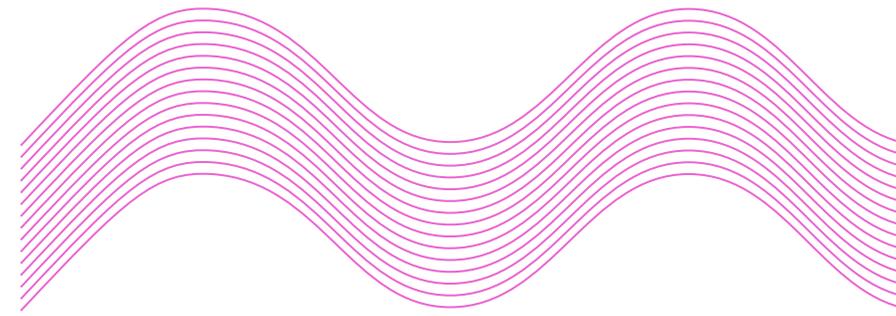


⚠ Die fünf Grundpfeiler effektiver Cyber-Resilienz für unstrukturierte Daten

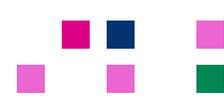
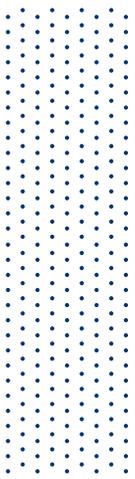
Warum herkömmliche Lösungen nicht ausreichen und welche Funktionen Sie für den zeitgemäßen Schutz Ihrer Daten benötigen.



INHALT



DAS EXPLOSIONSARTIGE WACHSTUM UNSTRUKTURIERTER DATEN.....	3
FÜNF UNVERZICHTBARE MERKMALE EINER LÖSUNG ZUM SCHUTZ UNSTRUKTURIERTER DATEN.....	5
Leistung im Petabyte-Umfang für den Schutz unstrukturierter Daten	5
Alle unstrukturierten Daten im Blick	6
Leistungsstarke Datensicherheit mit umfassender Anomalie-Erkennung	7
Identifizierung und Klassifizierung sensibler Daten	8
Präzise und effiziente Datenwiederherstellung	9
SCHÜTZEN SIE UNSTRUKTURIERTE DATEN AUF MODERNE WEISE.....	10



Rubrik (NYSE: RBRK) hat es zu seiner Mission gemacht, die Daten der Welt zu sichern. Mit Zero Trust Data Security™ helfen wir Unternehmen, sich vor Cyber-Angriffen, böswilligen Insidern und Betriebsunterbrechungen zu schützen. Rubrik Security Cloud basiert auf maschinellem Lernen und sichert Daten im Unternehmen, in der Cloud und in SaaS-Anwendungen. Wir unterstützen Unternehmen bei der Wahrung der Datenintegrität, der Sicherstellung der Datenverfügbarkeit auch unter widrigen Umständen, der kontinuierlichen Überwachung von Datenrisiken und -bedrohungen sowie der Wiederherstellung von Unternehmensdaten nach einem Angriff auf die Infrastruktur.

Weitere Informationen finden Sie unter www.rubrik.com/de, unter [@rubrikinc](https://twitter.com/rubrikinc) auf X (ehemals Twitter) sowie unter [Rubrik](https://www.linkedin.com/company/rubrik) auf LinkedIn.

Rubrik ist eine eingetragene Marke von Rubrik, Inc. Alle Firmennamen, Produktnamen und weiteren Bezeichnungen in diesem Dokument sind eingetragene Marken oder Marken des jeweiligen Unternehmens.



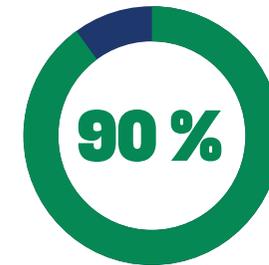
DAS EXPLOSIONSARTIGE WACHSTUM UNSTRUKTURIERTER DATEN

Die Menge der unstrukturierten Daten, also der Daten, die außerhalb von Datentools aufbewahrt werden, nimmt explosionsartig zu. Laut IDC sind 90 % aller Daten unstrukturiert – und ein Viertel der Unternehmen kann nach eigenen Angaben nicht mit der Geschwindigkeit des Datenwachstums mithalten.¹Das ist ein besorgniserregender Trend, da unstrukturierte Daten jede Menge sensibler Informationen enthalten, darunter geistiges Eigentum, personenbezogene Daten und Forschungsergebnisse.

