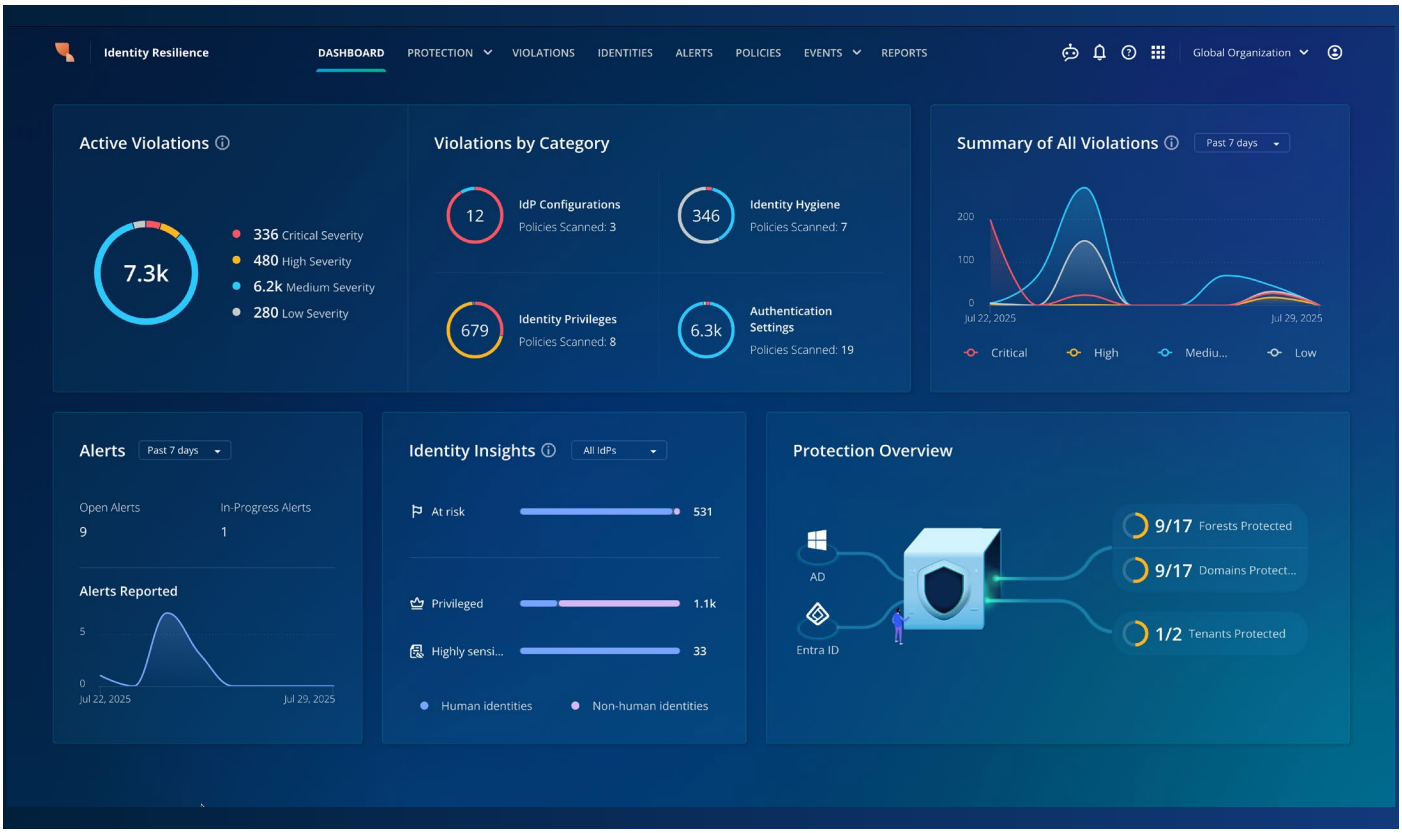
Rubrik Identity Resilience

Scheda tecnica

La tua infrastruttura delle identità è sotto attacco.

