COHESITY

LÖSUNGSBROSCHÜRE

DataHawk

Sicherheit und Resilienz für Ihre kritischen Daten

Wichtige Vorteile

- Identifizierung neuer Ransomware-Angriffe
- Erkennung von riskantem Benutzerverhalten
- Saubere Recovery-Daten
- Einfache und kosteneffektive Datenisolation
- Nutzung und Verstärkung der vorhandenen Sicherheitskontrollen

Ransomware und Cyberangriffe nehmen an Häufigkeit und Schwere zu, da Unternehmen von kriminellen Akteuren und Nationalstaaten aus finanziellen und politischen Gründen angegriffen werden. Herkömmliche Cybersicherheit ist zwar hilfreich, aber nicht mehr ausreichend. Deshalb müssen Unternehmen ihre Schutzmaßnahmen und Funktionen zur Wiederherstellung von Daten und Prozessen verstärken, für den Fall, dass ein Angriff ihre Abwehrmechanismen durchbricht. Die Wiederherstellung ist von entscheidender Bedeutung, da Cyber-Abwehrsysteme nie zu 100 % zuverlässig sind. Erweiterte Datensicherheits- und -managementlösungen bieten zusätzlichen Schutz und Recovery-Möglichkeiten, damit Unternehmen Cybervorfälle überstehen und sich davon erholen können. Solche Vorfälle umfassen Ransomware, zerstörerische Cyberangriffe, Insider-Bedrohungen, Naturkatastrophen und Systemausfälle.

Neben der Unveränderlichkeit, dem Zero-Trust-Prinzip und der sofortigen Wiederherstellung von Daten und Prozessen benötigen Unternehmen Lösungen, die in der Lage sind, Cyber-Bedrohungen zu erkennen, die Auswirkungen der Gefährdung sensibler Daten zu analysieren, Daten sicher zu isolieren und sich nahtlos in Sicherheitsabläufe zu integrieren. Daher sollten Unternehmen in Erwägung ziehen, ihre Sicherheit und Resilienz mit einem cloudbasierten Service zu modernisieren, um:

- die Erkennung von Bedrohungen zu vereinfachen und eine saubere Datenwiederherstellung zu gewährleisten
- die Gefährdung sensibler Daten zu erkennen
- Daten sicher vor Bedrohungen zu isolieren
- diesen in Sicherheitsabläufe zu integrieren

Verbessern Sie Ihre Cyber-Resilienz

Cohesity DataHawk bietet mehrere Cloud-Service-Angebote, die umfassende Data Security- und Recovery-Funktionen bereitstellen, um Cyber-Vorfällen zu widerstehen und sich davon zu erholen. Die Plattform erkennt mithilfe von KI und ML Benutzer- und Datenanomalien, die auf einen bevorstehenden Angriff hindeuten könnten, und nutzt Bedrohungsdaten, um sicherzustellen, dass die

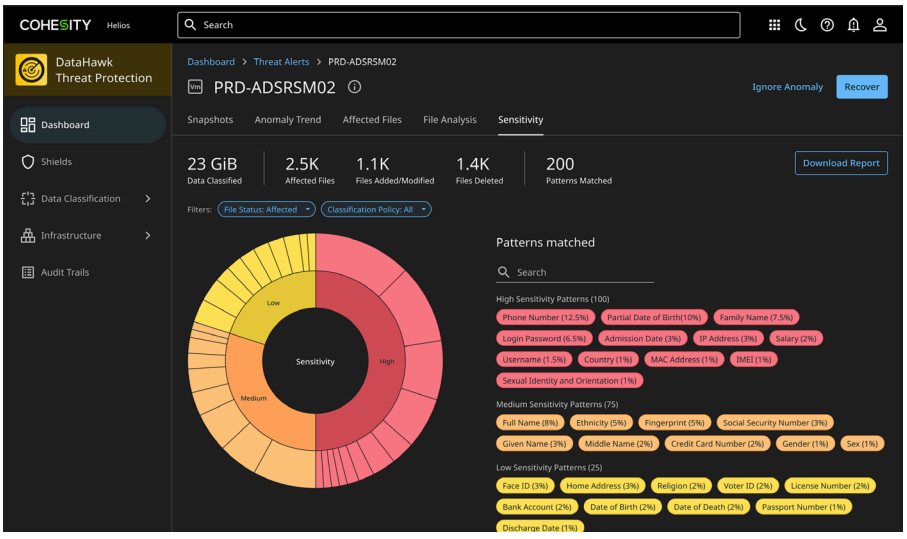

Abbildung 1: Identifizierung potenzieller Datenexfiltration mit Verhaltensanalysen

