Ransomware-Angriffe mit Cohesity bekämpfen

Wichtige Vorteile

- Schutz Ihrer Daten und Ihres Unternehmens mit einer Defense-in-Depth-Architektur
- Schnelle Identifizierung von potenziellen Angriffen durch auf maschinellem Lernen basierende Anomalieerkennung
- Verringerung der Ausfallzeit durch eine skalierbar schnelle Wiederherstellung

In der digitalen Wirtschaft stellen Daten ein Alleinstellungsmerkmal dar. Daher sind Daten gleichermaßen zum wertvollsten als auch zum begehrtesten Geschäftswert geworden. Cybersecurity Ventures erwartet, dass die weltweiten Kosten für Cyberkriminalität bis 2025 jährlich 10,5 Billionen US-Dollar erreichen und bis zum Jahr 2031 alle 2 Sekunden ein Unternehmen Opfer eines Ransomware-Angriffs werden wird[1]. Obwohl das Bewusstsein für dieses digitale Erpressungssystem steigt, bedrohen komplexere und gezieltere Angriffe, die zunehmend auf Backup-Daten und -Infrastrukturen abzielen, Unternehmen weltweit. Kompromittierte Unternehmen erleiden häufig erhebliche finanzielle Verluste, die durch das Misstrauen der Kunden und im Falle des Gesundheitswesens durch die Gefahr für Menschenleben noch verstärkt werden.

Cohesity bekämpft Ransomware-Angriffe effizient und verhindert, dass Ihr Unternehmen Lösegeld bezahlen muss. Die umfassende Next-Gen Data Management-Lösung von Cohesity nutzt einen mehrschichtigen Ansatz für den Schutz von Backup-Daten vor Ransomware und zur Erkennung und schnellen Erholung von einem Angriff. Die einzigartige unveränderliche Architektur von Cohesity gewährleistet, dass Ihre Backup-Daten nicht verschlüsselt, modifiziert oder gelöscht werden können. Mithilfe von maschinellem Lernen bietet sie Transparenz und überwacht kontinuierlich alle Anomalien in Ihren Daten. Und wenn der ungünstigste Fall eintritt, trägt Cohesity zur Lokalisierung einer sauberen Kopie der Daten überall in Ihrem globalen Fußabdruck bei, einschließlich öffentlicher Clouds, um sofort für eine Wiederherstellung zu sorgen und die Ausfallzeiten zu reduzieren.

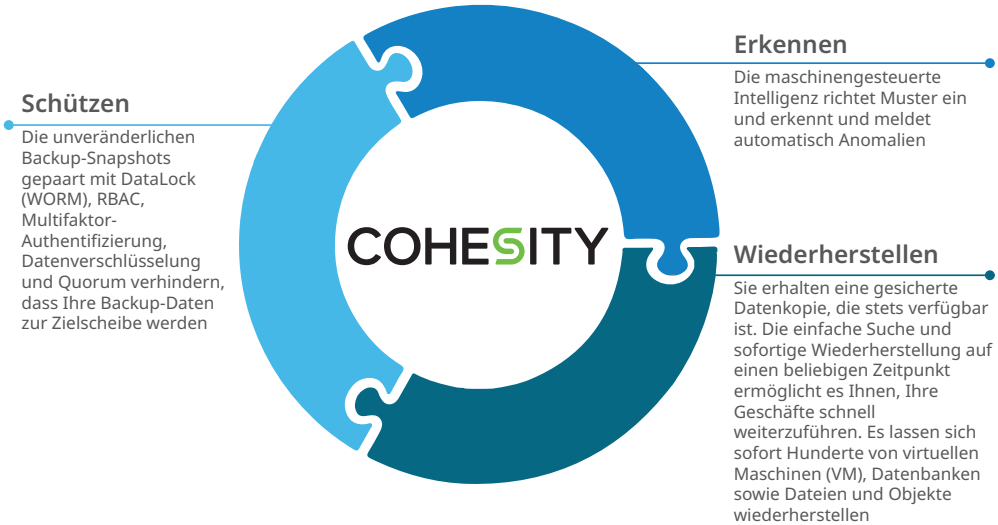

Abbildung 1: Cohesity bietet umfassende Funktionen zum Schützen und Erkennen von Ransomware-Angriffen sowie zur Wiederherstellung

1. Cybersecurity Ventures: Top 6 Cybersecurity Predictions And Statistics For 2021 To 2025 (30. Dezember 2021)

Schützen

Mit ausgeklügelter Ransomware wie Locky und Crypto wurden kürzlich Schattendatenduplikate zerstört und Punktdaten wiederhergestellt, wodurch die Backup-Infrastruktur des Unternehmens zu einem primären Ziel von Cyberkriminellen wird, sofern sie Teil der Verteidigung Ihres Unternehmens ist. Cohesity stoppt Eindringlinge, indem verhindert wird, dass Ihr Backup zum Angriffsziel wird.