Rubrik Identity Resilience consente alle organizzazioni di proteggere e ripristinare i propri sistemi di identità prima, durante e dopo un attacco. Grazie alla piattaforma integrata di Rubrik che unifica visibilità, rilevamento in tempo reale e ripristino orchestrato, le aziende possono rimediare ai rischi, annullare le modifiche critiche e ripristinare subito l'operatività, garantendosi la resilienza aziendale contro gli attacchi basati sulle identità.

Active Directory (AD) ed Entra ID costituiscono la base dell'accesso aziendale, ma proteggere questi sistemi è diventato sempre più complesso, in particolare negli ambienti ibridi e multi-cloud. Affidarsi a strumenti frammentati, script e valutazioni estemporanee crea lacune che espongono l'organizzazione a minacce legate all'identità. Le indagini e i tentativi manuali di identificare le minacce e annullare le modifiche introdotte da attori malevoli possono permettere agli aggressori di restare nascosti nell'ambiente. Nel frattempo, i processi manuali di ripristino prolungano i tempi di inattività, aumentando i rischi per l'azienda.



Gli attacchi basati sull'identità dominano il panorama delle minacce attuali: oltre l'80% delle intrusioni informatiche sfrutta credenziali compromesse, escalation di privilegi o controlli di accesso mal configurati per violare i sistemi, propagarsi lateralmente e compromettere l'operatività aziendale. Gruppi di attacco avanzati come Scattered Spider, sfruttano proprio questi punti ciechi nelle configurazioni e le lacune nel rilevamento per muoversi nella rete, sfuggendo agli strumenti di sicurezza tradizionali.

Una delle principali criticità deriva dalla natura frammentata degli stack di sicurezza IT esistenti, che spesso non dispongono di telemetria integrata in tempo reale né di visibilità cross-platform sullo stato e sul comportamento delle identità. Inoltre, molte soluzioni non offrono meccanismi per l'annullamento o il ripristino in caso di modifiche

non autorizzate alle configurazioni di identità o di accessi consentiti in modo improprio. Di conseguenza, i flussi di lavoro per il ripristino delle identità si basano spesso su processi manuali, backup potenzialmente compromessi o log di audit incompleti e alterabili.

Senza un framework integrato e resiliente per la sicurezza delle identità che combini enforcement continuo delle policy, monitoraggio a prova di manomissione e capacità di ripristino orchestrato, le organizzazioni restano vulnerabili a minacce crescenti legate all'identità, interruzioni operative e tempi prolungati di permanenza della violazione.

