Acronis

Microsoft 365 visé par les attaques : menaces ciblant l'identité et le plan de contrôle

Et comment Acronis Security Posture Management les détecte et y remédie.

Introduction

Microsoft 365 s'est imposé comme le plan de contrôle des opérations modernes des entreprises, gérant l'identité, l'accès, la communication et les données au sein des organisations. À mesure que sa prépondérance augmente, sa surface d'attaque également.

Mais la nature des attaques change fondamentalement.

Les menaces d'aujourd'hui ne reposent plus sur le malware ni sur la compromission d'un terminal. Au contraire, les attaquants exploitent les identités, les autorisations et les défauts de configuration, en opérant au sein des services Microsoft 365 légitimes. Un seul compte administrateur compromis, une autorisation négligée ou une stratégie d'accès conditionnel faible peut offrir aux attaquants un accès persistant à fort impact sans déclencher les alertes de sécurité traditionnelles.

Cette évolution induit un défi critique pour les fournisseurs de services managés (MSP). Les outils de sécurité traditionnels offrent souvent peu de visibilité sur ces attaques, tandis que les configurations erronées et les stratégies incohérentes entre tenants créent une exposition persistante.

Résultat : le risque s'accumule silencieusement entre les tenants.

Ce guide propose une présentation pratique à base de scénarios, de la manière dont les attaques modernes sur Microsoft 365 se déroulent, et de la façon dont Acronis Security Posture Management (SPM) aide les MSP à détecter ces risques, les prévenir et y remédier à grande échelle.

La nouvelle réalité : vous subissez déjà l’attaque

Vous vous connectez à un tenant client. Il n'y a ni alerte, ni malware, ni signe évident de compromission. Tout semble normal en surface, mais cela ne signifie pas pour autant que l'environnement est sécurisé.

Un attaquant peut déjà avoir accès. Il peut utiliser des identifiants valides ou des jetons persistants obtenus par phishing ou par abus du consentement. Plus important encore, il peut opérer entièrement au sein de Microsoft 365, se fondre dans l’activité légitime et éviter les mécanismes de détection traditionnels.

Les attaques modernes ne reposent pas sur une intrusion : elles opèrent dans le plan de contrôle.

Pour les MSP, cela change fondamentalement le problème. Il ne s'agit plus seulement de détecter les menaces actives : il s'agit d'identifier l'exposition avant qu’elle ne risque d'être exploitée, de la remédier en toute cohérence sur l’ensemble des tenants et de garantir que ces corrections restent appliquées à mesure que les environnements évoluent.

Cette présentation montre comment Acronis Security Posture Management (SPM) contribue à traiter dans la pratique ce défi.

Scénario 1

Pulvérisation de mots de passe

« Rien ne semble anormal, mais un compte vient de s’y connecter. »

Les attaquants n'ont pas besoin d'entrer par effraction : ils se connectent. En testant des mots de passe courants sur de nombreux comptes, ils évitent les verrouillages et finissent par accéder à l'un d'entre eux. Avec des identifiants valides, ils peuvent accéder aux boîtes mail et aux fichiers, et opérer comme un utilisateur légitime.

Il n'y a généralement ni alerte, ni malware, ni signal évident, juste une activité qui semble normale.

Acronis SPM fait passer l’accent de la détection à l’exposition. Ceci met en évidence des risques tels que l’absence de MFA, l’authentification héritée active et des configurations d’identité qui s’écartent des bonnes pratiques.

À partir de là, vous évaluez le tenant, appliquez la MFA, désactivez l’authentification héritée et déployez ces contrôles sur tous les tenants à l’aide de modèles de base. La surveillance continue garantit que toute dérive est détectée et corrigée.

Au lieu de traquer un compte compromis, vous éliminez les conditions qui ont rendu l’attaque possible.

Ce que vous faites (dans la plateforme)

1 **Lancer un audit à la demande**

- Évaluer instantanément le tenant par rapport à la base de sécurité.
- Identifier les faiblesses d’authentification.