Cohesity bietet mit SpanFS™, einem verteilten Dateisystem der dritten Generation, einen einzigartigen mehrschichtigen Schutz vor Ransomware-Angriffen. Unter anderem stellt Cohesity die höchste Schutzebene gegen Ransomware-Angriffe bereit, da es auf Unveränderlichkeit basiert.

- **Unveränderliche Snapshots** – Alle Datensicherungs-Snapshots werden in Cohesity standardmäßig in einem unveränderlichen Zustand gespeichert. Der ursprüngliche Snapshot (auch goldene Kopie genannt) wird niemals an externe Systeme oder Anwendungen gemountet oder offengelegt. Die einzige Möglichkeit, neue Daten zu schreiben oder die Datensicherung zur Wiederherstellung im Lesen-Schreiben-Modus zu mounten, besteht darin, die ursprüngliche Datensicherung kostenlos zu klonen, was automatisch durch das System erfolgt.
- **DataLock –** WORM–Funktionen für das Backup ermöglichen die rollenbasierte Erstellung und Anwendung einer DataLock-Richtlinie für ausgewählte Backup-Snaps. Die Rolle des Sicherheitsbeauftragten in Ihrem Unternehmen kann diese Funktion zum Speichern von Snaps im WORM-Format nutzen. Die zeitgebundene Einstellung zur Durchsetzung von Laufzeiten kann nicht gelöscht werden, auch nicht vom Administrator oder dem Sicherheitsbeauftragten. Dies bietet eine zusätzliche Schutzebene gegenüber Ransomware-Angriffen.
- **Rollenbasierte Zugriffskontrolle (Role-based access control, RBAC)** – Um das Risiko eines unbefugten Zugriffs auf Daten und Systeme zu verringern, versetzt Cohesity Ihre IT-Mitarbeiter in die Lage, jeder Person ein Mindestmaß an Zugriff auf das zu gewähren, was für eine bestimmte Aufgabe erforderlich ist.
- **Multifaktor-Authentifizierung (MFA) –** Sollte ein krimineller Akteur Ihr Systempasswort herausfinden, könnte er nicht auf das Cohesity-Backup zugreifen, ohne eine weitere Sicherheitsebene in Form der MFA oder der mehrstufigen Verifizierung zu überwinden. Cohesity unterstützt eine Vielzahl von Authentifizierungs- und Autorisierungsfunktionen, einschließlich enger Active Directory-Integration, MFA, Zugriffskontrolllisten, rollenbasierter Zugriffskontrolle (RBAC) mit gemischtem Modus und umfassender Überwachung auf System- und Produktebene.
- **Datenverschlüsselung** – Cohesity bietet Software-basierte FIPS-validierte AES-256-Standardverschlüsselung sowohl für Daten, die übertragen werden, als auch für solche, die sich im Ruhezustand befinden. Dieses kryptografische Modul wurde vom National Institute of Standards and Technology (NIST) der Vereinigten Staaten gemäß dem Standard Federal Information Processing Standards (FIPS) 140-2 Level 1 validiert und gilt weltweit als zuverlässig.
- **Quorum** – Um Ihre Daten und Systeme vor Insider-Bedrohungen und gestohlenen Zugangsdaten zu schützen, erfordert Cohesity, dass Root-Level- oder andere kritische Systemänderungen, die von einer beliebigen Person in Ihrem Unternehmen gewünscht werden, von mehr als einer Person autorisiert werden.

Cohesity Helios, eine Next-Gen Data Management-Plattform, bietet eine einzigartige Kombination aus unveränderlichen Snapshots, DataLock-Funktionen, RBAC, MFA und Quorum (auch bekannt als die Vier-Augen-Regel), um zu vermeiden, dass Backup-Daten Teil eines Ransomware-Angriffs werden.

Erkennen

Angesichts der weiteren Intensivierung und Modifizierung der Vorgehensweisen von Cyberkriminellen erleichtert Cohesity es Ihrem Unternehmen, Intrusionen mit einer globalen, unternehmensweiten SaaS-basierten Managementlösung zu erkennen. Cohesity-Kunden können auf einem einzigen Dashboard schnell globale Aktionen für ihre Daten und Anwendungen anzeigen, verwalten und durchführen. Im Kampf gegen Ransomware bietet das maschinelle Lernen (ML) von Cohesity Helios Erkenntnisse, die Menschen übersehen könnten, da es eine automatische und kontinuierliche Überwachung vornimmt und Sie informiert, wenn eine Anomalie erkannt wird.