Wiederherstellungsdaten frei von Malware sind. Außerdem ermöglicht sie Unternehmen durch Datenklassifizierung, die Gefährdung sensibler und privater Informationen im Falle eines Angriffs zu bestimmen. DataHawk bietet eine zusätzliche Sicherheitsebene für Recovery-Daten mit Datenisolation per Mausklick und lässt sich in Ihre Sicherheitsabläufe integrieren, damit Sie Ihre bestehenden Prozesse für die Reaktion auf Vorfälle und deren Behebung weiter nutzen können.

Verstärken Sie Ihre Datensicherheitsmaßnahmen und beschleunigen Sie die Wiederherstellung

Verbesserung der Bedrohungserkennung

Verbessern Sie die Erkennung von Ransomware und anderen Angriffen, indem Sie ungewöhnliche Änderungen in Backup-Daten ermitteln, die auf einen bevorstehenden Angriff hindeuten können, oder ein Benutzerverhalten, das auf eine unbefugte Datennutzung oder einen unbefugten Datenzugriff schließen lässt. Stellen Sie mit der auf Threat Intelligence und Deep Learning basierenden Bedrohungserkennung sicher, dass Ihre Backup-Daten frei von Malware sind.

Einschätzung der Auswirkungen von Angriffen

Ermitteln Sie, ob sensible Daten offengelegt wurden, um angemessene Abhilfemaßnahmen und Compliance-Prozesse zu gewährleisten.

Mehrschichtige Sicherheit mit Datenisolation

Unterstützen Sie Best Practices und neue Anforderungen für zusätzliche Sicherheit durch isolierte und ausgelagerte Datensicherung.

Nutzung vorhandener Prozesse und Kontrollen

Integrieren Sie die Erkennung von Datenanomalien und Benutzerverhalten in die Sicherheitsabläufe, um bestehende Prozesse zur Sichtung, Reaktion und Behebung von Vorfällen zu verstärken und zu erweitern.

Services für Sicherheit und Wiederherstellung

Threat Intelligence und Scanning

Erhöhen Sie die Datensicherheit durch die Bedrohungserkennung mit einem Klick, Scanning, Analyse des Benutzerverhaltens und ML-gesteuerte Erkennung von Datenanomalien.

Intelligente Datenklassifizierung

Datenerkennung und -klassifizierung von BigID mit ML-basiertem Mustervergleich zur Identifizierung sensibler und regulierter Daten.

Cohesity FortKnox

Service zur Isolation von Daten mit Management-, Netzwerk- und Standortisolation, unterstützt durch Unveränderlichkeit und Zero-Trust-Prinzipien bei gleichzeitiger Bereitstellung einer flexiblen und granularen Wiederherstellung.

Integrationen in Sicherheitsabläufe

Integration mit Playbooks zu Palo Alto Networks XSOAR, ServiceNow, Cisco SECUREX, CrowdStrike, Splunk und Securonix.

Ähnliche Produkte und Funktionen

Cohesity Helios® – Multicloud-Datenplattform und globale GUI, die eine umfassende Palette von Datenmanagement-Services On-Premises oder über ein SaaS-Modell bietet.

Cohesity DataProtect – umfassende Backup- und Recovery-Lösung für traditionelle und moderne Workloads auf einer sicheren und skalierbaren Multicloud-Plattform. Es bietet sofortige skalierbare Wiederherstellung über verschiedene Umgebungen hinweg.

Eine bewährte Plattform für Datensicherheit und -management

Tausende von Kunden genießen bereits die Einfachheit und den erwiesenen Wert der Cohesity Helios® Multicloud-Datenplattform. Ganz gleich, wo Sie sich in Sachen Datensicherheit und -management befinden, wir haben die richtige Lösung für Sie, damit Sie Ihre Daten sichern und optimal nutzen können. Wir bieten eine vollständige Suite von Services, die auf einer Multicloud-Datenplattform konsolidiert sind: Datensicherheit und -schutz, Datensicherung und -wiederherstellung, Notfallwiederherstellung, Datei- und Objektdienste, Entwicklung/Tests sowie Daten-Compliance und Analysen.

Erfahren Sie mehr auf Cohesity.com/de/.

COHESITY