2 **Appliquer la remédiation de base**

- Imposer la MFA à l’ensemble des utilisateurs.
- Désactiver l'authentification traditionnelle.

3 **Automatiser sur l’ensemble des tenants**

- Utiliser des modèles de base.
- Propager les stratégies à l'ensemble des clients.

4 **Activer la surveillance continue**

- Acronis SPM détecte toute dérive par rapport à la base.
- Alertes lorsqu’un nouvel utilisateur est créé sans protection.

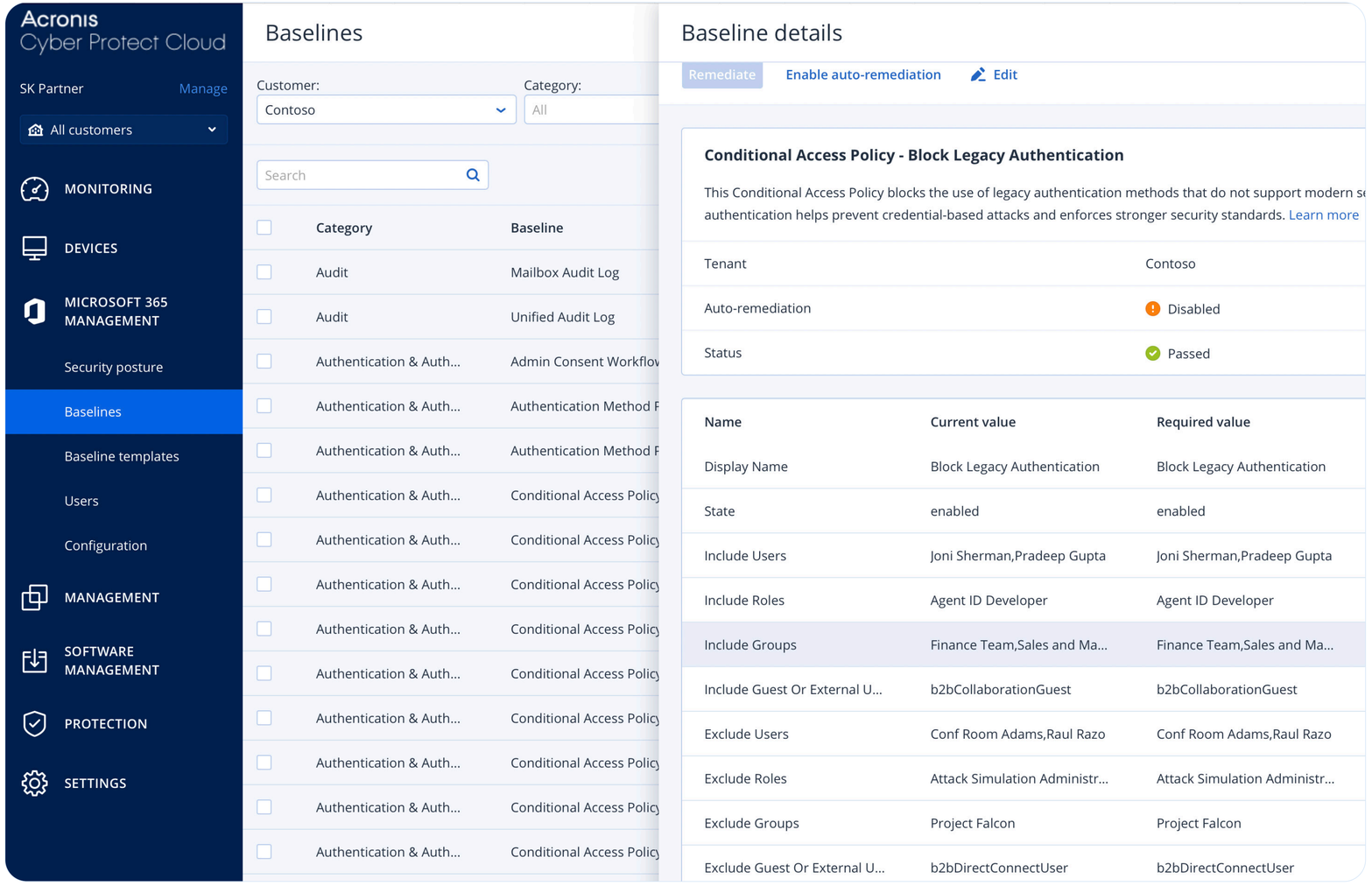
Que vient-il de se passer ?