Der ML-Algorithmus bewertet proaktiv Ihre IT-Anforderungen und automatisiert Infrastrukturressourcen regelmäßig. Wenn sich die Datenänderungsrate Ihres Unternehmens einschließlich der Dateneinspeisung außerhalb des normalen Bereichs befindet – basierend auf den täglichen Änderungsraten für logische Daten, gespeicherte Daten nach der globalen Deduplizierung oder der Einspeisung historischer Daten –, sendet die maschinengesteuerte Anomalieerkennung von Cohesity Helios eine Benachrichtigung an Ihre IT-Administratoren. Die IT wird sofort informiert, dass Datenänderungen nicht den normalen Mustern entsprechen.

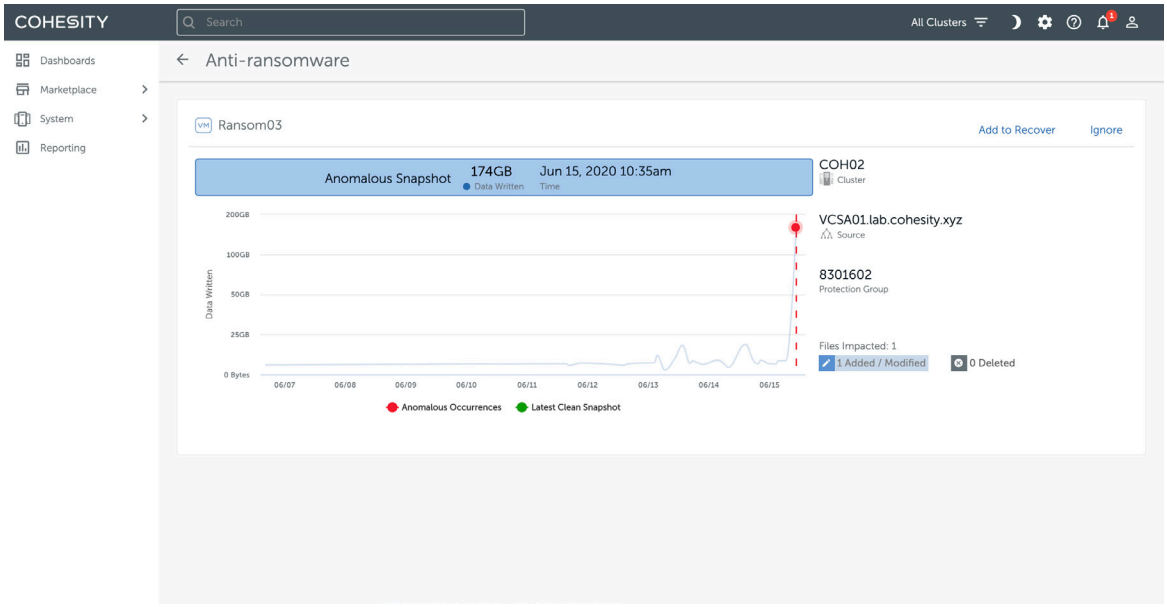

Abbildung 2: Mit Cohesity Helios erkennen Unternehmen Ransomware-Intrusionen

Da das maschinengesteuerte Helios-Lernen Muster festlegt und automatisch nach Anomalien bei der Dateneinspeisung/-änderung sucht, kann ein potenzieller Ransomware-Angriff gekennzeichnet werden. Sollte eine Anomalie erkannt werden, informiert die Plattform gleichzeitig das IT-Team Ihres Unternehmens und das Support-Team von Cohesity zur Beschleunigung der Behebung von Problemen.

Neben der Überwachung von Backup-Datenänderungsraten zur Ermittlung eines potenziellen Ransomware-Angriffs erkennt und warnt Cohesity auch bei Anomalien auf Dateiebene in unstrukturierten Dateien und Objektdaten. Dies umfasst die Analyse der Häufigkeit von Dateizugriffen, die Anzahl der Dateien, die von einem bestimmten Benutzer oder einer Anwendung geändert, hinzugefügt oder gelöscht wurde, und vieles mehr, um sicherzustellen, dass ein Ransomware-Angriff rasch erkannt wird.

Wiederherstellen

Cybersicherheits-Bedrohungen passieren sowohl intern als auch extern und außerdem sehr schnell. Deshalb muss die Wiederherstellung zuverlässig und in kürzester Zeit erfolgen. Cohesity beschleunigt den Wiederherstellungsprozess Ihrer erbeuteten Unternehmensdaten und -anwendungen – in großem Umfang. Neben den unveränderlichen Datensicherungen bietet Cohesity verschiedene richtlinienbasierte Methoden zur Isolierung Ihrer aufgabenkritischen Daten und zur Sicherung der letzten intakten Kopie. Zur Erfüllung Ihrer individuellen Anforderungen an Wiederherstellung und Sicherheit können Sie Ihre Daten in den von Cohesity verwalteten Cloud-Vault Cohesity FortKnox isolieren, sie auf einen anderen unveränderlichen Cluster replizieren oder sie kopieren und in einem externen Speicher wie Iron Mountain aufbewahren.

