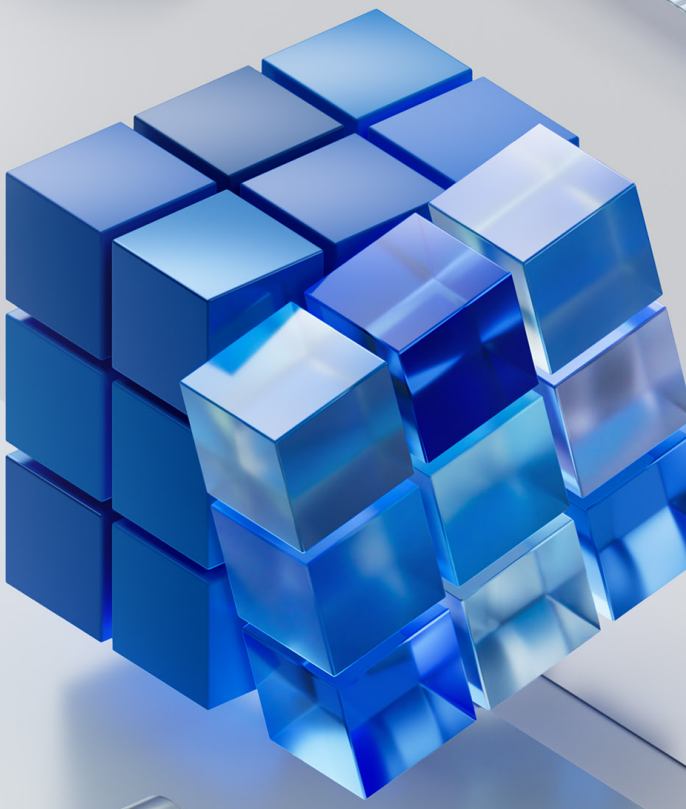
Acronis

Attaques contre l'identité et le plan de contrôle dans Microsoft 365



9 menaces concrètes, ce qu'elles exploitent et comment les MSP peuvent réduire les risques avec Acronis SPM

Les attaques actuelles contre Microsoft 365 ciblent davantage le plan de contrôle, les identités, applications OAuth, autorisations, sessions et configurations, que les terminaux.

Lors d'incidents récents constatés, les attaquants ont utilisé des flux d'authentification légitimes, des autorisations excessives, des contrôles d'accès insuffisants et des erreurs de configuration pour obtenir un accès persistant aux tenants Microsoft 365.

Cette liste de vérification fait le point sur :

- Les techniques d'attaque utilisées dans des incidents constatés.
- Ce que les attaquants ont exploité.
- Les contrôles Microsoft 365 recommandés pour réduire les risques.
- Comment Acronis SPM aide les MSP à surveiller et à appliquer une posture de sécurité renforcée sur l'ensemble des tenants.

1. Attaques par pulvérisation de mot de passe

Incident constaté

Midnight Blizzard (2024).

Technique d'attaque

Attaque par pulvérisation de mot de passe contre un compte tenant hérité hors production.

Ressources affectées

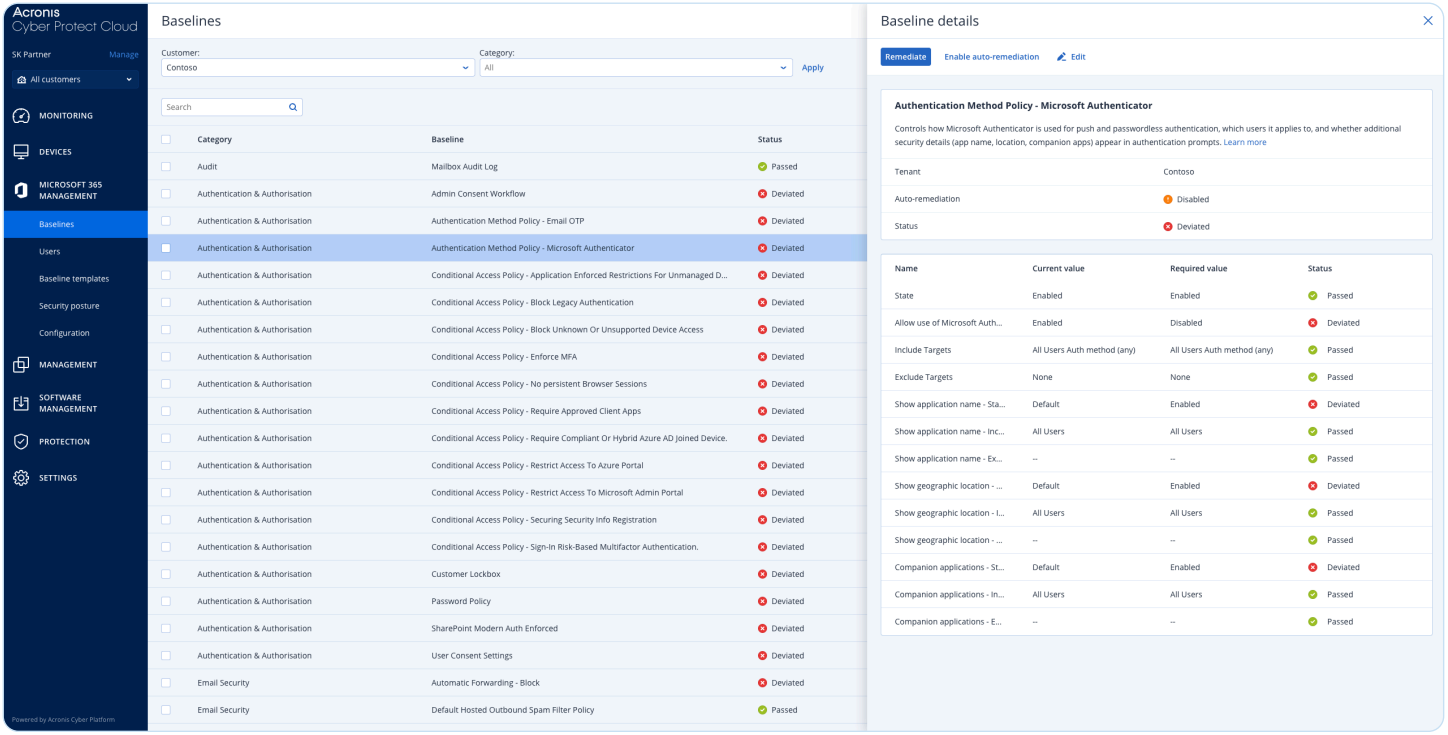
- Identifiants faibles.
- Absence d'authentification multifacteur sur un compte hérité.

