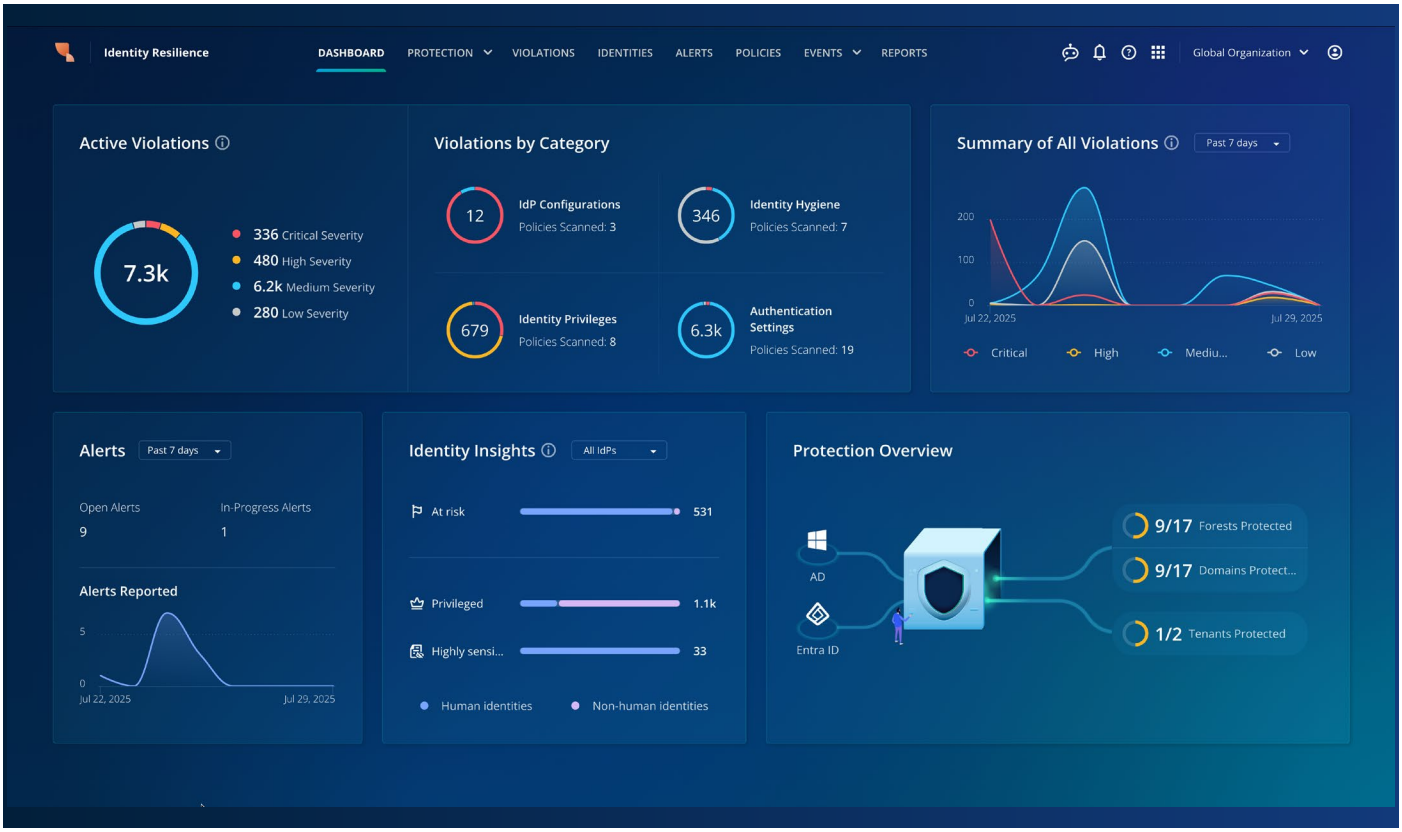
Rubrik Identity Resilience

Technischer Überblick

Angreifer haben Ihre Identitätsinfrastruktur im Visier.