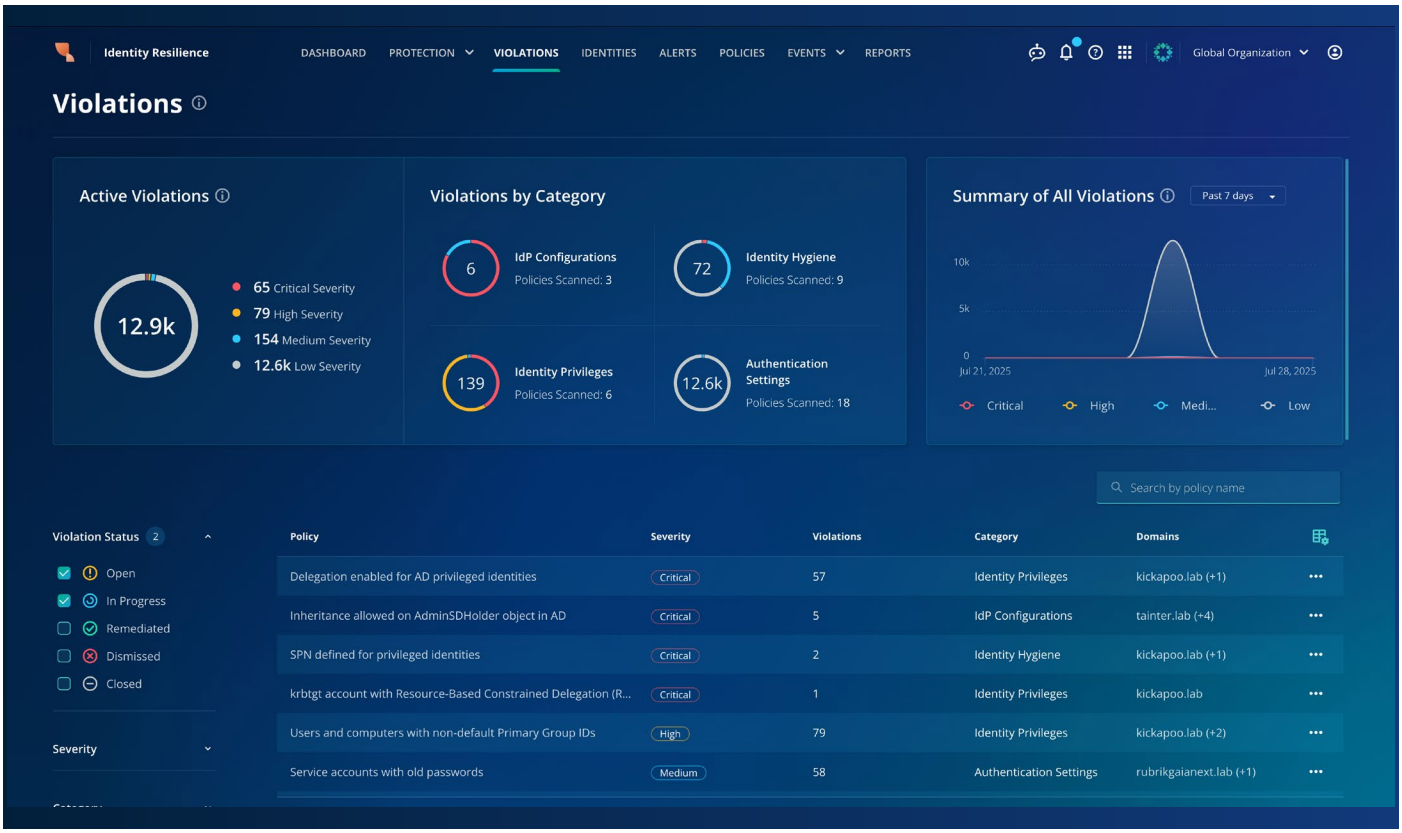
Rubrik Identity Resilience annulla questi gap offrendo visibilità completa sui punti più vulnerabili sfruttati dagli attori malevoli. Infatti, monitora e rileva continuamente e quasi in tempo reale le modifiche critiche, come quelle usate per la propagazione laterale e l'escalation dei privilegi, consentendo alle organizzazioni di intervenire tempestivamente, chiudere le falle ed espellere gli aggressori prima che possano arrecare ulteriori danni.