Mesures de sécurité pour réduire le risque

- Imposer l'authentification multifacteur.
- Éliminer les mots de passe faibles.
- Désactiver les anciens chemins d'authentification.
- Surveiller les anomalies de connexion.

Comment Acronis SPM vous accompagne

- Identifie les lacunes d'authentification multifacteur.
- Détecte les paramètres d'authentification non sécurisés.
- Surveille les écarts vis-à-vis de la base de référence sur l'ensemble des tenants.
- Aide les MSP à corriger les failles de sécurité liées à l'identité des configurations avant qu'elles ne deviennent des voies d'attaque.



2. Falsification de jetons et abus de session

Incident constaté

Storm-0558 (2023).

Technique d'attaque

Des jetons d'authentification falsifiés ont été utilisés pour accéder à des comptes e-mail cloud.

Ressources affectées

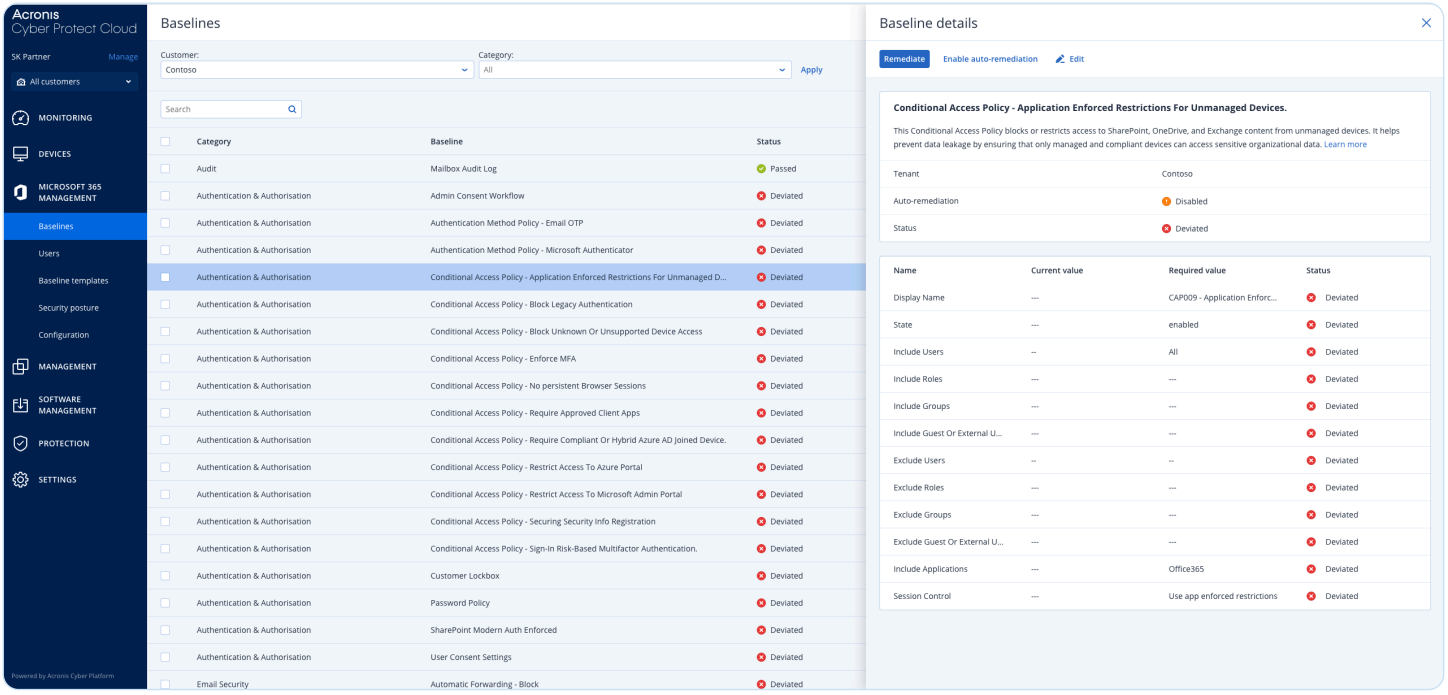
- Faiblesses de validation des jetons.
- Abus de la clé de signature.
- Visibilité limitée sur l'utilisation anormale des jetons.

