rubrik | Zero Trust Data Security™

WHITEPAPER

Die vertrauenswürdige Datensicherheitslösung für Cyber-Wiederherstellung

Inhalt

CYBERANGRIFFE: EIN ALLGEGENWÄRTIGES UND WACHSENDES RISIKO

Die digitale Transformation hat Unternehmen erhebliche Vorteile gebracht, darunter mehr Agilität und Flexibilität, aber sie hat auch bewirkt, dass es mehr Angriffsflächen für Cyberangriffe gibt. Laut einer Sophos-Umfrage im Jahr 2022 wurden 66 % der Unternehmen im letzten Jahr Ziel eines Ransomware-Angriffs. Die weiträumige Einführung von Cloud-Services und SaaS-Anwendungen (Software-as-a-Service) hat die Angriffsfläche vergrößert und die Verwaltung und Sicherung von Daten erschwert. Darüber hinaus haben es Cyberkriminelle durch den zunehmenden Einsatz von mobilen Geräten und Remote-Arbeit leichter, von überall aus und zu jeder Zeit Angriffe zu starten.

DIE AUSWIRKUNGEN VON RANSOMWARE AUF UNTERNEHMEN

Ransomware-Angriffe können Unternehmen lähmen. Lösegeldzahlungen können mehrere Millionen Dollar kosten, ohne dass es eine Garantie dafür gibt, dass die betroffenen Daten nach Zahlung des Lösegelds wiederhergestellt werden können. Angriffe können nicht nur Kosten für das Lösegeld selbst verursachen, sondern auch Ausfallzeiten, Umsatzeinbußen, Wiederherstellungskosten, Rufschädigung, Compliance-Anforderungen, Reputationsverlust bei Kunden, höhere Cyber-Versicherungsprämien und vieles mehr. Alles in allem liegen die Gesamtkosten oft in Millionenhöhe, und die vollständige Wiederherstellung kann Wochen bis Monate dauern. Ransomware hat im Jahr 2021 weltweit Kosten in Höhe von 20 Mrd. Dollar verursacht und man geht davon aus, dass dieser Wert bis 2031 auf 265 Mrd. Dollar steigen wird. Was das bedeutet, liegt auf der Hand: Wenn die Daten eines Unternehmens nicht verfügbar sind, läuft auch das Geschäft nicht.

HERKÖMMLICHE BACKUPS IM HINBLICK AUF CYBER-WIEDERHERSTELLUNG NICHT ZUVERLÄSSIG

Viele Unternehmen setzen immer noch auf herkömmliche Backups als letztes Bollwerk der Cybersicherheit. In diesen Systemen fehlen jedoch oft wichtige Sicherheitsfunktionen und sie sind nicht für den Schutz vor modernen Cyber-Bedrohungen ausgelegt. Neben all den Schwächen und Unzulänglichkeiten von herkömmlichen Backups gibt es einige weitere Gründe, weshalb sie im Hinblick auf die Cyber-Wiederherstellung nicht zuverlässig sind:

