

Eine einheitliche Plattform zum Schutz von Identitäten in Active Directory, Entra ID und Okta

Eine agentenbasierte Cyber-Resilienz-Plattform, die Identitätssysteme schützt, funktionsfähig hält und schnell wiederherstellt – ohne die hohen Kosten fragmentierter Tool-Landschaften.

Identitätslösungen wie Active Directory (AD), Entra ID und Okta werden **zunehmend** zum Ziel von Cyber-Angriffen. Nach dem Diebstahl von Zugangsdaten melden sich Hacker einfach an und verhindern so die Erkennung durch herkömmliche EDR-Tools und Malware-Detektoren. Legitime Benutzer werden ausgesperrt, Identitäten und Unternehmensdaten gekapert und das Unternehmen wird erpresst. Sind die Systeme erst einmal lahmgelegt, kommt der Geschäftsbetrieb zum Erliegen und das Unternehmen kann nur noch reaktiv handeln.

Die meisten Unternehmen setzen im Bereich der Bedrohungsabwehr auf punktuelle Lösungen, wodurch gefährliche tote Winkel entstehen. Das Sicherheitsteam muss zusammenhanglose Meldungen ohne übergreifenden Kontext interpretieren und aus isolierten Datenströmen ein schlüssiges Gesamtbild zusammenfügen. Die fragmentierte Tool-Landschaft zwingt das Team in Krisensituationen dazu, hochgradig komplexe Prozesse unter Zeitdruck zu koordinieren.

Der Einsatz von Punktlösungen verursacht:



Kritische Transparenzlücken und Verzögerungen



Einen höheren operativen Aufwand



Lange Wiederherstellungsprozesse



Höhere Gesamtbetriebskosten

EINE ORCHESTRIERTE WIEDERHERSTELLUNG IST UNVERZICHTBAR: ABHÄNGIGKEITEN BESTIMMEN DEN ERFOLG

1. Wiederherstellung von Entra vor AD → Verknüpfungen gehen verloren, Metaverse muss vollständig synchronisiert werden

Wird Entra vor Active Directory aus Backups wiederhergestellt, können Verknüpfungen zwischen Hybridobjekten verloren gehen. Dann muss nach der Wiederherstellung der Beziehungen ggf. eine vollständige Synchronisierung über Entra Connect durchgeführt werden. In größeren Umgebungen kann dies mehrere Tage dauern und zu längeren Systemausfällen führen.

2. Wiederherstellung von Richtlinien ohne Gruppen-ID-Zuordnung in Okta → Chaos bei Zugriffsrechten

Bei der Wiederherstellung von Gruppen aus Backups erhalten diese neue IDs, die nicht mehr mit den bisherigen Sicherheitsrichtlinien verknüpft sind. Dadurch sind die konfigurierten Zugriffsrechte für Ressourcen nicht mehr intakt und es können unbeabsichtigte Zugriffswege entstehen.