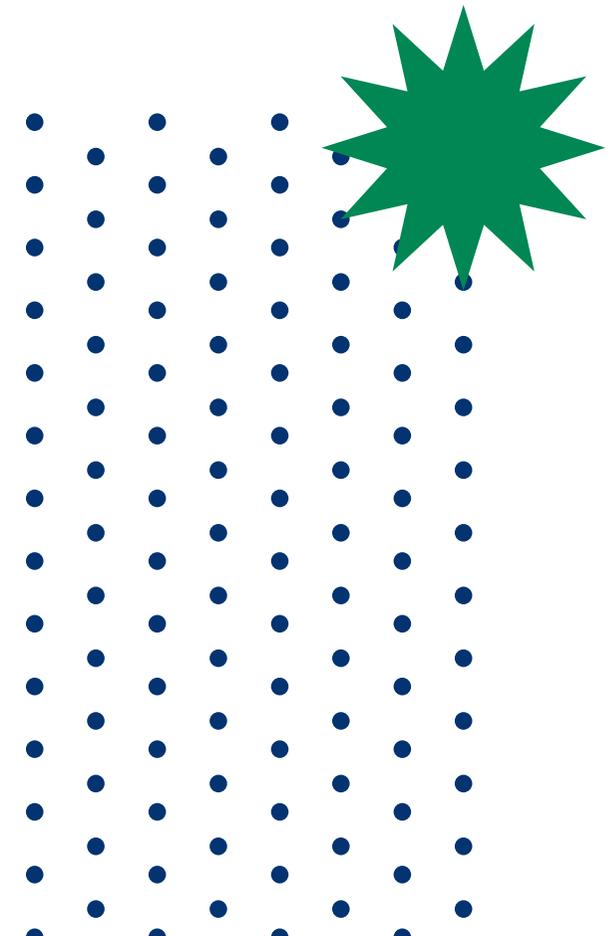
Das bedeutet: Falls Ihr kostbares geistiges Eigentum – wie Produktentwürfe, Quellcode, Entwicklungsmodelle, Forschungsdaten und andere wissenschaftliche Erkenntnisse (die alle zu den unstrukturierten Daten gehören) – in die Hände von Angreifern fällt, gehen Ihnen möglicherweise Jahre an Arbeit, unersetzliches Geschäftswissen und Ihr Wettbewerbsvorteil verloren.

Sie benötigen eine Methode, um sämtliche unstrukturierten Daten zu schützen. Doch das ist eine immense Herausforderung. Zum einen sprechen wir hier von einer riesigen Menge an Daten, zum anderen sind diese Daten auf verschiedene Speichersysteme und Standorte verteilt (von lokalen NAS-Geräten bis hin zu Objektspeichern), was es sehr viel schwerer macht, die Daten mit manuellen Prozessen im Blick zu behalten.

In der Vergangenheit haben Unternehmen in der Regel versucht, unstrukturierte Daten mit herkömmlichen Backup-Ansätzen zu schützen. Allerdings bieten diese Methoden weder die erforderliche Geschwindigkeit noch die nötige Transparenz oder Kontrolle.



Laut IDC sind 90 %
aller Daten unstrukturiert.



¹ IDC: „The Untapped Value of Unstructured Data“, <https://www.box.com/resources/unstructured-data-paper>

Beispiele:



Herkömmliche Backup-Lösungen sind nicht für den Umgang mit riesigen Datenmengen konzipiert. Das Sichern von Datensätzen, die mehrere Petabyte groß sind, kann Wochen dauern. Doch selbst wesentlich schnellere Sicherungsvorgänge können zu Verzögerungen und damit zu Leistungsproblemen in der Produktionsumgebung führen. Die Folge? Ungeschützte Daten.



Herkömmliche Backup-Lösungen bieten keine plattformübergreifende Transparenz. Mit anderen Worten: Es ist nicht möglich, sich einen Überblick über sämtliche Speichertypen gleichzeitig zu verschaffen. Auch ein effektives Sicherheitsmanagement ist angesichts der enormen Menge unstrukturierter Daten kaum realistisch.