INVENTARIO UNIFICATO DELLE IDENTITÀ

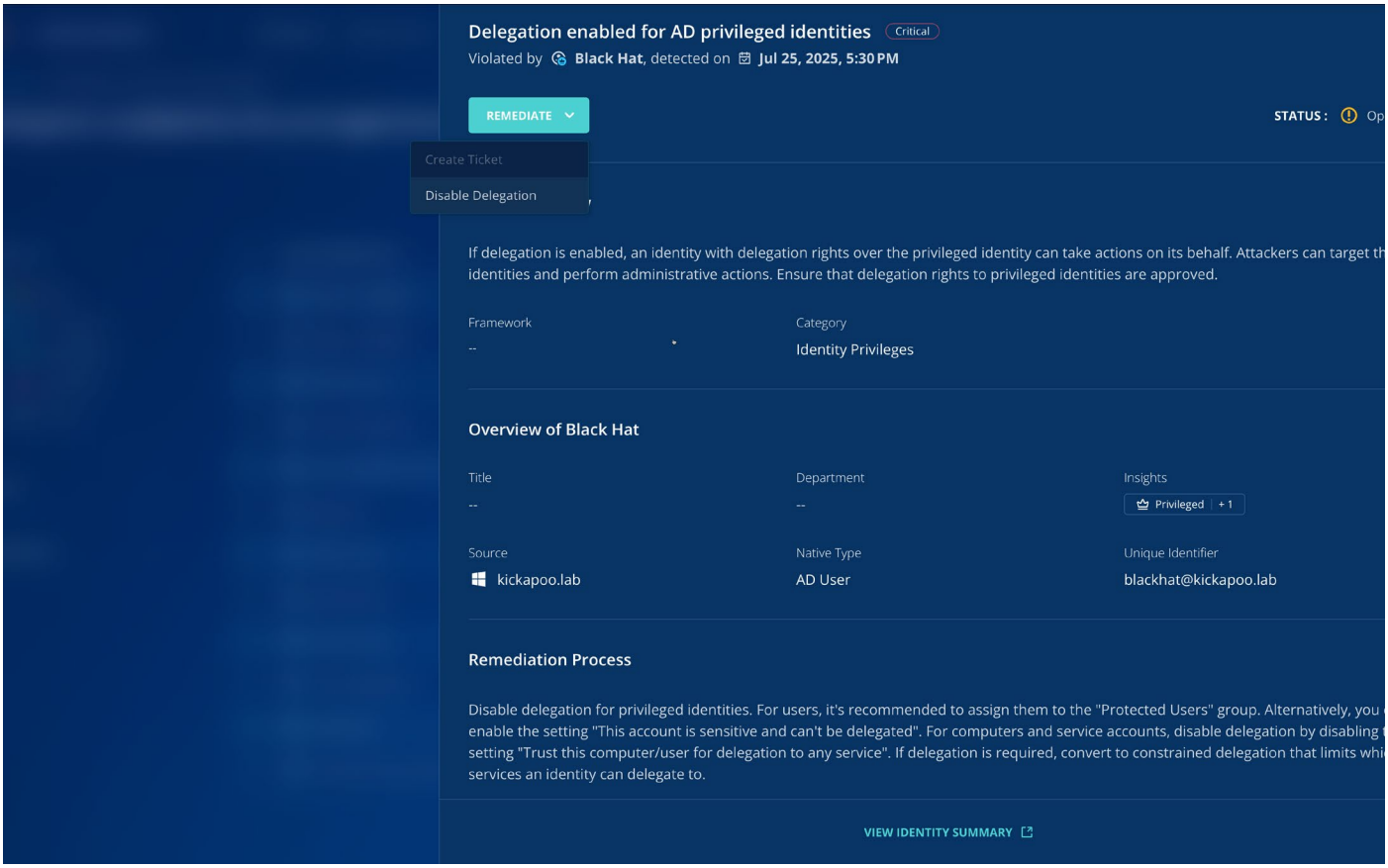
Con il crescente uso di sistemi su più cloud e tra diversi ambienti cloud, anche se molte organizzazioni mantengono ancora ingenti investimenti in infrastrutture on-premise, non è raro che i sistemi di identità siano distribuiti tra più provider. Rubrik Identity Resilience offre un inventario unificato delle identità che garantisce visibilità su tutte le identità – umane e non umane – e sui relativi rischi e alert, su tutti gli IdP integrati. Inoltre, quando utilizzato in combinazione con Rubrik DSPM, visualizza anche i dettagli dei dati sensibili a cui ogni identità ha accesso, consentendo di stabilire le priorità non solo in base ai privilegi associati all'IdP, ma anche al livello di accesso ai dati sensibili.