Vous n'avez pas traqué une connexion.

Vous :

- Identifiez des lacunes systémiques d’identité.
- Corrigez une fois pour toutes.
- Appliquez partout.
- Veillez à ce qu'elles ne réapparaissent pas.

Acronis SPM élimine les conditions qui font aboutir l'attaque par pulvérisation de mots de passe à grande échelle.



Scénario 2 :

Abus du consentement OAuth

« L'attaquant n'a plus besoin de l'utilisateur »

Un utilisateur approuve sans le savoir une appli OAuth malveillante. À partir de ce moment-là, l'attaquant n'a plus besoin d'identifiants. Il obtient un accès persistant, au niveau API, aux e-mails et aux fichiers via Microsoft Graph, souvent sans déclencher la moindre alerte.

Il n'y a pas de connexion compromise, pas d'activité de connexion suspecte, et tout semble légitime.

Acronis SPM met au jour cette couche cachée. Ce service offre une visibilité sur toutes les applis OAuth des tenants, sur les autorisations qui leur ont été accordées, telles que Mail.Read ou Files.Read.All, et met en évidence les applications risquées ou inconnues.

À partir de là, vous pouvez identifier rapidement les applications à privilèges élevés ou récemment ajoutées, révoquer leurs autorisations et supprimer les accès non autorisés. Les stratégies peuvent ensuite être standardisées, en limitant le consentement de l'utilisateur et en exigeant l'approbation d'un administrateur, tandis que l'automatisation garantit l'application de ces contrôles sur l'ensemble des tenants.

Au lieu de traquer les menaces fondées sur l'identité, vous découvrez et éliminez les accès persistants au niveau de la couche applicative et empêchez leur réapparition.

Ce que vous faites (dans la plateforme)

1 Identifier les applications à risque

- Filtrer les applications à haut niveau d'autorisation.
- Détecter les applications nouvellement ajoutées ou inconnues.

2 Remédier immédiatement

- Révoquer directement les autorisations des applications.
- Supprimer les intégrations non autorisées.

3 Standardiser la stratégie

- Restreindre le consentement de l'utilisateur.
- Exiger l'approbation de l'administrateur.