Die maschinengesteuerte Hilfe von Cohesity Helios unterstützt eine beschleunigte Wiederherstellung, indem sie eine saubere Kopie der Daten zum Wiederherstellen empfiehlt. Ansonsten können Sie auch die globalen Suchfunktionen der Plattform nutzen, um die Daten in verschiedenen Umgebungen schnell zu lokalisieren und darauf zuzugreifen.

Um eine saubere Wiederherstellung zu gewährleisten und eine erneute Cyberbedrohung oder Software-Schwachstelle in Ihrer Produktionsumgebung zu verhindern, erhalten Sie mit CyberScan von Cohesity umfassende Transparenz zu Zustand und Wiederherstellbarkeit geschützter Snapshots. CyberScan zeigt den Schwachstellen-Index sowie umsetzbare Empfehlungen für jeden Snapshot an, um Software-Schwachstellen zu beheben. So können Sie bei einem Ransomware-Angriff eine saubere, zuverlässige Wiederherstellung vornehmen.

Dank der Kombination komplett hydratisierter Snapshots mit der proprietären SnapTree's B+Tree Architektur von Cohesity, MegaFile und Instant Mount können Sie Ihre Ausfallzeiten durch die Wiederherstellung von Hunderten virtueller Maschinen (VMs), Dateien, Objekten und großen Datenbanken sofort drastisch reduzieren.

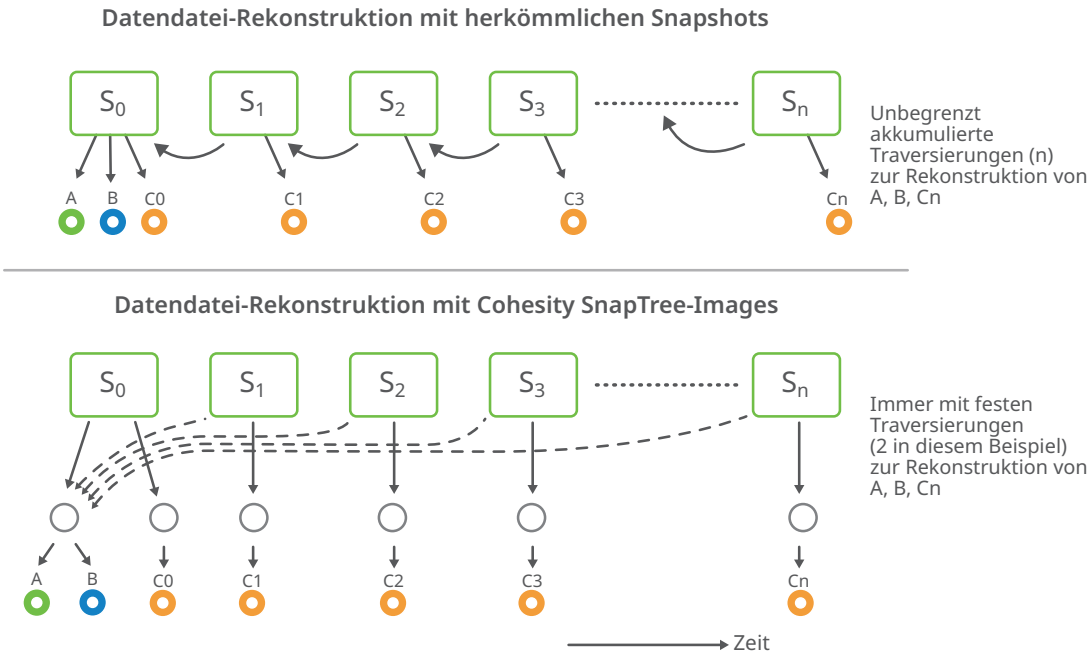

Abbildung 3: Die patentierte SnapTree-Technologie von Cohesity ermöglicht unbegrenzte Snaps ohne Mehraufwand und unterstützt die sofortige Wiederherstellung in großem Umfang

Ransomware-Angriffe mit Cohesity bekämpfen

Backups sind Ihre letzte Verteidigungslinie gegen ausgeklügelte, schwächende Ransomware-Angriffe. Die umfassende Anti-Ransomware-Lösung von Cohesity schützt, erkennt und – was am wichtigsten ist – sorgt für eine schnelle Wiederherstellung des Benötigten, um Ausfallzeiten zu reduzieren und die Geschäftskontinuität sicherzustellen.

Mehr dazu auf www.cohesity.com/de/solutions/ransomware

COHESITY