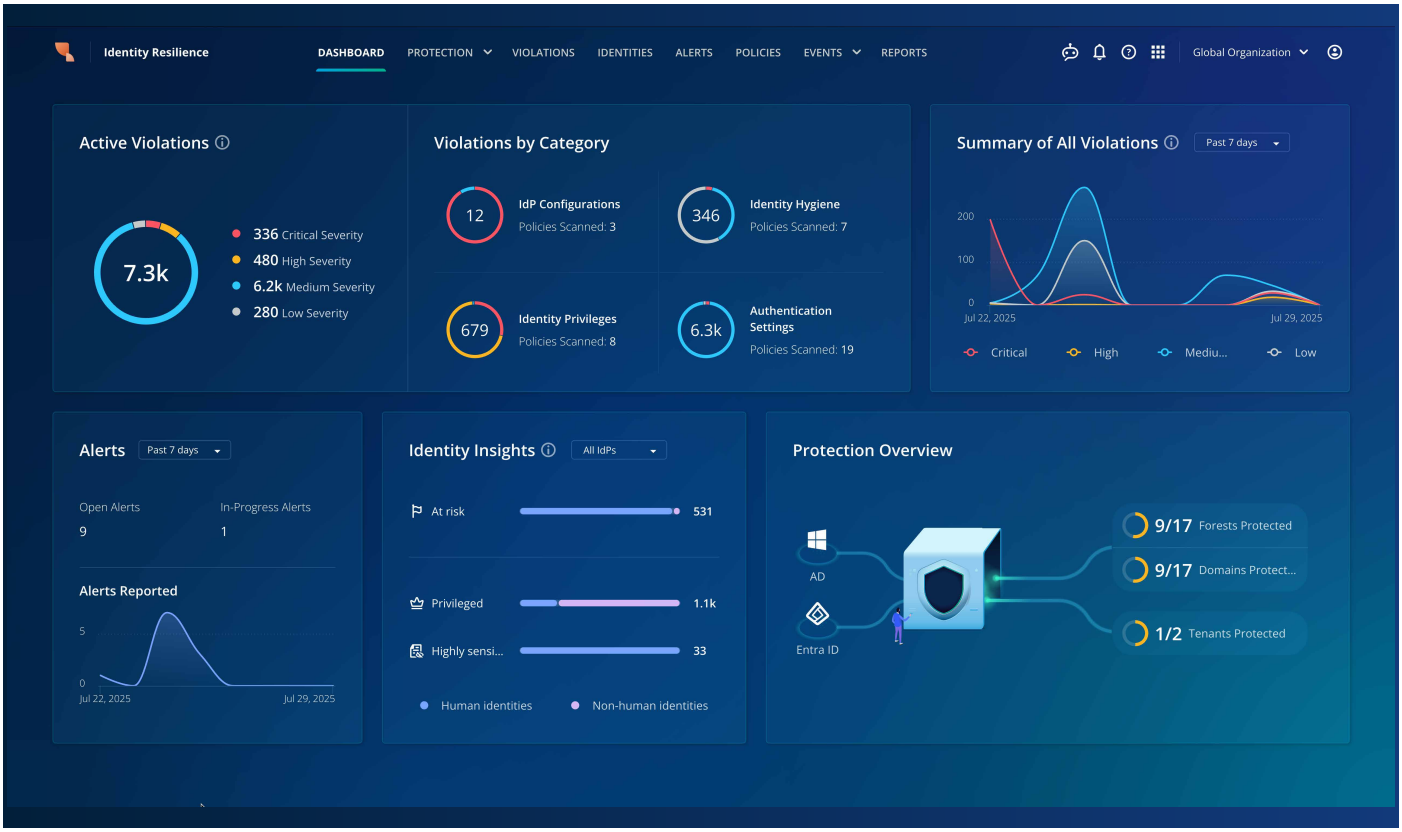
Rubrik Identity Resilience

Fiche technique

Votre infrastructure d'identités est en danger.