4 Automatiser l'application

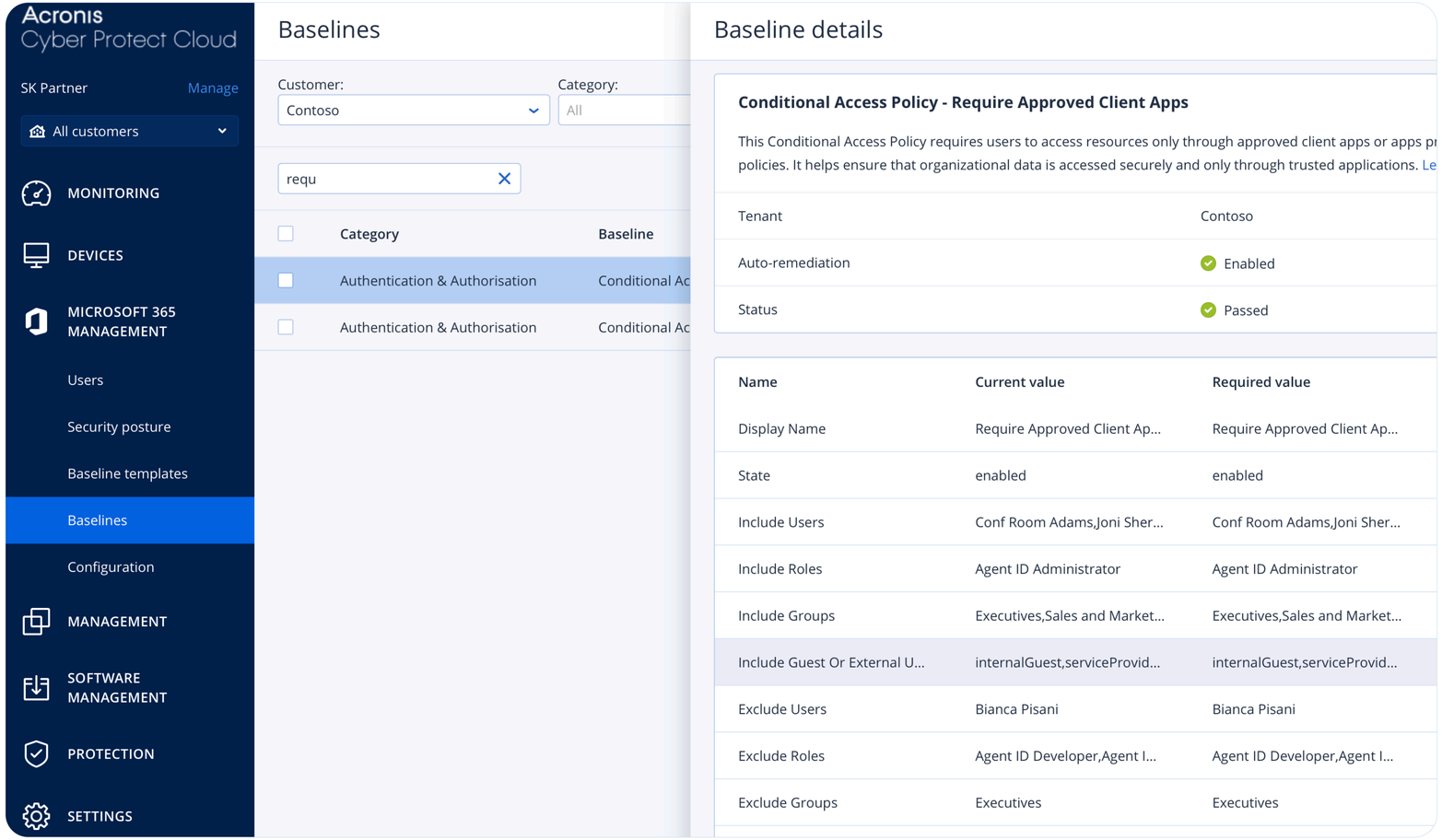
- Appliquer des stratégies de gouvernance des applications sur l'ensemble des tenants.
- Détecter automatiquement les nouvelles applications à risque.

Que vient-il de se passer ?

Vous :

- Avez révélé une persistance qui contourne l'identité.
- L'avez supprimée instantanément.
- Avez empêché sa réapparition.

Acronis SPM offre visibilité et contrôle sur la couche applicative sur laquelle les attaquants s'appuient pour conserver un accès à long terme.



Scénario 3 :

Phishing par code de terminal

« L'authentification multifacteur a fonctionné et l'attaquant est quand même entré. »

Un utilisateur effectue une connexion Microsoft légitime et passe l'authentification multifacteur, mais l'attaquant capture le jeton d'authentification. Ce faisant, il obtient un accès persistant, lit les e-mails et crée des règles de boîte aux lettres, le tout sans déclencher d'alertes évidentes.

Il n'y a aucun échec de connexion, et l'authentification multifacteur semble avoir fonctionné comme prévu.