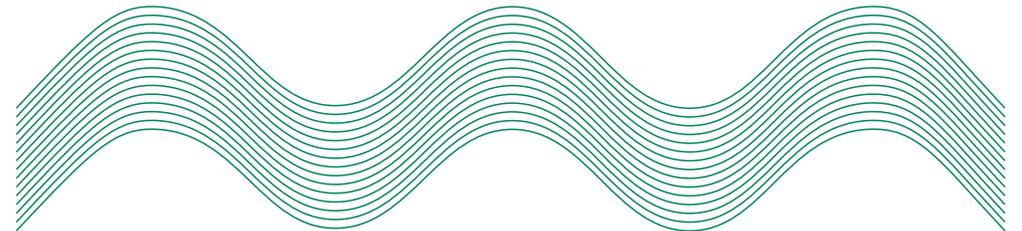
Sie wissen nicht, wo Ihre sensiblen Daten gespeichert sind und wer darauf Zugriff hat. So können Sie Risiken kaum einschätzen und Compliance-Anforderungen nur schwer nachkommen.



Herkömmlichen Backup-Lösungen fehlen die erforderlichen Schutzmaßnahmen für die Abwehr von Ransomware und anderen modernen Bedrohungen.



Die Wiederherstellung von Dateien und Ordnern erfolgt manuell. Das ist langsam und kann dazu führen, dass Sie Ihre SLAs nicht einhalten können.



Es ist offensichtlich: Die Menge unstrukturierter Daten wächst und herkömmliche Backup-Lösungen können einfach nicht mithalten. Doch eine moderne Lösung für das Management unstrukturierter Daten bietet fünf Vorteile, mit denen Sie Ihr Risiko mindern, Datenresilienz aufbauen und Ihren Betrieb auch im Falle eines Angriffs aufrechterhalten.

FÜNF UNVERZICHTBARE MERKMALE

EINER LÖSUNG ZUM SCHUTZ UNSTRUKTURIERTER DATEN

1

Leistung im Petabyte-Umfang für den Schutz unstrukturierter Daten

Wenn sich der Umfang unstrukturierter Daten bis in den Petabyte-Bereich bewegt, stoßen herkömmliche Backup-Systeme an ihre Grenzen. Dafür gibt es einen einfachen Grund: Diese Lösungen wurden nicht für die Mengen- und Durchsatzanforderungen konzipiert, die für den Schutz von Milliarden von Dateien nötig sind.

Diese enormen Datenmengen bringen traditionelle Backup-Systeme an ihr Limit: Es kommt zu Verzögerungen, und zwar sowohl beim Backup-System selbst als auch bei den Systemen, die gesichert werden sollen. Recovery Point Objectives (RPOs) können nicht mehr eingehalten werden und die Zeiträume zwischen den Sicherungsvorgängen werden zu lang. Das Ergebnis: Geschäftskritische Daten sind möglicherweise nicht mehr geschützt. Die Versuchung ist groß, das Problem mit neuer Hardware zu beheben, doch außer Kosten bringt dies nichts. Herkömmliche Ansätze wie NDMP (Network Data Management Protocol) bieten weder die nötige Anwendungskontrolle noch die erforderliche Skalierbarkeit für eine effiziente Verwaltung derartiger Datenmengen. Daher löst zusätzliche Hardware die angesprochenen Probleme nicht.

Was bietet sich stattdessen an? Um Milliarden von Dateien effizient abzusichern, benötigen Sie einen modernen Ansatz mit Parallelabfragen, -indizierung und -datenübertragung. Durchsatzmaximierung und dynamische Drosselung helfen, die Netzwerkauslastung zu optimieren, die Zeit zwischen Backups zu verkürzen und Ihre Daten umfassend zu schützen – und zwar ohne ein Vermögen auszugeben.



Expertentipp

Achten Sie darauf, dass Ihre Lösung für den Schutz unstrukturierter Daten Parallelverarbeitung und eine dynamische Dienstqualität für extrem leistungsstarke Backup-Vorgänge unterstützt, damit Daten im Petabyte-Bereich ohne Leistungseinbußen effizient geschützt werden.

