VERITAS

Der umfassende Ransomware-Leitfaden mit Veritas

White Paper | Januar 2023

VERITAS ALTA™

Inhalt

Zusammenfassung

Heutzutage sind Cybersicherheit und die Bedrohung durch Ransomware-Angriffe für jede Branche auf der ganzen Welt die größten Sorgen. Laut dem SonicWall Cyber Threat Report 2022 gab es jede Sekunde 19 Angriffe, weltweit waren es 623,3 Millionen. Mittlerweile ist klar, dass Ransomware die am schnellsten wachsende Form der Cyberkriminalität ist. Ransomware as a Service (RaaS) hat sich zu einem organisierten, lukrativen Geschäftsmodell herausgebildet und Angreifer entwickeln ständig kreative Techniken weiter, um selbst die besonders aufmerksamen Sicherheitskräfte an vorderster Front zu überwinden. Alte Techniken wie Phishing stehen noch immer im Vordergrund, aber neue, ausgefeilte Methoden wie Social Engineering, die auf Geräte und Infrastrukturen des Internets der Dinge (IoT) sowie Software-Schwachstellen abzielen, erfreuen sich zunehmender Beliebtheit. Aus diesem Grund ist es für IT-Teams von entscheidender Bedeutung, sich darüber im Klaren zu sein, dass sie durch Endpunktsicherheit allein keine echte Ransomware-Resilienz erreichen können. Stattdessen brauchen sie eine vielschichtige Strategie.

Viele Unternehmen betrachten Backups und Wiederherstellung ihrer Daten möglicherweise als letzte Verteidigungslinie gegen Ransomware-Angriffe. Veritas empfiehlt, Backup und Wiederherstellung als proaktiven, integralen und zuverlässigen Teil einer umfassenden Sicherheitsstrategie gegen Ransomware mit verschiedenen Ebenen zu priorisieren. Bei einem Angriff werden nicht nur Ihre Daten bedroht – sondern Ihr gesamtes Unternehmen.

Bei der Entwicklung der Veritas-Lösungen standen Widerstandsfähigkeit und Sicherheit im Mittelpunkt, sodass wir unseren Kunden zuverlässige Lösungen bieten konnten, um sicherzustellen, dass ihr Unternehmen mit nur minimalen Unterbrechungen seinen Betrieb fortsetzt. Unsere Lösungen schützen IT-Systeme und gewährleisten die Datenintegrität mit einer breiten Palette an Zero-Trust-Sicherheitskontrollen, Workload-Unterstützung und branchenführenden unveränderlichen und unlöschbaren Speicheroptionen für unterschiedliche Anforderungen. Außerdem bieten diese Lösungen vollständige Transparenz über Ihre gesamte Umgebung, einschließlich physischer, virtueller und Cloud-Workloads, vom Speicher bis zur Rechenleistung und sogar über andere Backup-Anbieter und -Dienste hinweg, um sicherzustellen, dass kein System durchs Raster fällt. Unsere Tools bieten Ihnen eine nahezu in Echtzeit erfolgende, auf künstlicher Intelligenz (KI) basierende Erkennung von anomalen Verhaltensweisen oder Aktivitäten, die sowohl mit Daten als auch mit Benutzeraktivitäten in Ihrer gesamten Umgebung zusammenhängen. Unser automatisierter und bedarfsgesteuerter Malware-Scan bietet zudem klare Warnmeldungen, Stichprobenprüfungen bekannter Hochrisikobereiche und die Wiederherstellung bereinigter Daten. Wenn es um Wiederherstellung geht, steht die Marke Veritas seit Jahrzehnten für Resilienz. Zuverlässige Veritas-Lösungen integrieren bewährte Technologie, sodass Sie mit flexiblen, automatisierten und orchestrierten Optionen schnell wiederhergestellt werden können und Ihr Unternehmen innerhalb von Minuten wieder betriebsbereit ist.

Einführung

Dieses Dokument konzentriert sich auf Veritas-Lösungen, die die umfangreichste, richtlinienkonformste und sicherste Ransomware-Resilienzplattform der Branche umfassen. Diese schenken Ihnen Zuversicht, reduzieren Risiken und stellen sicher, dass Sie Ihre Daten schützen, erkennen und wiederherstellen können und gegen die sich ständig weiterentwickelnde Bedrohung durch Ransomware gewappnet sind.

Dieses Dokument richtet sich an geschäftliche und technische Zielgruppen, darunter Kunden, Partner und andere, die mehr darüber erfahren möchten, auf welche Weise unsere Lösungen zum Schutz vor und zur Wiederherstellung nach einem böswilligen Angriff beitragen.

Dieses Whitepaper hilft Ihnen folgendermaßen:

- Sie erfahren, wie Sie Ihre IT-Systeme schützen und die Datenintegrität gewährleisten
- Sie lernen, wie Veritas-Lösungen Ihnen bei der Überwachung und Eindämmung von Bedrohungen und Schwachstellen helfen
- Sie entdecken Optionen für eine schnelle und vollständige systemübergreifende Wiederherstellung und entwickeln Ihren eigenen Plan zur Optimierung der Umgebung für die Wiederherstellung

Es ist wichtig zu beachten, dass es keine einheitliche Lösung für die Ransomware-Resilienz gibt und dieses Dokument nicht als allumfassend anzusehen ist. Veritas gibt Ihnen die Freiheit, aus einer Vielzahl von Lösungen auszuwählen, die den spezifischen Wiederherstellungsanforderungen jeder Anwendung am besten entsprechen. Sie sollten eine mehrschichtige und umfassende Strategie implementieren, die auf der Methodik des National Institute of Standards and Technology (NIST) basiert – Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Zusätzlich zu dem, was wir in diesem Whitepaper darlegen, empfehlen wir Ihnen, herkömmliche Sicherheitsmaßnahmen als primären Bestandteil der Verteidigungsstrategie Ihres Unternehmens beizubehalten. Vergessen Sie nicht, Firewalls, E-Mail- und Spamfilter sowie Anti-Malware- und Point-Protection-Software hinzuzufügen sowie segmentierte Netzwerkstrategien und Mitarbeiterschulungsprogramme einzuführen.

Unternehmen müssen ihre Strategie entwickeln, einstudieren und konsequent bewerten, um mit der zunehmenden Komplexität der Bedrohungen und ihrer Technologien Schritt zu halten. Das Üben regelmäßiger Proben und Validierungen ist für den Erfolg von entscheidender Bedeutung, um sicherzustellen, dass die verschiedenen Optionen tatsächlich funktionieren, wenn Sie sich im Krisenmodus befinden. Darüber hinaus ist es immer ratsam, eine externe Agentur zu beauftragen, die Ihre Strategie und Arbeit überprüft und Ihnen bei der Identifizierung von Schwachstellen hilft.

Werfen wir einen Blick auf unsere empfohlenen Best Practices für das Backup-Ökosystem (siehe Abbildung 1).

Abbildung 1. Empfohlene Best Practices für das Backup-Ökosystem einer Organisation.

Best Practices

Obwohl Ransomware Ihrem Unternehmen und Ihrem Ruf ernsthaften Schaden zufügen kann, ist sie nicht unbezwingbar. Tatsächlich ist sie nur so wirksam wie das schwächste Glied Ihres Unternehmens. Die gute Nachricht ist, dass Ihr Unternehmen wichtige Schritte unternehmen kann, um nicht zum Ziel von Cyberkriminalität zu werden und die Wahrscheinlichkeit zu verringern, von einem Angriff ernsthaft geschädigt zu werden.

NIST hat ein empfohlenes Cybersicherheits-Framework entwickelt, das Unternehmen dabei hilft, eine umfassende, strukturierte Methodik rund um fünf Schlüsselfunktionen einzuführen: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Veritas schließt sich diesem Ansatz an und empfiehlt die Implementierung unserer Lösungen im breiteren NIST-Rahmen.

Wenn es um das Backup-Ökosystem eines Unternehmens geht, empfiehlt Veritas, die in Abbildung 1 dargestellten wichtigsten Best Practices im Auge zu behalten.

Versionsverwaltung und zeitnahe Systemaktualisierungen

- Reduzieren Sie die Gefährdung durch Sicherheitslücken, indem Sie mit Patches und Releases, die Sicherheits-Updates enthalten, auf dem neuesten Stand bleiben.
- Informieren Sie sich über technische Warnungen von Veritas, indem Sie die Veritas-Support-Website oder die Veritas Services and Operations Readiness Tools (SORT) besuchen.

Zero-Trust-Modell und -Richtlinien

- Verinnerlichen Sie eine Perspektive, vor deren Hintergrund keinem Gerät oder Benutzer standardmäßig vertraut wird, selbst wenn er sich innerhalb des Unternehmensnetzwerks befindet.
- Anstatt nur ein Passwort zu verlangen (selbst wenn es lang und kompliziert ist), nutzen Sie Identitäts- und Zugriffsmanagement, indem Sie rollenbasierte Zugriffskontrolle (RBAC) und Zwei-Faktor-Authentifizierung (oder Multi-Faktor-Authentifizierung, MFA) implementieren, um damit den Zugriff ausschließlich auf die erforderliche Funktionalität für jede Person einzuschränken und zu verhindern, dass die Kontoübernahme mit nur einem Paar an Anmeldedaten erfolgt.
- Fordern Sie Benutzer immer dazu auf, sich mit ihren eigenen, selbst erstellten Anmeldeinformationen anzumelden.
- Verwenden Sie niemals werkseitige Passwörter. Ändern Sie integrierte generische Benutzer-IDs und Passwörter, einschließlich der Hostkonten „admin“, „maintenance“, RMM „sysadmin“ und „nbasecadmin“.
- Beschränken oder sperren Sie den Zugriff auf Backups, was eine gängige Eintrittsmethode für Ransomware ist, und ein weiteres Paar 10/25-Gb-Ethernet-Ports für den clientseitigen Datenschutzverkehr.