- Herkömmliche Backups sind anfällig für Cyberangriffe. Unternehmen, die auf herkömmlichen Backup setzen, verwenden häufig offene Speicherprotokolle, wodurch die Gefahr besteht, dass Hacker unerlaubt auf ihre Daten zugreifen und diese manipulieren. Besonders problematisch ist dies in Kombination mit Windows-Betriebssystemen und einer nicht implementierten oder nicht durchgesetzten Multi-Faktor-Authentifizierung. Ohne angemessene Authentifizierungs- und Zugangskontrollen können Cyberangreifer Schwachstellen in diesen Systemen ausnutzen, um unbefugten Zugang zu sensiblen Daten zu erlangen und die Sicherheitslage eines Unternehmens zu kompromittieren.
- Herkömmliche Backups bieten keine wichtigen Einblicke oder Transparenz dahingehend, welche Daten gefährdet sind oder von einem Cyberangriff betroffen waren. Dadurch können Unternehmen nicht schnell und effektiv auf den Vorfall reagieren. Die Aufgabe, festzustellen, welche Daten verloren gegangen sind oder beschädigt wurden, kann erdrückend sein und Wochen oder sogar Monate in Anspruch nehmen, wodurch sich kostspielige Ausfallzeiten verlängern können.
- Herkömmliche Backups wurden entwickelt, um einzelne Dateien, virtuelle Maschinen oder Datenbanken von einem bekannten Zeitpunkt im Zusammenhang mit einer Katastrophe wiederherzustellen. Bei der Cyber-Wiederherstellung kann es jedoch sehr schwierig sein, festzustellen, was wiederhergestellt werden muss, wann der Angriff stattfand, wie weit der Angreifer vorgedrungen ist und wie groß der Schaden ist, den er verursacht hat. Dieses Zusammentragen von Informationen ist sehr zeitaufwendig und kann den Wiederherstellungsprozess erheblich verzögern.

- Cyber-Wiederherstellung erfordert auch ein ganz neues Maß an Aufmerksamkeit im Hinblick auf sensible Daten. Anders als bei herkömmlichen Backups ist es für die Cyber-Wiederherstellung von entscheidender Bedeutung, den Umfang des Angriffs und die potenzielle Gefährdung sensibler Daten zu bestimmen, insbesondere wenn Unternehmen, wie beispielsweise im Zusammenhang mit der DSGVO, verpflichtet sind, Compliance-Stellen zu informieren.
- Herkömmliche Backups bieten keinen Schutz vor einer erneuten Infektion mit Malware. In einem Cyber-Wiederherstellungs-Szenario kann das Wiederherstellen von Backups, die Malware enthalten, in einer sauberen Umgebung bewirken, dass der Angriff erneut ausgelöst wird, was zu noch mehr Schäden und Datenverlusten führen kann. Die Folgen eines solchen Angriffs können für Unternehmen verheerend sein und bedeuten, dass sie auf Monate oder sogar Jahre hinaus Geld und Kundenvertrauen verlieren.
- Und schließlich bieten herkömmliche Backup-Systeme Unternehmen nicht die Möglichkeit, ihre Wiederherstellungsprozesse zu simulieren und zu testen, was sie im Falle eines Cyberangriffs in eine prekäre Lage bringt. Unternehmen müssen sich auf Glück oder Zufall verlassen, um ihre Systeme vollständig wiederherstellen zu können, was zu Datenverlusten, Systemausfallzeiten und erheblichem Imageschaden führen kann.