Acronis SPM met en lumière le problème : des failles de stratégie. Le service révèle des stratégies d'accès conditionnel faibles ou manquantes, l'absence de contrôles de session et des configurations d'identité qui s'écartent des bonnes pratiques.

De ce fait, vous appliquez un accès conditionnel plus strict, définissez des restrictions de session et standardisez ces contrôles sur l'ensemble des tenants. La surveillance continue garantit que toute dérive est détectée et corrigée.

Au lieu de détecter l'abus de jetons, vous éliminez les conditions en amont.

Ce que vous faites (dans la plateforme)

1 **Exécuter une vérification de conformité de base**

- Comparer les stratégies du tenant aux bonnes pratiques.

2 **Renforcer les contrôles d'identité**

- Renforcer l'accès conditionnel.
- Appliquer des restrictions de session.

3 **Automatiser la remédiation**

- Appliquer des stratégies sur l'ensemble des tenants.
- Corriger automatiquement les écarts.

4 **Maintenir une application continue**

- Acronis SPM surveille la dérive des stratégies.
- Signaler tout assouplissement des contrôles.

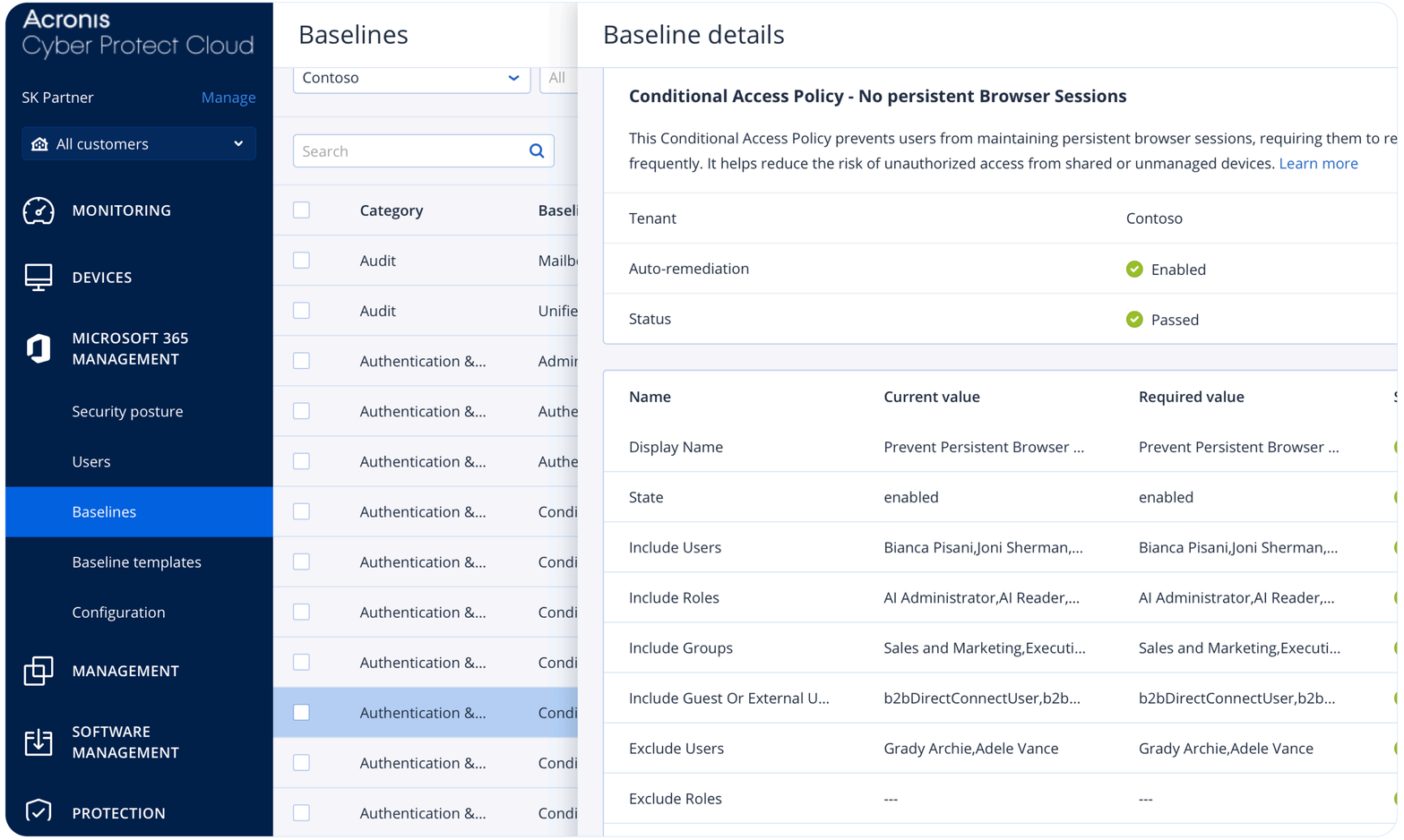
Que vient-il de se passer ?