2

Alle unstrukturierten Daten im Blick

Da unstrukturierte Daten über zahlreiche NAS-Plattformen und Standorte verteilt sind, lässt sich nur schwer erkennen, wo sie sich genau befinden, wer Zugriff auf sie hat und ob sie angemessen geschützt sind.

Herkömmliche Backup-Lösungen erleichtern die Sache nicht wirklich, da es sich meist um Punktlösungen handelt, die jeweils eigene Richtlinien, Zeitpläne und Kontrollmaßnahmen erfordern und es damit so gut wie unmöglich machen, eine konsistente, SLA-basierte Datensicherheitsstrategie zu verfolgen. Einen ganzheitlichen Überblick über Ihren globalen unstrukturierten Datenbestand zu erhalten, ist damit ebenfalls nicht realistisch. Ohne zentrale Einblicke in das Wachstum der Daten, Nutzungsmuster und Trends können Sie den Lebenszyklus der Daten nicht effektiv verwalten. Sie können auch keine fundierten Entscheidungen darüber treffen, was aufbewahrt und was archiviert werden soll. Hinzu kommt: Wenn Sie Daten in einer Cloud-Umgebung sichern, kann es sehr kostspielig werden, Daten in einer falschen Speicherklasse aufzubewahren.

Es ist an der Zeit, mit einem einheitlichen Ansatz und einer zentralen Oberfläche die Kontrolle über all Ihre unstrukturierten Daten zu erlangen. Zentralisierte Dashboards sollten praxisrelevante Einblicke für eine proaktive Datenverwaltung liefern und gleichzeitig die konsistente Durchsetzung von Richtlinien ermöglichen.



Expertentipp

Bestehen Sie auf einer Lösung mit einer einheitlichen Steuerebene, damit Sie unstrukturierte Daten über alle NAS-Geräte und Standorte hinweg verwalten und schützen können. Ein zentraler, ganzheitlicher Überblick ist der Schlüssel zu einem zuverlässigen, rechtskonformen Datenlebenszyklus.

3

Leistungsstarke Datensicherheit mit umfassender Anomalie-Erkennung

Angreifer verstärken ihre Bemühungen und haben Ihre Daten im Visier. 93 % der befragten Unternehmen berichten, dass böswillige Akteure während eines Cyber-Angriffs versucht haben, Daten-Backups zu kompromittieren, und 73 % dieser Unternehmen gaben an, dass die Versuche zumindest teilweise erfolgreich waren.²

Ein Teil des Problems besteht darin, dass herkömmliche Lösungen Backup-Daten oft ohne logisches Air-Gapping online aufbewahren und zugänglich machen. **Air-Gapping** sorgt dafür, dass Ihre Backups „versteckt“ separat gespeichert werden, damit Angreifer sie nicht finden können. Backups sind ohne Air-Gaps anfällig und falls sie kompromittiert werden, ist Ihre Fähigkeit, kritische Daten und Anwendungen nach einem Cyber-Angriff wiederherzustellen, stark beeinträchtigt.

Das ist auch der Grund, weshalb **unveränderliche Backups** – also Backups, die nicht verändert oder gelöscht werden können – so wichtig sind. Auch das ist ein Merkmal, das bei vielen herkömmlichen Tools fehlt. Wenn Ihre Backups nicht unveränderlich sind, können sie bei einem Angriff überschrieben werden, wodurch jegliche sauberen Wiederherstellungspunkte verloren gehen.

Hinzu kommt, dass in den meisten Legacy-Tools die Funktionen für die **rollenbasierte Zugangskontrolle** zu stark beschränkt, die Berechtigungen hingegen zu weit gefasst sind. Diese Sicherheitslücke öffnet

böswilligen Insidern und Hackern, die es auf Anmeldedaten abgesehen haben, Tür und Tor. Ohne präzise rollenbasierte Zugangskontrollen, die das Least-Privilege-Prinzip durchsetzen, haben Benutzer (aber auch Hacker mit gestohlenen Anmeldedaten) Zugriff auf Daten, die sie gar nicht benötigen. Dadurch steigt das Risiko, dass Ihre Daten missbraucht werden.

Sie müssen unstrukturierte Daten auf moderne Weise schützen. Dazu eignen sich Lösungen mit integrierten Sicherheitskontrollen. Ihre Checkliste bei der Auswahl einer Lösung sollte folgende Aspekte umfassen: Air-Gapping, unveränderliche Backups, rollenbasierte Zugangskontrollen und **Anomalie-Erkennung**.

