Enterprise Strategy Group | **Getting to the bigger truth.™**

Technische Validierung

Cybersicherheit mit Veritas

Ransomware-Schutz von Veritas

Von Craig Ledo, IT-Validierungsanalyst

September 2022

Diese technische ESG-Validierung wurde von Veritas in Auftrag gegeben und wird unter Lizenz von TechTarget, Inc. vertrieben.

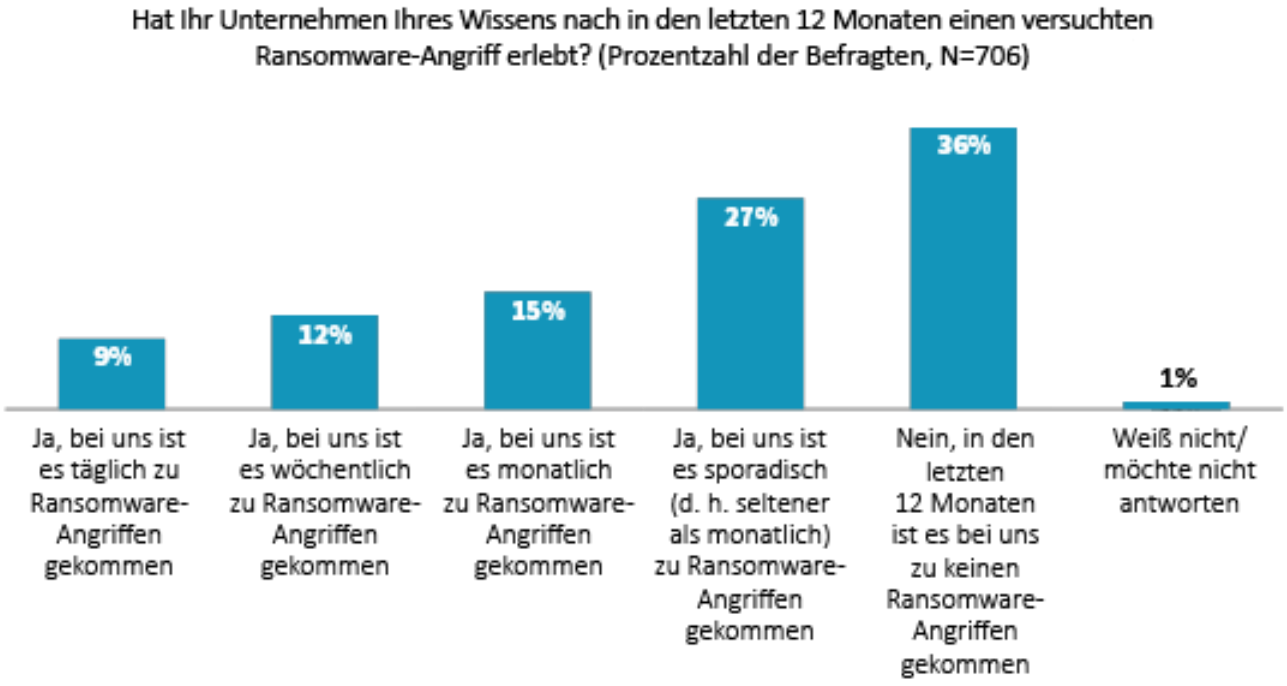
Einführung

Hierin ist die detaillierte Bewertung der Veritas-Lösung dokumentiert, einschließlich der Ergebnisse beim Schutz von Daten, bei der Erkennung von Bedrohungen und der Wiederherstellung im großen Maßstab. Insbesondere umfasste diese Bewertung die Validierung von 12 Testszenarien mit dem gesamten Veritas-Portfolio an Cybersicherheitslösungen.

Hintergrund

Führungskräfte von Unternehmen und IT-Abteilungen sind nach wie vor sehr besorgt über Ransomware-Angriffe, und das aus gutem Grund: Diese gefährden den Zugriff auf das Lebenselixier eines Unternehmens – Daten. Die anhaltenden Ransomware-Angriffe haben zu enormen Kosten geführt, etwa durch Ausfallzeiten, Produktivitätseinbußen, Geräte- und Netzwerkwiederherstellung, verlorene Geschäftschancen, Lösegeld, Schaden am Markenwert usw. Jährlich werden Millionen von Dollar ausgegeben, um Zugangspunkte zu Daten zu schützen, aber dennoch unterschätzen viele Unternehmen immer noch den strategischen Wert von besserem Datenschutz. ESG-Untersuchungen zeigen, dass 36 % der Umfrageteilnehmer angaben, dass ihr Unternehmen in den letzten 12 Monaten mindestens einmal monatlich Sondierungsangriffe erlebt hat, darunter 9 % täglich und 12 % wöchentlich (siehe Abbildung 1).[1]

Abbildung 1. Häufig kommt es zu wiederkehrenden Ransomware-Angriffen



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Weitere 27 % der Befragten erlebten sporadischere Ransomware-Angriffe. Daher ist es für Unternehmen von entscheidender Bedeutung, starke proaktive und defensive Maßnahmen gegen Ransomware-Angriffe zu implementieren, um sie erfolgreich abzuwehren, insbesondere da Opfer von diesen Kriminellen erneut attackiert werden können und meist auch werden.

Außerdem ist eine fortschrittliche, mehrschichtige Resilience-Strategie erforderlich, um sicherzustellen, dass IT-Services sicher, robust und wiederherstellbar sind und gleichzeitig das reibungslose Erlebnis bieten, das Endbenutzer erwarten. So helfen z. B. Lösungen, die gehärtete Software und Hardware umfassen und unveränderbare und unlöschbare Speicher unterstützen, bei der Bereitstellung einer umfassenden, mehrschichtigen Cybersicherheitsstrategie.

[1] Quelle: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

Überblick über die Veritas-Lösung für Cybersicherheit

Veritas bietet einen einheitlichen, mehrschichtigen Plattformansatz, der proaktiven Schutz, Erkennung und Backup- und Wiederherstellungsfunktionen nahtlos integriert. Insbesondere stellt Veritas ein Zero-Trust-Sicherheitsmodell zur Verfügung, mit dem eine bessere Zugriffskontrolle implementiert, Sicherheitsverletzungen eingedämmt, Vermögenswerte geschützt und potenzielle Schäden gemindert werden können.

Schutz:

- Stellt sicher, dass kritische Daten und die IT-Infrastruktur vor unbekannten und unerwarteten Problemen geschützt sind, indem alle Teile der Umgebung mit universellem Schutz gesichert werden, der intelligent angewendet und automatisch verwaltet wird, um immer richtig skaliert zu sein.
- Die Backup-Infrastruktur und gesicherte Daten ermöglichen es Unternehmen, diese Komponenten zu einem wesentlichen Teil für erfolgreiche Resilience zu machen.
- Veritas NetBackup bietet Unterstützung von Edge zu Core und Cloud, die mehr als 800 Datenquellen, mehr als 1.400 Speicheranbieter und mehr als 60 Cloud-Provider umfasst, damit selbst die anspruchsvollsten und breitesten Umgebungen gesichert werden können.
- Veritas Intelligent Policies bieten höhere Automatisierungsgrade, sodass Administratoren von einem höheren Maß an Effizienz profitieren.
- Veritas bietet eine Air-Gap-Lösung zum Schutz der Datenintegrität, damit Backup-Dateien sicher bleiben und und böswillige Eindringlinge sie nicht kompromittieren können.
- Backup-Images sind mit einer intern verwalteten, sicheren Compliance-Uhr unveränderbar und unlöschbar.

