liste der neuen Funktionen finden Sie in unseren Release-Notes.

So können Sie AvePoint-Produkte kaufen
0049 89 21 90 98 900 | Sales_de@avepoint.com
Starten Sie noch heute Ihre kostenlose Testversion: www.avepointonlineservices.com
AvePoint Deutschland GmbH | Nymphenburger Str. 380335 | Munich Germany

Accessible content available upon request