Durch das Identifizieren von Lösch-, Änderungs- und Verschlüsselungsvorgängen hilft die Anomalie-Erkennung, den Umfang eines Cyber-Angriffs zu ermitteln und effektive Ransomware-Untersuchungen durchzuführen. Stehen Ihnen diese Informationen zur Verfügung, können Sie gezielt die Daten wiederherstellen, die Sie benötigen, anstatt einen umfassenden (und daher langwierigen) Wiederherstellungsvorgang zu starten. So können Sie den Betrieb schneller wiederaufnehmen.



Expertentipp

Priorisieren Sie Lösungen, die logisches Air-Gapping, unveränderliche Backups, feinkörnige rollenbasierte Zugangskontrollen und Anomalie-Erkennung bieten. Dieser mehrschichtige Sicherheitsansatz schützt Ihre Backup-Daten vor nicht autorisiertem Zugriff, verhindert ungewollte Änderungen und lässt Sie den Betrieb nach einem Angriff schneller wieder aufnehmen.

² Der Stand der Datensicherheit: die bittere Wahrheit, <https://www.rubrik.com/de/zero-labs/2023-spring>

4

Identifizierung und Klassifizierung sensibler Daten

Als sensible Daten werden alle Informationen bezeichnet, deren Kompromittierung einen Schaden für Einzelpersonen, Organisationen oder Unternehmen verursachen kann. Dazu gehören personenbezogene Daten (PII), Finanzdaten, geistiges Eigentum, Patientenakten und alle anderen vertraulichen Informationen, die aus Datenschutz-, Sicherheits- und Compliance-Gründen geschützt werden müssen.

Wenn es um die Erfüllung gesetzlicher Vorgaben und das Erhalten des Kundenvertrauens geht, haben die Governance und die Absicherung sensibler Daten oberste Priorität. Allerdings wächst der Umfang unstrukturierter Daten mittlerweile in den Petabyte-Bereich, wodurch das Identifizieren sensibler und regulierter Daten zu einer enormen Herausforderung geworden ist.

Herkömmliche Backup-Tools bieten keine nativen Funktionen für die Erkennung und Klassifizierung von Daten. Doch wenn Sie nicht wissen, welche Arten von sensiblen Daten in Ihrer Umgebung vorhanden sind und wo diese aufbewahrt werden, nehmen Sie riskante tote Winkel in Bezug auf Compliance und Sicherheit in Kauf.

Wenn Sie nicht in der Lage sind, personenbezogene und andere sensible Daten in Ihren unstrukturierten Datensätzen zu identifizieren, riskieren Sie, dass diese Daten unabsichtlich offengelegt werden oder dass Sie Datenschutzvorgaben wie die DSGVO, den HIPAA oder den CCPA (California Consumer Protection Act) verletzen. Wenn Sie nicht wissen, wo sich Ihre kritischen Daten befinden, können Sie sie auch nicht angemessen schützen.

Fehlendes Bewusstsein rund um Daten verursacht eine ineffiziente Nutzung von Backup-Ressourcen und lässt die Kosten steigen. Wenn Sie den Wert und den Vertraulichkeitsgrad Ihrer Daten nicht kennen, müssen Sie alle Daten gleich behandeln. Doch das unnötige Sichern und Replizieren nicht-kritischer Daten treibt letztendlich die Speicherkosten in die Höhe.

Um die Gefährdung sensibler Daten einzudämmen und die Compliance zu vereinfachen, benötigen Sie moderne Lösungen, die Datensicherheit und Content Intelligence miteinander kombinieren. Indem sensible Daten automatisch erkannt, klassifiziert und protokolliert werden, können Sie Daten ein Risikoprofil zuweisen, um den Schutz der kritischsten Daten zu priorisieren, und Kosten besser kontrollieren.



Expertentipp

Suchen Sie nach Lösungen mit integrierten Funktionen für die Erkennung und Klassifizierung sensibler Daten. Die Identifizierung regulierter Daten und die Möglichkeit, Datenschutz- und Sicherheitsrisiken einzuschätzen, stärken Ihre Daten-Governance und die Compliance. Ein besserer Überblick über Ihren Datenbestand sorgt dafür, dass Ihre wichtigsten Daten immer geschützt sind, und ermöglicht Ihnen, nur die benötigten Daten wiederherzustellen.