Erkennung:

- Veritas bietet Lösungen für eine umfassende Infrastrukturübersicht, die alle dunklen Daten in der Unternehmensumgebung sichtbar machen.
- Zudem schenkt Veritas das beruhigende Wissen, dass alles in der Umgebung sicher und geschützt ist, und trägt dazu bei, dass Ransomware seinen Schrecken verliert.
- Veritas bietet auch KI-gestützte Anomalie- und Malware-Erkennung für Primär- und Sicherungsdaten sowie ereignisgesteuerte Malware-Scans, welche die Chance erhöhen, rechtzeitig zu handeln, bevor Cyberkriminelle oder bösartiger Code Schaden anrichten.

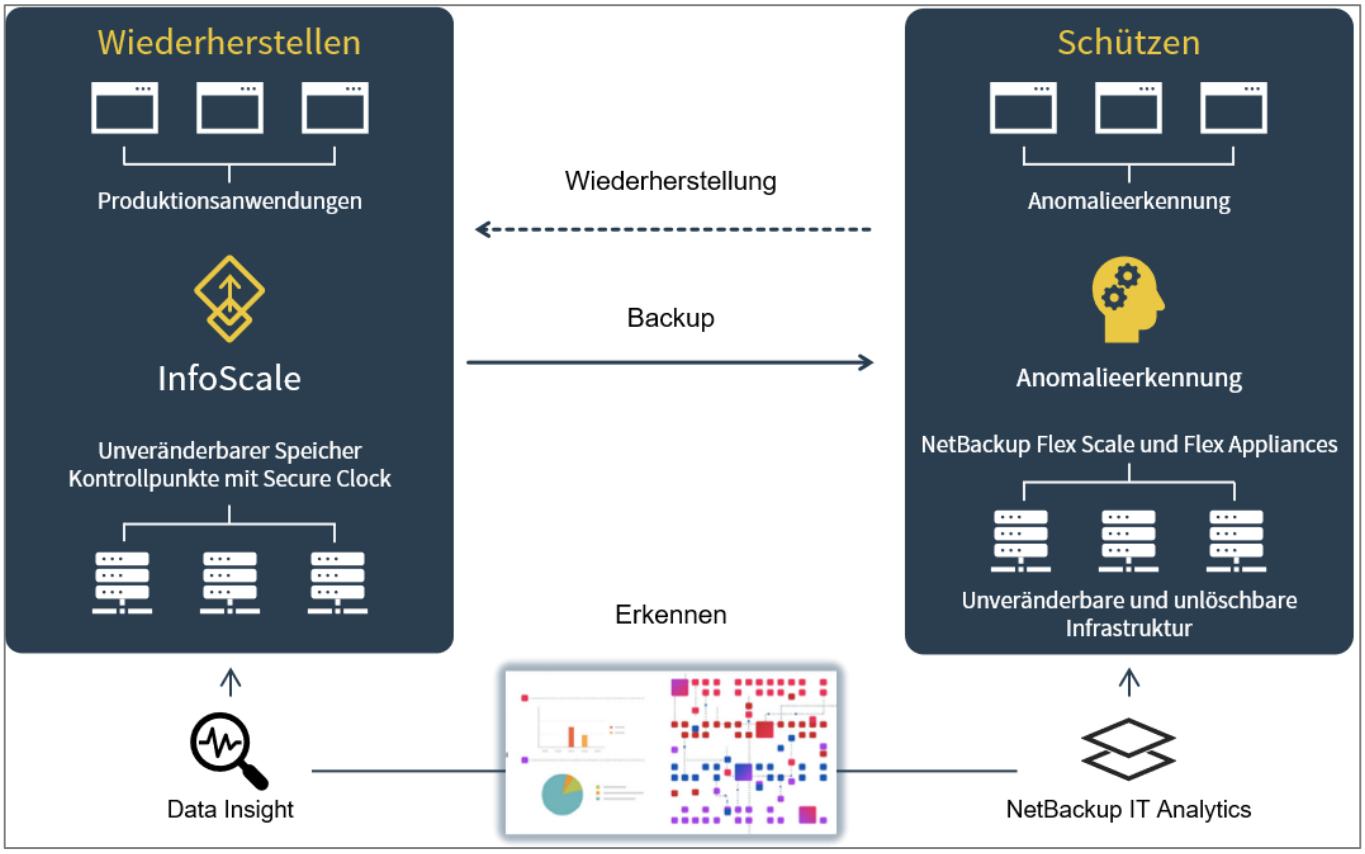
Wiederherstellung:

- Mit Veritas-Lösungen als wesentlicher Komponente für den Erfolg der Ausfallsicherheit werden Umgebungen für die Wiederherstellung optimiert.
- Veritas verfügt über integrierte Sicherheitslösungen, mit deren Hilfe saubere und Ransomware-freie Daten und Umgebungen rasch wieder online sind.
- Manchmal sind sämtliche Daten betroffen, daher müssen Unternehmen möglicherweise ein komplettes Rechenzentrum in der Cloud und auf Abruf wiederherstellen.

- Ein anderer Vorfall betrifft vielleicht nur einen Teil der Umgebung, daher kann es entscheidend sein, über Lösungen zu verfügen, die die Flexibilität bieten, einzelne Datenbanken und Dateien schnell wieder in die Produktion zurückzuführen.
- Falls ganze Server verschlüsselt wurden, müssen Unternehmen diese anderswo schnell wiederherstellen.
- Unternehmen müssen möglicherweise eine große Anzahl von Anwendungsinstanzen wiederherstellen.
- Veritas bietet Lösungen für die Wiederherstellung im großen Maßstab, einschließlich orchestrierter und Massenwiederherstellung.

Die Lösungen von Veritas stellen sicher, dass Daten immer verfügbar und geschützt sind, tragen zur Hochverfügbarkeit von Anwendungen bei und bieten Wiederherstellung in großem Maßstab. Veritas betrachtet die Ausfallsicherheit gegen Ransomware aus der Perspektive des Geschäftsnutzens und bietet eine robuste Resilienzstrategie, die Schutz, Erkennung und Wiederherstellung im Fall eines Ransomware-Angriffs ermöglicht (siehe Abbildung 2).

Abbildung 2. Überblick über die Veritas-Lösung für Cyber Resilience



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Technische Validierung von ESG

ESG hat eine technische Validierung der Cybersicherheitslösung von Veritas durchgeführt, einschließlich des Schutzes von Daten, der Erkennung von Bedrohungen und der Wiederherstellung im großen Maßstab.

Schutz von Daten

Veritas bietet ein breites Spektrum an Funktionen, die Sie bei der Datensicherung unterstützen, darunter:

- **Identitäts- und Zugriffsmanagement**: rollenbasierter Zugriff, Single Sign-On und anpassbare Authentifizierung.
- **Datenverschlüsselung**: bei der Übertragung und im Speicher.
- **Verwaltung und Speicherung unveränderbarer Images**: Flexible, speicherunabhängige Image-Verwaltung und WORM-Speicher (Write Once, Read Many) für Images.
- **Lösungshärtung**: NetBackup Flex und NetBackup Flex Scale wurden hinsichtlich Software und Hardware gehärtet, um eine vollständig sichere Lösung anzubieten, die unveränderbare Speicher unterstützt.