Mesures de sécurité pour réduire le risque

- Renforcer la posture de sécurité de l'identité.
- Imposer l'authentification multifacteur et l'accès conditionnel.
- Restreindre le consentement d'accès aux applis.
- Protéger l'accès privilégié.
- Surveiller les anomalies de jetons et de session.

Comment Acronis SPM vous accompagne

- Aide à standardiser le niveau de sécurité de l'authentification multifacteur et de l'accès conditionnel.
- Identifie les dérives de configuration de l'identité.
- Prend en charge l'application de bases de référence pour un accès administrateur sécurisé.
- Réduit l'exposition adjacente des identités côté tenant.



3. Détournement de session et phishing AiTM

Incident constaté

Plusieurs incidents réels.

Technique d'attaque

Vol de cookies de session via phishing par proxy inverse.

Ressources affectées

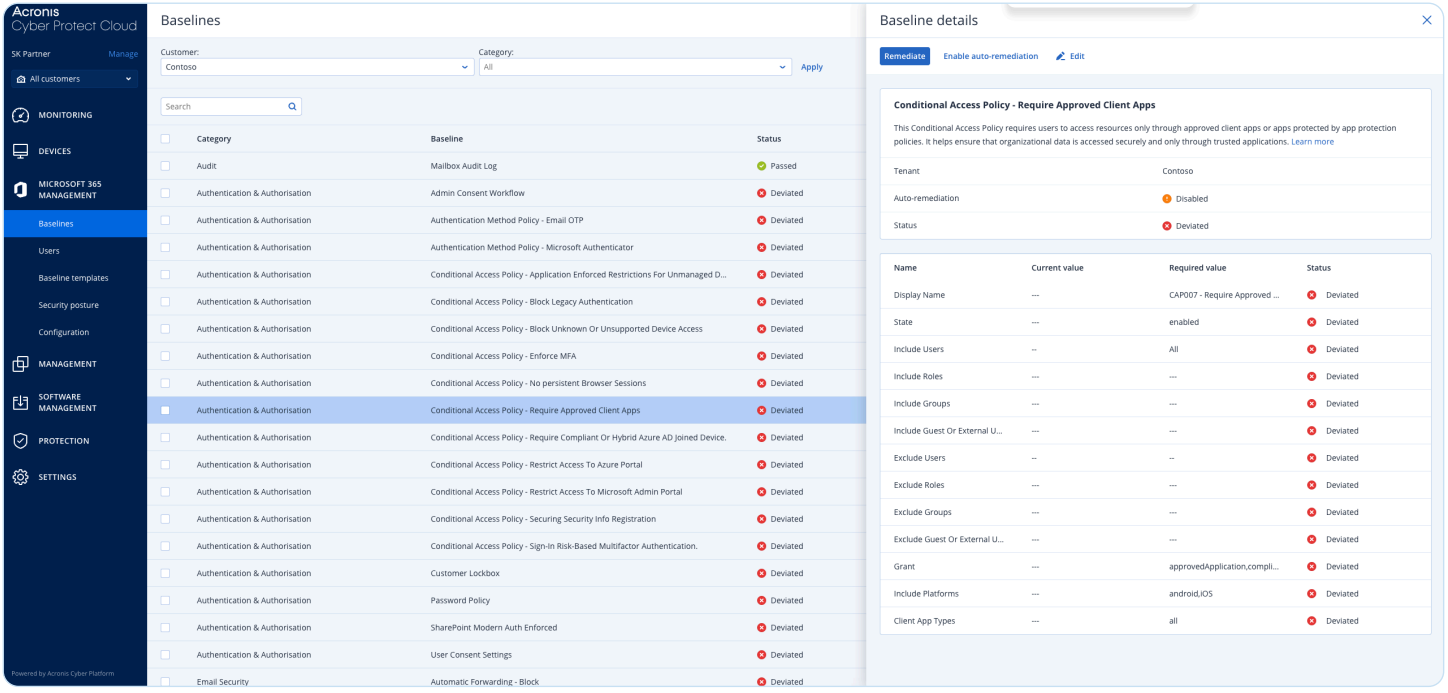
- Vol de cookies de session authentifiés.
- Application faible de l'accès conditionnel.
- Absence de restrictions d'accès basées sur le terminal.

Mesures de sécurité pour réduire le risque

- Exiger des terminaux conformes ou managés
- Appliquer l'accès conditionnel.
- Surveiller les comportements de session anormaux.
- Utiliser l'évaluation continue de l'accès si possible.

Comment Acronis SPM vous accompagne

- Détecte les écarts dans la posture d'accès conditionnel.
- Aide à maintenir des bases de référence d'accès sécurisé.
- Prend en charge la standardisation des contrôles d'identité et d'accès aux terminaux sur l'ensemble des tenants.