RILEVAMENTO DEI RISCHI DI IDENTITÀ BASATO SU POLICY

Rubrik Identity Resilience costruisce un inventario completo di tutte le identità presenti negli IdP configurati, comprese le identità umane e non umane (NHI). Una volta creato, l'inventario viene aggiornato automaticamente a ogni snapshot. Un potente motore di policy monitora quindi i dettagli di configurazione, eseguendo scansioni continue per verificare la conformità con le policy definite. Identity Resilience include numerose policy predefinite, allineate a framework di sicurezza e best practice riconosciuti come MITRE ATT&CK, D3FEND, OWASP e ANSSI. Queste policy vengono applicate in modo unificato agli IdP, dove necessario. Esempi di queste policy includono identità privilegiate con delega abilitata, utenti senza MFA attiva o con autenticazione debole e account di servizio con password obsolete, che potrebbero indicare la mancata rotazione delle credenziali.



Quando viene rilevata una violazione delle policy, l'interfaccia utente la evidenzia, con opzioni per aprire automaticamente un ticket in un sistema ITSM come ServiceNow e, dove possibile, correggere direttamente la violazione nell'IdP. Inoltre, le violazioni di sicurezza possono essere inviate a strumenti SIEM e SOAR tramite webhook, abilitando l'attivazione automatica di workflow da questi strumenti.