ESG hat insbesondere die folgenden wichtigen Datensicherungsfunktionen validiert.

Unveränderbarkeit von Cloud-Daten

Die Lösung stellt sicher, dass Daten für einen bestimmten Zeitraum nicht geändert werden können, um sie vor Cyberkriminellen und internen Bedrohungen zu schützen. Um die Sicherheit weiter zu verbessern, befindet sich das Backup in einem sicheren Datenspeicher, der nur für den NetBackup-Speicherdienst sichtbar und zugänglich ist – Benutzer und Dateisystemdienste können nicht darauf zugreifen.

Gehärtete Undurchdringlichkeit

Der gesamte NetBackup Appliances-Stack wurde für Sicherheit gehärtet, einschließlich Linux-Betriebssystem, Management-Zugriff, Anwendungs-Binärdateien und Konfigurationseinstellungen. Er enthält proprietäre Sicherheitsrichtlinien, die konform mit den STIG-Richtlinien sind und eine obligatorische Zugriffskontrolle erzwingen. Weitere Vorteile sind Intrusion Detection- und Protection-Dienste, die den Zugriff auf Prozesse und Ressourcen einschränken und einen Audit-Trail wichtiger Benutzer- und Systemaktionen führen.

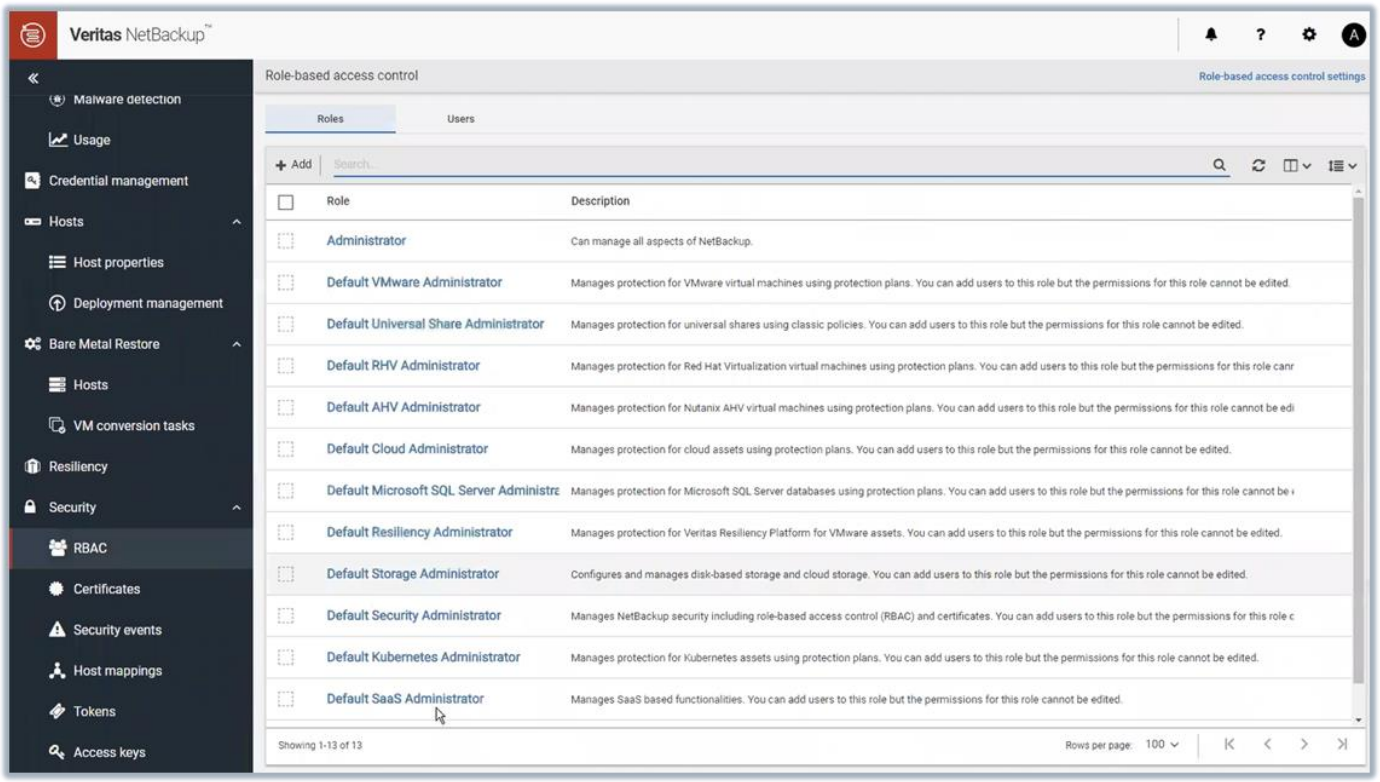
Manipulationssichere Hardware

Appliances, die unveränderbaren Speicher hosten, können zu einem erhöhten Sicherheitsgrad wechseln, um sowohl Daten als auch Infrastruktur zu schützen. Administratoren werden daran gehindert, Änderungen am Betriebssystem und an internen Komponenten vorzunehmen, alle Endgeräte sind vor unbefugtem Zugriff geschützt und der Zugriff auf alle Services ist nur authentifizierten Benutzern möglich.

Gesicherte Zugriffskontrollen

Die Lösung bietet Vorlagen für die rollenbasierte Zugriffskontrolle („Role-based Access Control“, RBAC), wie in Abbildung 3 dargestellt. Diese erleichtern es Administratoren, Benutzern oder Benutzergruppen den entsprechenden Zugriff oder die entsprechenden Berechtigungen zu erteilen. Administratoren können auch die einzelnen Vorlagen aufschlüsseln, um die detaillierten Berechtigungen zu sehen (z. B. NetBackup-Verwaltung, -Schutz, -Sicherheit und -Speicher). Zudem können sie eigene Benutzer- oder Gruppenzugriffe bzw. -berechtigungen erstellen. Diesen benutzerdefinierten Rollen können Workloads (d. h. die Workload-Assets, die Benutzer verwalten können), Schutzpläne (d. h. die Schutzpläne, die Benutzer verwalten können) und Anmeldeinformationen (d. h. die Anmeldeinformationen, die Benutzer verwalten können) zugewiesen werden.