4. Attaques par rejeu de jeton

Incident constaté

Plusieurs incidents réels.

Technique d'attaque

Réutilisation de jetons récemment réactualisés.

Ressources affectées

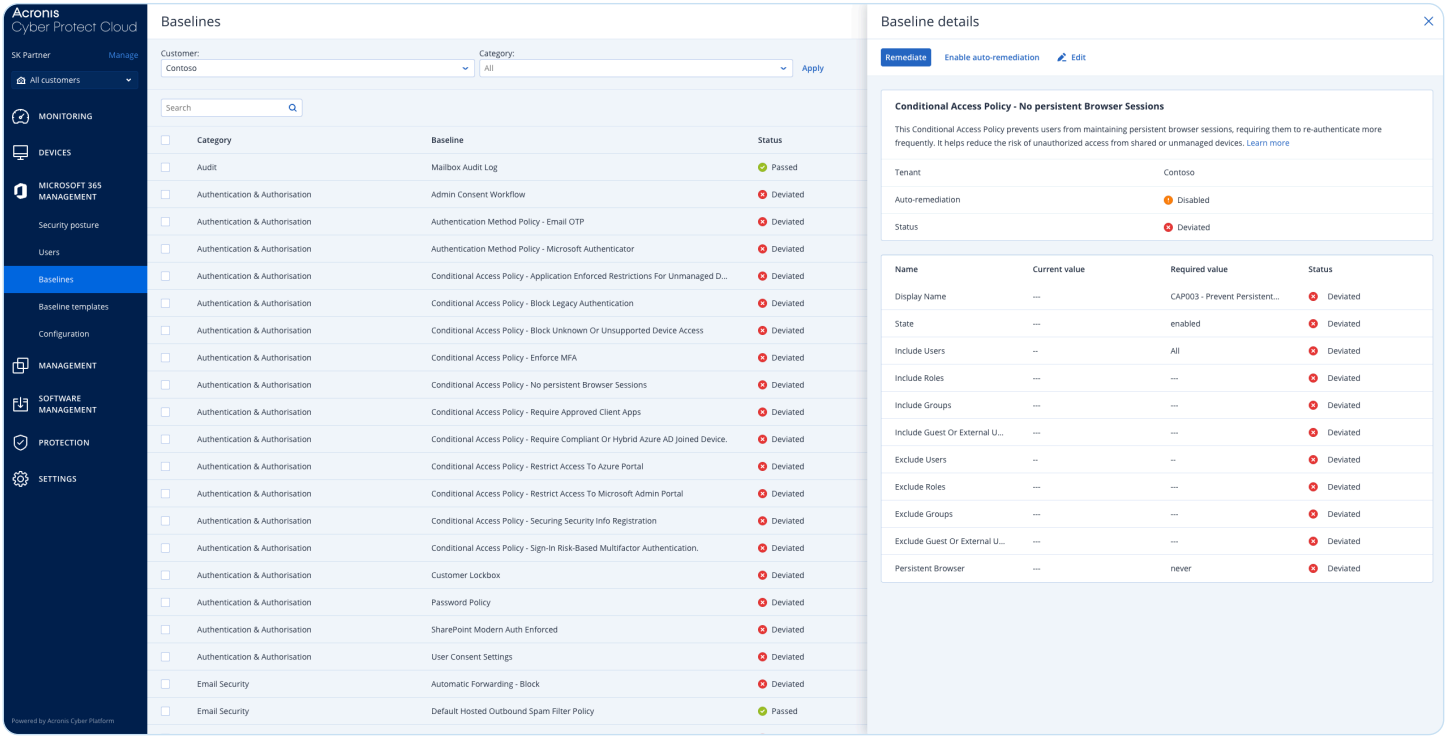
- Absence de protection des jetons / de la session.
- Faible application en cours de session.

Mesures de sécurité pour réduire le risque

- Appliquer la protection des jetons, si possible.
- Utiliser les contrôles de session de l'accès conditionnel.
- Limiter l'accès depuis des équipements non managés

Comment Acronis SPM vous accompagne

- Aide les MSP à surveiller la posture d'authentification en continu.
- Détecte les écarts vis-à-vis de la base de référence concernant l'accès conditionnel et la configuration de la session.
- Prend en charge l'application des bases de référence sécurisées pour l'identité et l'accès.



5. Phishing de consentement OAuth

Incident constaté

Plusieurs incidents réels.

Technique d'attaque

Accords de consentement applicatif malveillants.

