rubrik

Protégez les identités sur Active Directory, Entra ID et Okta avec une plateforme unifiée

Découvrez la plateforme de cyber-résilience agentique qui garantit des systèmes d'identités sécurisés, opérationnels et restaurables, sans la complexité ni le coût total de possession (TCO) élevé des outils fragmentés.

Aujourd'hui, les attaquants ciblent **de plus en plus** les fournisseurs d'identités (IdP) tels qu'Active Directory (AD), Entra ID et Okta pour accéder aux systèmes. Une fois les identités compromises, il leur suffit de s'authentifier pour contourner les outils EDR traditionnels et les solutions de détection des malwares. Dès lors, ils ont le champ libre pour bloquer l'accès des utilisateurs légitimes, prendre les identités et les données en otage, et exiger une rançon pour leur libération. Résultat : l'activité est paralysée et les équipes IT doivent réagir dans l'urgence pour tenter de reprendre le contrôle.

Pour se défendre, la plupart des entreprises accumulent les solutions spécialisées, au prix d'une visibilité fragmentée et de risques élevés. Les équipes IT et de sécurité reçoivent un flux continu d'alertes isolées, sans contexte global. Elles doivent alors reconstituer les pièces du puzzle pour comprendre ce qui se passe. En situation de crise, la multiplication des outils et des silos de données rend la coordination des workflows encore plus complexe pour les équipes.

Conséquences d'un patchwork de solutions :

- **Angles morts et retards critiques**
- **Charge opérationnelle accrue**
- **Temps de reprise allongés**
- **TCO en hausse**

LES DÉPENDANCES IMPOSENT UNE PARFAITE ORCHESTRATION DE LA REPRISE

1. **Restauration d'Entra avant AD → Perte des liens, besoin d'une synchronisation complète via Entra Connect**
   En cas de restauration d'Entra ID avant Active Directory, les objets hybrides risquent d'être dissociés, ce qui exigera une synchronisation complète d'Entra Connect une fois la relation rétablie. Dans de vastes environnements, cette opération peut prendre plusieurs jours et prolonger l'arrêt de l'activité.
2. **Restauration des politiques sans alignement des groupes Okta → Perturbation des accès**
   Les groupes restaurés à partir des sauvegardes ont de nouvelles identités de groupes qui ne correspondent pas aux politiques de sécurité auparavant associées. En plus de bloquer l'accès existant aux ressources, ce désalignement risque de favoriser les accès indésirables.
3. **Restauration d'identifiants obsolètes → Effondrement de l'automatisation**
   Rétablir des comptes de services à un état antérieur peut réactiver des mots de passe obsolètes, non reconnus par les scripts et outils actifs, et ainsi immédiatement stopper les workflows en arrière plan. Pire, cela peut passer totalement inaperçu si ce service interrompu était chargé de surveiller d'autres services.
4. **Restauration de solutions cloisonnées → Persistance des attaquants**
   Le manque de visibilité entre des outils de reprise isolés peut entraîner la persistance d'un attaquant sur une plateforme, malgré son éviction d'une autre. Dès lors, vos systèmes restaurés ne sont pas à l'abri d'une nouvelle compromission.

Risques systémiques sur les identités : l'onde de choc d'une seule compromission IdP

Pour résoudre ces problèmes, Rubrik offre une plateforme unifiée de résilience des identités. Sa mission : protéger les systèmes d'identités hybrides, permettre aux entreprises d'investiguer les incidents, maintenir la disponibilité opérationnelle et rétablir la confiance.

AVANTAGES D'UNE PLATEFORME UNIFIÉE POUR PROTÉGER LES SYSTÈMES IDP HYBRIDES

1. **Posture de sécurité, protection et conformité simplifiées –** Bénéficiez d'une observabilité approfondie sur votre posture de sécurité. Le système de référence (SoR) immuable de Rubrik garantit une télémétrie fiable sur l'évolution des identités et leurs modifications. Quant au journal d'activités immuable et à l'attribution précise des actions, ils simplifient les audits de conformité et les analyses forensiques.

2. **Continuité opérationnelle assurée –** Suivi des changements d'identités, détection des perturbations, analyse des causes profondes, rollback des configurations… Rubrik met à disposition une large palette de fonctionnalités pour détecter, diagnostiquer et résoudre rapidement les incidents liés aux identités. Outre la réduction des interruptions et des risques opérationnels, la plateforme accélère la réponse à incident et favorise une reprise en quelques clics sur les environnements AD, Entra ID et Okta.

3. **Réponse accélérée –** Plus besoin de jongler entre des outils disparates pour corréler les données. Rubrik vous permet de retracer la propagation d'une menace dans vos systèmes, sans avoir à reconstituer manuellement des informations fragmentées. Résultat, vous pouvez annuler les changements depuis la plateforme et éradiquer les mécanismes de persistance des attaquants tout en préservant les changements légitimes.

4. **TCO réduit –** Licences, maintenance, formation… Diminuez les coûts et la complexité opérationnels associés à la multiplication des outils de sécurité et de sauvegarde pour AD, Entra ID et Okta en les remplaçant par une plateforme unifiée.

5. **Roll forward des changements légitimes –** Les capacités de roll forward de Rubrik permettent de restaurer les systèmes d'identités à un point antérieur sûr, tout en conservant les changements autorisés. Ainsi, vous éradiquez les mécanismes de persistance des attaquants sans effacer des mois de mises à jour.

UNE SOLUTION MULTI-IDP GARANTE D'UNE PROTECTION SIMPLIFIÉE

1. **Sécurité unifiée sur une seule et même plateforme –** Des objets AD on-prem jusqu'aux configurations Okta cloud-native, protégez tout votre parc d'identités via une plateforme unique et intuitive, spécialement pensée pour les environnements composites.

2. **Restauration orchestrée et granulaire –** Gérez les interdépendances complexes en toute simplicité. Qu'il s'agisse de restaurer un tenant AD tout entier ou un objet Okta/Entra ID spécifique, Rubrik assure un rétablissement fidèle des systèmes du premier coup.

3. **Continuité opérationnelle –** Pour simplifier la restauration de votre environnement d'identités, garantir la disponibilité des applications et assurer l'accès des utilisateurs, détectez la compromission éventuelle de plusieurs IdP, isolez les dysfonctionnements et rétablissez le tout en quelques clics.

4. **Architecture inaltérable –** Sécurisez vos données et identités critiques avec une architecture « bunkerisée » assurant des sauvegardes immuables et séparées par un air-gap logique qui les protège des compromissions.

SÉCURISEZ L'AVENIR DE VOS SYSTÈMES D'IDENTITÉS

Face à des attaques toujours plus sophistiquées et à la complexité croissante des environnements hybrides, le coût de la fragmentation est trop élevé pour être ignoré. Grâce à Rubrik Identity Resilience, les systèmes d'identités restent fiables, opérationnels et restaurables. Les entreprises peuvent ainsi maintenir les accès, investiguer les incidents et restaurer l'infrastructure d'identités dans leurs environnements hybrides. Rubrik réduit le risque de persistance des attaquants et préserve les changements légitimes pour garantir une restauration fiable, sans perdre des mois de travail. Résultat, vos systèmes restent intègres et à jour.

Demandez une démo pour découvrir la restauration orchestrée des identités en action.