Abbildung 3. Gesicherte Zugriffskontrollen

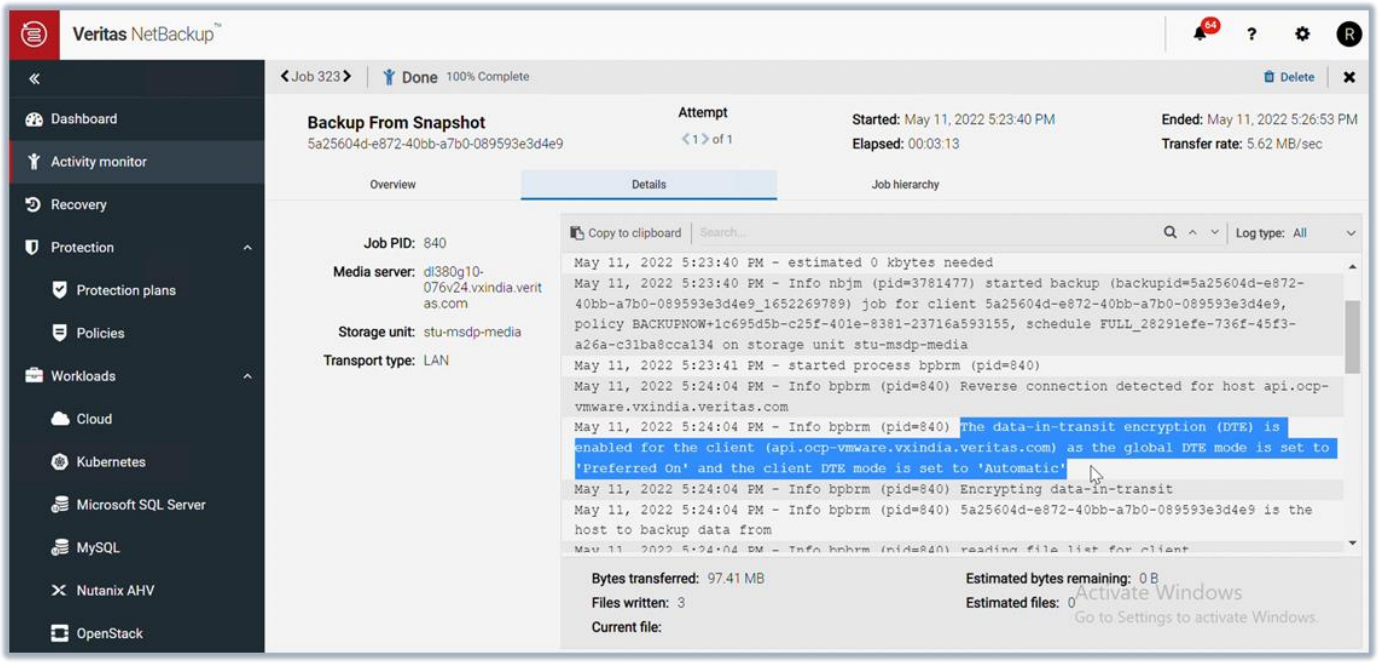


Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Schutz für moderne Infrastrukturen

Die Lösung bietet Datensicherungstechnologien der nächsten Generation für moderne Infrastrukturen, einschließlich Big Data-, hyperkonvergente oder quelloffene MySQL/NoSQL-Datenbanken. NetBackup ermöglicht es Unternehmen, Multicloud-, virtuelle, physische und moderne Workloads zu schützen, unabhängig davon, wo sie sich befinden, und alles von einer Konsole aus. Abbildung 4 zeigt ein Backup von einem Snapshot. Beim Backup war Data-in-Transit-Verschlüsselung (DTE) für den Client aktiviert, da der globale DTE-Modus auf „Bevorzugt ein“ und der Client-DTE-Modus auf „Automatisch“ eingestellt ist. Benutzer können bei Bedarf von diesem Backup wiederherstellen, für das DTE aktiviert ist, da der DTE-Modus des Backup-Images auf „Ein“ gesetzt ist.

Abbildung 4. Schutz für moderne Infrastrukturen



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Warum das wichtig ist

Da sich Ransomware-Angriffe ständig weiterentwickeln und ausgeklügelter werden, ist es für Unternehmen wichtig, sich mühelos an neue Bedrohungsvektoren anzupassen, um Serviceausfallzeiten und Datenverluste zu vermeiden. Der fortschrittliche Datenschutz und die sicheren Appliances von Veritas bieten mehrere Funktionen zur Bekämpfung von Ransomware, wie z. B. integrierte Anomalieerkennung, Malware-Scanning, eine Zero-Trust-Architektur und unveränderbaren und unlöschbaren Speicher.

Erkennung von Bedrohungen

Veritas bietet ein breites Spektrum an Funktionen, die Sie bei der Bedrohungserkennung unterstützen, darunter:

- Übersicht über die gesamte Backup- und Speicherinfrastruktur: NetBackup IT Analytics bietet eine durchgängige Backup-Überwachung, die eine Schadensbegrenzungsanalyse, Quellen mit aufeinanderfolgenden Ausfällen, Quellen ohne aktuelles Backup und Backup-Ausfälle nach Anwendungen umfasst.
- Anomalie-Erkennung: NetBackup liefert KI-gestützte Anomalie-Erkennung, die ungewöhnliche Daten in der gesamten Umgebung identifiziert und Warnmeldungen zu verdächtigen Anomalien nahezu in Echtzeit ausgibt.
- Erkennung primärer Speicher: Veritas verarbeitet sekundäre Backup-Daten mit NetBackup und primäre Speicherdaten mit Veritas Data Insight, das bestehende Sicherheitserkennungs-Tools ergänzt, indem es anomales Verhalten im Benutzer- und Datenkontext nahezu in Echtzeit erkennt, benutzerdefinierte Ransomware-spezifische Abfragevorlagen bereitstellt und Dateierweiterungen identifiziert, die für die Erkennung von Ransomware nützlich sind.
- Malware-Erkennung: Veritas bietet sowohl automatisierte als auch On-Demand-Scans für geschützte Backups. Die automatisierte Malware-Scanfunktion beseitigt menschliche Abhängigkeiten und nutzt künstliche Intelligenz/maschinelles Lernen (KI/ML), um nach Malware zu suchen.

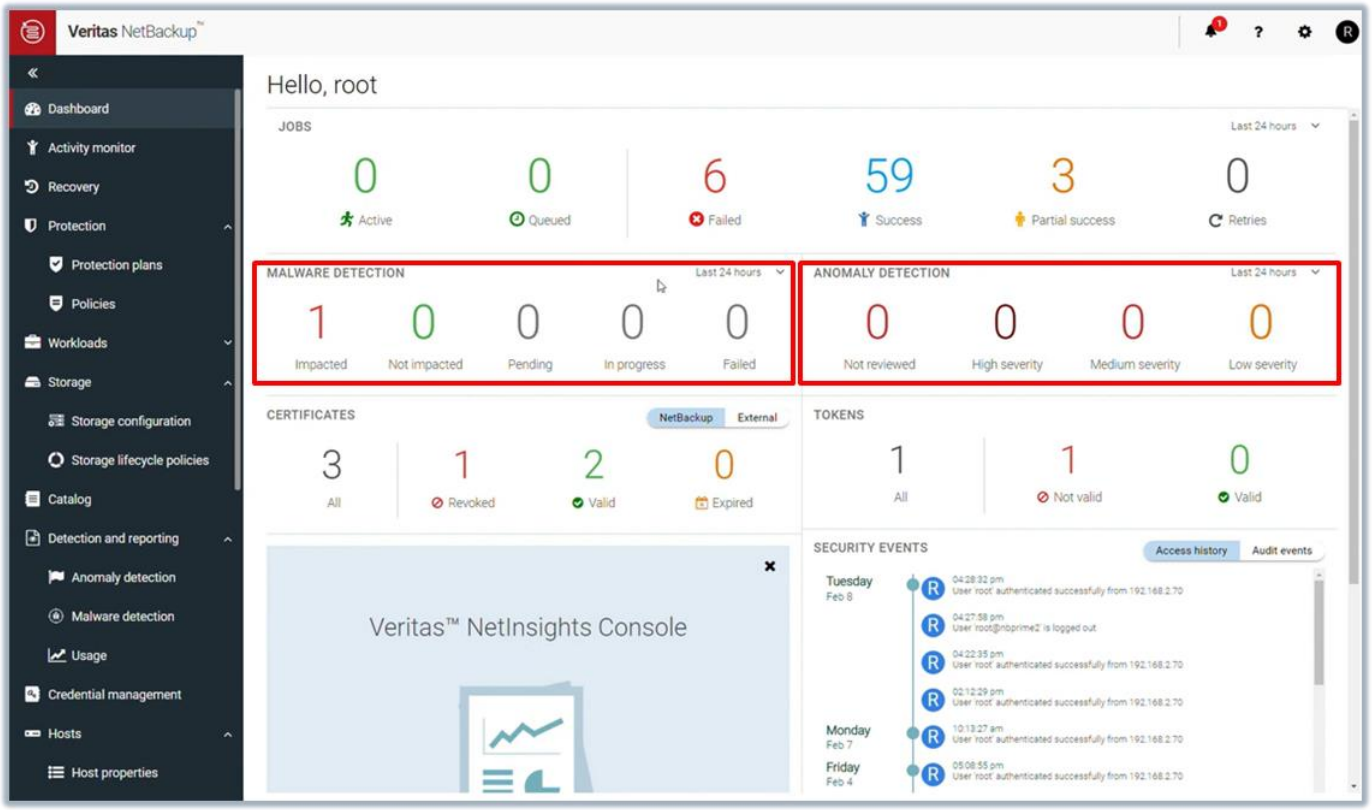
ESG hat insbesondere die folgenden wichtigen Bedrohungserkennungsfunktionen validiert.