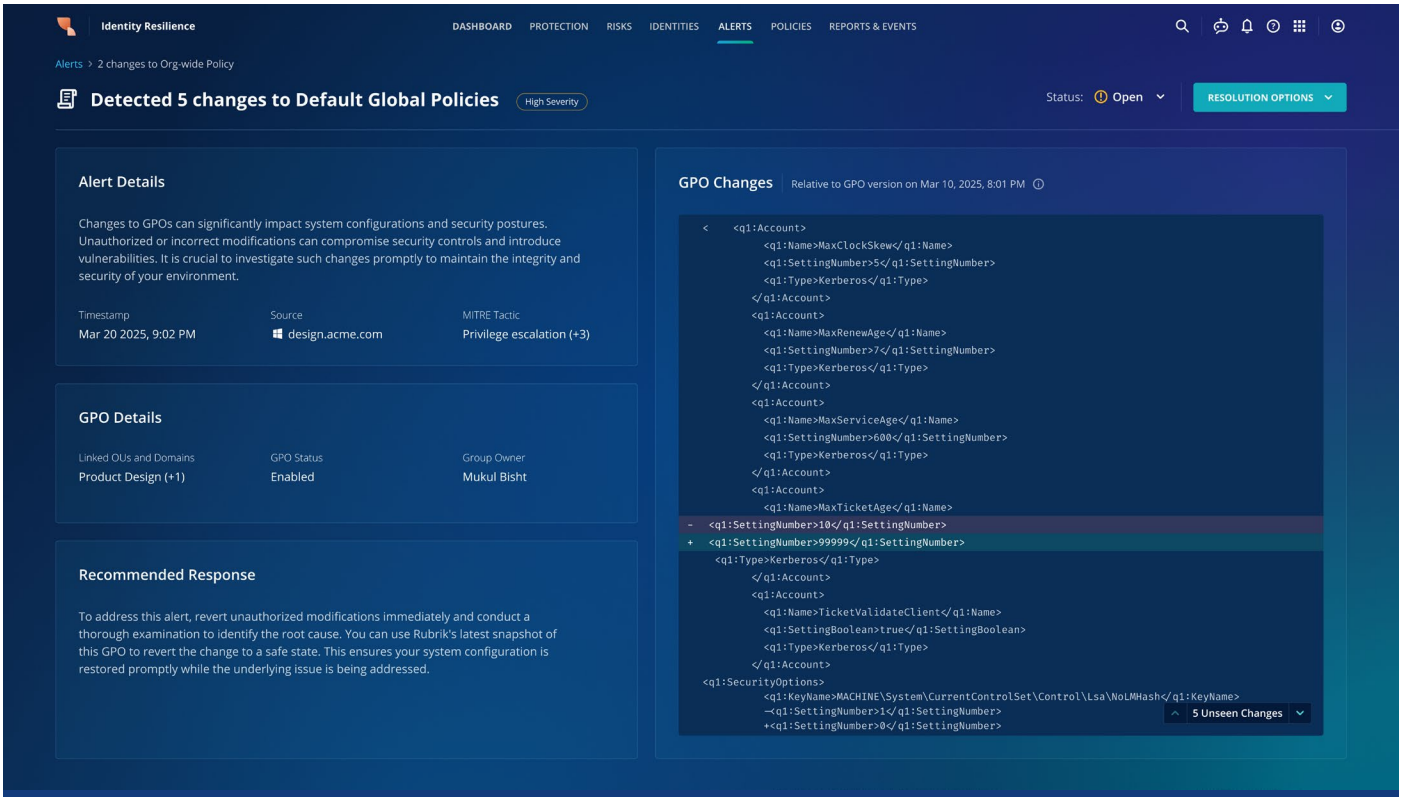


MONITORAGGIO QUASI IN TEMPO REALE DELLE MODIFICHE CRITICHE

Alcuni strumenti di monitoraggio analizzano i log eventi di Windows o si basano su Windows Event Forwarding (WEF) per individuare attività sospette. Purtroppo, gli aggressori conoscono bene queste tecniche e sanno anche che i file di log si possono facilmente sovrascrivere con dati arbitrari o cancellare per nascondere le proprie tracce. Senza un tracciamento degli eventi efficace, rilevare attività dannose può diventare quasi impossibile.

Rubrik Identity Resilience monitora in modo continuo Active Directory in maniera indipendente dai log eventi di Windows. Questo approccio unico è a prova di manomissione, il che rende molto più difficile per un hacker agire inosservato. Una volta che i dati degli eventi vengono scritti dall'IdP alla piattaforma Rubrik, diventano immutabili, esattamente come i backup dei dati, garantendo l'integrità delle informazioni raccolte.

Quando viene rilevata un'attività sospetta, come l'escalation dei privilegi o la modifica dei criteri di gruppo (GPO), viene generato un avviso per attivare il triage e le azioni correttive necessarie.



Segnalazione e risposta

Generazione di avvisi in tempo quasi reale: gli eventi sospetti generano avvisi corredati da dettagli rilevanti, tra cui identità coinvolte, data e ora, risorse interessate e azioni consigliate per la risposta.

Integrazione con piattaforme ITSM: le minacce e le violazioni di sicurezza possono attivare automaticamente la creazione di ticket in piattaforme ITSM per avviare indagini. Rubrik offre un'integrazione a livello di API con ServiceNow ITSM.

Integrazione Webhook: gli avvisi e gli eventi possono essere inviati tramite webhook a strumenti SIEM e SOAR, da cui possono essere attivati workflow automatizzati per triage e risposta.

RIPRISTINO DEI PROVIDER DI IDENTITÀ

Sebbene Identity Resilience sia progettato per ridurre i rischi e rilevare attività sospette prima che causino danni, è essenziale adottare una strategia robusta che includa l'assunzione preventiva di una compromissione ("Assume Breach"). Rubrik Identity Recovery, incluso in Identity Resilience, consente il ripristino completo di Active Directory ed Entra ID, comprese le configurazioni ibride. Questo approccio strategico permette alle organizzazioni di ridurre al minimo i rischi attraverso una gestione proattiva della propria superficie d'attacco, garantendo al contempo la possibilità di ripristinare tempestivamente l'infrastruttura in caso di compromissione di un componente critico.

ARCHITETTURA DELLA SOLUZIONE E CONSIDERAZIONI SUL DEPLOYMENT

Sicurezza e conformità

- Attraverso il controllo granulare degli accessi (RBAC), è possibile assegnare autorizzazioni solo alla funzione Identity Resilience (escludendo le altre funzionalità Rubrik, per team IAM e GRC) o viceversa (escludendo Identity per gli amministratori di backup).
- Piattaforma e supporto certificati e conformi agli standard. Per ulteriori informazioni sulla conformità di Rubrik Security Cloud, consulta la pagina https://www.rubrik.com/compliance-program.