Rubrik Identity Resilience unterstützt Unternehmen bei der Sicherung und Wiederherstellung ihrer Identitätssysteme vor, bei und nach einem Angriff. Die Lösung vereint Transparenz, Echtzeiterkennung und orchestrierte Wiederherstellung in einer zentralen Plattform, mit der Kunden kritische Änderungen bei Bedarf rückgängig machen, den Betrieb nach einem Vorfall schnell wieder aufnehmen, Risiken minimieren und ihre Resilienz gegenüber identitätsbasierten Angriffe stärken können.

Active Directory (AD) und Entra ID bilden in vielen Unternehmen die Grundlage für das Zugriffsmanagement, doch die Sicherung dieser Systeme – insbesondere in hybriden und Multi-Cloud-Umgebungen – ist über die Jahre immer komplexer geworden. Wenn dazu fragmentierte Tools, Skripte und Sicherheitsbewertungen zu individuellen Zeitpunkten genutzt werden müssen, können gefährliche Sicherheitslücken entstehen, die die ganze Infrastruktur anfällig für identitätsbasierte Angriffe machen. Wenn zudem die Untersuchung von Bedrohungen und die Entfernung der von Hackern genutzten Backdoors und Schwachstellen manuell erfolgen, gelingt es den Angreifern mitunter, sich ihren Systemzugriff zu erhalten. Ebenso problematisch ist eine manuelle Wiederherstellung, die die Wiederaufnahme des Betriebs hinauszögern und das Geschäftsrisiko somit steigern kann.



Identitätsbasierte Angriffsvektoren dominieren derzeit die Bedrohungslandschaft – bei über 80 % der Cyber-Vorfälle nutzen die Angreifer gestohlene Anmeldedaten oder falsch konfigurierte Zugriffskontrollen, um in ein System einzudringen, sich darin auszubreiten, ihre Privilegien auszuweiten und den Geschäftsbetrieb zu beeinträchtigen. APT-Gruppen wie Scattered Spider suchen gezielt nach solchen Fehlkonfigurationen und Lücken in der Überwachung und nutzen sie aus, um Netzwerke auszukundschaften und dabei konventionelle Sicherheitstools zu umgehen.

Fragmentierte IT-Sicherheits-Stacks tragen maßgeblich zu diesem Problem bei, denn sie bieten weder integrierte Echtzeittelemetrie noch plattformübergreifenden Einblick in den Status und das Verhalten von Identitäten. Außerdem bieten

die meisten konventionellen Lösungen keine Funktionen, mit denen unbefugte Änderungen an Identitätseinstellungen oder die nicht autorisierte Gewährung von Zugriffsrechten rückgängig gemacht oder der Zustand vor der Änderung wiederhergestellt werden können. Infolgedessen müssen Identitäten oft manuell und mithilfe potenziell kompromittierter System-Backups oder unvollständiger, nicht schreibgeschützter Audit-Protokolle wiederhergestellt werden.

Ohne integrierte, robuste Identitätssicherheit mit Funktionen für die kontinuierliche Durchsetzung von Richtlinien, manipulationssichere Überwachung und orchestrierte Wiederherstellung bleiben Unternehmen anfällig für die immer häufiger auftretenden identitätsbasierten Bedrohungen. Diese können nicht nur Betriebsstörungen verursachen, sondern auch dazu führen, dass Angreifer längere Zeit unbemerkt Zugang zu Ihren Umgebungen haben.