Unveränderbarer und unlöschbarer Speicher

Eine der wirksamsten Methoden zum Schutz Ihrer Daten vor Ransomware, besteht darin, einen unveränderlichen und unlöschbaren Speicher mit einer intern verwalteten Compliance-Uhr zu implementieren und eine Isolate Recovery Environment (IRE) einzurichten.

Datenverschlüsselung

- Implementieren Sie eine Verschlüsselung während der Übertragung, um Ihre Daten vor der Gefährdung innerhalb des Netzwerks zu schützen.
- Implementieren Sie eine Verschlüsselung im Ruhezustand, um zu verhindern, dass Ransomware oder Cyberkriminelle Ihre Daten stehlen und damit drohen, sie zu veröffentlichen oder andere böswillige Aktionen durchzuführen.

Konfiguration und Netzwerksegmentierung

- Befolgen Sie die Sicherheitsimplementierungsleitfäden.
- Härten Sie die Umgebung, indem Sie Firewalls aktivieren, die den Zugriff auf Ports und Prozesse einschränken.
- Aktualisieren Sie die standardmäßige Backup-Richtlinie für den Primärkatalog.
- Richten Sie eine Backup-Richtlinie für den NetBackup Key Management Server (KMS) ein.

Bereitstellung und die 3-2-1-1-Backup-Strategie

- Übernehmen Sie den „3-2-1“-Best-Practice-Ansatz der Datensicherung, der von der US-amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) empfohlen wird: Bewahren Sie drei Kopien der Daten auf zwei verschiedenen Medientypen auf, eine davon extern. Wir empfehlen, diesen Ansatz noch einen Schritt weiter zu gehen und eine 3-2-1-1-Strategie zu schaffen, indem mindestens eine Kopie auf unveränderlichem und unlöschbarem Speicher aufbewahrt wird (siehe Abbildung 2).
- Verwenden Sie die AIR-Technologie (Auto Image Replication), um auf Zieldomänen zu replizieren.

Abbildung 2. Bewahren Sie drei Kopien der Daten auf zwei Arten von Speicher auf, wobei eine Kopie extern und eine auf unveränderlichem Speicher gespeichert ist.

Vollständige Endgerätesichtbarkeit

In den meisten Unternehmen besteht ein erheblicher Mangel an Transparenz über entfernte Endpunkte. Mittlerweile ist es für Kriminelle zur gängigen Praxis geworden, die Sicherheitskräfte an vorderster Front zu umgehen und abzuhängen, wo sie lange genug untätig bleiben, um Schwachstellen zu lokalisieren und den passenden Zeitpunkt für einen Angriff zu finden. Es ist entscheidend, dass Sie Tools implementieren, die vollständige Transparenz über Ihre gesamte Umgebung bieten, Anomalien erkennen und böswillige Aktivitäten in Ihrem Netzwerk aufspüren und Sie darauf aufmerksam machen, sodass Ransomware keinen Platz zum Verstecken hat. Dieser Ansatz hilft Ihnen, Bedrohungen und Schwachstellen abzuschwächen, bevor Cyberkriminelle die Möglichkeit haben, einzugreifen.

Für schnelle Wiederherstellung optimieren

Die meisten Ransomware-Angreifer hoffen auf zwei Dinge: Zeit, damit sich der Angriff ausbreitet, und Geld (von Ihnen), um ihn zu stoppen. In der Vergangenheit konnte die Wiederherstellung Wochen oder sogar Monate dauern, wenn es sich um einen manuellen, arbeitsintensiven Prozess handelte, an der mehrere Stakeholder beteiligt waren. Jetzt kann die Wiederherstellung mit flexiblen und alternativen Optionen – wie dem raschen Aufbau eines Rechenzentrums bei einem Anbieter öffentlicher Clouds – orchestriert und automatisiert werden, was Ausfallzeiten verkürzen und Alternativen zur Zahlung eines Lösegelds bieten kann. Mit den richtigen Systemen können die Wiederherstellungszeiten Ihres Unternehmens bei Bedarf auf Sekunden verkürzt werden.

Häufige und sorgfältige Proben

Sobald Sie Ihre Strategie festgelegt haben, ist es wichtig, sie regelmäßig zu testen und zu proben. Diese Vorgehensweise trägt nicht nur dazu bei, die Reaktionszeiten auf Bedrohungen zu verkürzen und die Auswirkungen eines Angriffs zu minimieren, sondern die verbesserte Transparenz hilft Ihnen auch dabei, Problembereiche zu identifizieren, die gelöst und verbessert werden müssen. Ihr Resilienzplan ist nur so gut wie Ihr letzter Test, daher ist es von Vorteil, Ihre Resilienzstrategie zu üben und laufend zu überarbeiten.

Mitarbeiter schulen

Es ist allgemein bekannt, dass Mitarbeiter oft das Einfallstor für einen Angriff sind. Moderne Phishing-Angriffe und Social Engineering sind inzwischen so weit fortgeschritten, dass sie selbst Sicherheitsexperten täuschen.

Konzentrieren Sie sich darauf, Ihre Mitarbeiter darin zu schulen, Phishing- und Social-Engineering-Taktiken zu erkennen, sichere Passwörter zu erstellen, sicher zu surfen, MFA zu verwenden und immer ein VPN zu verwenden, niemals öffentliches WLAN. Außerdem sollten alle Mitarbeiter wissen, was zu tun ist und wen sie alarmieren müssen, fall sie zu Opfern werden.

Unsere Strategie: Schützen, erkennen, wiederherstellen

Veritas ermöglicht es unseren Kunden, Angriffe zu erkennen, abzuwehren und sich davon zu erholen, mit einer breiten Palette an Produktmerkmalen und Funktionen, die sie an ihre individuellen Bedürfnisse und Anforderungen anpassen können. Schauen wir uns die Details an, die die drei strategischen Säulen der Ransomware-Resilienzstrategie von Veritas ausmachen.

Schützen

Der erste Schritt zur Widerstandsfähigkeit gegen Ransomware besteht darin, sicherzustellen, dass Ihr kritischer und wichtigster Vermögenswert – Ihre Daten – und Ihre IT-Infrastruktur vor Unbekanntem und Unerwartetem geschützt bleiben. Achten Sie darauf, dass alle Teile Ihrer Umgebung – von physisch und virtuell bis hin zu Cloud und Containern – mit universellem Schutz gesichert sind, der intelligent angewendet und automatisch verwaltet wird, um eine ordnungsgemäße Skalierung zu gewährleisten. Dann werden Ihre Backup-Infrastruktur und die gesicherten Daten zur letzten Verteidigungslinie vor einem Angriff und letztendlich zum Schlüssel zur Wiederherstellung Ihres Unternehmens. Veritas bietet mit über 800 Datenquellen, über 1.400 Speicher und über 60 Cloud-Anbietern die umfassendste Unterstützung vom Edge über den Core bis zur Cloud, sodass Ihre Umgebung immer geschützt und jederzeit wiederherstellbar ist.

Cloud-, Datenbank- und VM-Administratoren sparen viel Zeit durch den Einsatz intelligenter Richtlinien, die eine Anwendung oder Recheninstanzen automatisch erkennen und das entsprechende Schutzniveau dafür anwenden.

Veritas konzentriert sich auf den Schutz der Datenintegrität, um sicherzustellen, dass Backup-Dateien sicher und vor böswilligen Eindringlingen geschützt bleiben. Zur Wahrung der Datenintegrität bieten wir eine breite Palette von Sicherheitskontrollen an, die den Schutz unterstützen.

Identitäts- und Zugriffsmanagement

- **Rollenbasierter Zugriff:** Granulare Zugriffskontrollen, die Sie an Bedürfnisse spezifischer Personen anpassen können, indem Sie festlegen, wer auf Daten zugreifen kann und welche Aktionen sie ausführen können und welche nicht (siehe Abbildung 3).
- **Single Sign-On:** Unterstützung für Active Directory und LDAP sowie SAML 2.0. Unternehmen können ihren Authentifizierungsanbieter nutzen, um eine Zwei-Faktor-Authentifizierung zu erreichen.
- **Anpassbare Authentifizierung:** NetBackup Flex Appliances unterstützen eine konfigurierbare Authentifizierungsstärke.