Ressources affectées

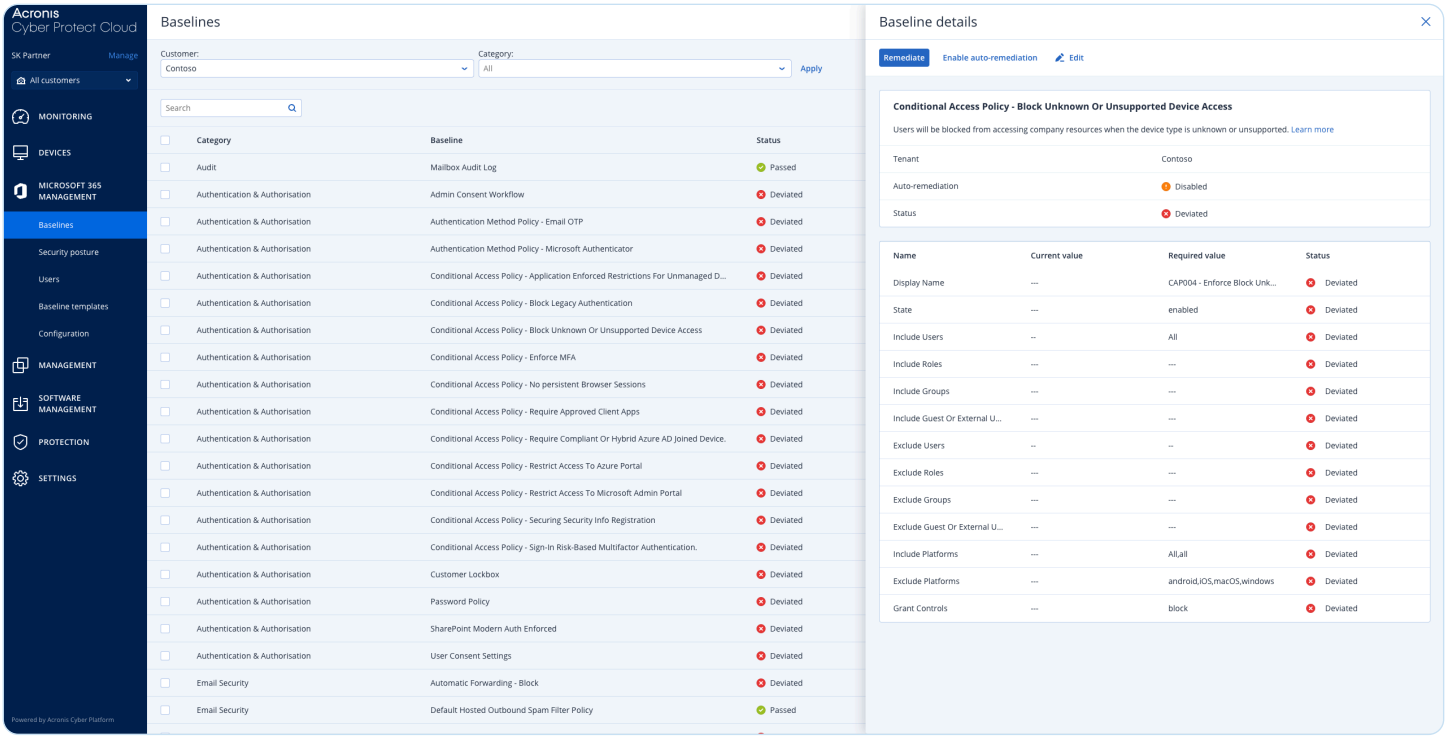
- Consentement utilisateur non restreint.
- Gouvernance insuffisante des applications.

Mesures de sécurité pour réduire le risque

- Restreindre le consentement utilisateur.
- Exiger une approbation administrateur pour les applications.
- N'autoriser que les éditeurs vérifiés et les autorisations à faible risque.

Comment Acronis SPM vous accompagne

- Standardise les contrôles liés à l'autorisation.
- Détecte les écarts par rapport aux stratégies de consentement applicatif approuvées.
- Aide les MSP à maintenir une posture d'autorisation Microsoft 365 sécurisée sur l'ensemble des tenants.



6. Abus d'appli OAuth et exfiltration de données via l'API Graph

Incident constaté

Plusieurs incidents réels.

Technique d'attaque

Accès aux données et exfiltration via l'API au moyen d'applications surautorisées.