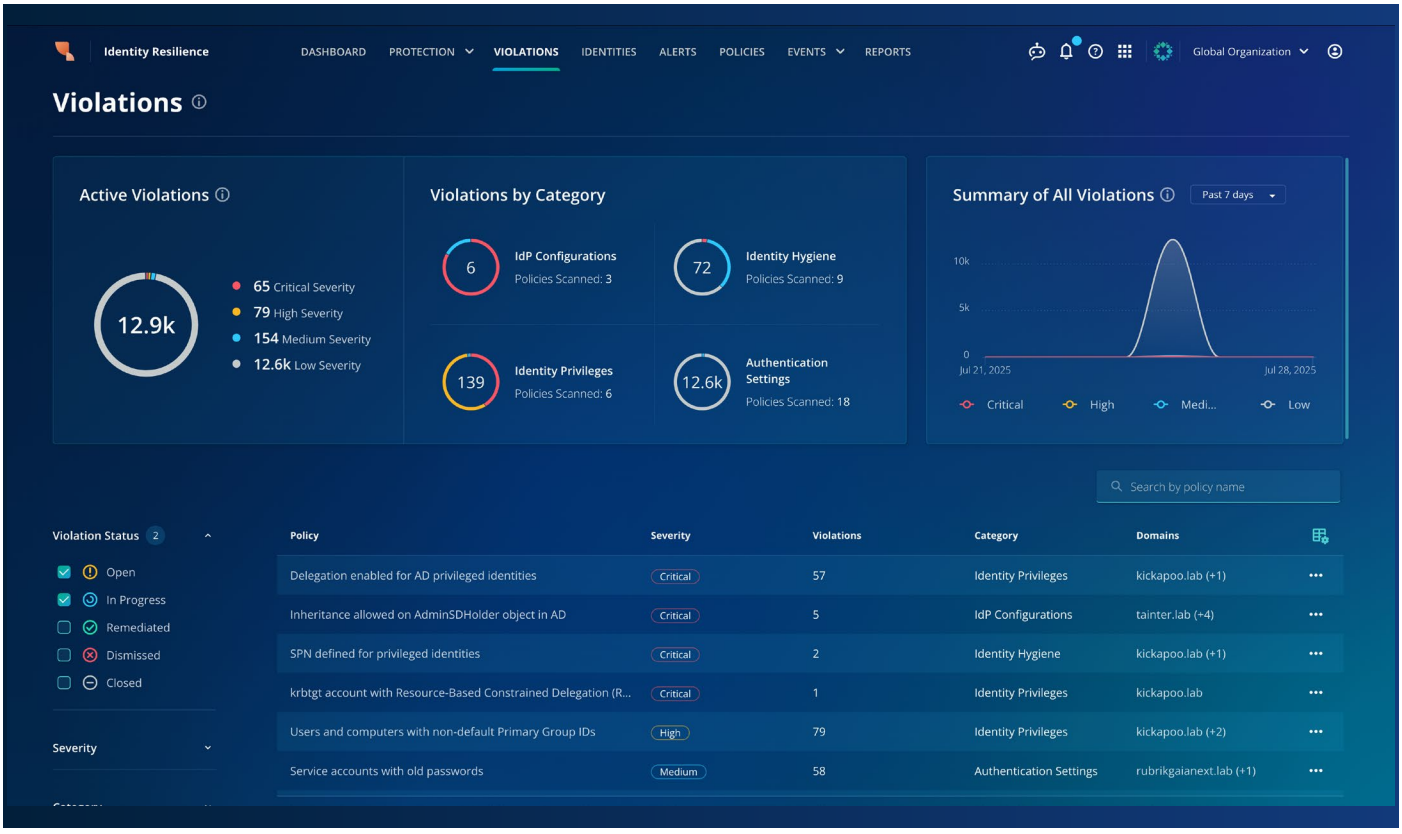
Rubrik Identity Resilience trägt mit einem umfassenden Überblick über die gefährlichsten potenziellen Angriffspunkte einer Infrastruktur zur Behebung dieses Problems bei. Außerdem überwacht die Lösung ihre Umgebung kontinuierlich und erkennt kritische Systemänderungen, die auf eine laterale Ausbreitung oder eine nicht autorisierte Ausweitung von Zugriffsrechten hindeuten, nahezu in Echtzeit. Dadurch können Risiken und potenzielle Einfallstore rasch behoben und Eindringlinge ausgesperrt werden, bevor sie weiteren Schaden anrichten.