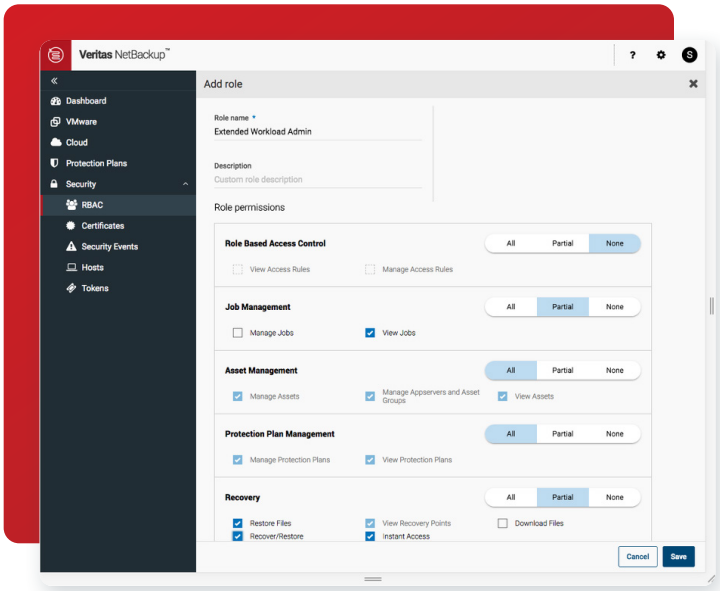


Abbildung 3. Das Zugriffsberechtigungs-Dashboard in NetBackup.

Datenverschlüsselung

- **Während der Übertragung:** Stellt sicher, dass Ihre Daten an authentifizierte Umgebungen gesendet werden und während der Übertragung geschützt sind. Diese Lösung nutzt Veritas- oder vom Kunden bereitgestellte TLS 1.2-Zertifikate mit 2048-Bit+-Schlüsselunterstützung, um die Verschlüsselung des Datentransports während der Übertragung sicherzustellen.
- **Im Ruhezustand:** Wenn es Angreifern gelingt, an Ihre Daten zu gelangen, schützt die Verschlüsselung sie vor Missbrauch. Veritas bietet AES 256-Bit, FIPS 140-2-zertifizierte Kryptografie mit unserer eigenen Schlüsselverwaltung und ermöglicht Ihnen gleichzeitig die Nutzung Ihrer bevorzugten Schlüsselverwaltung mithilfe des Key Management Interoperability Protocol (KMIP).

Unveränderliche/unlöschbare Bildverwaltung und -speicherung

- Flexible, speicherunabhängige Bildverwaltung
  - Flexible Optionen, einschließlich BYO, Appliance, Cloud und Software as a Service (SaaS)-Unveränderlichkeit sorgen dafür, dass Ihre Daten unabhängig vom Standort sicher und richtlinienkonform sind.
  - Mit der OpenStorage Technology (OST) API können Sie unveränderliche Backup-Images mit Veritas oder Speicherlösungen von Drittanbietern verwalten.
  - Unterstützt primäre, sekundäre (Duplizierung) und domänenübergreifende Replikation (mit AIR) und bietet Ihnen unbegrenzte Konfigurationsoptionen für alle Backup-Speicherebenen.
  - Verwenden Sie unveränderlichen Cloud-Speicher mit Amazon S3 Object Lock, um sicherzustellen, dass Ihre Cloud-Daten sicher sind und nicht gefährdet werden können. Weitere Informationen zum unveränderlichen Cloud-Speicher von NetBackup finden Sie im technischen Überblick über die Object Lock-Unterstützung für AWS.
  - Die Bereitstellung von NetBackup Flex Appliance bietet sowohl unveränderlichen als auch unlöschbaren Speicher.
- Im WORM-Speicher (Write Once, Read Many) gespeicherte Bilder
  - NetBackup Flex umfasst einen WORM-Speicherserver, der eine sichere, Container-basierte MSDP-Lösung bietet.
  - NetBackup Flex bietet Enterprise- und Compliance-Sperrmodi, sodass Sie die richtige Stärke der Unveränderlichkeit wählen können (siehe Abbildung 4).

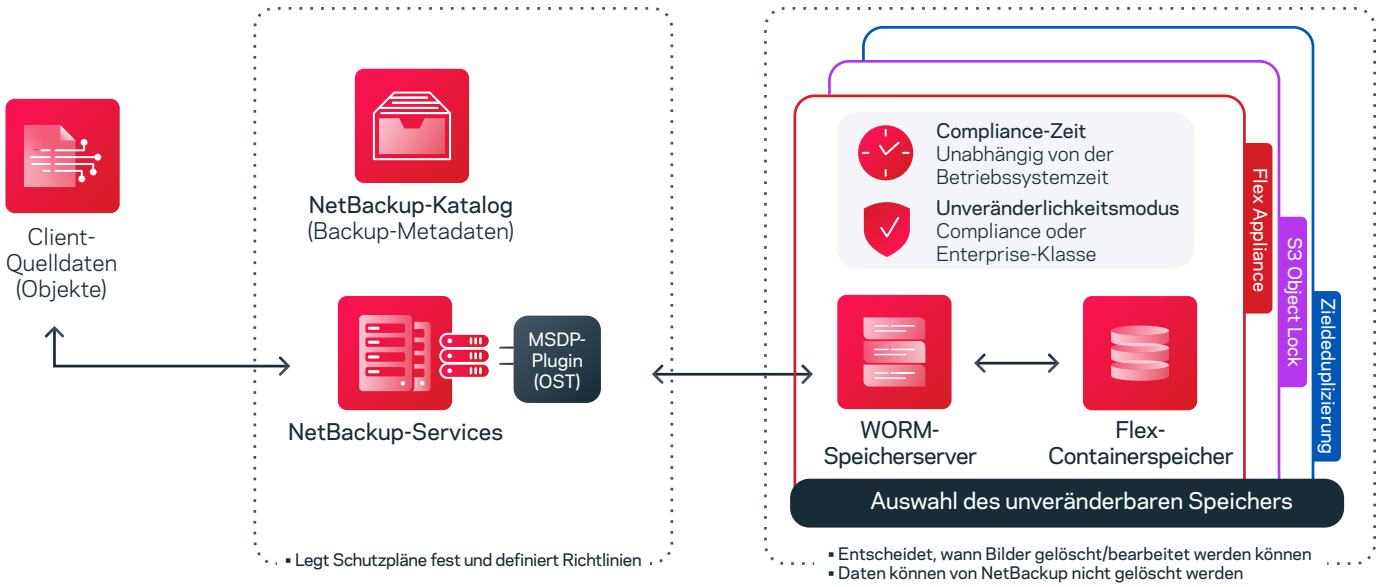


Abbildung 4. Eine Übersicht über unveränderliche Speicheroptionen in NetBackup.

  - Der Compliance-Modus ermöglicht eine unveränderliche Speicherung, bei der kein Benutzer – einschließlich des Root-Benutzers – während eines vordefinierten Aufbewahrungszeitraums Daten löschen kann.
  - Der Enterprise-Modus schützt Daten vor dem Löschen während eines vordefinierten Aufbewahrungszeitraums, und nur Benutzer mit speziellen Berechtigungen können die Aufbewahrungseinstellungen ändern oder die Daten mittels doppelter Autorisierung löschen. Zwei Personen mit unterschiedlichen RBAC-Stufen müssen zustimmen, Änderungen an der Aufbewahrungszeit vorzunehmen oder Daten zu ändern oder zu löschen.
  - NetBackup Flex Appliance hat eine unabhängige Unveränderlichkeitsbewertung von Cohasset Associates durchgeführt, einem branchenweit anerkannten Gutachter für Unveränderlichkeitskontrollen, insbesondere SEC-Regel 17a-4(f), FINRA-Regel 4511(c) und die Grundsätze der Commodity Futures Trading Commission (CFTC) in Regulation 17 CFR § 1 31(c)-(d).
  - Um die Bewertung von NetBackup durch Cohasset Associates zu lesen, besuchen Sie Veritas.com.

Lösungshärtung

NetBackup Flex und NetBackup Flex Scale wurden aus Software- und Hardware-Sicht gestärkt, um eine vollständig sichere Lösung anzubieten, die unveränderlichen und unlöschbaren Speicher unterstützt. Die Lösung bietet einen sicheren WORM-Speicherserver und Hardware-Sicherheitsfunktionen.

- Während des gesamten Entwicklungszyklus analysiert Veritas den Code von NetBackup Flex und Flex Scale auf Schwachstellen mithilfe anerkannter Erkennungstools von Drittanbietern, die Folgendes durchführen:
  - Statische Codeanalyse
  - Schwachstellenprüfungen zur Laufzeit
  - Penetrationstests
- NetBackup Flex und Flex Scale verfügen über eine Vielzahl von Sicherheitsfunktionen, darunter:
  - Verbesserte Betriebssystemsicherheit, einschließlich Security-Enhanced Linux (SELinux)
  - Intrusion Detection System (IDS)/Intrusion Protection System (IPS)
  - Robuste, rollenbasierte Authentifizierung
  - Gesperrter Speicher
  - Ein sicheres, robustes und verbessertes Veritas-Dateisystem

Weitere Details finden Sie im Whitepaper Veritas Flex Appliances with NetBackup Security zur Unterstützung einer sicheren Bereitstellung sowie im Whitepaper Veritas Flex Appliances with NetBackup.

Erkennen

Kriminelle suchen nach Ihren schwächsten Gliedern, den dunklen Ecken, in denen es in Ihrer Umgebung möglicherweise nur begrenzte Sicherheit und/oder Kontrolle gibt. Veritas bietet Lösungen, die einen vollständigen Einblick in die Infrastruktur ermöglichen, Licht auf alle dunklen Daten in Ihrer Umgebung werfen und sicherstellen, dass Sie alles in Ihrer Umgebung wissen und alles sicher und geschützt ist und die Bedrohung durch Ransomware abwehren kann. Veritas bietet außerdem eine Anomalie- und Malware-Erkennung, die eine wertvolle Chance zum Handeln darstellt, bevor Cyberkriminelle oder bösartiger Code die Möglichkeit dazu haben.