Vous n'avez pas détecté le vol du jeton.

Vous :

- Comblé les lacunes de stratégie qui le permettaient.
- Standardisé les contrôles sur l'ensemble des tenants.
- Assuré une application à long terme.

Acronis SPM sécurise les flux d'authentification, et non seulement les identités.



Scénario 4

Élévation des privilèges

« Un seul compte devient l'ensemble du tenant. »

Un attaquant compromet un seul compte et commence à explorer. Il trouve des privilèges excessifs, plusieurs administrateurs globaux et une faible séparation des rôles. La remontée d'un problème est alors très simple, avec un contrôle total du tenant.

Aucune alerte n'est alors générée. La dérive des privilèges se produit progressivement, sans visibilité centralisée, le risque passe alors inaperçu.

Acronis SPM fait un état des lieux clair en affichant les rôles d'administration sur l'ensemble des tenants, en identifiant les comptes surdotés en privilèges et en attribuant un niveau de risque en fonction de l'exposition.

Ce que vous faites (dans la plateforme)

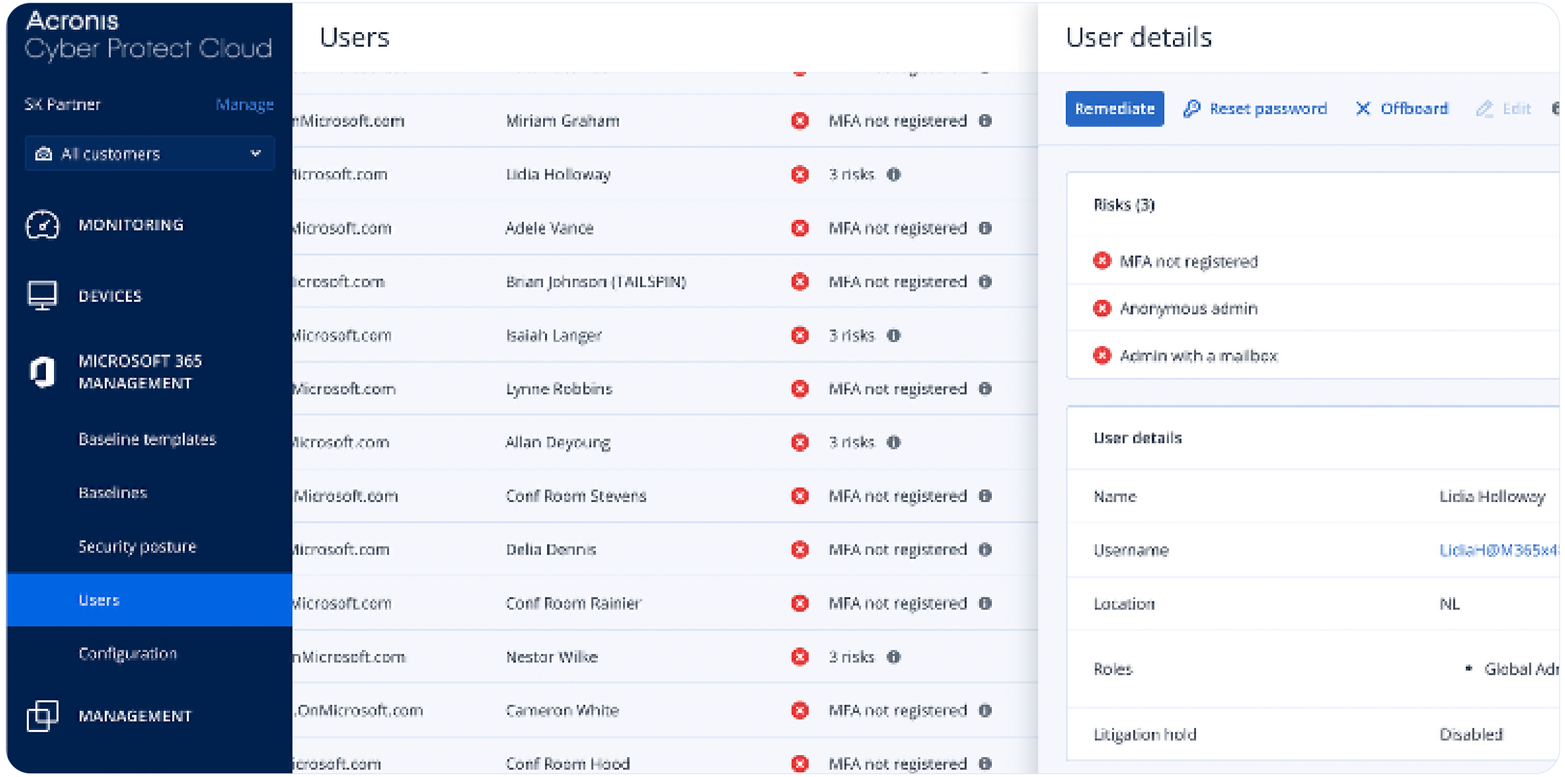
1. **Auditer les rôles privilégiés**
   - Identifier les comptes administrateur excessifs.
2. **Appliquer le moindre privilège**
   - Réduire les administrateurs globaux.
   - Standardiser les affectations de rôles.
3. **Automatiser à l'échelle des tenants**