Rubrik Identity Resilience donne aux entreprises les moyens de protéger et de restaurer leurs systèmes d'identité avant, pendant et après une attaque. En réunissant visibilité, détection en temps réel et restauration orchestrée sur une même plateforme intégrée, Rubrik renforce la cyber-résilience et aide à neutraliser les risques, à annuler les modifications indésirables (rollback) et à rebondir rapidement après une attaque contre les identités.

Active Directory (AD) et Entra ID constituent le socle même des accès en entreprise. Toutefois, leur sécurisation se fait de plus en plus complexe, en particulier dans les environnements hybrides et multicloud. Outils fragmentés, scripts et audits ponctuels laissent des angles morts qui exposent l'infrastructure aux menaces basées sur les identités. Pour les cybercriminels, il est d'autant plus facile d'échapper aux systèmes de détection que tout est encore fait à la main, de l'investigation des menaces aux tentatives d'identification et d'élimination des backdoors et fragilités laissés dans le sillage des attaquants. Idem pour les processus de restauration manuels qui prolongent les délais d'interruption et mettent un peu plus en péril l'activité de l'entreprise.



Les identités constituent aujourd'hui le vecteur d'attaque de prédilection : plus de 80 % des intrusions ont exploité des identifiants compromis, l'élévation des privilèges ou des contrôles d'accès mal configurés pour infiltrer les systèmes, se propager latéralement et perturber les opérations. Ces angles morts dans la détection et la configuration font le bonheur des hackers qui, à l'image du groupe Scattered Spider, s'y engouffrent pour explorer les réseaux en échappant à toute détection par les outils de sécurité traditionnels.

En cause ? La nature fragmentaire des stacks de sécurité actuelles, souvent dépourvues d'une télémétrie temps réel intégrée et d'une visibilité multiplateforme sur l'état et les comportements des identités. Pour ne rien arranger, la plupart des solutions ne proposent pas de mécanisme de rollback en cas de modifications non autorisées de la configuration des

identités ou d'abus des autorisations d'accès. Résultat, les workflows de restauration des identités reposent sur un socle bancal composé de processus manuels, de sauvegardes système potentiellement compromises ou de journaux d'audit incomplets et muables.

La solution : un cadre de sécurité intégré et résilient pour les identités, qui combine application continue des politiques, monitoring inaltérable et capacités de restauration orchestrée. À défaut, les entreprises demeurent exposées à la prolifération de menaces contre les identités, aux interruptions opérationnelles et à la présence prolongée des attaquants dans leurs environnements.