Integrierte Erkennung von Malware und Anomalien

Die Anomalieerkennung verfolgt Image-Metadaten getrennt von der Malware-Erkennung; diese kann jedoch Anomalieerkennungswerte nutzen. Malware-Erkennungsereignisse werden für die „letzten 24 Stunden“ als „Betroffen“, „Nicht betroffen“, „Ausstehend“, „In Bearbeitung“ und „Fehlgeschlagen“ kategorisiert, wie in Abbildung 5 dargestellt. Der Zeitrahmen ist auch auf die „letzten 48 Stunden“ oder die „letzten 72 Stunden“ konfigurierbar. Benutzer können für jeden Bereich (z. B. „Betroffen“) weitere Details anzeigen. Für jedes betroffene Backup-Image können Benutzer Maßnahmen ergreifen, einschließlich das Verfallen aller Kopien oder das Anzeigen infizierter Dateien. Das Malware-Erkennungs-Dashboard bietet die folgenden Informationen: Client, Backup-Zeit, Scan-Ergebnis, Backup-Typ, Scan-Datum, Malware-Anwendungs-Scanner, Anzahl betroffener Dateien, Scan-Hostname und Backup-ID. Die Scanzeit für Malware hängt von mehreren Faktoren ab, einschließlich der Image-Größe und der Anzahl der Dateien.

Anomalieerkennungsereignisse werden für die „letzten 24 Stunden“ als „Nicht überprüft“, „Hoher Schweregrad“, „Mittlerer Schweregrad“ und „Niedriger Schweregrad“ kategorisiert, wie in Abbildung 5 dargestellt. Der Zeitrahmen ist auch auf die „letzten 48 Stunden“, die „letzten 72 Stunden“ oder die „letzten 7 Tage“ konfigurierbar. Benutzer können auch nach dem Überprüfungsstatus (Nicht überprüft, Falschmeldung, Anomalie, Ignorieren) und dem Schweregrad der Anomalie (Hoch, Mittel, Niedrig) filtern. Das Anomalieerkennungs-Dashboard enthält die folgenden Informationen: Job-ID, Kundenname, Richtlinientyp, Anzahl, Punktzahl, Anomalie-Schweregrad, Anomalie-Zusammenfassung, Empfangen, Überprüfungsstatus, Richtlinienname, Zeitplanname und Zeitplantyp. Benutzer können die folgenden Aktionen in Bezug auf Anomalien durchführen: „Als ‚Ignorieren‘ markieren“, „Als Anomalie bestätigen“ und „Als Falschmeldung melden“.

Abbildung 5. Integrierte Erkennung von Malware und Anomalien



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Berichterstellung und Benachrichtigung

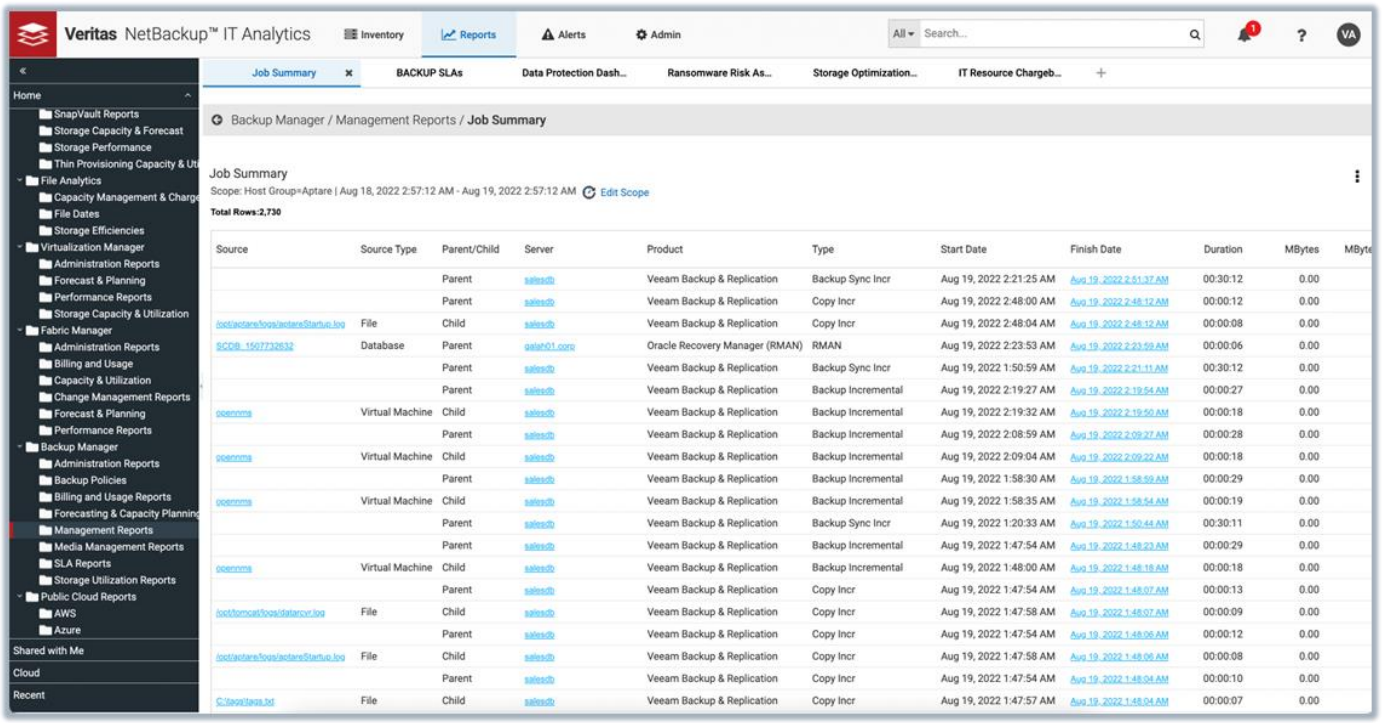
Veritas NetBackup IT Analytics bietet ein sofort einsatzbereites Dashboard zur Ransomware-Risikobewertung. Damit erhalten Benutzer eine schnelle Ansicht der vordefinierten Berichte, die mithilfe von vorausschauenden Analysen potenzielle Risiken in einer Backup-Umgebung aufzeigen (siehe Abbildung 6). Durch die Analysen lässt sich sicherstellen, dass die Backup-Umgebung sowohl optimiert als auch sicher ist, und zwar dank umfassender Berichte zu mehreren Datenpunkten, darunter:

- **Erkennung** – Benutzer können alle Änderungen innerhalb der Sicherungsumgebung verfolgen, um Ransomware zu erkennen und schnell zu reagieren. Es können über 850 bekannte Ransomware-Erweiterungen erkannt werden.
- **Risikovisualisierung** – Intuitive Diagramme geben Benutzern einen historischen Überblick über alle in der Umgebung generierten Risiken, markieren Hosts, die im Backup-Zeitplan fehlen, und visualisieren Anwendungen mit fehlgeschlagenen Backups.
- **Backup-Überwachung** – Benutzer können Änderungen innerhalb der Backup-Umgebung mit zusammenfassenden Diagrammen überwachen und identifizieren, die umsetzbare Erkenntnisse liefern. Durch die Identifizierung von Anomalien anhand einer Basislinie erfolgreicher Backups lassen sich Risiken mindern.

Neben der Erkennung von Dateien mit bekannten Ransomware-Erweiterungen lassen sich mit NetBackup IT Analytics diese Informationen auf sinnvolle Weise zu organisieren, um einen schnellen Aktionsplan ausführen zu können. Benutzer können die erkannten Ransomware-Dateien nach Hosts, Orten mit den meisten Ransomware-Dateien, Arten von Ransomware-Erweiterungen und Eigentümern von Dateien anzeigen.

NetBackup IT Analytics prüft auch erfolgreiche Backups, um mögliche Falschmeldungen zu identifizieren, indem es vergangene Backups mit dem neuen vergleicht und dabei Anomalien wie eine deutlich längere Dauer von Jobs, Änderungen der Image-Größe und/oder Änderungen an der Richtlinienkonfiguration identifiziert. Dies gibt Benutzern die Gewissheit, dass kritische IT-Services geschützt sind.

Abbildung 6. Berichterstellung und Benachrichtigung



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Warum das wichtig ist

Wie bereits erwähnt, haben sich Ransomware-Angriffe weiterentwickelt und sind immer ausgefeilter geworden. Angesichts dessen bietet Veritas einen ganzheitlichen Echtzeitüberblick zum Status von Anwendungen und Daten mit Anomalieerkennung sowie konfigurierbare Analysen, die helfen, Malware-Infiltrierung sowohl in Primär- als auch in Backup-Daten zu erkennen.

Skalierte Wiederherstellung

Veritas bietet ein breites Spektrum an Funktionen zur skalierten Wiederherstellung, darunter:

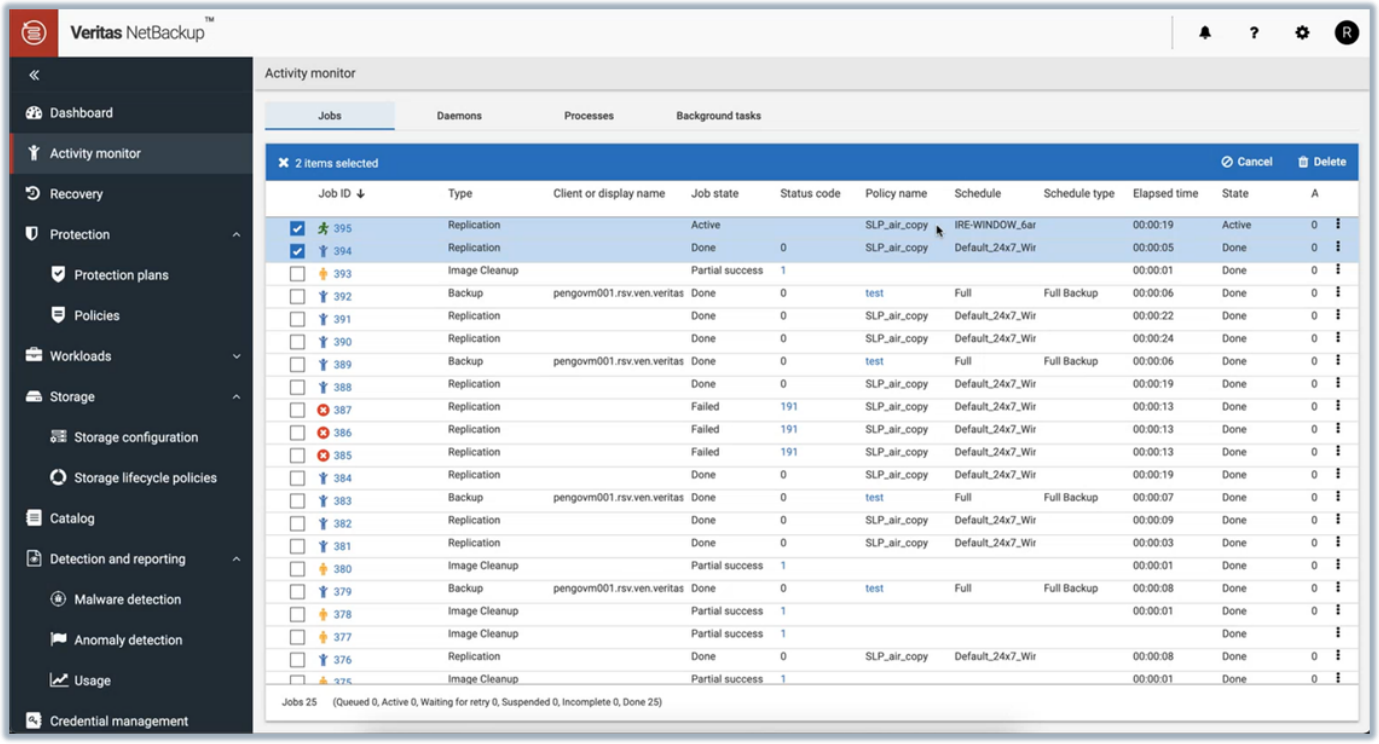
- NetBackup Resiliency: NetBackup Resiliency bietet automatisierte Orchestrierung über die gesamte heterogene Umgebung eines Unternehmens hinweg mit einer konsistenten Benutzererfahrung und Verweis auf die besten Wiederherstellungsoptionen basierend auf deren Verfügbarkeit.
- NetBackup Instant Rollback for VMware: Ermöglicht die VM-Wiederherstellung in Hochgeschwindigkeit durch Einsatz von Reverse Change Block Tracking, um zu ermitteln, welche eindeutigen Blöcke wiederhergestellt werden müssen, sodass nur diese Änderungen angewendet werden, um VMs in Sekundenschnelle wieder in einen integren Zustand zu versetzen.
- VM-Wiederherstellung: Bietet acht Wiederherstellungstypen für ein Backup von VMware-VMs, einschließlich vollständiger VMs, einzelner VMDKs, Dateien und Ordner, vollständiger Anwendungen, Instant Access, Datei-Downloads, Anwendungs-GRT und AMI-Konvertierungen.
- Instant Access for MSSQL and VMware: Ermöglicht nahezu sofortige Wiederherstellung virtueller Maschinen (z. B. 1.600 VMs), ohne auf die Übertragung der VM-Daten aus dem Backup warten zu müssen. Zudem können VMs direkt aus dem Backup-Speicher getestet oder wiederhergestellt werden.
- NetBackup CloudPoint: NetBackup CloudPoint verwendet Cloud-native Snapshot-Technologie auf eine Cloud-Anbieter-agnostische Weise, die einen einfachen Schutz von Hybrid- und Multi-Cloud-Infrastrukturen ermöglicht.
- Universelle Freigabe und Schutzpunkte: Ermöglicht Unternehmen die Bereitstellung von durch Deduplizierung gesichertem Speicher auf dem NetBackup-Server als sichere Freigaben, sodass Datenbanken oder andere Workloads geschützt sind, wenn kein Agent oder keine Backup-API vorhanden ist.
- NetBackup Universal Shares for Oracle: Damit können Oracle DB-Administratoren Datenbanken direkt aus dem Speicher einer NetBackup Appliance zu starten.
- Langfristiges Aufbewahrungsarchiv: Eine kostengünstige und langlebige Lösung mit Deduplizierung und Komprimierung von Daten, einschließlich der Verwendung von Objektspeicher und privaten oder öffentlichen Clouds mit dieser Methode. Traditionelle Wiederherstellungen umfassen die granulare Wiederherstellung einer bestimmten Datei, die Wiederherstellung kompletter Server/Anwendungen sowie die DR-Wiederherstellung (Disaster Recovery) an einem anderen Standort oder in der Cloud. Dank der Veritas Resiliency Platform können Unternehmen die herkömmliche Wiederherstellung mit nur einem Knopfdruck automatisieren und orchestrieren und so den DR-Prozess optimieren.
- Bare Metal Restore: Automatisiert den Wiederherstellungsprozess des Servers, sodass Betriebssysteme nicht neu installiert oder Hardware manuell konfiguriert werden muss. Damit können Unternehmen Systeme schnell von Grund auf neu aufzubauen und das Betriebssystem und die Anwendungsdaten in einem einzigen Vorgang wiederherzustellen.