Kenntnis der Backup- und Speicherinfrastruktur

Bei Ransomware kommt es auf jede Sekunde an. Veritas Alta™ Analytics für die Cloud und NetBackup IT Analytics für On-Premises können Ihrem Unternehmen helfen, das Ausmaß und die Tiefe eines Ransomware-Angriffs zu verstehen, damit Sie sich strategisch wiederherstellen können. Mit den korrelierten Einblicken von NetBackup IT Analytics in die Umwelt – vor Ort, in der Cloud, Datenschutz und Speicherung – sind Warnungen und Berichte umfassend und einfach einzurichten. Dank dieser Analyseberichtsoptionen gewinnen Sie die nötigen Erkenntnisse, um im Falle eines Angriffs fundierte Entscheidungen treffen zu können. Sie verschaffen Ihnen Einblick in Ihre Backup-Umgebung und ermöglichen Ihrem Unternehmen Folgendes:

- Finden Sie alle Hosts oder VMs in Ihrer Infrastruktur und vergleichen Sie sie mit den durch NetBackup geschützten VMs
- Kennzeichnen Sie Hosts, die in den Backups fehlen oder keine aktuellen Backups haben, als potenzielle Risiken
- Erkennen Sie potenziell von Ransomware betroffene Dateien zusammen mit ihrer Größe und ihrem Speicherort in der Umgebung
- Verwenden Sie interaktive Diagramme, die eine historische Ansicht der generierten Risiken bieten

NetBackup Analytics bietet eine umfassende Backup-Überwachung, die Folgendes enthält:

- Schadensminderungsanalyse (siehe Abbildung 5)
- Quellen mit aufeinanderfolgenden Ausfällen
- Quellen ohne aktuelles Backup
- Backup-Ausfall nach Anwendung

NetBackup Analytics identifiziert potenzielle Falschmeldungen, indem es historische Backups mit dem neuen Backup vergleicht und Anomalien wie erhebliche Änderungen in der Jobdauer, Variationen in der Image-Größe und/oder Änderungen der Richtlinienkonfiguration identifiziert.

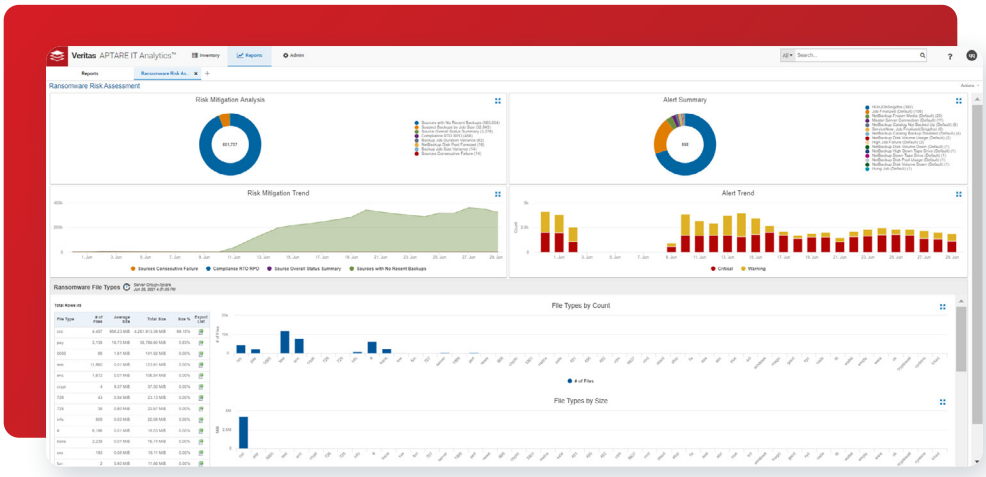


Abbildung 5. Das Dashboard zur Ransomware-Risikobewertung in NetBackup IT Analytics.

Weitere Informationen finden Sie unter Erhöhung der Ransomware-Resilienz: Erlangen Sie mit NetBackup IT Analytics ein vollständiges Infrastrukturbewusstsein.

Anomalieerkennung

Veritas erkennt seltsame Daten und Benutzeraktivitäten in Ihrer gesamten Umgebung und warnt Sie nahezu in Echtzeit vor verdächtigen Anomalien mithilfe der KI-gestützten Anomalieerkennung mit Veritas Alta™ Data Protection für die Cloud und NetBackup für On-Premises. Die Technologie wurde entwickelt, um eine enorme Menge an Daten zu analysieren, die Überwachung und Berichterstattung zu automatisieren und umsetzbare Einblicke in alle Vorgänge in der Umgebung zu liefern. Bei Warnungen kann es sich beispielsweise um ungewöhnliche Dateischreibaktivitäten handeln, die auf eine Infiltration hinweisen könnten, es könnte sich aber auch um die Erkennung bekannter Ransomware-Dateierweiterungen, Dateizugriffsmuster, Datenverkehrsmuster, Code-Downloads, Zugriffsanfragen, Speicherkapazitätsspitzen, externe Datenverkehrspfade usw. oder um unerwarteten Anstieg der Aktivität im Vergleich zu den typischen Mustern bestimmter Personen handeln.

Diese Funktion stellt sicher, dass Ihre Daten jederzeit wiederhergestellt werden können, und ermöglicht es Ihnen, bei Ransomware-Angriffen sofort Maßnahmen zu ergreifen, Backups mit Malware zu isolieren und deren Auswirkungen zu begrenzen. Veritas-Lösungen geben Administratoren die Möglichkeit, Daten einzusehen und jederzeit Empfehlungen im Zusammenhang mit Anomalien abzugeben, indem sie alle Geräte überwachen und eine Frühwarnung vor etwaigen Angriffen einrichten, sodass Sie den Überblick über auftretende Probleme behalten. Beispielsweise lässt sich die KI-gestützte Anomalieerkennung von Veritas nahtlos in den primären Server integrieren und ermöglicht es ihm, anomale Formen von Beobachtungen zu erkennen – wobei diejenigen, die nicht in den Cluster fallen, als Anomalien oder Ausreißer betrachtet werden. Mit dieser Funktion kann ein Backup-Administrator Anomalien erkennen und einen Drilldown durchführen, um Bedenken zu identifizieren. Sie bietet die Möglichkeit, große Datenmengen zu durchsuchen und verwertbare Informationen zur Bewältigung von Ransomware-Ereignissen oder einfach Änderungen in der Umgebung bereitzustellen, über die ein Administrator informiert sein sollte (siehe Abbildung 6).

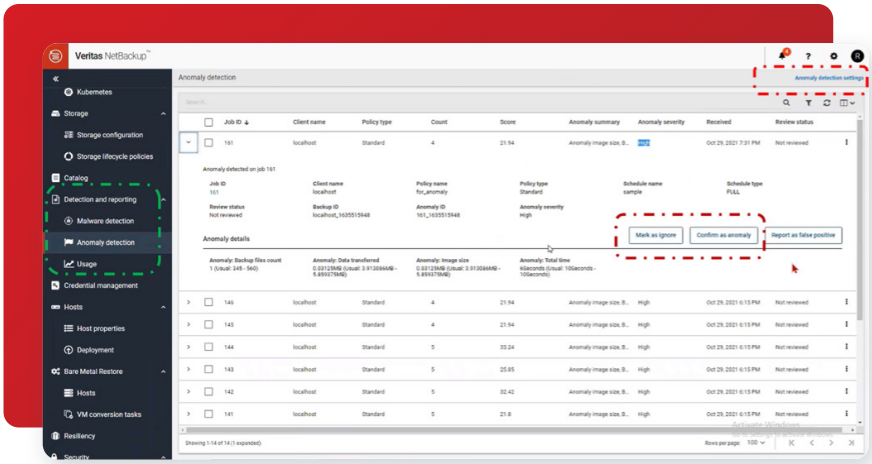


Abbildung 6. Verwenden Sie NetBackup, um Anomalien zu erkennen und entsprechende Maßnahmen zu ergreifen.

Weitere Informationen zu den Funktionen zur Anomalieerkennung finden Sie im technischen Überblick über die Anomalieerkennung von Veritas.

Primärspeichererkennung

Veritas adressiert mit NetBackup nicht nur sekundäre Backup-Daten, sondern auch den primären Speicher – dort, wo sich die Anwendung befindet – mit Veritas Alta™ Data Insight für die Cloud und NetBackup Data Insight für On-Premises. Data Insight ergänzt bestehende Sicherheitserkennungstools durch die Bereitstellung der Erkennung von Anomalien, benutzerdefinierter Ransomware-spezifischer Abfragevorlagen und der Identifizierung von Dateierweiterungen, die für die Erkennung von Ransomware nützlich sind. Data Insight umfasst richtlinienbasierte Überwachung und Warnungen nahezu in Echtzeit, die dabei helfen, böswilliges oder anomales Verhalten von Benutzerkonten zu erkennen. Dazu scannt es die unstrukturierten Datensysteme, die es überwacht, und sammelt Audits aller Benutzeraktivitäten, die an allen Dateien durchgeführt werden – wie Lesen, Schreiben, Erstellen, Löschen und Umbenennen – und führt gleichzeitig Sicherheits- und Dateizählungen für jeden Benutzer durch (siehe Abbildung 7).