Ressources affectées

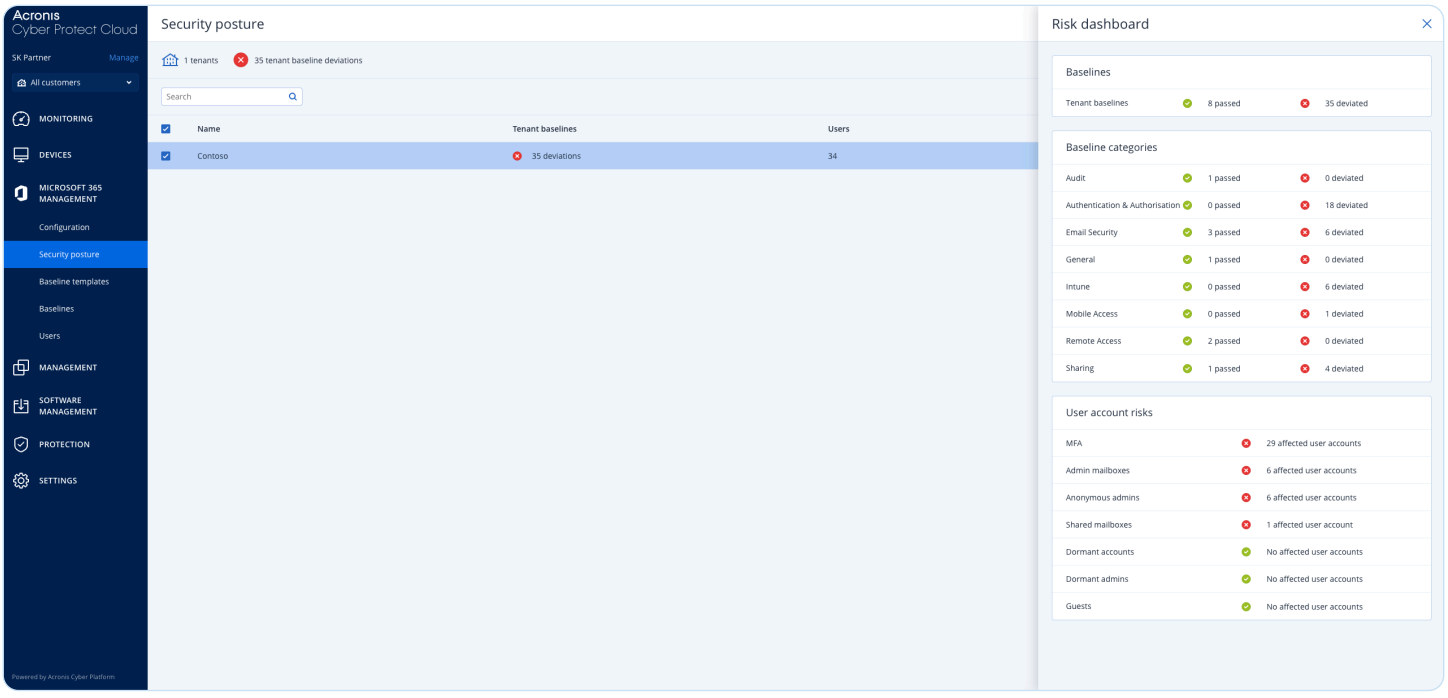
- Autorisations Graph excessives.
- Faible visibilité sur le comportement des applis.
- Accès non managé aux applications.

Mesures de sécurité pour réduire le risque

- Auditer régulièrement les autorisations liées aux applications.
- Enquêter sur les activités Graph inhabituelles.
- Examiner les applis autorisées par des utilisateurs externes.

Comment Acronis SPM vous accompagne

- Aide à maintenir la gouvernance des autorisations des applications et de l'état du consentement.
- Détecte les dérives d'autorisation et l'exposition des applications non gérées.
- Améliore la visibilité sur l'état d'accès des applications Microsoft 365.



7. Élévation de privilèges et usage excessif des rôles

Incident constaté

Multiples élévations de privilèges Entra ID / Midnight Blizzard.

Technique d'attaque

Élévation de privilèges via des privilèges d'administrateur excessifs et permanents.

Ressources affectées

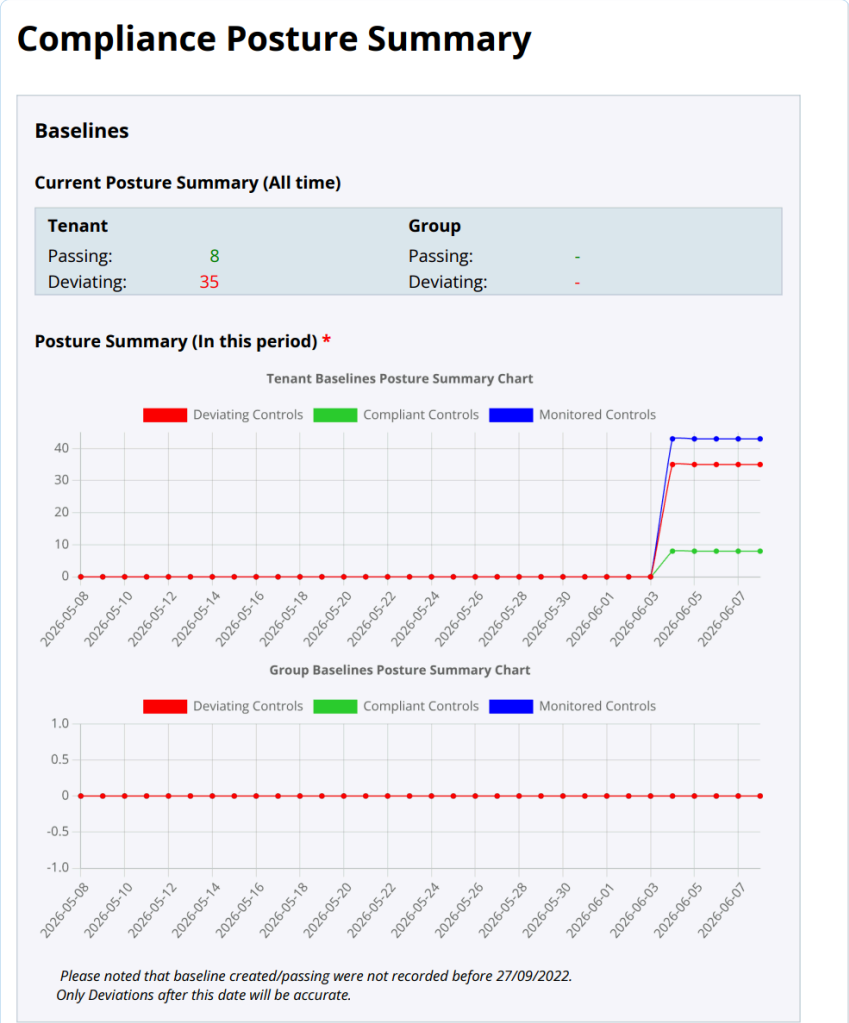
- Trop d'administrateurs globaux.
- Dérive des privilèges.
- Faible gouvernance des rôles.