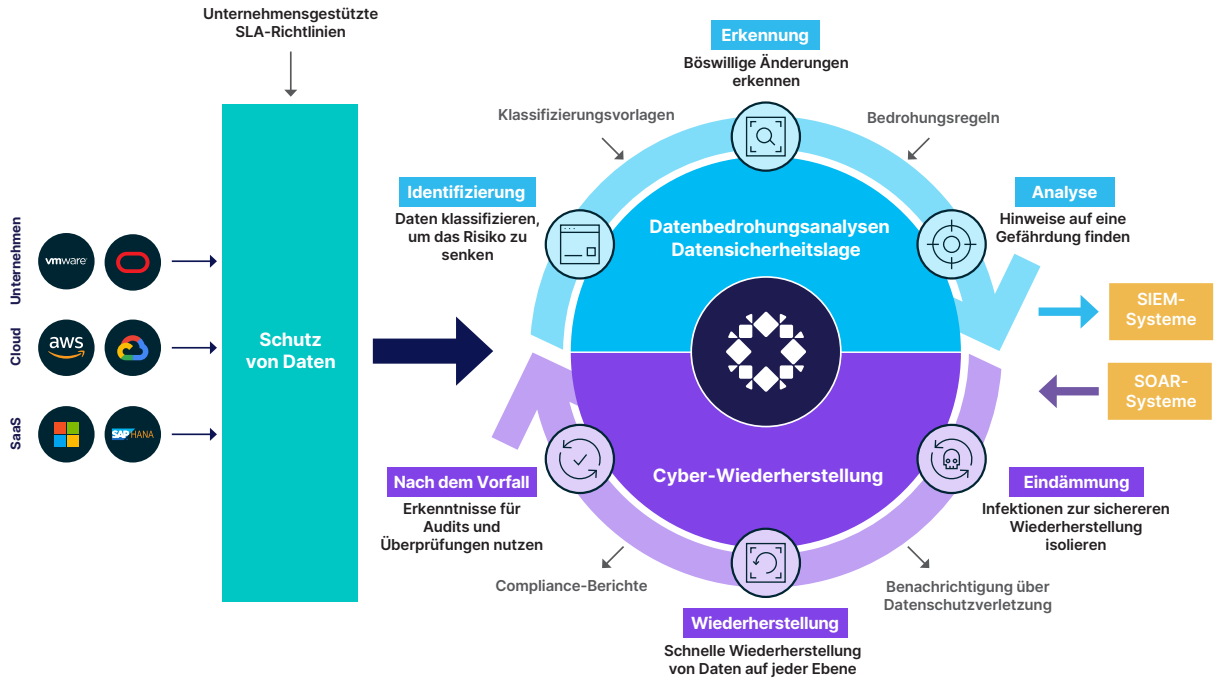
Herkömmliche Backup-Systeme sind modernen Cyber-Bedrohungen ganz offensichtlich nicht gewachsen. Im heutigen wettbewerbsintensiven Umfeld können es sich Unternehmen nicht leisten, bei der Cyber-Wiederherstellung auf Zeit zu spielen, sondern müssen in Lösungen investieren, die speziell für die Cyber-Wiederherstellung entwickelt wurden, um langfristig erhebliche Probleme zu vermeiden.

DATENSICHERHEIT: DER ANSATZ DER WAHL BEI CYBER-WIEDERHERSTELLUNG

Angesichts dieser dynamischen Bedrohungslandschaft müssen Unternehmen jederzeit auf Datenschutzverletzungen vorbereitet sein. Daten zu sichern, ist die einzige Möglichkeit für ein Unternehmen, sein Geschäft wirklich zu schützen, insbesondere in einer Zeit, in der Ransomware eine so weit verbreitete Bedrohung darstellt, die sich für Angreifer nach wie vor finanziell lohnt. IT- und Cybersicherheitsteams müssen sicherstellen, dass Daten verfügbar, geschützt und im Falle eines Vorfalls wiederherstellbar sind. Da Daten das Ziel von Angreifern sind, benötigen Unternehmen Sicherheit auf Datenebene – „Datensicherheit" –, um dafür zu sorgen, dass Daten dauerhaft sicher sind und schneller wiederhergestellt werden können.

Datensicherheit umfasst drei Säulen:

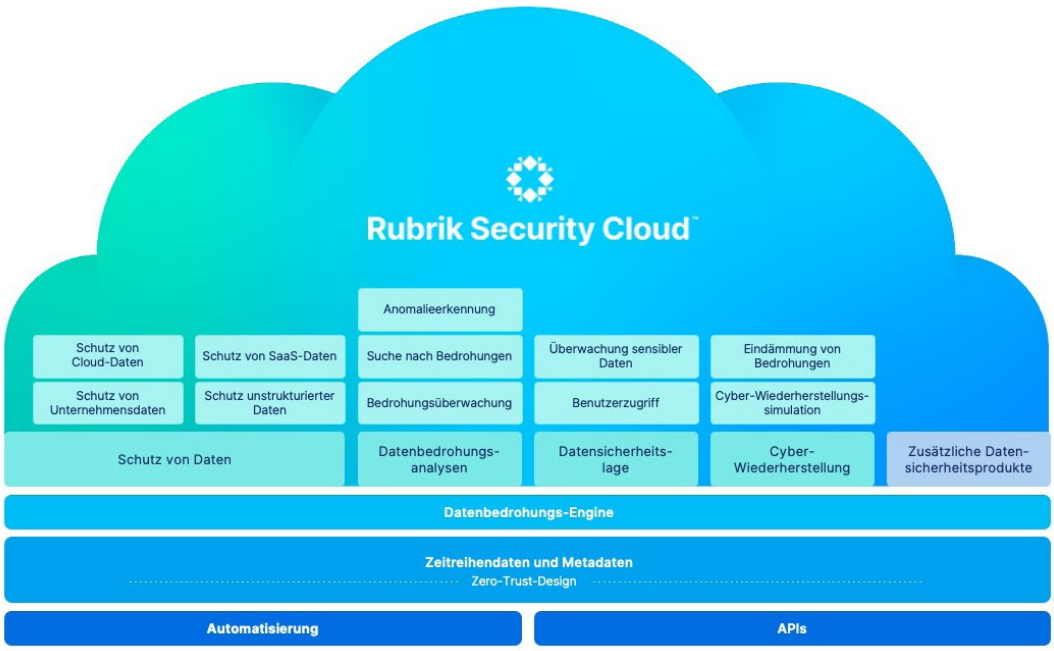
1. **Datenschutz** – Schützen Sie Ihre Daten vor Insider-Bedrohungen oder Ransomware mit per Air Gap getrennten, unveränderlichen, zugriffsgesteuerten Backups.
2. **Datenbedrohungsanalysen** – Überwachen Sie kontinuierlich Risiken für Ihre Daten, einschließlich Ransomware, Datenvernichtung und Indikatoren für eine Gefährdung.
3. **Datensicherheitslage** – Identifizieren und überwachen Sie die Gefährdung sensibler Daten und nutzen Sie intelligente Einblicke in Risiken, um die Datensicherheit zu maximieren.
4. **Cyber-Wiederherstellung –** Verbessern Sie Ihre Cyber-Bereitschaft und Ihre Reaktion auf Vorfälle durch einfaches Testen und Orchestrieren von Cyber-Wiederherstellungs-Workflows.



Datensicherheit sorgt für sichere Daten und erleichtert die Reaktion auf Cyberangriffe.

RUBRIK SECURITY CLOUD SCHÜTZT DATEN VOR CYBERANGRIFFEN, ÜBERWACHT KONTINUIERLICH DATENRISIKEN UND STELLT DATEN UND ANWENDUNGEN SCHNELL WIEDER HER.

Rubrik Security Cloud bietet Unternehmen einen zentralen Ort, an dem sie ihre Daten sichern können, egal wo sie gespeichert sind – sei es in Unternehmens-, Cloud- oder SaaS-Anwendungen.



Rubrik Security Cloud bietet Zero-Trust-Datensicherheit, die sich aus Datenschutz, der Analyse von Datenbedrohungen, der Datensicherheitslage und Cyber-Wiederherstellung zusammensetzt.

DATENSCHUTZ

Mit Rubrik können Unternehmen sicher sein, dass ihre kritischen Daten vor Löschung, Beschädigung oder Verschlüsselung geschützt sind. Denn dank per Air Gap geschützten, unveränderlichen, zugriffsgesteuerten Backups können sie Cyberangriffe, böswillige Insider und Betriebsunterbrechungen bewältigen.

Daten werden in einem unveränderlichen Format gespeichert und können nicht gelesen, geändert oder gelöscht werden. Außerdem werden Daten während der Übertragung und im Ruhezustand verschlüsselt, und Backup-Daten werden in einem speziellen Append-only-Dateisystem gespeichert.

Und schließlich sind die gesicherten Daten durch einen logischen Air Gap geschützt, d. h. sie sind offline und nicht über Standard-Netzwerkprotokolle zugänglich. Die Systemschnittstellen sind sicher, rollenbasiert und durch das Prinzip der geringstmöglichen Berechtigungen und durch Multifaktor-Authentifizierung (MFA) geschützt, um das Risiko eines erfolgreichen Angriffs weiter zu verringern.