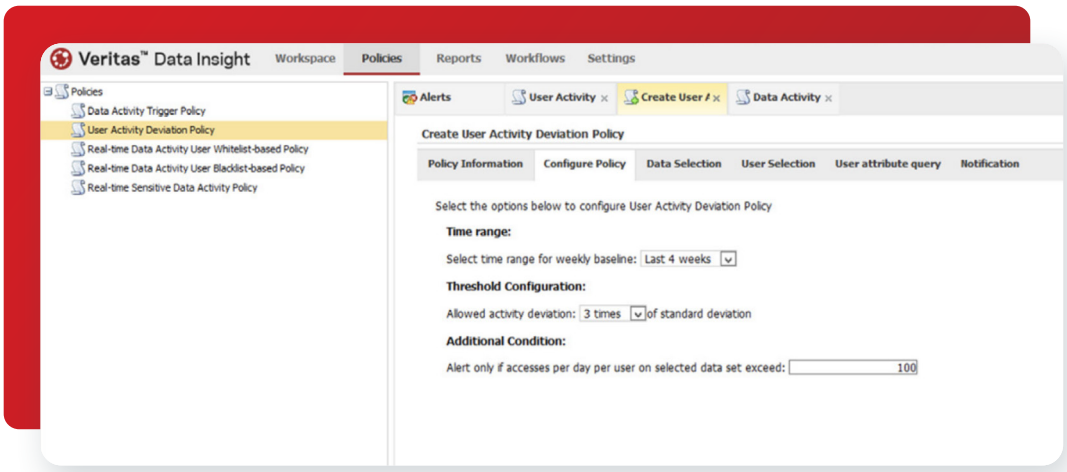


Abbildung 7. Einrichten einer Richtlinie zur Erkennung von Benutzeraktivitäten in Data Insight.

Diese Technologie vergleicht die gesammelten historischen Daten und sucht nach statistischen Standardabweichungen, um anomales Verhalten zu erkennen und gleichzeitig Konten zu identifizieren, die möglicherweise durch Ransomware kompromittiert wurden. Data Insight kann außerdem bösartige Benutzerkonten oder Ransomware-spezifische Aktivitäten erkennen und den Speicherort potenzieller Ransomware-Dateien ermitteln.

Malware-Erkennung

Veritas bietet sowohl automatisierte als auch On-Demand-Scans für geschützte Backups. Die automatische Malware-Scanfunktion beseitigt menschliche Abhängigkeiten und ermöglicht es der Technologie der künstlichen Intelligenz/maschinellen Lernens (KI/ML), einzugreifen und nach Malware zu scannen. Der AI/ML-Malware-Scan wird automatisch durch einen hohen Anomalie-Score ausgelöst Das Scannen umfasst unstrukturierte Daten, sowohl von Windows als auch von Linux. Diese Aufnahme ist von entscheidender Bedeutung, da Malware häufig über ein Hauptverzeichnis in Ihre Umgebung gelangt, weil dort meist große Mengen unstrukturierter Daten vorhanden sind.

Wird eine Wiederherstellung nötig, werden die Backup-Daten gescannt. Klare visuelle Darstellungen und Warnhinweise machen auf infizierte Backups aufmerksam und stellen sicher, dass alle wiederhergestellten Daten sauber und unbeeinträchtigt sind. Diese Vorgehensweise wird oft als Wiederherstellen der letzten als funktionierend bekannten Kopie bezeichnet (siehe Abbildung 8).

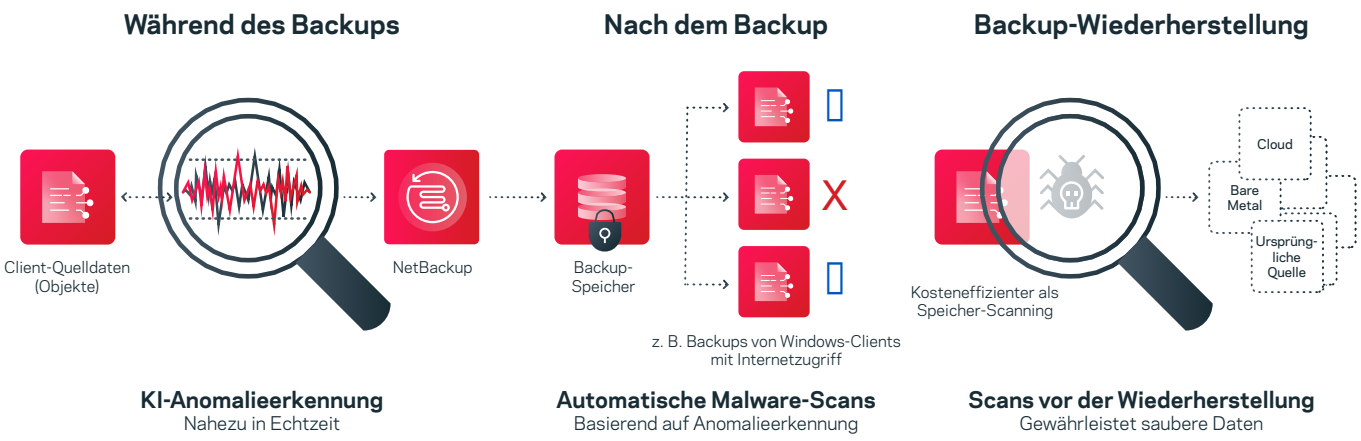


Abbildung 8. Ein allgemeiner Überblick über die Malware-Erkennung in NetBackup.

Wiederherstellen

Cyberangriffe erfolgen nie nach demselben Prinzip. Angesichts der sich laufend weiterentwickelnden Bedrohungslandschaft von heute ist es von entscheidender Bedeutung, eine optimierte Strategie zu entwickeln, die weit über Wiederherstellungspunkte und einzelne Backup-Kopien hinausgeht. Dank einer optimierten und vereinfachten Wiederherstellungserfahrung sind Sie unabhängig von der Größenordnung innerhalb von Minuten statt Stunden und Tagen wieder einsatzbereit.

Bislang betrachteten Unternehmen Backup und Wiederherstellung als die letzte Verteidigungslinie, doch mit Veritas-Lösungen werden Umgebungen für die Wiederherstellung optimiert und sie wird zu einem wesentlichen Bestandteil für den Erfolg der Ausfallsicherheit. Veritas stellt eine Vielzahl von Lösungen bereit, die die betriebliche und geschäftliche Ausfallsicherheit gewährleisten, indem sie die Flexibilität und Auswahl bieten, die für eine schnelle Wiederherstellung erforderlich sind. Warum ist diese Flexibilität wichtig? In manchen Fällen sind sämtliche Daten betroffen. Dann muss möglicherweise ein komplettes Rechenzentrum in der Cloud auf Abruf wiederhergestellt werden. Andererseits ist möglicherweise nur ein Teil Ihrer Umgebung betroffen. Daher kann es von entscheidender Bedeutung sein, über Lösungen zu verfügen, mit denen Sie einzelne Datenbanken und Dateien abrufen können, um diese schnell wieder in die Produktion zu überführen. Wenn ganze Server verschlüsselt werden, müssen Sie diese Server möglicherweise schnell an anderer Stelle wiederherstellen. Oder vielleicht müssen Sie einfach eine große Anzahl von VMs wieder in die Produktion wiederherstellen.

Wiederherstellung im großen Umfang ist komplex

Heterogenität

Mischung aus Rechenumgebungen über Rechenzentren hinweg – von Edge über den Core bis zur Cloud. (Physisch, virtuell, Cloud, Hybrid, Band)

Flexible, hybride und schnelle Wiederherstellung. Eine Wiederherstellung zurück zum Original oder eine Skalierung von der Objektebene zur Datencenter-Wiederherstellung ist nicht immer möglich.

Kostengünstige, unterbrechungsfreie Wiederherstellungsproben. Erhöhte Produktivität und reduzierte Ausfallzeiten.

Abhängigkeiten

Management komplexer Infrastruktur, Netzwerke, Speicher und funktionsübergreifender Teams. (vor Ort, Hybrid, Cloud)

Multi-Tier-Anwendungen mit mehreren Komponenten.
Wiederherstellung aus bereinigten Daten – von einem Ort zum anderen (von Edge zu Core und Cloud)

Kann ein zeitaufwändiger, mühsamer und manueller Prozess sein.
Schulungs- und Qualifikationsdefizite.

Abbildung 9. Die komplexe Wiederherstellung im großen Maßstab, die Veritas-Lösungen bewältigen.

Veritas bietet Lösungen für die in Abbildung 9 dargestellten Wiederherstellungskomplexitäten im großen Maßstab.

Veritas Resiliency Platform

Veritas Resiliency Platform löst diese Herausforderungen, indem es eine automatisierte Orchestrierung in der gesamten heterogenen Umgebung Ihres Unternehmens mit einer konsistenten Benutzererfahrung und Einblick in die besten Wiederherstellungsoptionen basierend auf den verfügbaren Optionen bereitstellt, sodass Sie Ihr Wiederherstellungszeitziel (RTO) und Ihr Wiederherstellungspunktziel erreichen können (RPO) (siehe Abbildung 10).