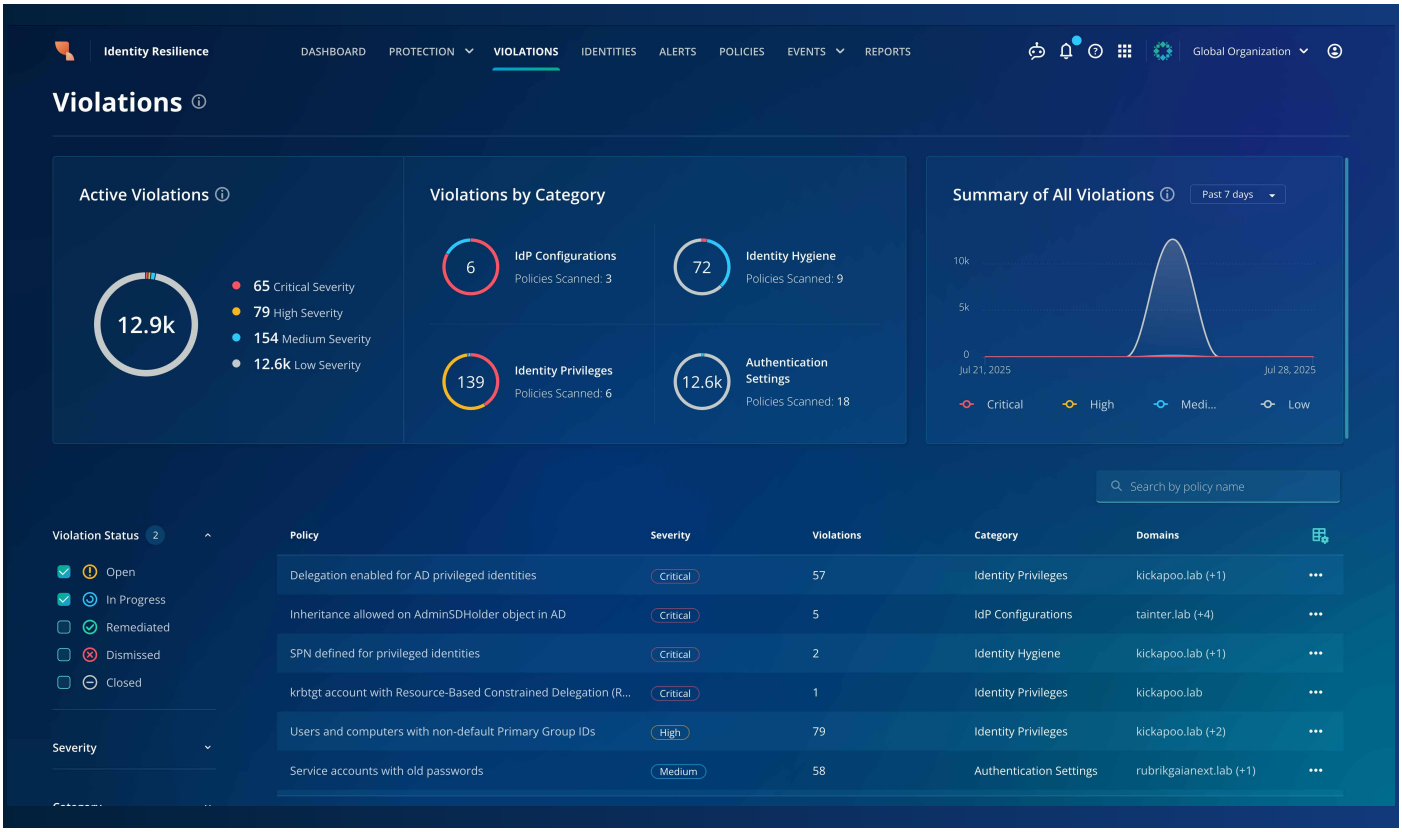
Pour combler ces lacunes, Rubrik Identity Resilience offre une visibilité complète sur les failles les plus exploitées par les acteurs malveillants. Elle surveille l'infrastructure en continu afin de détecter en quasi temps réel les modifications critiques, notamment celles facilitant la latéralisation et l'élévation des privilèges. Ainsi alertées, les équipes interviennent rapidement pour neutraliser les risques, corriger les expositions et éradiquer les acteurs malveillants avant qu'ils ne commettent davantage de dommages.