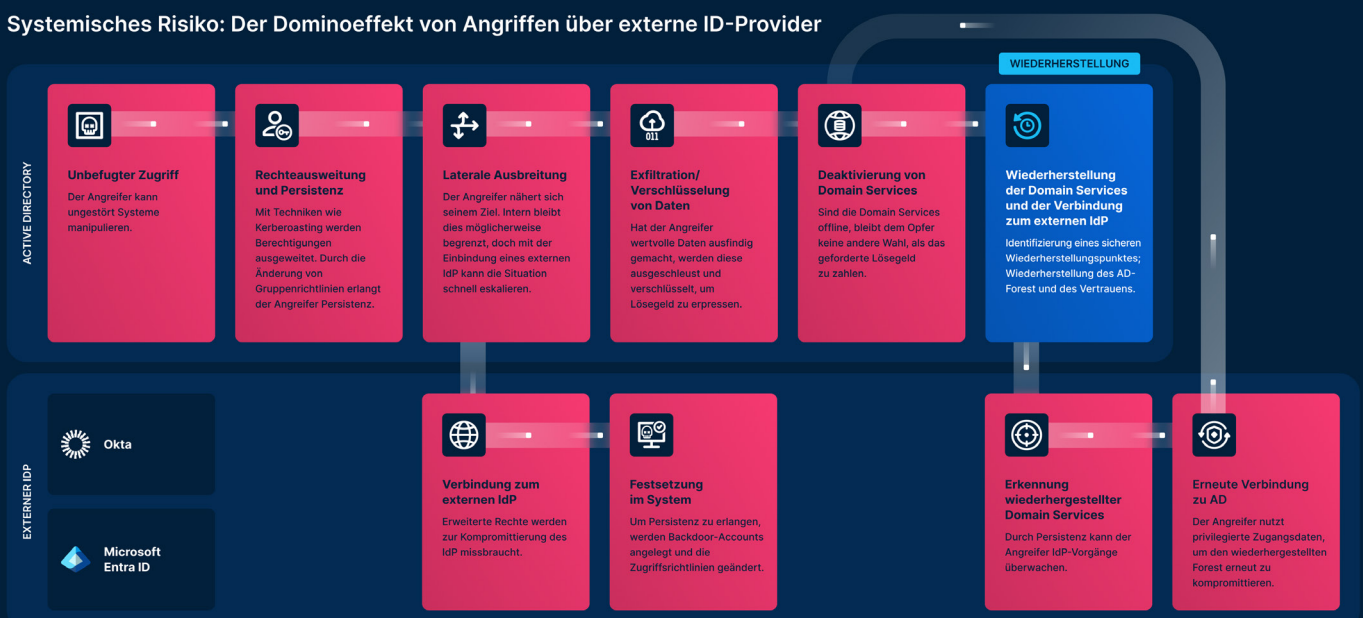
3. Wiederherstellung veralteter Service-Zugangsdaten → Automatisierung bricht zusammen

Werden Service-Accounts auf einen früheren Zustand zurückgesetzt, können alte Passwörter reaktiviert werden, die von den aktuellen Skripten und Tools nicht erkannt werden. Dadurch werden kritische Hintergrundprozesse sofort gestoppt. Wenn der betroffene Service andere Dienste überwacht, bleibt diese Fehlfunktion vollständig unbemerkt.

4. Unkoordinierte Wiederherstellung mit Punktlösungen → Angreifer erlangen Persistenz

Fehlende Transparenz zwischen Wiederherstellungstools kann dazu führen, dass die Bereinigung infizierter Systeme nicht von Dauer ist, weil die Angreifer auf einer anderen Plattform weiterhin präsent sind und das wiederhergestellte System erneut kompromittieren können.

Systemisches Risiko: Der Dominoeffekt von Angriffen über externe ID-Provider



Rubrik schließt diese Lücken mit einer einheitlichen Plattform für Identitätsresilienz in hybriden Systemen. Die Lösung ermöglicht Unternehmen, Identitätsvorfälle zu untersuchen, den Betrieb aufrechtzuerhalten und Vertrauen wiederherzustellen.

STRATEGISCHE VORTEILE EINER ZENTRALEN PLATTFORM ZUM SCHUTZ HYBRIDER IDENTITÄTSSYSTEME

- 1. Einfacheres Sicherheitsmanagement, besserer Schutz und höhere Compliance:** Rubrik schafft umfassende Transparenz über Ihre Sicherheitslage. Mit der Lösung erhalten Sie eine unveränderliche Quelle für zuverlässige historische Identitätsdaten und telemetrische Aufzeichnungen geänderter Identitäten. Das unveränderliche Protokoll mit Zuordnung von Aktivitäten erleichtert zudem Compliance-Prüfungen und forensische Untersuchungen.
- 2. Kontinuierliche Systemverfügbarkeit:** Die Lösung ermöglicht die Nachverfolgung von Identitätsänderungen, Störungsüberwachung, Ursachenanalysen und das Zurücksetzen von Konfigurationen. So kann das IAM-Team Fehler im Identitätsmanagement schneller erkennen, diagnostizieren und beheben. Mit nur wenigen Klicks lassen sich Ausfallzeiten und betriebliche Risiken reduzieren sowie die Response- und Recovery-Prozesse in AD, Entra ID und Okta beschleunigen.
- 3. Schnellere Incident Response:** Reduzieren Sie den Stress beim Datenabgleich zwischen verschiedenen Tools. Sie müssen die zahlreichen Logdateien nicht mehr manuell zusammenfügen und können dennoch nachvollziehen, wie sich Bedrohungen in Ihren Systemen ausbreiten. Manipulationen können Sie direkt über das Produkt rückgängig machen, während legitime Änderungen erhalten bleiben und persistente Angriffe abgewehrt werden.
- 4. Geringere Gesamtbetriebskosten:** Reduzieren Sie die Lizenz-, Wartungs- und Schulungskosten, die durch den Einsatz separater Backup- und Sicherheitstools für AD, Entra ID und Okta entstehen. Ersetzen Sie isolierte Punktlösungen durch eine zentrale Plattform mit überschaubaren Lizenzkosten und geringerem Verwaltungsaufwand.
- 5. Erhalt legitimer Änderungen:** Sie können einen sauberen Zustand wiederherstellen und anschließend alle legitim geänderten Identitäten übernehmen. So werden Persistenzmechanismen beseitigt und Updates der Identitätssysteme aus den Vormonaten beibehalten.