Datenresilienz-Services umfassen:

- **Schutz von Unternehmensdaten –** zum Schutz Ihrer Unternehmensdaten vor Angriffen oder Katastrophen.
- **Schutz von Cloud-Daten –** um sicherzustellen, dass Ihre Cloud-Daten vor Kompromittierung geschützt sind.
- **Schutz von SaaS-Daten –** zum Sichern Ihrer SaaS-Anwendungsdaten mit automatisiertem Schutz.
- **Schutz unstrukturierter Daten –** zum Schutz, zur Überwachung und zur schnellen Wiederherstellung unstrukturierter Daten im Petabyte-Bereich.

DATENBEDROHUNGSANALYSEN

Unternehmen, die Rubrik nutzen, sind gut aufgestellt, um ihre Daten im Kampf gegen Ransomware einzusetzen. Das liegt daran, dass Rubrik die Zeitreihenhistorie der Daten im Längsschnitt erfasst. Zusätzlich verwaltet Rubrik Metadaten, einschließlich ihrer Inhalte, Benutzer und Zugriffsrechte. Durch das Scannen von Hunderten von Snapshots generiert die Datenbedrohungsanalyse-Engine von Rubrik Signale, die in ein umfassend trainiertes maschinelles Lernmodell eingespeist werden und eine historische Ausgangsbasis bilden, mit der neue Daten verglichen werden können, um anomale Änderungen, Löschungen und Verschlüsselungen zu finden.

Die Datenbedrohungsanalyse-Services umfassen:

- **Anomalie-Erkennung –** zum Ermitteln des Umfangs von Ransomware-Angriffen mithilfe von zuverlässigem maschinellem Lernen zur Erkennung von Löschungen, Änderungen und Verschlüsselungen.
- **Gefahrenüberwachung –** zum frühzeitigen Erkennen von Gefahren durch die automatische Identifizierung von Hinweisen auf eine Gefährdung innerhalb von Backups mithilfe eines aktuellen Feeds mit gesammelten Bedrohungsdaten.
- **Suche nach Bedrohungen –** zum Verhindern einer erneuten Malware-Infektion durch das Analysieren des zeitlichen Verlaufs der Daten auf Indikatoren für eine Gefährdung, um Ausgangspunkt, Umfang und Zeitpunkt der Infektion zu ermitteln.

DATENSICHERHEITSLAGE

Sensible Daten, die von der Datensicherheitslage-Engine erkannt werden, können mit zuvor gefundenen Datenanomalien in Beziehung gesetzt werden, um festzustellen, ob sensible Daten betroffen sind, was ein potenzielles Double-Extortion-Risiko darstellen könnte. Durch das Durchsuchen des Zeitreihenverlaufs von Daten nach Indikatoren für eine Beschädigung lässt sich die letzte bekannte saubere Kopie für Wiederherstellungsvorgänge leicht finden.

Zusätzlich können Unternehmen mit dem Data Security Command Center fortlaufend überprüfen, ob ihre von Rubrik verwalteten Daten sicher und nach einem Cyberangriff wiederhergestellt werden können. Über ein benutzerfreundliches Dashboard mit Risikobewertungen können sich IT- und Sicherheitsteams einen Überblick über Datenrisiken verschaffen, Sicherheitslücken identifizieren und umsetzbare Anleitungen erhalten, um ihre Daten sicherer zu machen.

Datensicherheitslage-Services umfassen:

- **Benutzerzugriff –** zum Verringern des Risikos einer Datengefährdung durch das Identifizieren und Begrenzen des Benutzerkreises, der Zugriff auf sensible Daten hat.
- **Überwachung sensibler Daten –** zum Verringern der Gefährdung sensibler Daten und um dem Risiko einer Datenexfiltration entgegenzuwirken, indem ermittelt wird, welche Arten von sensiblen Daten Sie haben und wo diese gespeichert sind.
- **Data Security Command Center –** zum Identifizieren von Sicherheitslücken, zum Ermitteln des Datenrisikos und zur Bereitstellung umsetzbarer Empfehlungen zur Verbesserung der Datensicherheitslage.