INVENTAIRE UNIFIÉ DES IDENTITÉS

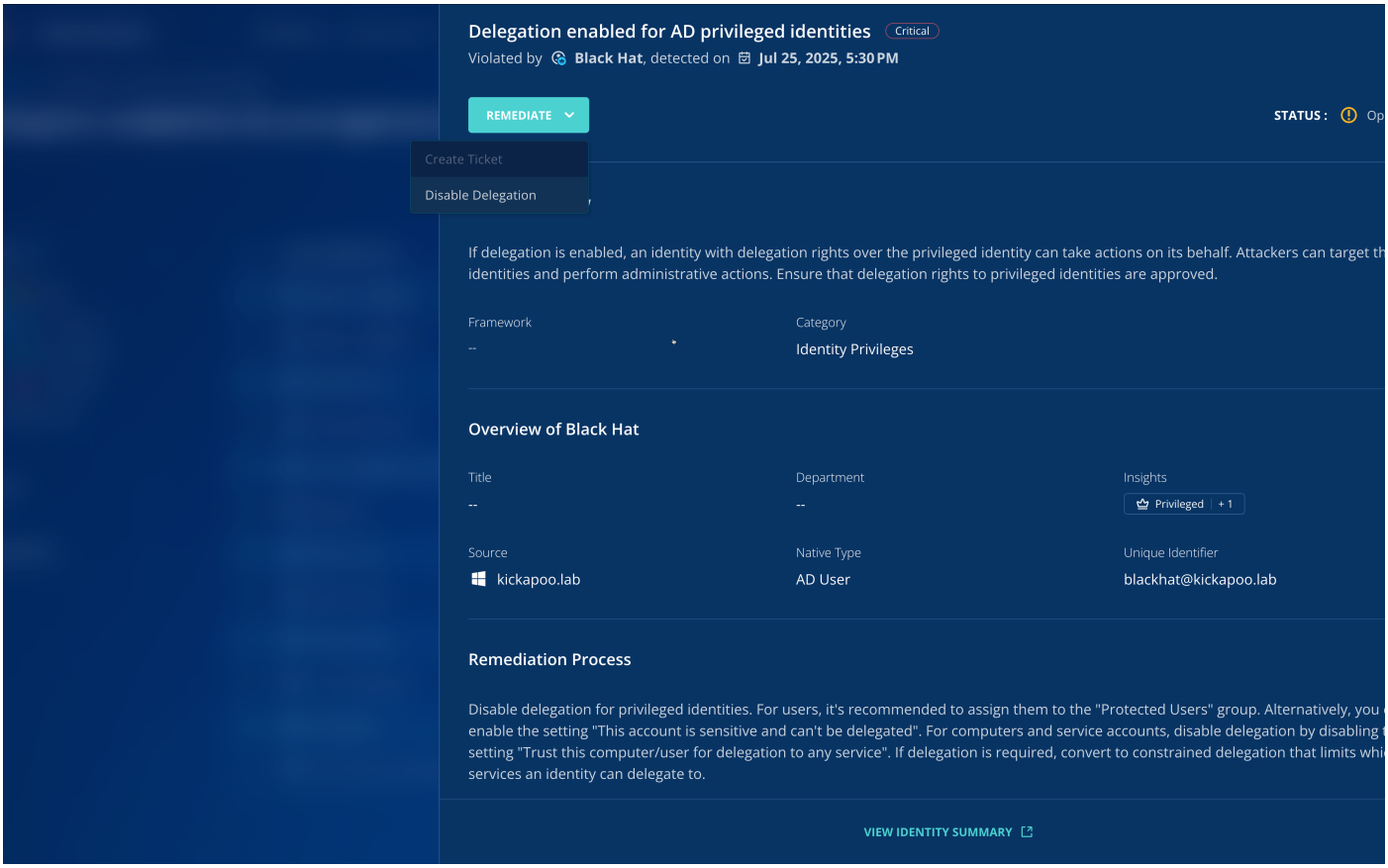
Bien que de nombreuses entreprises continuent d'investir considérablement dans les infrastructures on-prem, il n'est pas rare que, compte tenu de l'essor des systèmes cloud et multicloud, les identités soient réparties entre plusieurs IdP. Rubrik Identity Resilience établit un inventaire unifié et centralisé, garant d'une visibilité sur les identités (humaines et non humaines), les risques associés et les alertes pour tous les IdP intégrés. Conjuguée à Rubrik DSPM, la solution indique également le détail des informations sensibles auxquelles a accès une identité, offrant deux nouveaux axes de priorisation : 1) en fonction des privilèges définis dans la solution IdP ou 2) du niveau d'accès aux données sensibles.