ESG hat insbesondere die folgenden wichtigen Funktionen für die skalierte Wiederherstellung validiert.

Isolated Recovery Environment

Die Isolated Recovery Environment von Veritas NetBackup ermöglicht Wiederherstellungspläne für Tausende von VMs, die möglicherweise Teil komplexer, mehrstufiger Umgebungen sind, und die Ausführung von Tests derselben in einer isolierten Umgebung (siehe Abbildung 7). Sie unterstützt integrierte Unveränderbarkeit und Unlöschbarkeit, einschließlich für Drittanbieter-Hardware, Cloud-basierte Object Lock-Speicher und SaaS-Workload-Backups. Außerdem kann NetBackup deduplizierte Daten direkt an AWS S3 Object Lock senden und effizient speichern.

Abbildung 7. Isolated Recovery Environment (IRE)

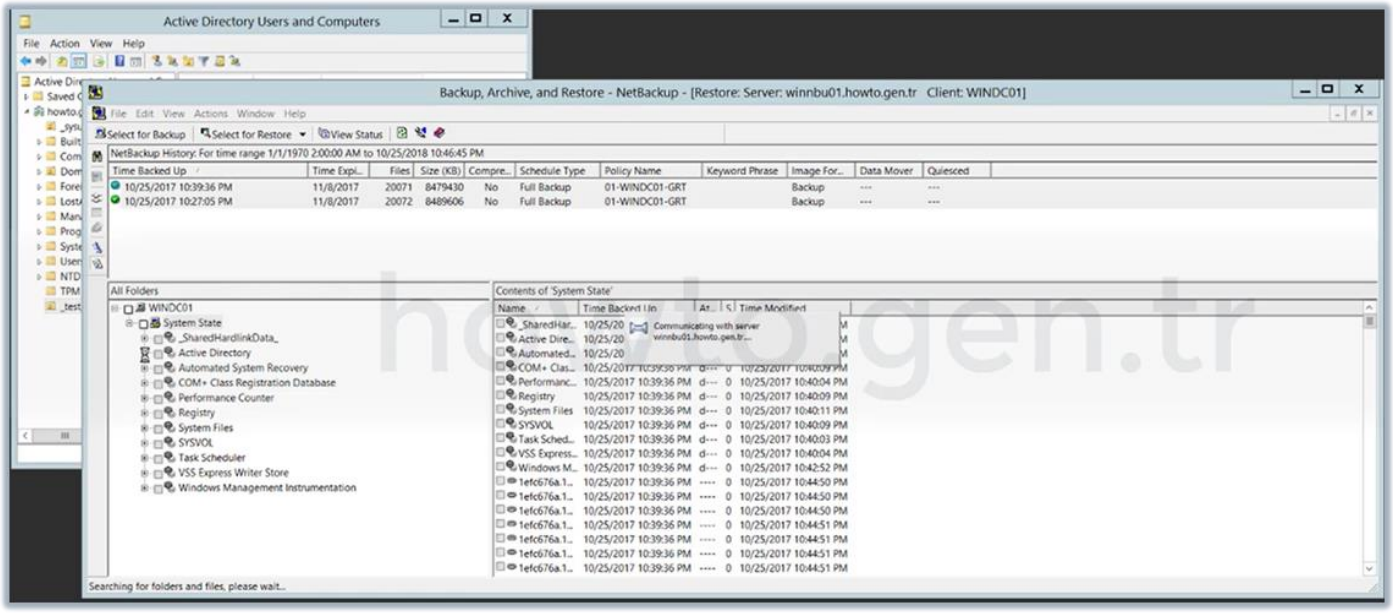


Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Wiederherstellung verlorener Active Directorys

Die Veritas NetBackup-Lösung bietet die Möglichkeit, durch das Durchsuchen der Active Directory-Backups ein verlorenes Active Directory wiederherzustellen (siehe Abbildung 8). Anschließend initiiert der Benutzer einfach die ordnungsgemäße AD-Sicherung. Der Benutzer kann auch den Fortschritt der Wiederherstellung anzeigen, bis der angeforderte Vorgang erfolgreich abgeschlossen wurde.