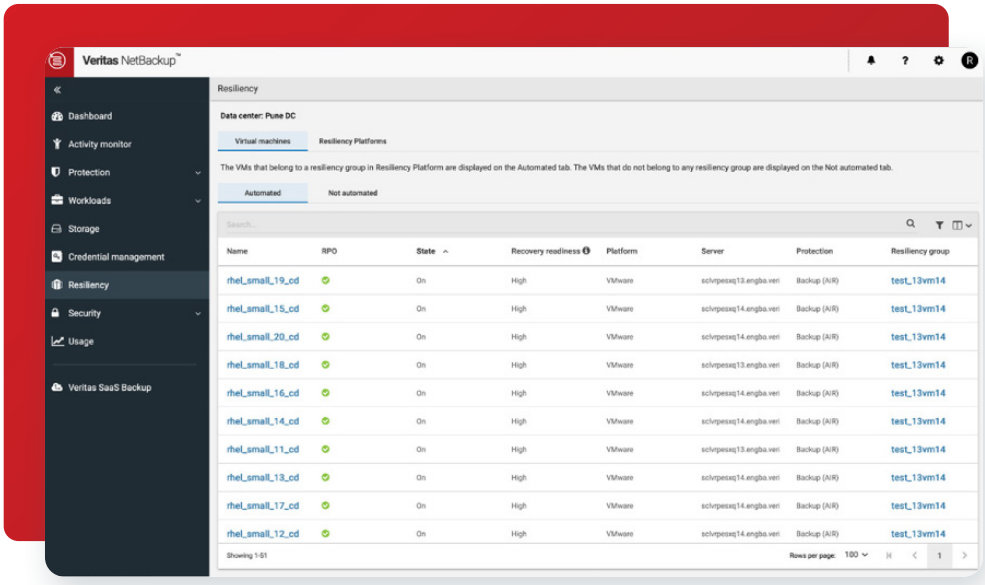


Abbildung 10. Das Ausfallsicherheits-Dashboard in der NetBackup-Web-Benutzeroberfläche.

Für das effizienteste RTO bietet Veritas Einblicke in Wiederherstellungsvorgänge, die dabei helfen, die beste Wiederherstellungsmethode zu ermitteln, indem Sie Ihre RTOs, Workload(s) und Anwendungen im gesamten Rechenzentrum verstehen.

Veritas Resiliency Platform ermöglicht die Orchestrierung in heterogenen Umgebungen, die die Workload und die Anwendung sowie die entsprechenden Daten umfassen, indem automatisierte Replikation, speicherbasierte Replikation oder der integrierte Data Mover von NetBackup verwendet werden. Mit dem integrierten Data Mover von NetBackup können Sie das RTO und RPO auswählen, das den Geschäftsanforderungen Ihrer Anwendung entspricht.

Insbesondere unterstützt die Lösung die Automatisierung durch die Nutzung von virtuellen Business-Services (Notfallwiederherstellungsschutz für eine mehrschichtige Anwendung) mit Ausfallsicherheits- und Evakuierungsplänen (dem Runbook), sodass Sie die Wiederherstellung im großen Maßstab zwischen Rechenzentren oder Cloud-Infrastrukturen automatisieren können.

Die Lösung ermöglicht auch eine einstudierte Validierung auf Knopfdruck in isolierten Netzwerken. In Ransomware-Wiederherstellungsszenarien können Unternehmen benutzerdefinierte Skripts nutzen, um sie in Virenscanlösungen von Drittanbietern in den Workflow zu integrieren und vor der Rückkehr in die Produktion auf Malware zu validieren.

Aus RPO-Sicht bieten NetBackup für On-Premises und Veritas Alta™ Data Protection für Cloud Continuous Data Protection (CDP) zusätzliche Ausfallsicherheit durch granulare Wiederherstellung von VMs mit einem RPO von nahezu Null. CDP gewährleistet die Wiederherstellungsfähigkeit für Anwendungen in Ihrer heterogenen Umgebung mithilfe granularer Wiederherstellungspunkte in der Datenreplikation von Resiliency nahezu in Echtzeit (siehe Abbildung 11). Diese Funktion unterstützt die Wiederherstellung nach Malware oder Beschädigung, wenn diese bereits repliziert wurde.

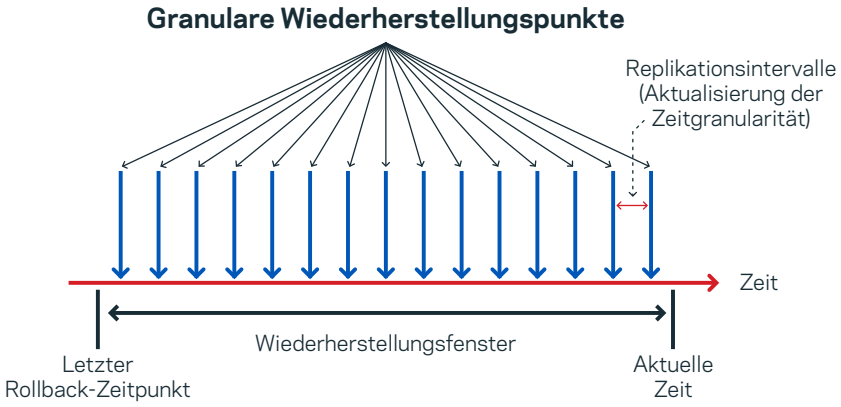


Abbildung 11. Ein Überblick über den kontinuierlichen Datenschutz von NetBackup.

Erfahren Sie mehr über Continuous Data Protection für VMware und erweiterte Ausfallsicherheitsoptionen für den VMware-Anwendungsschutz, in den entsprechenden Blogs.

Andere Wiederherstellungsmethoden mit NetBackup

Veritas bietet eine Vielzahl weiterer Wiederherstellungsmethoden zur Erfüllung Ihrer RTOs und RPOs und gibt Ihnen so die Flexibilität, die optimale Wiederherstellungsmethode für Ihr Unternehmen auszuwählen. Abbildung 12 zeigt die optimale Wiederherstellungsoption basierend auf RPOs und RTOs.

RTO- und RPO-Ziele bestimmen die optimale Option

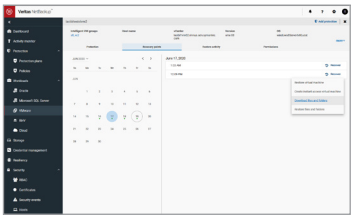
Abbildung 12. Auswahl einer optimalen Wiederherstellungsoption basierend auf RTOs und RPOs.

NetBackup Instant Recovery für VMware: Bietet eine schnelle VM-Wiederherstellung, indem mithilfe der Änderungsblockverfolgung ermittelt wird, welche eindeutigen Blöcke wiederhergestellt werden müssen, und nur diese Änderungen angewendet werden, um Ihre VM innerhalb von Sekunden wieder in einen fehlerfreien Zustand zu versetzen – nach einer Katastrophe oder einem Ransomware-Angriff, statt nach Minuten oder gar Stunden. Dieser Prozess stellt mühelos 1 oder 100 Maschinen wieder her und ermöglicht eine schnelle Massenwiederherstellung, unabhängig davon, wo sich Ihre Infrastruktur befindet.

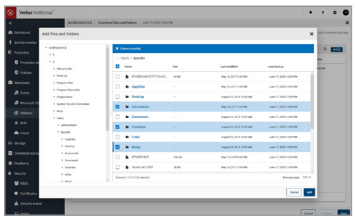
Weitere Informationen zu Instant Recovery für VMware finden Sie in diesem Blog.

VM-Wiederherstellung: Für ein Backup von VMware-VMs stehen acht Arten der Wiederherstellung zur Verfügung: vollständige VM, einzelne VMDK, Datei und Ordner, vollständige Anwendung, Sofortzugriff, Dateidownload, Anwendungs-GRT und AMI-Konvertierung. Die zusätzliche Unterstützung für vTPM gewährleistet Sicherung und Wiederherstellung für Hochsicherheitsumgebungen.

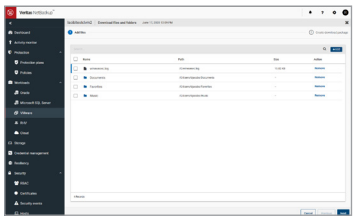
Instant Access für MSSQL und VMware: Mit Instant Access für VMware können Sie jeden Rechner fast sofort wiederherstellen, ohne auf die Übertragung der VM-Daten aus dem Backup warten zu müssen (siehe Abbildung 13). Sie können ein Backup auch verwenden, um VMs direkt aus dem Backup-Speicher zu testen oder wiederherzustellen. Diese VMs werden automatisch als reguläre Gäste in der VMware-Infrastruktur angezeigt. Zudem können Sie einzelne Dateien direkt in der NetBackup-Web-Benutzeroberfläche durchsuchen und wiederherstellen. Für schnelle Wiederherstellungsszenarien können Sie VMware Storage vMotion verwenden, um die VM während der Nutzung vom Backup-Speicher in die Produktion zu migrieren.



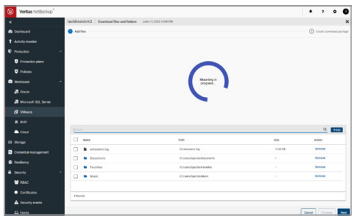
Durchsuchen Sie verfügbare Wiederherstellungspunkte für eine geschützte virtuelle VMware-Maschine.



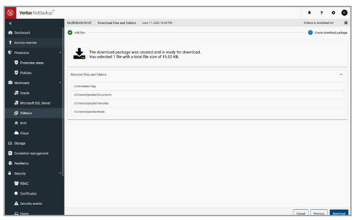
Wählen Sie die wiederherzustellenden Dateien oder Ordner aus.