EINFACHER SCHUTZ VON AD-, ENTRA ID- UND OKTA-UMGEBUNGEN MIT EINER MULTI-IDP-LÖSUNG

- 1. Zentrale Plattform für einheitlichen Schutz:** Sichern Sie Ihre gesamte Identitätslandschaft einschließlich lokaler AD-Objekte und cloudnativer Okta-Implementierungen über eine intuitive Konsole, die speziell für komplexe Umgebungen entwickelt wurde.
- 2. Präzise orchestrierte Wiederherstellung:** Komplexe Abhängigkeiten verlieren ihren Schrecken. Ganz gleich, ob Sie ganze AD-Mandanten oder einzelne Okta- und Entra ID-Objekte wiederherstellen müssen – mit Rubrik sind Ihre Systeme von Anfang an korrekt konfiguriert.
- 3. Betriebliche Kontinuität:** Vereinfachen Sie die Wiederherstellung Ihrer Identitätsumgebung. Sie können feststellen, ob ein Identitätsanbieter kompromittiert wurde, jeden Fehler isolieren und die Systemverfügbarkeit für Anwendungen und Benutzer mit nur wenigen Klicks wiederherstellen und aufrechterhalten.
- 4. Manipulationssichere Architektur:** Die hochsichere Architektur von Rubrik schützt kritische Identitätsdaten durch logische Air Gaps und ermöglicht unveränderliche, manipulationssichere Backups.



SICHERN SIE DIE ZUKUNFT IHRER IDENTITÄTSSYSTEME

Die zunehmende Komplexität von Identitätsumgebungen und identitätsbasierten Angriffen treibt die Kosten der Fragmentierung in neue Höhen. Mit Rubrik Identity Resilience stellen Sie sicher, dass Ihre Systeme stets vertrauenswürdig, betriebsbereit und wiederherstellbar sind. Damit gewährleisten Sie einen kontinuierlichen Zugriff auf Ihre Ressourcen. Sie können Vorfälle untersuchen und die Identitätsinfrastruktur auch in hybriden Umgebungen wiederherstellen. Rubrik verringert das Risiko persistenter Angriffe und übernimmt legitime Änderungen an Identitätsdaten, sodass Sie Identitäten einwandfrei wiederherstellen können, ohne die Ergebnisse monatelanger Arbeit zu verlieren. Mit Rubrik bleiben Ihre Systeme stets sauber und aktuell.

Fordern Sie eine Demo an und überzeugen Sie sich von den Vorteilen der orchestrierten Wiederherstellung von Identitäten.

SAFE-HARBOR-ERKLÄRUNG: In diesem Dokument angeführte unveröffentlichte Services oder Funktionen sind derzeit nicht verfügbar. Ob und wann diese allgemein bereitgestellt werden, liegt im Ermessen von Rubrik. Die angeführten Services oder Funktionen stellen keine Lieferversprechen, Zusagen oder Verpflichtungen von Rubrik, Inc. dar und können nicht vertraglich festgehalten werden. Kunden sollten ihre Kaufentscheidung auf Services und Funktionen stützen, die derzeit allgemein verfügbar sind.

HINWEIS: Kunden und Interessenten sollten vor einer Kaufentscheidung mit einem Vertreter von Rubrik sprechen, um die Verfügbarkeit und den Funktionsumfang der Produkte und Services von Rubrik zu bestätigen.