   - Utiliser des modèles de référence pour appliquer les stratégies de rôles.
4. **Maintenir le contrôle du cycle de vie**
   - Affecter les bons rôles en cours d’intégration.
   - Révoquer l'accès, les sessions et les licences en cas de départ.

Que vient-il de se passer ?

Vous :

- Avez réduit le rayon d'impact de la compromission.
- Avez standardisé les privilèges de l'ensemble des environnements.
- Avez assuré la sécurité du cycle de vie de l'identité.

Acronis SPM transforme la prolifération des privilèges en une stratégie contrôlée et applicable.



Vous pouvez alors auditer les rôles privilégiés, réduire le nombre de superadministrateurs globaux et appliquer des stratégies de moindre privilège sur tous les tenants à l'aide de modèles de référence. La gestion continue du cycle de vie garantit l'accès en cours d'intégration et une totale révocation lors du départ.

Au lieu de réagir à la remontée d'un problème, vous limitez le rayon d'impact dès le départ.

Ce qui relie toutes ces attaques

Dans tous les scénarios :

Attaque	Cause racine
Pulvérisation de mots de passe	Contrôles d'identité faibles
Abus d'OAuth	Mauvaises configurations des autorisations d'appli
Phishing par code de terminal	Lacunes de stratégie
Élévation des privilèges	Autorisations excessives

Le modèle

L'entrée équivaut à l'identité.

La persistance équivaut à la configuration.

L''mpact équivaut à l'ensemble du tenant.