5

Präzise und effiziente Datenwiederherstellung

Die von Information Technology Intelligence Consulting (ITIC) veröffentlichte Studie *2024 Hourly Cost of Downtime Survey* hat ergeben, dass eine einzige Stunde Ausfallzeit 90 % der mittleren und großen Unternehmen mehr als 300.000 US-Dollar kostet.³ Bei einem Cyber-Vorfall zählt jede Sekunde und um Ihre Verluste so gering wie möglich zu halten, müssen Sie in der Lage sein, den Betrieb schnell und präzise wiederaufzunehmen. Doch mit veralteten Backup-Lösungen ist das kaum zu erreichen.

Die Datenwiederherstellung mit herkömmlichen Backup-Tools ist mit der sprichwörtlichen Suche nach der Nadel im Heuhaufen vergleichbar. Ohne detaillierte Suchfunktionen sind IT-Administratoren gezwungen, Unmengen von Daten zu durchsuchen, die über die gesamte Infrastruktur verteilt sind, um herauszufinden, welche Daten bei einem Angriff oder einer Naturkatastrophe gestohlen oder beschädigt wurden.

Wenn Sie nicht identifizieren können, welche Daten betroffen sind, müssen Sie Systeme im Gesamten wiederherstellen. Das verursacht Engpässe im Netzwerk, überfordert die Speichergeräte und verlangsamt letztendlich die Wiederherstellung. Außerdem stellt sich die Frage: Können Sie mit Gewissheit sagen, dass die gesicherten Daten „sauber“ sind?

Das ist ein weiterer Bereich, in dem herkömmliche Lösungen oft zu kurz greifen. Da sie die Integrität der Backups nicht prüfen, kann es dazu kommen, dass Sie unwissentlich beschädigte oder infizierte Daten wiederherstellen. Dann stehen Sie plötzlich doch wieder ohne Daten da, haben aber kostbare Zeit und Ressourcen verschwendet. Zudem können Sie die Wiederherstellung mit Legacy-Tools nicht automatisieren, was den Prozess verlangsamt.

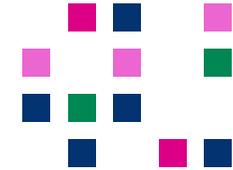
Um Datenverlust zu vermeiden und die Wiederherstellung zu beschleunigen, benötigen Sie moderne Lösungen, die eine schnelle, gezielte und umfassende Wiederherstellung ermöglichen. Detaillierte Suchfunktionen, feinkörnige Wiederherstellungsoptionen, Integritätsprüfungen und automatisierte Workflows sorgen dafür, dass Sie schnellstens wieder Zugang zu den erforderlichen Daten erhalten.



Entscheiden Sie sich für Lösungen, mit denen Sie bestimmte Daten schnell und gezielt abrufen können, ohne komplette Systeme wiederherstellen zu müssen. Zudem sollten Sie nach Integritätsprüfungen und Automatisierungsfunktionen Ausschau halten, um die Wiederherstellung einfacher und effizienter zu gestalten und das Risiko von Bedienfehlern zu senken.

³ ITIC 2024 Hourly Cost of Downtime Report Part 1, <https://itic-corp.com/itic-2024-hourly-cost-of-downtime-report>

SCHÜTZEN SIE UNSTRUKTURIERTE DATEN AUF MODERNE WEISE



Herkömmliche Backup-Lösungen haben in der Vergangenheit gute Dienste geleistet. Doch sowohl die Daten- als auch die Bedrohungslandschaft hat sich verändert. Unstrukturierte Daten müssen heute ebenso rigoros geschützt und verwaltet werden wie alle anderen kritischen Daten.

Um diese Herausforderungen zu meistern, benötigen Sie eine Lösung, die auf den Umgang mit unstrukturierten Daten im Petabyte-Bereich ausgelegt ist. Rubrik NAS Cloud Direct bietet die erforderlichen Funktionen, mit denen Sie Ihre wertvollsten Assets zuverlässig schützen können – heute und in Zukunft.