CYBER-WIEDERHERSTELLUNG

Mit den Cyber-Wiederherstellungsfunktionen von Rubrik können Unternehmen ihre Cyber-Bereitschaft und ihre Reaktion auf Vorfälle durch einfaches Testen, Validieren und Orchestrieren von Wiederherstellungs-Workflows verbessern. Mit Rubrik können Unternehmen testen, ob ihr Wiederherstellungsplan funktioniert, einschließlich des Ablaufs, des Zeitplans und der Schwachstellen. Unternehmen können außerdem Produktionsdaten in isolierten Wiederherstellungsumgebungen klonen, um Snapshots auf Malware zu untersuchen, und Sicherheitstools ihrer Wahl nutzen, um Bewertungen ihrer Cyber-Bereitschaft durchzuführen, beispielsweise Penetrationstests oder Red Teaming, ohne negative Auswirkungen auf die Produktion.

Rubrik ermöglicht es auch, Backups mithilfe von Dateimustern, Datei-Hashes und YARA-Regeln (Yet Another Recursive Acronym) zu scannen, um alle Objekte im Backup auf Anzeichen einer Kompromittierung zu untersuchen. Unternehmen können auch einen Zeitreihen-Verlauf von Backup-Snapshots analysieren, um saubere, nicht infizierte Snapshots für die Wiederherstellung zu ermitteln. Zusätzlich können sie die von Rubrik bereitgestellten Erkenntnisse nutzen, um Daten in beliebigem Umfang wiederherzustellen und dabei das Risiko eines erneuten Einbringens von Malware zu verringern.

Die Cyber-Wiederherstellungsfunktionen umfassen:

- **Eindämmung von Bedrohungen –** zum Sicherstellen einer sicheren und schnellen Datenwiederherstellung, indem mit Malware infizierte Daten unter Quarantäne gestellt werden.
- **Cyber-Wiederherstellungssimulation –** zum Verbessern der Cyber-Bereitschaft und der Reaktion auf Vorfälle durch das einfache Erstellen, Testen und Validieren von Cyberwiederherstellungs-Workflows.

Darüber hinaus ermöglichen Integrationen mit gängigen Sicherheitslösungen den Sicherheitsverantwortlichen, ihre bestehenden Tools (d. h. SIEM- und SOAR-Lösungen) zu nutzen, um die von Rubriks Datenbedrohungsanalyse- und Datensicherheitslage-Services generierten Warnungen anzuzeigen und Rubriks Workflows für Gefahrenüberwachung und -suche sowie für die Cyber-Wiederherstellung aufzurufen, ohne die Rubrik-Schnittstelle zu verwenden. Durch die Zusammenführung von Datenschutz und Datensicherheit in einer einzigen Plattform mit einer einheitlichen Kontrollebene und integrierten Workflows fördert Rubrik Security Cloud eine engere Zusammenarbeit zwischen IT- und Sicherheitsteams und trägt zu einer schnelleren Wiederherstellung nach Ransomware-Angriffen bei.

ZERO TRUST

Alle Rubrik Security Cloud-Funktionen folgen dem Zero-Trust-Prinzip, das besagt, dass Benutzern, Administratoren und dem Netzwerkverkehr nur dann vertraut wird, wenn sie gründlich authentifiziert sind. Dies trägt dazu bei, dass Daten entsprechend den vom National Institute of Standards and Technology (NIST) der US-Regierung festgelegten Standards durch Rubrik geschützt sind.

WARUM RUBRIK?