Les avantages d'Acronis SPM

SPM ne se contente pas de signaler le risque.

Il permet aux MSP d'exercer la sécurité à grande échelle.

Surveillance continue

- Détection 24 h/24 et 7 j/7 de la dérive de posture.
- Identification en temps réel des nouveaux risques.

Sécurité optimisée par les référentiels

- Référentiels de bonnes pratiques prédéfinis.
- Modèles de référentiel personnalisés.
- Standardisation de l'ensemble des tenants.

Remédiation automatisée et manuelle

- Corrigez les problèmes dans la console directement.
- Automatisez la remédiation des risques récurrents.
- Éliminez les tâches manuelles répétitives.

Gestion multitenant

- Contrôle centralisé de l'ensemble des clients.
- Propagation des stratégies à grande échelle.

Contrôle complet du cycle de vie de l’identité

- Intégration sécurisée avec les bons rôles et les bonnes stratégies.
- Départ sécurisé avec révocation des sessions et nettoyage.

Intégration opérationnelle

- Intégration avec les outils PSA.
- Workflows simplifiés pour les équipes MSP.

En conclusion

Les attaques modernes contre Microsoft 365 aboutissent parce que :

- Personne ne voit l'exposition.
- Personne ne la corrige de manière cohérente.
- Personne ne l'impose en continu.

Acronis SPM change cela.

Il confère aux MSP la possibilité de :

- Détecter les risques dans chaque tenant.
- Les corriger instantanément.
- L'imposer automatiquement.
- Assurer les correctifs dans le temps.

Gestion de la posture de sécurité : un pilier central de Protected 365

La gestion de la posture de sécurité (SPM) n'est pas un module complémentaire facultatif, mais une capacité fondamentale de la solution Acronis Protected 365 qui permet de tenir la promesse de la plateforme : une protection complète, optimisée par l'intelligence artificielle, en 7 en 1 pour Microsoft 365. SPM fonctionne de concert avec la sauvegarde, la sécurité des e-mails, la sécurité de collaboration, XDR, l'archivage des e-mails et les formations et sensibilisations à la sécurité pour combler l'ensemble des lacunes de responsabilité partagée Microsoft sur Exchange, Teams, SharePoint et OneDrive.

SPM joue un rôle critique dans la phase « Élimination des lacunes avec une protection standard » du modèle de maturité Protected 365, faisant évoluer les organisations d'une protection de base vers une résilience proactive. Alors que la sauvegarde et la sécurité des e-mails assurent une protection essentielle, SPM introduit une évaluation continue des risques, l'application de stratégies et la remédiation automatisée, garantissant que les environnements restent alignés sur les bonnes pratiques et conformes aux standards en constante évolution.

En surveillant les configurations en continu, en détectant les écarts et en permettant une remédiation rapide, SPM traite directement l'un des risques les plus courants et les plus souvent négligés dans Microsoft 365 : la mauvaise configuration des utilisateurs et la dérive de sécurité. Ce service transforme la sécurité d'un processus réactif en une discipline proactive, pilotée par les stratégies, qui réduit l'exposition, renforce la conformité et améliore la cyberrésilience globale.

Surtout, SPM est fourni au sein de la même plateforme Acronis multitenant, renforçant la proposition de valeur principale de Protected 365 : un seul fournisseur, un seul contrat, une seule solution intégrée. Cela élimine la prolifération des outils, réduit la charge opérationnelle et permet aux MSP et aux équipes IT d'évoluer efficacement tout en améliorant la qualité de service et la rentabilité.

Passez à l'action : comblez les lacunes dès maintenant

Les erreurs de configuration n'attendent pas. Vous ne devriez pas non plus. Commencez dès aujourd'hui votre essai d'Acronis Security Posture Management et découvrez instantanément les risques, appliquez les bonnes pratiques et renforcez la sécurité de Microsoft 365.

ESSAI GRATUIT

Acronis

Pour plus d'informations,
acronis.com