DÉTECTION DES RISQUES PILOTÉE PAR DES POLITIQUES

Rubrik Identity Resilience dresse un inventaire complet des identités, humaines et non humaines, sur l'ensemble des IdP utilisés. Une fois créé, l'inventaire se met automatiquement à jour à chaque snapshot. Ensuite, un puissant moteur de politiques surveille tous les paramètres de configuration en continu, à la recherche du moindre manquement aux règles définies. La solution Rubrik Identity Resilience propose toute une panoplie de politiques prêtes à l'emploi, adaptées aux frameworks de sécurité et de bonnes pratiques les plus répandus, notamment l'ANSSI, MITRE ATT&CK, D3FEND, OWASP. Ces politiques peuvent être unifiées sur l'ensemble des IdP, selon les besoins. En voici quelques exemples : identités privilégiées avec délégation autorisée, utilisateurs avec une MFA faible ou inactivée et comptes de service avec mots de passe anciens, signe que la rotation des identifiants n'est pas assez fréquente.



En cas de manquement aux politiques, les anomalies sont signalées dans l'interface utilisateur, laquelle permet de créer un ticket dans un outil ITSM comme ServiceNow, voire de remédier à l'infraction directement dans la solution IdP lorsque cela est possible. Par ailleurs, les violations de politiques de sécurité peuvent être envoyées aux outils SIEM et SOAR par le biais de webhooks, dans le but de déclencher des workflows automatisés.