Rubrik Security Cloud ist die führende Datensicherheitsplattform und baut auf einer einzigartigen Backup-Architektur auf, die Daten sichert. Rubrik wendet Zero-Trust-Prinzipien an und setzt einen logischen Air Gap, sichere Protokolle, native Unveränderlichkeit, Verschlüsselung und Zugangskontrollen ein. Mit globaler richtliniengesteuerter Automatisierung hilft Rubrik dabei, die Verfügbarkeit von Daten, Richtlinienkonformität und optimierte Wiederherstellungs-Workflows sicherzustellen, während die Datenklassifizierungs-Engine die Gefährdung sensibler Daten aufzeigt und die Anomalie-Erkennungs-Engine eine schnellere Untersuchung von Bedrohungen und die Verhinderung einer erneuten Malware-Infektion ermöglicht. Darüber hinaus erleichtert die API-Erweiterungsfunktion die Zusammenarbeit mit funktionsübergreifenden Teams, indem sie eine gemeinsame Sicht auf Datenrisiken und Erkenntnisse über Bedrohungen für alle Tools bietet.

Der wichtigste wirtschaftliche Nutzen von Rubrik ist die Senkung der Kosten im Zusammenhang mit der Bekämpfung von Cyber-Bedrohungen. Die Datensicherheitsfunktion schützt Daten mithilfe von sicheren Backups. Datenbedrohungsanalysen erleichtern die Überwachung von Datenrisiken und beschleunigt die Untersuchung von Bedrohungen. Die Datensicherheitslage-Funktion trägt dazu bei, das Risiko einer Datengefährdung proaktiv zu verringern. Die Cyber-Wiederherstellung hilft, den Geschäftsbetrieb schneller wiederherzustellen.

ESTÉE LAUDER SICHERT GEFÄHRDETE DATEN FÜR WACHSENDES BEAUTY-IMPERIUM MIT RUBRIK

90 %+ Verkürzung der benötigten Zeit zum Sichern von Datenbanken mit mehr als 10 TB

Das Kosmetikunternehmen Estée Lauder besitzt mehr als 25 Beauty-Marken in 150 Ländern. Die IT-Abteilung des Unternehmens unterstützt mehr als 48.000 Mitarbeiter weltweit und schützt Daten im Umfang von mehreren Petabyte. Eine der größten Herausforderungen des Unternehmens ist die Anpassung an sich ändernde Daten und verschiedene Plattformen mit unterschiedlichen Betriebssystemen, insbesondere bei der Einführung und Übernahme neuer Marken. Das Unternehmen ist nun auf Standardisierungskurs, und Rubrik stellt dabei die einheitliche Datensicherheitsstruktur für alle Standorte und alle SLA-Anwendungsfälle dar und liefert verbesserte Backup-Leistung und schnellere Wiederherstellungszeiten. Außerdem bestanden bei Estée Lauder blinde Flecken in Bezug auf die eigenen gefährdeten sensiblen Daten und es fanden sich häufig PCI-Informationen in Dateien, in denen sie nicht hätten sein dürfen. Das Team nutzte die Datensicherheitslage-Engine von Rubrik, um die Speicherorte von Dateien mit sensiblen Daten zu erkennen, zu klassifizieren und zu melden, ohne die Produktion zu beeinträchtigen. Dadurch konnte das Unternehmen Maßnahmen ergreifen, um die sensiblen Daten zu entfernen und zu bereinigen, um sowohl Kunden- als auch Unternehmensdaten vor Offenlegung zu schützen.

ESTĒE LAUDER

Wir sind sehr beeindruckt von Rubriks Fähigkeit, Daten sofort wiederherzustellen. Während andere Lösungen ähnliche Funktionen anboten, hob sich Rubrik dadurch ab, wie einfach wir in der Lage waren, ein Backup zu erstellen und es sofort per Live-Mount verfügbar zu machen. Das war für uns ein wichtiges Verkaufsargument, und wir nutzen es ständig, um dafür zu sorgen, dass unsere Daten schnell verfügbar sind.

Pankaj Govil
Executive Director, Global Storage Infrastructure

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
USA

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

wp-the-trusted-data-security-solution-for-cyber-recovery_DE / 20240110