rubrik

Proteggi le identità su Active Directory, Entra ID e Okta con un'unica piattaforma unificata

Una piattaforma agentica di cyber resilience che mantiene i sistemi di identità sicuri, operativi e ripristinabili, eliminando l'elevato TCO associato a strumenti frammentati.

Gli aggressori compromettono **sempre più spesso** Identity Provider come Active Directory (AD), Entra ID e Okta per ottenere l'accesso ai sistemi. Compromettendo le identità, gli attaccanti effettuano un semplice login ed eludono il rilevamento dei tradizionali strumenti EDR e antimalware. Una volta dentro, i cybercriminali bloccano gli utenti legittimi e prendono in ostaggio dati e identità, esigendo riscatti. Con l'accesso ai sistemi aziendali completamente paralizzato, l'operatività si ferma e i team si trovano a gestire una situazione catastrofica.

La maggior parte delle organizzazioni si affida a soluzioni singole per difendersi, generando pericolosi punti ciechi. Infatti, i team IT e di sicurezza ricevono spesso avvisi frammentati e privi di un contesto cross-domain, dovendo poi ricostruire una visione coerente degli eventi a partire da flussi di dati isolati. Di conseguenza, l'uso di strumenti multipli obbliga i team a coordinare workflow complessi proprio nel momento in cui la pressione è massima.

L'utilizzo di più soluzioni singole comporta:

- **Lacune critiche di visibilità e ritardi**
- **Sovraccarico operativo**
- **Tempi di recovery più lunghi**
- **TCO più elevato**

IL RECOVERY ORCHESTRATO NON È UN'OPZIONE: IL RUOLO DELLE DIPENDENZE NEL SUCCESSO DEL RECOVERY

1. **Ripristino di Entra prima di AD → Associazioni perse, richiesta sincronizzazione completa del metaverse**
   Se Entra viene ripristinato dai backup prima di Active Directory, gli oggetti ibridi possono perdere la loro associazione e può essere necessaria una sincronizzazione completa di Entra Connect una volta ristabilita la relazione. In ambienti di grandi dimensioni, questo processo può richiedere giorni e aumentare sensibilmente il downtime.
2. **Ripristino di policy senza mappatura ID dei gruppi Okta → Caos negli accessi**
   I gruppi ripristinati dai backup ricevono nuovi ID che non vengono mappati alle policy di sicurezza associate in precedenza. Questo blocca l'accesso alle risorse e può, in alcuni casi, consentire accessi non autorizzati.
3. **Ripristino di credenziali di servizio obsolete → Blackout dell'automazione**
   Il ripristino degli account di servizio a uno stato precedente può reintrodurre vecchie password che script e strumenti attivi non sono più in grado di riconoscere, bloccando all'istante workflow critici in background. E se il servizio interrotto è responsabile del monitoraggio di altri servizi, il problema passerà del tutto inosservato.
4. **Ripristini basati su soluzioni singole frammentate → Persistenza dell'attaccante**
   Le lacune di visibilità tra strumenti di recovery isolati possono far sì che un attaccante venga rimosso da una piattaforma, ma resti presente su un'altra. Questo consente agli aggressori di compromettere nuovamente i sistemi ripristinati.

Rischio sistemico delle identità: l'effetto domino di una singola compromissione dell'IdP

Rubrik risolve questi problemi con una piattaforma unificata di identity resilience che protegge i sistemi di identità ibridi e consente alle organizzazioni di analizzare gli incidenti di sicurezza, mantenere la continuità operativa e ripristinare la fiducia.

PROTEGGERE I SISTEMI DI IDENTITÀ IBRIDI SU UN'UNICA PIATTAFORMA: VANTAGGI STRATEGICI

1. **Semplifica la postura di sicurezza, la protezione e la conformità:** ottieni piena visibilità sulla tua postura di sicurezza. Rubrik è un sistema di riferimento immutabile che fornisce uno stato storico attendibile delle identità e la telemetria delle relative modifiche. Ti consente inoltre di utilizzare un registro attività immutabile con attribuzione dell'attore per semplificare gli audit di conformità e le indagini forensi.

2. **Mantieni la continuità operativa:** grazie a tracciamento delle modifiche all'identità, monitoraggio delle interruzioni, analisi delle cause radice e rollback delle configurazioni, i team IAM possono rilevare, diagnosticare e risolvere rapidamente le interruzioni legate alle identità. Questo riduce il downtime e i rischi operativi, accelerando al contempo la risposta agli incidenti e il recovery su AD, Entra ID e Okta in pochi clic.

3. **Accelera la risposta agli incidenti:** riduci l'attrito operativo dovuto alla correlazione dei dati tra strumenti frammentati. Scopri come una minaccia si è mossa all'interno dei tuoi sistemi senza dover ricostruire manualmente i log provenienti da strumenti diversi. Ripristina le modifiche direttamente dalla piattaforma, rimuovi la persistenza dell'attaccante e preserva le modifiche legittime.

4. **Riduci il TCO:** riduci i costi di licenza, manutenzione e formazione legati alla gestione di strumenti di backup e sicurezza separati per AD, Entra ID e Okta. Sostituisci soluzioni frammentate con un'unica piattaforma per ridurre i costi di licenza e la complessità amministrativa.

5. **Preserva le modifiche legittime:** ripristina una baseline pulita e preserva le modifiche approvate alle identità, in modo da eliminare i meccanismi di persistenza dell'attaccante senza cancellare mesi di aggiornamenti sui tuoi sistemi.

SEMPLIFICARE LA PROTEZIONE PER AD, ENTRA ID E OKTA CON UNA SOLUZIONE MULTI-IDP

1. **Protezione unificata su un'unica piattaforma:** metti in sicurezza il tuo patrimonio di identità, dagli oggetti AD on-premise alle configurazioni Okta cloud-native, all'interno di un'unica console intuitiva progettata specificamente per ambienti complessi.

2. **Recovery orchestrato e granulare:** gestisci con facilità le interdipendenze complesse. Che si tratti del ripristino di un intero tenant AD o di un singolo oggetto Okta o Entra ID, Rubrik ti aiuta a riportare online i sistemi al primo tentativo.

3. **Continuità operativa:** semplifica il ripristino del tuo ambiente di identità. Mantieni l'uptime per utenti e applicazioni rilevando se sono stati compromessi più IdP, isolando i guasti e avviando il recovery in pochi clic.

4. **Architettura resistente alle manomissioni:** Proteggi identità e dati critici con l'architettura "Bunker in a Box" di Rubrik, che offre backup immutabili e logicamente air-gapped a prova di compromissione.

PROTEGGI IL FUTURO DEI TUOI SISTEMI DI IDENTITÀ

Attacchi alle identità più sofisticati e ambienti sempre più complessi hanno fatto crescere in misura non sostenibile il costo della frammentazione. Identity Resilience garantisce che i sistemi di identità rimangano attendibili, operativi e ripristinabili, consentendo alle aziende di mantenere gli accessi, analizzare gli incidenti e ripristinare l'infrastruttura di identità negli ambienti ibridi. Rubrik riduce il rischio di persistenza degli attaccanti e preserva le modifiche legittime alle identità, permettendoti di effettuare un recovery pulito senza perdere mesi di lavoro. Grazie a Rubrik, puoi mantenere i sistemi puliti e costantemente aggiornati.

Richiedi una demo per vedere il recovery orchestrato delle identità in azione.