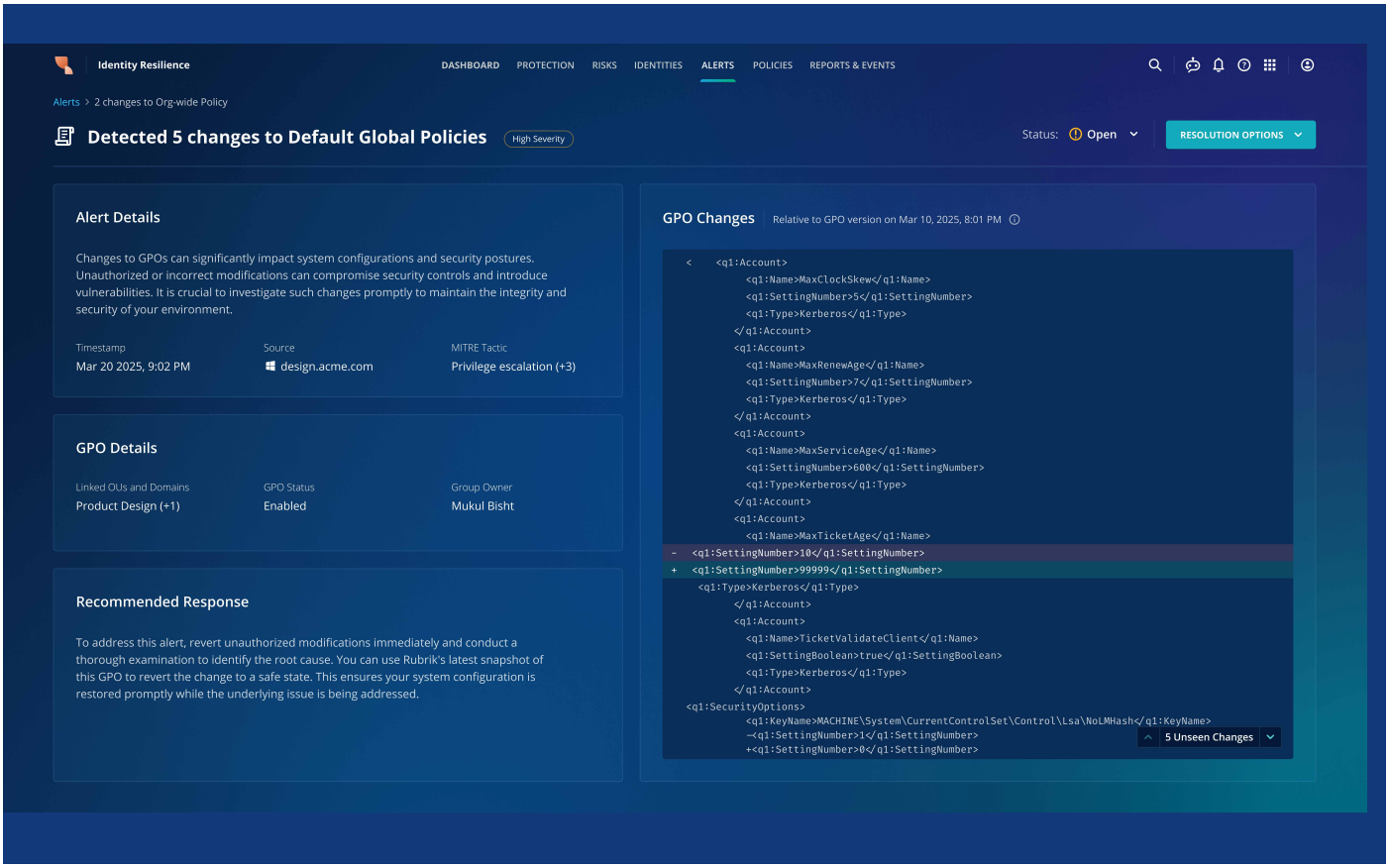


SURVEILLANCE EN QUASI TEMPS RÉEL DES MODIFICATIONS CRITIQUES

Certains outils de monitoring se contentent d'analyser le journal des événements Windows ou passent par Windows Event Forwarding (WEF) pour détecter les activités suspectes. Les cyberattaquants le savent. Et ils savent également qu'il est facile d'écraser des journaux avec leurs propres fichiers ou de les effacer pour éliminer toute trace de leur passage. Sans un solide suivi des événements, les activités malveillantes deviennent presque impossibles à détecter.

Rubrik Identity Resilience surveille Active Directory en continu, indépendamment des journaux d'événements Windows. Une approche unique qui a l'avantage de résister aux tentatives d'altération et complique donc la tâche de tout acteur malveillant tentant de passer sous les radars. Une fois que les données des événements sont transcrites de l'IdP vers la plateforme Rubrik, elles deviennent tout aussi immuables que les sauvegardes, ce qui garantit leur intégrité.

En cas de détection d'une activité suspecte (élévation de privilèges, etc.) ou d'une modification des objets de stratégie de groupe (GPO), une alerte est déclenchée pour faciliter la priorisation et la neutralisation de la menace.



Alerte et réponse

Génération d'alertes en quasi temps réel : les événements suspects génèrent des alertes contextualisées, avec les identités de parties prenantes, les horodatages, les ressources touchées et les actions recommandées.

Intégration aux plateformes ITSM : les menaces et les violations de politiques de sécurité peuvent déclencher la création de tickets en vue d'une investigation sur une plateforme ITSM. Par défaut, Rubrik propose une intégration par API à ServiceNow.

Intégration des webhooks : les alertes et les événements sont transférés par le biais de webhooks aux outils SIEM et SOAR, lesquels peuvent déclencher des workflows de tri et de remédiation.

RESTAURATION DES FOURNISSEURS D'IDENTITÉ

La solution Identity Resilience réduit les risques et détecte les activités suspectes pour contenir la capacité de nuisance des acteurs malveillants, à condition de s'inscrire dans une stratégie fondée sur le principe qu'une compromission est inévitable. La solution Rubrik Identity Recovery, incluse dans Identity Resilience, assure la restauration complète d'Active Directory et d'Entra ID, y compris sur des configurations hybrides. Fortes de cette approche stratégique, les entreprises ont toutes les cartes en main pour gérer proactivement la surface d'attaque de leurs identités, mais aussi pour rebondir en cas de compromission voire de destruction par une attaque de ce rouage essentiel de l'infrastructure.

ARCHITECTURE DE LA SOLUTION ET ENJEUX TECHNIQUES DE DÉPLOIEMENT

Sécurité et conformité

- En complément, des contrôles d'accès basés sur les rôles (RBAC) granulaires peuvent limiter les autorisations à la solution Identity Resilience uniquement, sans accès aux autres outils Rubrik pour les équipes IAM et GRC ; et inversement, bloquer l'accès à Identity Resilience aux administrateurs de sauvegarde, de sorte que ces derniers n'ont pas accès aux fonctionnalités de gestion des identités.
- Notre plateforme est conforme, certifiée et appuyée par notre équipe support. Pour en savoir plus sur la conformité de Rubrik Security Cloud, rendez-vous sur https://www.rubrik.com/compliance-program.