Überprüfen Sie die Liste der herunterzuladenden Dateien oder Ordner.



NetBackup Instant Access mountet das Backup-Image, um Dateien in ein Paket zu extrahieren.



Die gepackten Dateien oder Ordner stehen zum Download zur Verfügung.

Abbildung 13. Verwenden Sie VMware Instant Access zum Sichern von VMs in Ihrer gesamten Infrastruktur.

Die vollständige Konfiguration und Einzelheiten finden Sie im Administratorhandbuch für Veritas NetBackup für VMware.

Instant Access für MSSQL bietet sofortige Verfügbarkeit von Datenbanken und eine granulare Wiederherstellung von Datenbankelementen mithilfe von Backup-Speicher (siehe Abbildung 14). Self-Service-Funktionen ermöglichen Datenbankadministratoren die schnelle Bereitstellung von MSSQL-Datenbanken für ihre Entwicklungs-/Testanforderungen. Wenn einige Datenkopien von Ransomware betroffen sind, bietet Ihnen NetBackup die Flexibilität, mithilfe unserer Schnittstelle und APIs jede verfügbare Sicherungskopie wiederherzustellen (siehe Abbildung 15).

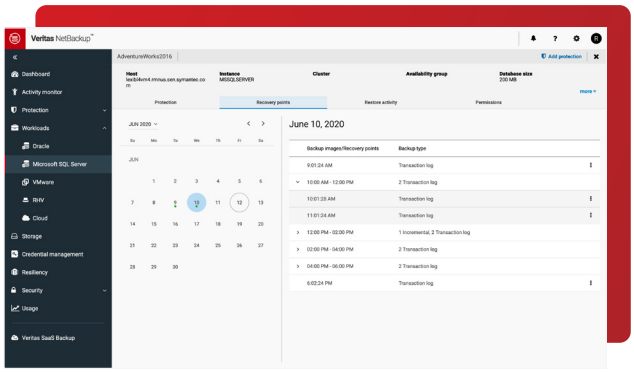


Abbildung 14. NetBackup bietet granulare Point-in-Time-Wiederherstellungsoptionen für MSSQL.

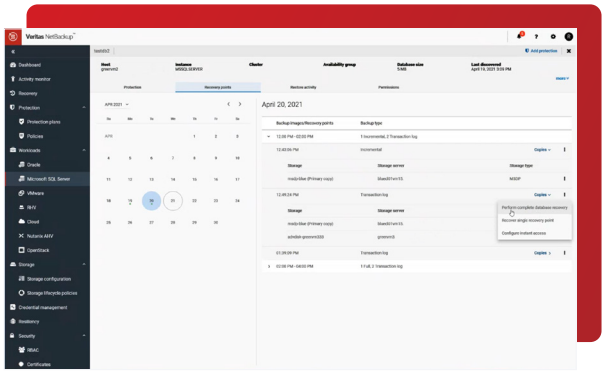


Abbildung 15. Stellen Sie Datenbanken aus jeder Kopie eines MSSQL-Backups wieder her.

NetBackup Snapshot Manager: Nutzung von Container-Technologie und Cloud-Dienstanbietern Unabhängig von der Speicherplattform nutzt NetBackup Snapshot Manager Cloud-native Snapshot-Technologie auf eine vom Cloud-Anbieter unabhängige Weise, die einen einfachen Schutz von Hybrid- und Multi-Cloud-Infrastrukturen ermöglicht. Darüber hinaus bietet Snapshot Manager Funktionen, die über die Grundfunktionen einer öffentlichen Cloud hinausgehen, und ermöglicht anwendungsbezogene Snapshots, die Wiederherstellung einzelner Dateien und die Snapshot-Migration in mehrere Regionen. Durch die Unterstützung mehrerer Konten durch Snapshot Manager können Backups sicher in einem anderen Konto gespeichert werden, wodurch die Auswirkungen im Falle eines kompromittierten Kontos verringert werden.

Universal Share und Schutzpunkte: Mit Universal Share, einer MSDP-Funktion, können Sie durch Deduplizierung gesicherten Speicher auf dem NetBackup-Server als sichere Freigaben bereitstellen und so Datenbanken oder andere Workloads schützen, für die kein Agent oder keine Backup-API vorhanden ist. Sie können Universal Share als Network Attached Storage (NAS) verwenden, um Daten mithilfe von Komprimierung und Deduplizierung zu speichern. Mit vollständiger API-Unterstützung und zentraler Verwaltung von Freigaben und Schutzpunkten in der NetBackup-Web-Benutzeroberfläche sowie Unterstützung von Benutzerkontingenten und Active Directory-Integration bieten NetBackup HA Appliances verbesserte Verwaltungsschutzpunkte für universelle Freigaben, mit denen Sie eine Point-in-Time-Kopie davon erstellen können Daten auf der Freigabe, erstellen Sie sofort ein Backup-Image und verwenden Sie es dann wie jedes andere Backup.

Weitere Informationen finden Sie im Abschnitt „Universal Shares“ im Veritas NetBackup-Administratorhandbuch.

NetBackup Universal Shares für Oracle: Aufbauend auf den Funktionen von Oracle ermöglicht die neueste Version von NetBackup Universal Shares für Oracle allen Oracle-Datenbankadministratoren, Datenbanken direkt aus dem Speicher einer NetBackup Appliance zu starten.

Weitere Informationen finden Sie im Handbuch für Veritas NetBackup™ für Oracle-Administratoren.

Langzeitaufbewahrungsarchiv: Wenn Sie Daten über einen längeren Zeitraum aufbewahren müssen, bietet diese Option eine kostengünstige und dauerhafte Lösung mit Deduplizierung und Komprimierung von Daten. Mit dieser Methode können Sie auch Objektspeicher und private oder öffentliche Clouds nutzen. Für private Cloud-Anwendungsfälle bietet die Veritas Access Appliance in unserer Enterprise Data Services Platform eine langfristige Aufbewahrung (LTR). Bedenken Sie bei der Entscheidung für eine Wiederherstellungsmethode, dass LTR-Lösungen kosteneffektiv und optimal für Gesundheitssysteme und andere Einrichtungen sind, die Daten über einen langen Zeitraum aufbewahren müssen. Für Unternehmen, die weiterhin Bandtechnologien nutzen möchten, bieten wir die umfassendste bandbasierte Lösung, einschließlich einer zuverlässigen Air-Gap-Methode zur Wiederherstellung nach Ransomware.

Traditionelle Wiederherstellung: Diese Methode umfasst die granulare Wiederherstellung einer bestimmten Datei, eine vollständige Server-/Anwendungswiederherstellung und eine Disaster Recovery (DR)-Wiederherstellung an einem anderen Standort oder in der Cloud. Mit der Veritas Resiliency Platform können Sie die traditionelle Wiederherstellung per Knopfdruck automatisieren und orchestrieren und so den DR-Prozess optimieren.

Bare Metal Restore: Wenn bei einer Ransomware-Wiederherstellung betroffene Hardware genutzt werden muss, kann Bare Metal Restore (BMR) ein wertvoller Ausweg sein, wenn Sie über begrenzte Ressourcen verfügen. BMR automatisiert den Serverwiederherstellungsprozess und macht eine Neuinstallation von Betriebssystemen oder eine manuelle Hardwarekonfiguration überflüssig. Wenn Systeme beschädigt sind und vollständig überschrieben werden müssen, können Sie mit BMR Systeme schnell von Grund auf neu erstellen und das Betriebssystem und die Anwendungsdaten in einem einzigen Vorgang wiederherstellen.

Differenzierung im Wettbewerb

Unsere Veritas-Lösungen stellen sicher, dass Ihre Daten immer verfügbar und geschützt sind, unterstützen die Hochverfügbarkeit von Anwendungen und bieten eine bewährte Wiederherstellung in großem Maßstab – und das alles bei gleichzeitiger Aufrechterhaltung der Geschäftskontinuität im Falle von Angriffen auf Daten und Infrastruktur. Traditionelle Wettbewerber, ob primäre Speicherriesen oder Scale-out-Anbieter, gehen die Ransomware-Resilienz nicht so umfassend an wie Veritas. Im Vergleich zur Konkurrenz nähert sich Veritas der Ransomware-Resilienz aus geschäftlicher Sicht und bietet eine robuste Strategie für den Schutz, die Erkennung und die Wiederherstellung nach Ransomware.

Es folgen einige wichtige Fragen, die Sie bei der Auswahl eines Datenschutzanbieters berücksichtigen sollten:

- Bietet die Lösung Ransomware-Resilienz im Kern, an der Peripherie und in der Cloud?
- Bietet sie unveränderlichen Speicher, unabhängig davon, ob sie als BYO, Appliance, Cloud oder SaaS bereitgestellt wird?
- Unterstützt die Lösung die 3-2-1-1-Sicherungskopieregel in jedem Szenario?