EINHEITLICHES IDENTITÄTSINVENTAR

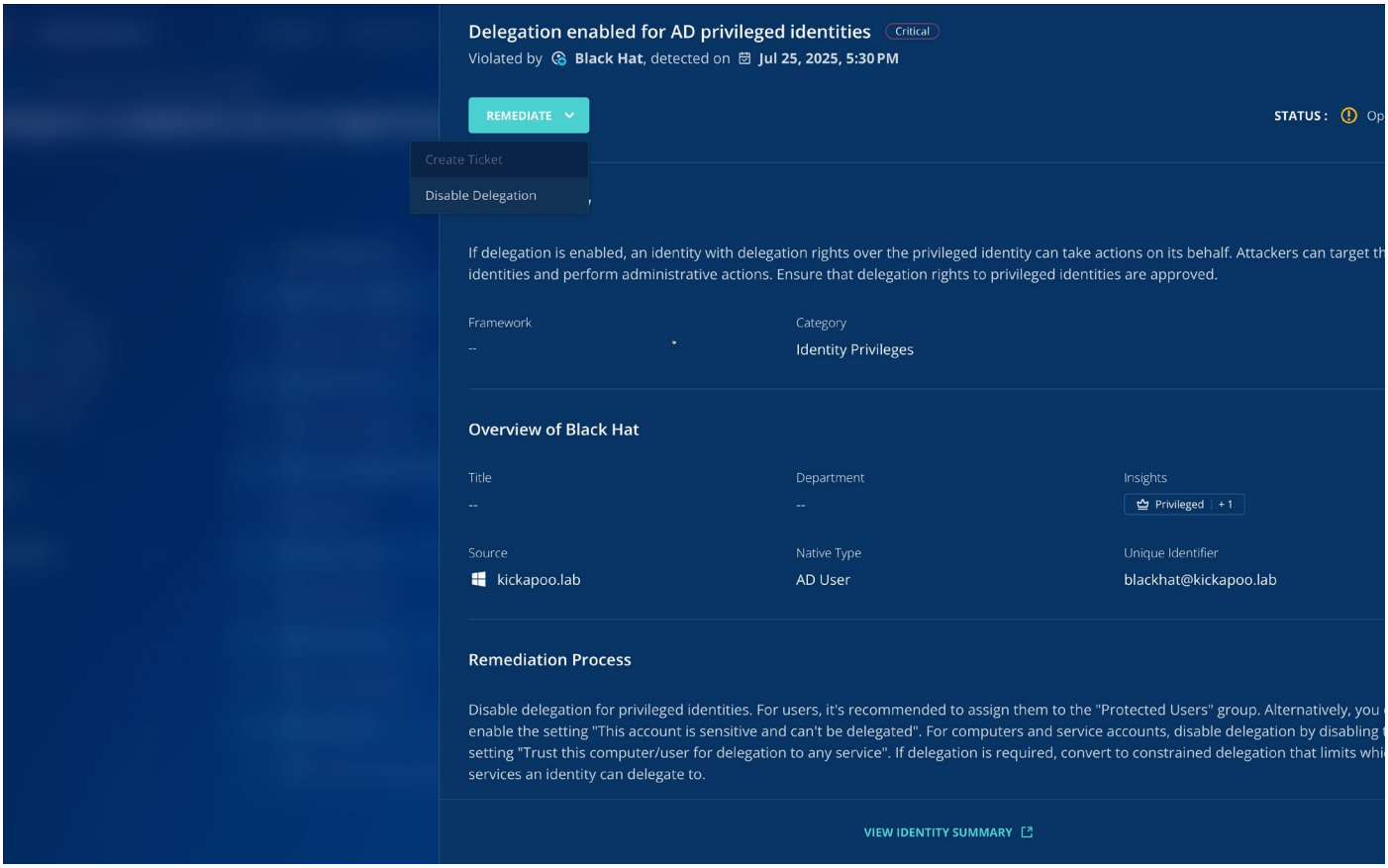
Obwohl die Cloud- und Multi-Cloud-Nutzung zunehmen, investieren viele Unternehmen gleichzeitig weiterhin in lokale Infrastrukturen und beziehen ihre Identitätsservices daher von mehreren unterschiedlichen Anbietern. Mit Rubrik Identity Resilience profitieren Kunden von einem einzigen, einheitlichen Inventar und somit einem anbieterübergreifenden Überblick über alle menschlichen und sonstigen Identitäten sowie in die mit ihnen einhergehenden Risiken und Warnmeldungen. In Kombination mit Rubrik DSPM werden zusätzlich Informationen zu den sensiblen Daten bereitgestellt, auf die eine Identität Zugriff hat. Somit kann die Sicherung von Identitäten nicht nur nach Zugriffsrechten, sondern auch nach dem Risiko für sensible Datenbestände priorisiert werden.