- Tutti i dati vengono crittografati sia a riposo che in transito, e l'accesso amministrativo è regolato da rigorosi controlli basati sui ruoli (RBAC).
- I dati di backup, una volta scritti sulla piattaforma, diventano immutabili, offrendo garanzie di ripristinabilità.

Supporto per ambienti ibridi

- Rubrik Backup Service viene distribuito sui controller di dominio per raccogliere i dati di Active Directory (e per eseguire i backup, se necessario), senza esporre credenziali sensibili di accesso o richiedere modifiche estese alla rete.
- I dati degli eventi AD vengono elaborati localmente all'interno del data center, mentre i metadati vengono inviati a Rubrik Security Cloud per l'elaborazione successiva.
- Per quanto riguarda Entra ID, l'onboarding avviene tramite un singolo login amministrativo che crea un'applicazione aziendale (service principal) con i privilegi minimi necessari.
- Le definizioni delle policy di sicurezza e gli avvisi sono unificati, indipendentemente dalla posizione, per semplificare la governance tra ambienti on-premise, ibridi e multi-cloud.
- Il ripristino di Active Directory è orchestrato tra più cluster, per consentire di eseguire il backup in locale e ripristinare tutto da un'unica interfaccia.

Pannello di controllo globale e semplificato

- Un'interfaccia pluripremiata e facile da usare per gestire la postura di sicurezza di identità e dati, oltre alla protezione e al ripristino di dati e identità.
- Ripristino orchestrato end-to-end dei servizi critici, dall'identità ai dati, in caso di attacco riuscito.
- Resilienza informatica di livello enterprise, scelta da oltre 4.000 clienti per proteggere i servizi di identità a livello globale.

PACKAGING

Rubrik protegge le identità dei propri clienti da molti anni, e oltre 4.000 organizzazioni si affidano alla sua tecnologia per la sicurezza dei servizi di identità. La tabella seguente mostra le funzionalità disponibili nelle diverse soluzioni Rubrik, inclusa Identity Resilience.

	Rubrik Foundation/ Business/ Enterprise Edition	Rubrik Identity Recovery	Rubrik Identity Resilience (Include Identity Recovery)
Protezione e ripristino di utenti, gruppi e controller di dominio di Active Directory	✓	✓	✓
Protezione e ripristino di utenti, gruppi e ruoli di Entra ID	✓	✓	✓
Ripristino granulare degli oggetti per AD ed Entra ID	✓	✓	✓
Ripristino orchestrato completo di Forest AD		✓	✓
Confronto e ripristino degli attributi degli oggetti AD		✓	✓
Workflow di ripristino ibrido per ambienti AD ed Entra ID		✓	✓
Inventario unificato delle identità umane e non umane in tutti gli IdP			✓
Rilevamento dei rischi basato su policy nelle configurazioni IdP e delle identità			✓
Correzione in-app dei rischi rilevati			✓
Avvisi quasi in tempo reale per modifiche critiche o attività sospette, con monitoraggio anti-manomissione			✓

SINTESI

Identity Resilience sfrutta un motore avanzato basato su policy, in combinazione con tecniche di monitoraggio degli eventi a prova di manomissione, per offrire una protezione multilivello delle identità aziendali in ambienti Microsoft Active Directory ed Entra ID.

Con la validazione continua della conformità delle configurazioni, il rilevamento quasi in tempo reale di attività anomale e insight utili con possibilità di intervento direttamente dall'interfaccia, Identity Resilience permette alle organizzazioni di gestire in modo proattivo il rischio legato all'identità, proteggere le superfici di attacco più critiche e garantire la resilienza operativa.

rubrik

Sede internazionale
3495 Deer Creek Road
Palo Alto, CA 94304
Stati Uniti

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com/it

brf-rubrik-identity-resilience-Rubrik_IDML-it-IT#DTP_DDDNUV# / 20251202