Veritas kann all das und noch mehr:

- Bietet mehrere Bereitstellungsoptionen und die Ransomware-Resilienz bleibt für jedes Unternehmens-Bereitstellungsszenario verfügbar
- Verfolgt einen mehrschichtigen Sicherheitsansatz zum Schutz von Backup-Daten und schließt Hintertüren wie Cluster-Resets, externe Uhren oder BIOS
- Verwendet ein gehärtetes Betriebssystem, um die Angriffsfläche von Ransomware zu reduzieren
- Entwirft Lösungen auf der Grundlage der 3-2-1-1-Best Practices und bietet Kopierstandards für Bandunterstützung, unveränderliche Speicherung und Air-Gap
- Erstellt Appliances mit gehärteten Containerbereitstellungen, was Angriffe noch schwieriger macht als herkömmliche physische oder VM-Formfaktoren
- Beinhaltet integrierte Einbrucherkennung und Schutz in Appliances, die den Aufwand für IT- und Sicherheitsteams eliminieren
- Bietet Erkennung nicht nur auf der Ebene der Backup-Überwachung, sondern weitet diese auch auf die Infrastruktur und das primäre Datenzugriffsmuster aus und bietet die Möglichkeit, bekannte Ransomware zu löschen sowie ein potenziell gehacktes Konto zu deaktivieren, um die Auswirkungen von Ransomware zu minimieren
- Bietet die Möglichkeit, nur Änderungen an VMs durch Ransomware-Angriffe rückgängig zu machen, wodurch die Wiederherstellung nach Ransomware effizient und schnell erfolgt

Wir bei Veritas wissen, wie wichtig Ausfallsicherheit ist. Betrachten Sie zwei Arten von Sicherheitssystemen, die eine Einrichtung überwachen: Das eine betrachtet nur den Verlauf der Sicherheitsaufnahmen, um Einbrüche zu erkennen, und das andere betrachtet die Live-Feeds der Überwachung sowie das historische Filmmaterial. Das System, das die Live-Feeds prüft, kann auch den Zugang zur Einrichtung sperren, wenn es Anzeichen eines Einbruchs feststellt. Welches System ist Ihrer Meinung nach das bessere? Veritas bietet Ransomware-Erkennung durch Überwachung von Produktionssystemen. Diese Überwachung geht über Größe und Erweiterungen hinaus und deckt gleichzeitig Daten und Infrastruktur ab. Es kann Abweichungen in den Datenzugriffsmustern erkennen und Konten sperren, die möglicherweise zum Ausführen von Ransomware/Malware verwendet werden. Durch die Analyse von Änderungen in Backup-Attributen mithilfe von KI/ML können Veritas Alta™ Data Protection für die Cloud und NetBackup für On-Premises Unternehmen vor möglichen Ransomware-Einbrüchen warnen.

Wir sind uns der Notwendigkeit bewusst, Daten auf möglichst effiziente und schnelle Weise wiederherstellen zu müssen. NetBackup bietet Funktionen wie die sofortige Rollback-Wiederherstellung und bietet die Möglichkeit, durch Ransomware verursachte Schäden zu beseitigen, ohne dass vollständige VM-Wiederherstellungen und -Abschaltungen erforderlich sind. Veritas Alta™ Data Protection für die Cloud und NetBackup für lokale Anwendungen ermöglicht Wiederherstellungspläne für Tausende von VMs, die Teil komplexer, mehrschichtiger Umgebungen sein können, sowie die Möglichkeit, Tests derselben in einer isolierten Umgebung durchzuführen. NetBackup Flex und Flex Scale Appliances weisen einige der besten Zahlen ihrer Klasse für optimierten Sofortzugriff und Wiederherstellungen wichtiger Workloads auf. Veritas Alta™ SaaS Protection (vormals Netbackup Saas Protection) bewältigt nachweislich auch Wiederherstellungen im Petabyte-Bereich. All dies sind wichtige Forschungspunkte, wenn man die Vollständigkeit der Ransomware-Resilienz von Veritas mit der eines Mitbewerbers vergleicht.

Fazit

Ransomware und interne Personen mit böswilligen Absichten stellen ein ernstzunehmendes Risiko dar. Es werden ständig neue Schwachstellen in Betriebssystemen entdeckt und regelmäßig neue Varianten von bekannter Malware und Ransomware entwickelt. Ransomware ist ein äußerst lukratives Geschäft, weshalb Kriminelle motiviert sind, weiterhin nach neuen Wegen zu suchen, um in die Infrastruktur eines Unternehmens einzudringen und seinen Geschäftsbetrieb lahmzulegen. Selbst wenn System- und Backup-Administratoren erhebliche Anstrengungen unternehmen, um Unternehmensdaten zu schützen, können Ransomware und böswillige Insider gelegentlich dennoch eindringen und die kritischsten Daten eines Unternehmens beeinträchtigen. Deshalb ist eine ganzheitliche, vielschichtige und umfassende Strategie unerlässlich – und die beste Verteidigung.

Veritas hat den Prozess für Sie vereinfacht. Unsere Lösungen wurden unter dem Gesichtspunkt der Ausfallsicherheit entwickelt und bieten eine einzige, einheitliche Plattform, die Ihnen dabei hilft, IT-Systeme und Datenintegrität zu schützen, durch Überwachung und Schadensbegrenzung zu erkennen und durch Automatisierung und Orchestrierung rasch wiederherzustellen. Unsere Lösungen reduzieren Schwachstellen, beseitigen Inseln oder potenzielle Angriffsflächen und sind einfach zu skalieren, zu aktualisieren und zu warten. Keine Daten bleiben ungeschützt – von der Peripherie über den Kern bis zur Cloud. Obwohl Backup und Wiederherstellung für viele die letzte Verteidigungslinie gegen Ransomware-Angriffe sind, empfehlen wir, sie als sinnvollen und zuverlässigen Teil Ihrer umfassenden, mehrschichtigen Strategie zum Schutz, zur Erkennung und zur Wiederherstellung der Cybersicherheit zu betrachten.

Für weitere Informationen zu unseren Lösungen finden Sie unter https://www.veritas.com/ransomware oder kontaktieren Sie uns unter https://www.veritas.com/form/requestacall/requestacall.

Referenzen

Regierung

- Das National Cybersecurity Centre of Excellence (NCCoE), Teil des National Institute of Standards and Technology (NIST), hat eine Sonderpublikation mit dem Titel „Data Integrity, Recovering from Ransomware and Other Destructive Events“ herausgegeben. Hierbei handelt es sich um ein umfassendes, dreiteiliges Dokument, das die Strategien, die Unternehmen zum Schutz vor böswilligen Aktivitäten ergreifen sollten, sowie die Wiederherstellungsschritte nach einem Vorfall in Sachen Cybersicherheit detailliert beschreibt.
  NIST Special Publication 1800-11
  „Data Integrity: Recovering from Ransomware and other Destructive Events“ (Hauptseite)
  - NIST SP 1800-11a: Executive Summary
  - NIST SP 1800-11b: Approach, Architecture, and Security Characteristics – what we built and why
  - NIST SP 1800-11c: How-To Guides – instructions for building the example solution
- United States Computer Emergency Readiness Team: „Data Backup Options“

Veritas

- „Insider Threat 101: Detect and Protect with Veritas Data Insight“

Weitere Informationen zu den Ransomware-Berichtsvorlagen finden Sie in den folgenden Abschnitten im Veritas Data Insight-Benutzerhandbuch:

- Informationen zu benutzerdefinierten Data Insight-Berichten
- Informationen zu DQL-Abfragevorlagen

- Veritas Flex Appliances mit NetBackup Security
- Veritas Flex Appliances mit NetBackups
- Veritas Data Insight – Handbuch für Administratoren
- Veritas Data Insight – Benutzerhandbuch
- Veritas NetBackup – Handbuch für Administratoren, Band I
- Veritas NetBackup Appliance – Handbuch für Administratoren
- Veritas NetBackup Appliance Fibre Channel-Leitfaden
- Veritas NetBackup Appliance – Sicherheitshandbuch
- Veritas NetBackup Cloud – Handbuch für Administratoren
- Veritas NetBackup – Deduplizierungshandbuch
- Veritas NetBackup – Handbuch zu Sicherheit und Verschlüsselung
- Veritas NetBackup für Oracle – Handbuch für Administratoren
- Veritas NetBackup für VMware – Administratorhandbuch

1 https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-

Über Veritas

Veritas Technologies ist ein weltweit führender Anbieter im Bereich Multicloud-Datenmanagement. Über 80.000 Kunden – darunter 95 Prozent der Fortune 100 – vertrauen darauf, mit Lösungen von Veritas den Schutz, die Wiederherstellbarkeit und Compliance ihrer Daten zu gewährleisten. Veritas steht für skalierte, zuverlässige Produkte, welche die Widerstandsfähigkeit bieten, die seine Kunden im Fall von Cyberangriffen wie Ransomware benötigen. Kein anderer Anbieter erreicht Veritas' Leistungsfähigkeit mit Unterstützung für mehr als 800 Datenquellen, über 100 Betriebssystemen, über 1.400 Speicherzielen und über 60 Clouds im Rahmen eines einzigen, einheitlichen Ansatzes. Mithilfe der Cloud Scale Technology setzt Veritas heute seine Strategie für autonomes Datenmanagement um, die den betrieblichen Aufwand reduziert und gleichzeitig einen größeren Mehrwert bietet. Weitere Informationen finden Sie unter veritas.com/de/de und folgen Sie uns auf Twitter unter @veritastechllc.

VERITAS

Veritas (Deutschland) GmbH
Theatinerstr. 11, 8. Etage
80333 München
Tel.: 0800-724 40 75
veritas.com/de/de

Für Kontaktinformationen weltweit besuchen Sie:
veritas.com/de/de/company/contact

V1726 01/23