RICHTLINIENGESTÜTZTE RISIKOERKENNUNG FÜR IDENTITÄTEN

Rubrik Identity Resilience erstellt ein umfassendes, anbieterübergreifendes Inventar sämtlicher menschlicher und sonstiger Identitäten, das mit jedem neuen Snapshot aktualisiert wird. Eine leistungsfähige Richtlinien-Engine überprüft die Konfigurationsdetails kontinuierlich auf potenzielle Verstöße gegen geltende Richtlinien. Identity Resilience wird mit einsatzbereiten Richtlinien für bekannte Sicherheits- und Best Practice-Frameworks wie MITRE ATT&CK, D3FEND, OWASP und ANSSI geliefert. Diese Richtlinien lassen sich bei Bedarf über sämtliche Identitätsanbieter hinweg vereinheitlichen und unter anderem für privilegierte Identitäten mit Delegationsrechten, Benutzer mit schwacher oder ohne MFA-Durchsetzung sowie Service-Accounts mit alten Passwörtern, die offenbar nicht regelmäßig geändert werden, nutzen.



Richtlinienverstöße werden in der Benutzeroberfläche aufgezeigt, mit der Option, ein Ticket in einem ITSM-Tool wie ServiceNow zu erstellen und den Verstoß, wo möglich, direkt beim Identitätsanbieter zu beheben. Außerdem können Sicherheitsverstöße über Webhooks an SIEM- oder SOAR-Tools gemeldet werden, wo sie automatisch geeignete Workflows auslösen.