Dank der folgenden Eigenschaften bietet Rubrik NAS Cloud Direct Sicherheit für unstrukturierte Daten:

Schnelle Backups und zuverlässige Leistung bei riesigen Datenvolumen

Mit Rubrik NAS Cloud Direct können Sie Daten im Petabyte-Bereich sowie Milliarden von Dateien schneller und effizienter sichern und wiederherstellen als mit NDMP. Die parallele Verarbeitung beim Abfragen, Indizieren und Übertragen von Daten sorgt für maximalen Durchsatz, während intelligente Dienstqualität sicherstellt, dass die Produktionsabläufe nicht beeinträchtigt werden.

”

Unkomplizierte Einrichtung, extrem schnelle Backups und ganz einfache Wiederherstellung.

IT-Führungskraft (Infrastrukturmanagement)
Unterhaltungs- und Freizeiteinrichtung

“

Einheitliche Verwaltung und Transparenz

Über die zentralisierte Steuerebene von NAS Cloud Direct lassen sich unstrukturierte Daten konsistent verwalten. Einheitliche Dashboards bieten praxisrelevante Einblicke und verbessern den Schutz, die Archivierung und die Compliance. Die konsistente Durchsetzung von Richtlinien in der gesamten Infrastruktur vereinfacht den Betrieb.

”

Dank Rubrik NAS Cloud Direct sind wir schneller und effizienter geworden.

Führungskraft im Produktdesign
Finanzunternehmen

“



Moderne Datensicherheit mit Anomalie-Erkennung

Rubrik NAS Cloud Direct stärkt die Datensicherheit mit logischem Air-Gapping, unveränderlichen Backups und rollenbasierter Zugangskontrolle. Außerdem sorgt die Anomalie-Erkennung von Rubrik dafür, dass Sie über Fehler, Probleme und Auffälligkeiten benachrichtigt werden und mögliche Auswirkungen eines Angriffs zeitnah einschätzen können. Dank Rubrik können Sie den Angriffsverlauf nachvollziehen, böswillige Aktivitäten erkennen, zügig reagieren und den Betrieb schnell wiederaufnehmen.

”

Wir haben unsere NAS-Backups jetzt im Blick und können sie analysieren. Bei Auffälligkeiten werden wir benachrichtigt und können sofort eine Untersuchung einleiten.

Kevin Mortimer

Betriebsleitung, University of Reading

“



Überwachung sensibler Daten und Compliance

NAS Cloud Direct vereint den Schutz von Daten mit Content Intelligence, um die Erkennung, Klassifizierung und Protokollierung sensibler Daten zu unterstützen. Die automatisierte Identifizierung von PII-, PHI-, Finanz- und anderen regulierten Daten hilft bei der Bewertung von Compliance-Risiken und bei der Absicherung geschäftskritischer Datenbestände.



Schnelle, präzise Wiederherstellung im großen Umfang

Rubrik NAS Cloud Direct unterstützt Sofortsuchen und granulare Wiederherstellungsprozesse, um Datenverluste und Ausfallzeiten auf ein Minimum zu begrenzen. Im Falle eines Angriffs durchsucht NAS Cloud Direct Milliarden von Dateien in kürzester Zeit und orchestriert die Wiederherstellung, damit Sie den Betrieb schnellstmöglich wieder aufnehmen können.

”

NAS Cloud Direct überwacht das System und informiert mich über Anomalien. Nun kann ich nachts wesentlich besser schlafen.

Travis Spurley

Leitender Systemingenieur, Quantum Spatial

“

”

Die Möglichkeit, Millionen, wenn nicht Milliarden von Dateien zu durchsuchen, ist fantastisch. Die Rubrik-Lösung hat es uns definitiv ermöglicht, unsere Arbeit besser zu machen.

Carl Lucas

VP of Information Technology, Quantum Spatial

“



Lassen Sie nicht zu, dass eine veraltete Backup-Lösung Ihre unstrukturierten Daten gefährdet. Mit Rubrik können Sie enorme Mengen unstrukturierter Daten wirksam verwalten und schützen sowie Resilienz gegen Bedrohungen aufbauen, die sich stetig weiterentwickeln.



Jetzt ist der richtige Zeitpunkt für einen moderneren Ansatz.
Informieren Sie sich noch heute über [Rubrik](#) und [NAS Cloud Direct](#).