Abbildung 8. Wiederherstellung verlorener Active Directorys

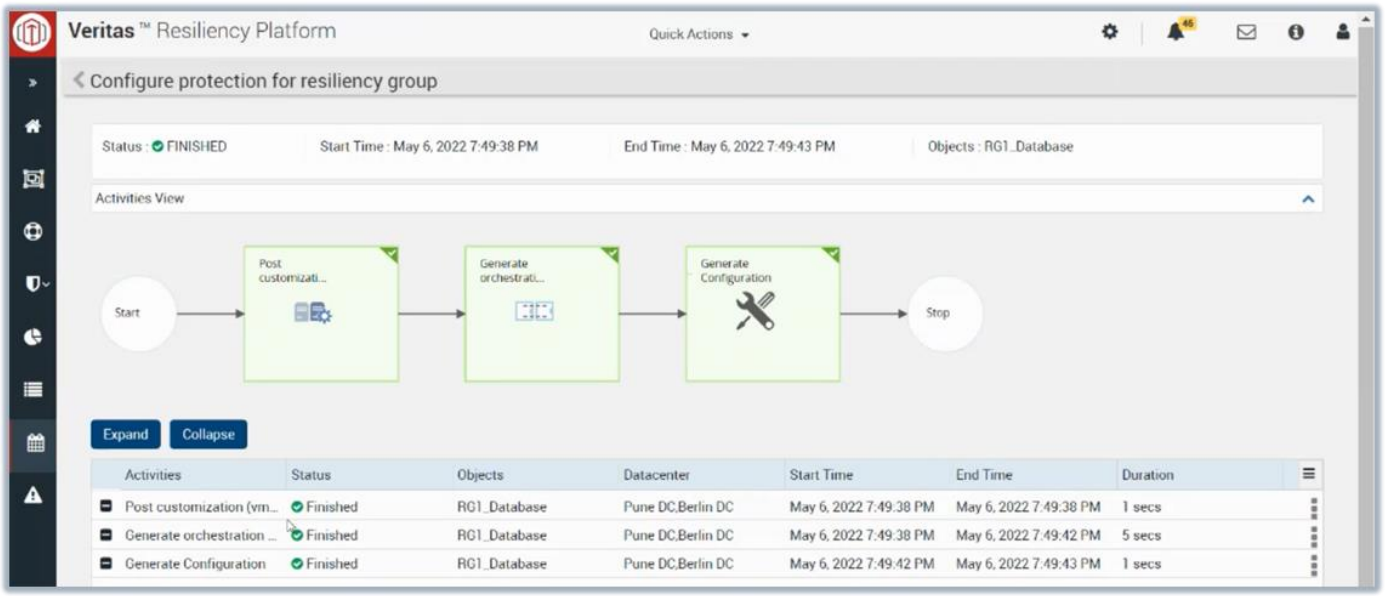


Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Mehrstufige Wiederherstellungsorchestrierung

Mit den Virtual Business Services von Veritas NetBackup Resiliency können Benutzer die Wiederherstellung für mehrstufige Anwendungen als eine einzige konsolidierte Einheit verwalten. Die Wiederherstellung einer komplexen, mehrstufigen Anwendung, die sich über mehrere Systeme erstreckt, lässt sich vollständig automatisieren. Im Falle eines Ransomware-Angriffs bietet dies eine einfachere, schnellere Wiederherstellung und minimale Anwendungsausfallzeiten. Insbesondere bietet die Veritas Resiliency Platform eine mehrstufige Recovery-Orchestrierung durch die Konfiguration von Virtualisierungs- und privaten Clouds (z. B. VMware vCenter), NetBackup-Primärservern, Netzwerken (z. B. Netzwerkkopplung), physischen Servern, Datenbanken usw. Siehe Abbildung 9 für die vollständige Schutzkonfiguration der Resilienzgruppen.

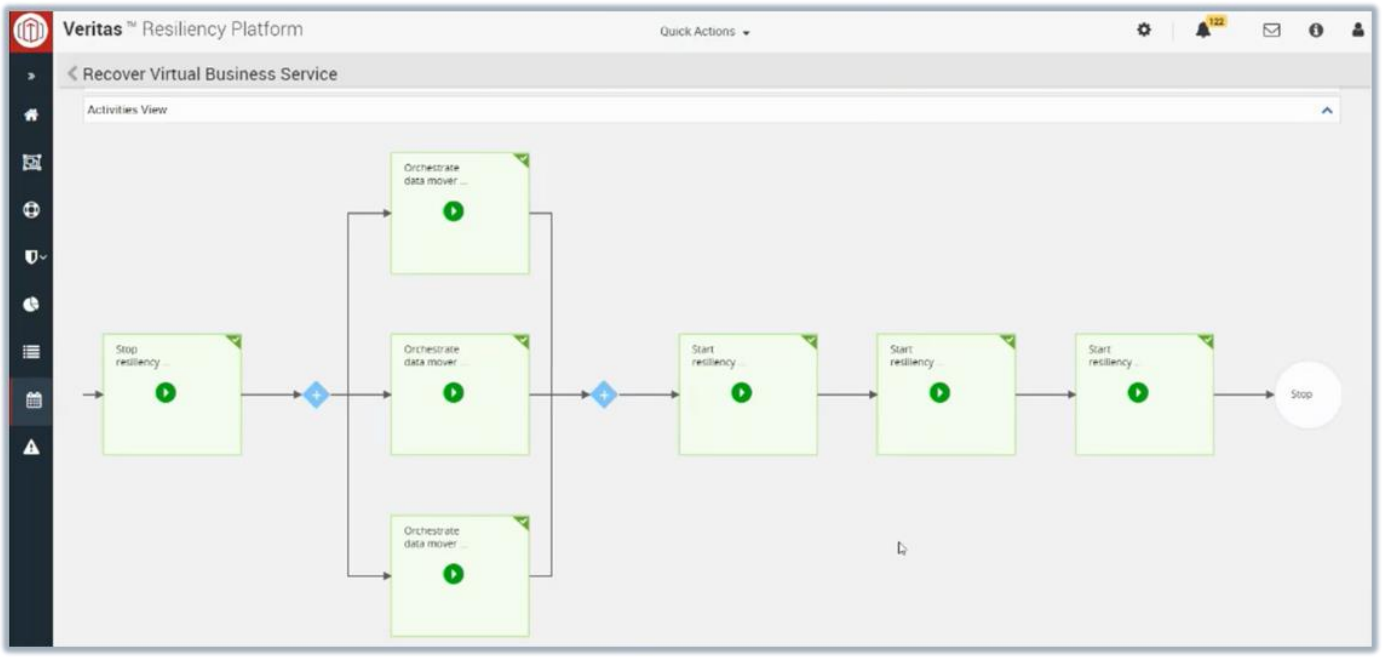
Abbildung 9. Konfiguration der mehrstufigen Wiederherstellung



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Nachdem der Schutz der Resilienzgruppen konfiguriert wurde, muss der Benutzer den mehrstufigen Virtual Business Service einrichten. Als Nächstes kann die mehrstufige Wiederherstellung des Virtual Business Service orchestriert werden (siehe Abbildung 10).

Abbildung 10. Mehrstufige Wiederherstellungsorchestrierung



Quelle: ESG, ein Geschäftsbereich von TechTarget, Inc.

Warum das wichtig ist

Aufgrund der steigenden Zahl von Ransomware-Angriffen ist es wichtig, dass Unternehmen über eine umfassende Ransomware-Strategie für Ausfallsicherheit und Wiederherstellung verfügen. Veritas bietet erweiterten Speicher und schnelle Wiederherstellungsfunktionen für Primärdaten mit integrierter Speicherresilienz, Unveränderbarkeit und Datenisolierung, die alle gemeinsam die Verfügbarkeit von Anwendungen sowie die Sicherheit und Integrität von Daten gewährleisten.

Die ganze Wahrheit

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.

ESG hat in 12 Testszenarien die Cybersicherheitslösung von Veritas validiert, einschließlich des Schutzes von Daten, der Erkennung von Bedrohungen und der Wiederherstellung im großen Maßstab. Eine ganzheitliche, vielschichtige und umfassende Cybersicherheitsstrategie ist immer die beste Verteidigung gegen Ausfallzeiten und Datenverlust durch Malware-Infiltration. Veritas ist sich bewusst, dass dies eine komplexe Herausforderung sein kann, und stellt daher eine solide Grundlage bereit, mit der Unternehmen ihre IT-Services im Rahmen einer umfassenden Cybersicherheitsstrategie schützen können. Mit Veritas profitieren Unternehmen von Tools, Funktionen und der Gewissheit, dass IT-Services stets hochverfügbar, ausfallsicher und vor Ransomware geschützt sind.

© 2022 TechTarget, Inc. Alle Rechte vorbehalten.