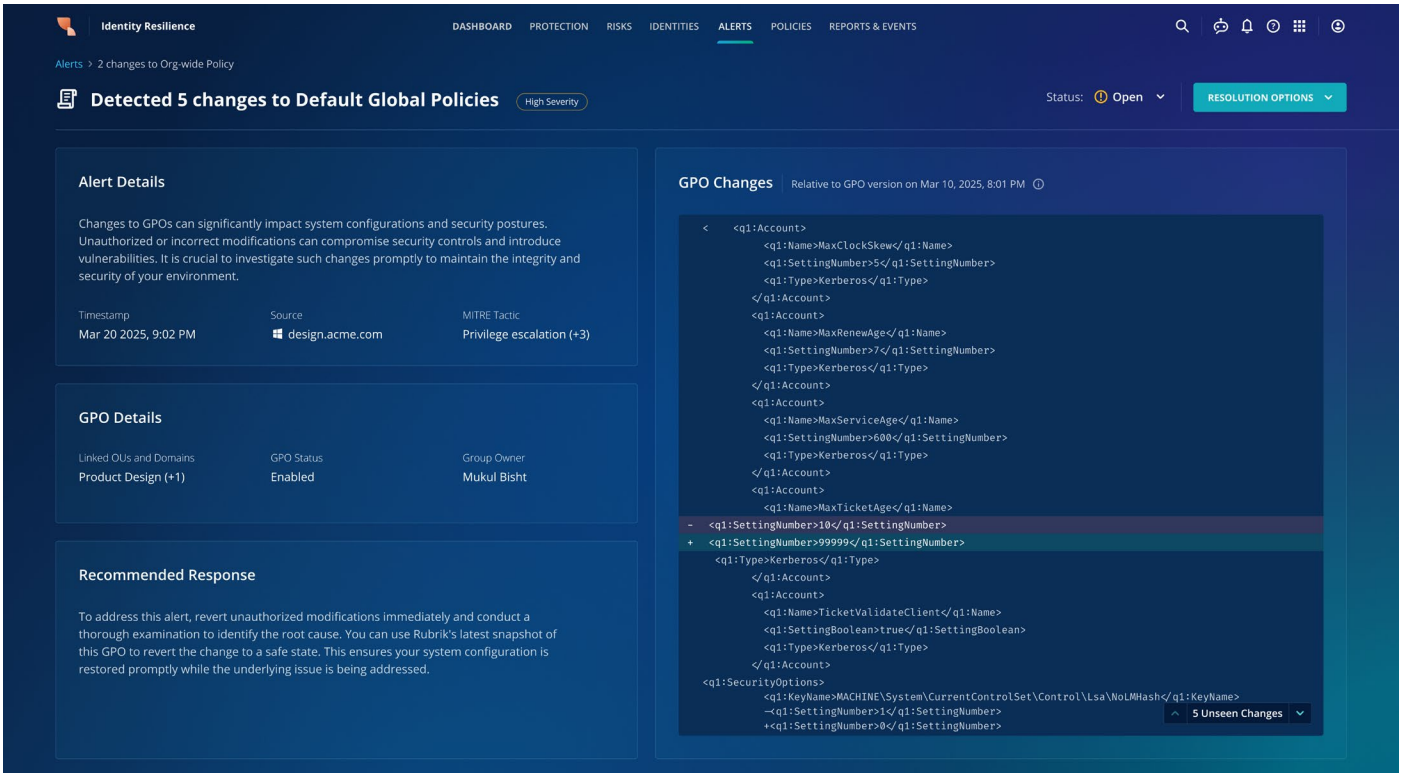


ÜBERWACHUNG AUF KRITISCHE ÄNDERUNGEN NAHEZU IN ECHTZEIT

Einige Überwachungstools scannen Windows-Ereignisprotokolle auf verdächtige Aktivitäten oder nutzen dazu Windows Event Forwarding (WEF). Leider ist das vielen Hackern bekannt und sie wissen außerdem, dass sie Protokolldateien bei Bedarf leicht mit anderen Daten überschreiben oder einfach löschen können, um ihre Spuren zu verwischen. Ohne robustes Ereignis-Tracking kann es nahezu unmöglich sein, schädliche Aktivitäten in Protokolldateien zu identifizieren.

Rubrik Identity Resilience scannt nicht nur Windows-Ereignisprotokolle, sondern führt zusätzlich eine kontinuierliche Überwachung von Active Directory-Umgebungen durch. Dieser einzigartige Ansatz ist manipulationssicher, was es für Hacker erheblich schwieriger macht, unentdeckt in einer Umgebung zu verweilen. Sobald Ereignisdaten vom Identitätsanbieter auf die Rubrik-Plattform übertragen werden, sind sie ebenso unveränderlich wie in Rubrik-Backups gespeicherte Daten. Dies gewährleistet die Integrität der Ereignisdaten.