Mesures de sécurité pour réduire le risque

- Appliquer le principe du moindre privilège.
- Restreindre l'accès administrateur permanent.
- Examiner continuellement les rôles à privilèges.

Comment Acronis SPM vous accompagne

- Identifie les rôles administrateurs excessifs et l'exposition aux privilèges.
- Aide les MSP à standardiser un état de sécurité des rôles sur l'ensemble des tenants.
- Soutient l'application des lignes de base d'identité et d'autorisation.



8. Exposition de SharePoint et OneDrive

Incident constaté

Plusieurs incidents réels.

Technique d'attaque

Partage externe excessif ou accidentel.

Ressources affectées

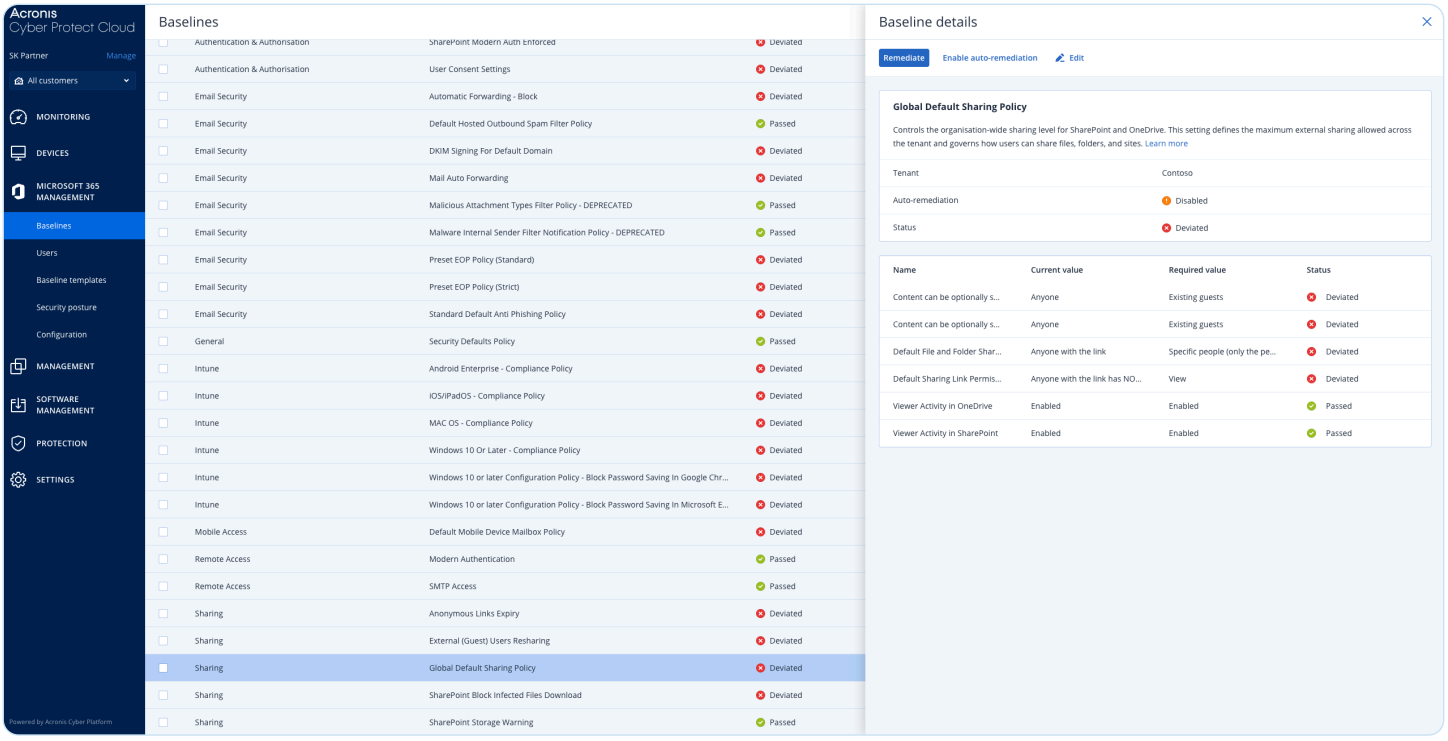
- Faible gouvernance du partage.
- Paramètres d'accès externe trop permissifs.

Mesures de sécurité pour réduire le risque

- Configurer les stratégies de partage externe dans toute l'organisation.
- Restreindre le partage si nécessaire.
- Examiner régulièrement l'état du partage.

Comment Acronis SPM vous accompagne

- Valide en continu l'état du partage par rapport aux lignes de base.
- Détecte les configurations de partage à risque.
- Réduit la dérive de configuration à long terme entre les tenants.



9. Lacunes d'audit et d'investigation

Incident constaté

Investigation sur incidents

Technique d'attaque

Activité post-compromission masquée par un audit insuffisant.