- Les données au repos et en transit sont chiffrées, tandis que des règles RBAC strictes sont appliquées aux administrateurs.
- Une fois écrites sur la plateforme, les données de sauvegarde sont immuables, ce qui garantit leur récupérabilité.

Prise en charge des environnements hybrides

- Rubrik Backup Service est déployé sur les contrôleurs de domaine afin de collecter des données AD et de les sauvegarder si nécessaire. Le tout, sans exposer d'identifiants sensibles ni imposer de changements majeurs sur le réseau.
- Les données des événements AD sont traitées sur les clusters dans votre datacenter, les métadonnées étant envoyées à Rubrik Security Cloud pour analyse.
- Pour Entra ID, l'onboarding s'opère par le biais d'une seule connexion administrateur pour créer un principal de service (Enterprise App) avec des privilèges limités au strict nécessaire.
- La définition des politiques et les alertes de sécurité sont unifiées, peu importe l'environnement, ce qui simplifie la gouvernance des déploiements on-prem, hybrides et multicloud.
- La récupération d'Active Directory est orchestrée sur plusieurs clusters, pour une sauvegarde locale et une restauration depuis une seule et même interface.

Console simple et centralisée

- Notre interface intuitive primée centralise la gestion de la posture de sécurité ainsi que la protection et la restauration des identités et des données.
- En cas d'attaque, la solution assure une restauration orchestrée intégrale des services critiques, des identités jusqu'aux données.
- La cyber-résilience renforcée des solutions Rubrik protège les services d'identité de plus de 4 000 entreprises à travers le monde.

FONCTIONNALITÉS INCLUSES

Depuis des années, Rubrik protège les services d'identité d'entreprises du monde entier. Aujourd'hui, plus de 4 000 clients font confiance à Rubrik pour assurer leur cyber-résilience. Retrouvez dans le tableau ci-dessous le détail des fonctionnalités offertes par les différentes solutions Rubrik, y compris Identity Resilience.

	Rubrik Foundation / Business / Enterprise Edition	Rubrik Identity Recovery	Rubrik Identity Resilience (inclut Identity Recovery)
Protection et restauration des utilisateurs, groupes et contrôleurs de domaine Active Directory	✓	✓	✓
Protection et restauration des utilisateurs, groupes et rôles Entra ID	✓	✓	✓
Restauration granulaire des objets Active Directory et Entra ID	✓	✓	✓
Restauration orchestrée de forêts AD complètes		✓	✓
Comparaison et restauration des attributs d'objets AD		✓	✓
Workflow de restauration pour les environnements hybrides AD et Entra		✓	✓
Inventaire unifié des identités humaines et non humaines sur tous les IdP			✓
Détection des risques pilotée par des politiques dans les configurations des IdP et des identités			✓
Remédiation in-app des risques détectés			✓
Alerte en quasi temps réel lors de modifications critiques ou d'activités suspectes grâce à un monitoring inaltérable			✓

CONCLUSION

La solution Identity Resilience est propulsée par un moteur complet basé sur des politiques, combiné à des techniques de monitoring inaltérable des événements. Sa mission : assurer une protection multicouche des identités dans les environnements Active Directory et Entra ID d'entreprise.

Validation continue de la conformité des configurations, détection des activités anormales en quasi temps réel, capacités de remédiation in-app, leviers d'actions concrets… Identity Resilience propose une gamme complète de fonctionnalités pour gérer proactivement les risques liés aux identités, sécuriser la surface d'attaque la plus critique et assurer la résilience opérationnelle.

Siège mondial
3495 Deer Creek Road
Palo Alto, CA 94304
États-Unis

+31 208 113 222
france@rubrik.com
www.rubrik.com/fr

brf-rubrik-identity-resilience-Rubrik_IDML-fr-FR#DTP_DDDNUX# / 20251119