Werden verdächtige Aktivitäten – wie eine nicht autorisierte Ausweitung von Zugriffsrechten oder die Bearbeitung von Group Policy Objects (GPOs) – erkannt, wird eine Warnmeldung generiert, um die Vorfallseinschätzung und -behebung einzuleiten.



Warnung und Reaktion

Warnmeldungen nahezu in Echtzeit: Verdächtige Aktivitäten lösen Warnmeldungen aus, die detaillierte Kontextinformationen zu den im Vorfall involvierten Identitäten und betroffenen Ressourcen sowie Zeitstempel und empfohlene Maßnahmen beinhalten.

Integration in ITSM-Plattformen: Bedrohungen und Verstöße gegen Sicherheitsrichtlinien können die Erstellung von Tickets in einer ITSM-Plattform auslösen. In Rubrik Identity Resilience ist eine sofort einsatzbereite API-Integration für ServiceNow ITSM enthalten.

Webhook-Integration: Warnmeldungen und Ereignisse können über Webhooks an SIEM- und SOAR-Tools geschickt werden und dort Workflows für die Einschätzung und Eindämmung auslösen.

WIEDERHERSTELLUNG VON IDENTITÄTSANBIETERN

Rubrik Identity Resilience ist ein leistungsstarkes Tool für die Reduzierung des Cyber-Risikos, Erkennung verdächtiger Aktivitäten und Unterbindung schädlicher Aktionen. Trotzdem sollten Unternehmen auf den Ernstfall vorbereitet sein, eine entsprechende Strategie entwickeln und im Zweifelsfall davon ausgehen, dass sie es mit einem Angriff zu tun haben. Rubrik Identity Recovery ist in Identity Resilience inbegriffen und ermöglicht eine umfassende Wiederherstellung von Active Directory-, Entra ID- und hybriden Umgebungen. Mit einem solchen strategischen Ansatz sind Organisationen gut aufgestellt, ihre Angriffsfläche und somit das Geschäftsrisiko durch ein proaktives Identitätsmanagement zu reduzieren und ihre Umgebungen im Falle eines Cyber-Angriffs effektiv wiederherzustellen.

ARCHITEKTUR UND BEREITSTELLUNG DER LÖSUNG

Sicherheit und Compliance

- Granulare rollenbasierte Zugriffskontrollen können genutzt werden, um Benutzern oder Rollen nur Zugriff auf Identity Resilience und nicht auf andere Rubrik-Funktionen zu gewähren. (Dies empfiehlt sich für IAM- und GRC-Teams.) Umgekehrt können zum Beispiel Backup-Administratoren nur Zugriff auf die Funktionen von Rubrik und nicht auf die von Identity Resilience gewährt bekommen.
- Kunden stehen eine zertifizierte, konforme Plattform und ein Support-Team zur Verfügung. Weitere Informationen zum Thema Compliance in Rubrik Security Cloud erhalten Sie unter https://www.rubrik.com/compliance-program.
- Daten werden im Ruhezustand und bei der Übertragung verschlüsselt und es werden strenge rollenbasierte Zugriffskontrollen (RBAC) für Administratoren durchgesetzt.

- Backup-Daten werden auf der Plattform im unveränderlichen Zustand gespeichert und dienen somit als sichere Kopien für die Wiederherstellung.

Unterstützung für hybride Umgebungen

- Der Rubrik Backup Service wird auf Domänencontrollern bereitgestellt, um AD-Daten zu erfassen und wo nötig AD-Backups zu erstellen, ohne sensible Anmeldedaten offenzulegen oder weitreichende Netzwerkänderungen zu erfordern.
- Daten zu AD-Vorfällen werden im Cluster innerhalb des Rechenzentrums des Kundenunternehmens verarbeitet und Metadaten werden zur weiteren Verarbeitung in die Rubrik Security Cloud übertragen.
- Bei Entra ID verläuft das Onboarding durch die einmalige Anmeldung über einen Administrator-Account, um einen Dienstprinzipal (Unternehmensanwendung) mit nur den nötigsten Zugriffsrechten zu erstellen.
- Definitionen und Warnmeldungen für Sicherheitsrichtlinien werden an zentraler Stelle zusammengeführt, was die Governance von lokalen, hybriden und Multi-Cloud-Bereitstellungen vereinfacht.
- Die Wiederherstellung von Active Directory-Umgebungen wird Cluster-übergreifend orchestriert, sodass Unternehmen lokale Backups erstellen und die Wiederherstellung über eine einzige Benutzeroberfläche verwalten können.