Ressources affectées

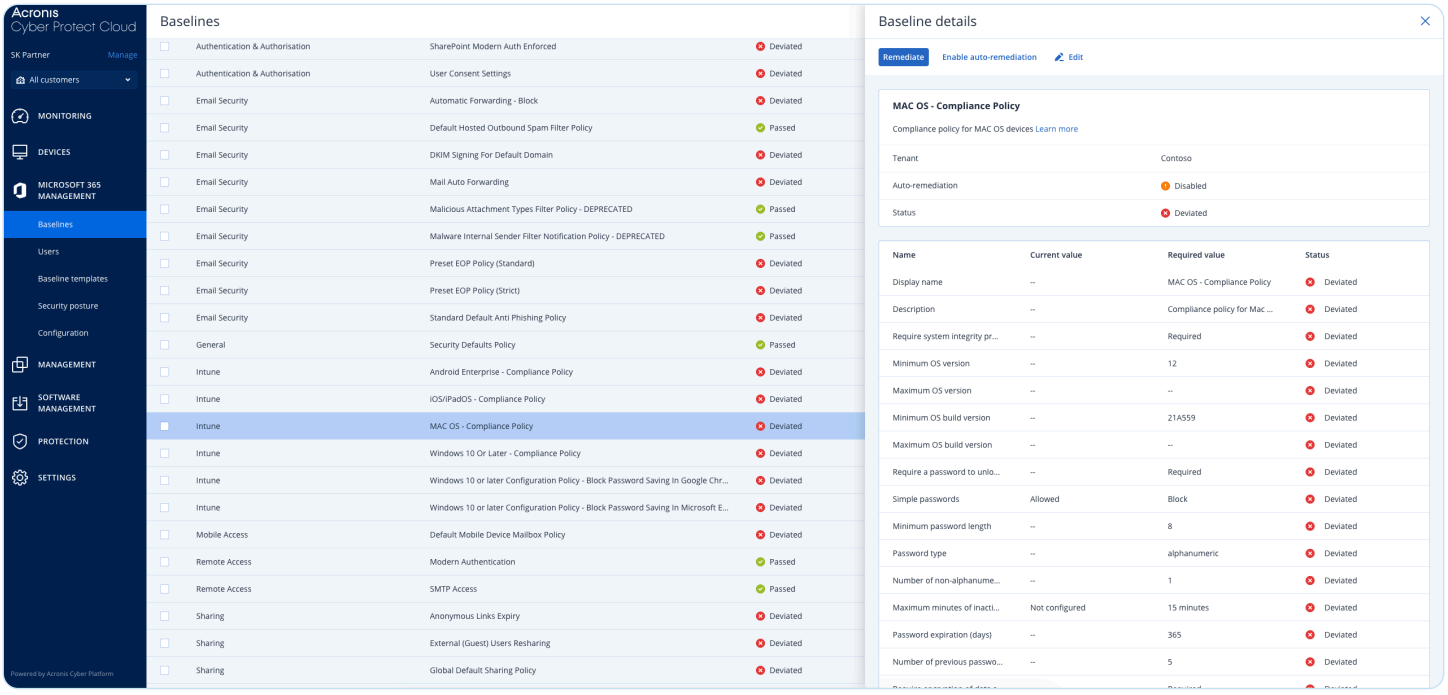
- Preuves d'audit absentes ou incomplètes.
- Insuffisance de préparation à l'investigation.

Mesures de sécurité pour réduire le risque

- Conserver l'activation de l'audit Microsoft Purview.
- S'assurer que les enquêteurs disposent d'un accès approprié.
- Maintenir la capacité de recherche dans les audits.

Comment Acronis SPM vous accompagne

- Aide les MSP à surveiller l'état de configuration lié à l'audit.
- Détecte les dérives dans les paramètres de journalisation et d'audit.
- Soutient l'investigation continue et la préparation à la conformité.



Ce que ces attaques ont en commun

Pour tous les incidents :

- L'entrée est basée sur l'identité.
- La persistance est basée sur la configuration.
- L'impact s'étend à l'ensemble du tenant.
- Les contrôles traditionnels des terminaux offrent une visibilité limitée.

Pourquoi la gestion continue de la posture de sécurité est décisive

Les attaques actuelles contre Microsoft 365 réussissent lorsque :

- Les erreurs de configuration persistent.
- La posture de sécurité se dégrade au fil du temps.
- Les écarts de visibilité passent inaperçus d'un tenant à l'autre.

Comment Acronis SPM aide les MSP à réduire les risques

- Gérez la posture de Microsoft 365 de manière centralisée sur l'ensemble des tenants.
- Surveillez continuellement la posture de sécurité par rapport aux bases de référence.
- Détectez automatiquement les nouveaux risques et les dérives de configuration.
- Appliquez des modèles de base réutilisables.
- Automatisez et rationalisez la remédiation.
- Simplifiez les workflows d'intégration et de désactivation.
- Standardisez la posture de sécurité Microsoft 365 à grande échelle.

Découvrez comment Acronis SPM aide les MSP à sécuriser Microsoft 365 à grande échelle

Scannez pour réserver une démonstration d'Acronis SPM

Acronis

Pour en savoir plus : acronis.com