Benutzerfreundliche, globale Kontrollebene

- Eine preisgekrönte, benutzerfreundliche Oberfläche für die Verwaltung von Identitäten und dem Datensicherheitsniveau sowie die Sicherung und Wiederherstellung von Daten und Identitäten
- Funktionen für eine umfassende, orchestrierte Wiederherstellung kritischer Services (unter anderem für Identitäten und Daten) im Falle eines erfolgreichen Cyber-Angriffs
- Cyber-Resilienz der Enterprise-Klasse, die von über 4.000 Kunden weltweit für die Sicherung ihrer Identitätsservices genutzt wird

VERSCHIEDENE SICHERUNGSSTUFEN

Derzeit vertrauen über 4.000 Kundenunternehmen für die Sicherung ihrer Identitätsservices auf die jahrelange Erfahrung von Rubrik. In der folgenden Tabelle wird der Funktionsumfang verschiedener Rubrik-Produkte für die Identitätssicherung aufgeführt, darunter auch von Identity Resilience.

	Rubrik Foundation/ Business/ Enterprise Edition	Rubrik Identity Recovery	Rubrik Identity Resilience (inklusive Identity Recovery)
Sicherung und Wiederherstellung von Active Directory(AD)-Benutzern, -Gruppen und -Domänencontrollern	✓	✓	✓
Sicherung und Wiederherstellung von Entra ID-Benutzern, -Gruppen und -Rollen	✓	✓	✓
Granulare Wiederherstellung von AD- und Entra ID-Objekten	✓	✓	✓
Orchestrierte Wiederherstellung ganzer AD Forests		✓	✓
Vergleich und Wiederherstellung von AD-Objekteigenschaften		✓	✓
Hybride Wiederherstellung für hybride AD- und Entra ID-Umgebungen		✓	✓
Einheitliches Inventar menschlicher und sonstiger Identitäten über alle Identitätsanbieter hinweg			✓
Richtlinienbasierte Erkennung von Risiken in Identitätsservices und -konfigurationen			✓
Behebung aufgedeckter Risiken in der Anwendung			✓
Warnmeldungen nahezu in Echtzeit bei kritischen Änderungen oder verdächtigen Aktivitäten und manipulationssichere Überwachung			✓

ZUSAMMENFASSUNG

Rubrik Identity Resilience nutzt eine Kombination aus robuster, manipulationssicherer Vorfallsüberwachung und einer umfassenden, richtliniengestützten Engine, um mehrschichtige Sicherheit für Unternehmensidentitäten in Microsoft AD- und Entra ID-Umgebungen zu bieten.

Die Lösung validiert kontinuierlich die Konfigurationskonformität, erkennt anomale Aktivitäten nahezu in Echtzeit und stellt praktische Einblicke und In-App-Behebungsfunktionen zur Verfügung. So unterstützt sie Unternehmen beim proaktiven Risikomanagement für ihre Identitätsservices, der Sicherung der kritischsten Ressourcen und der Stärkung der betrieblichen Resilienz.

rubrik

Hauptsitz
3495 Deer Creek Road
Palo Alto, CA 94304
USA

+1-844-478-2745
inquiries@rubrik.com
www.rubrik.com/de

brf-rubrik-identity-resilience-Rubrik_IDML-de-DE#DTP_DDDNUW# / 20251203