COHESITY

WHITEPAPER

August 2022

Verstärken Sie Ihre Ransomware-Abwehr: Schützen, Erkennen und Wiederherstellen

Next-Gen Data Management schützt vor Ransomware und datenzentrierten Bedrohungen

Inhaltsverzeichnis

Schützen, Erkennen und Wiederherstellen mit Cohesity 3
Die letzte Verteidigungslinie gegen Ransomware 3
Daten und Plattform sichern, Daten und Benutzer im Auge behalten 4
Im Detail 5
Datenresilienz: Stellen Sie die Integrität und Verfügbarkeit von Plattformdaten sicher 5
- Verschlüsselung von Daten im Ruhezustand und in Bewegung 5
- Fehlertoleranz 6
- Unveränderliche Daten 6

Zugriffskontrolle: Zero-Trust-Architektur 6
- Multifaktor-Authentifizierung (MFA) 6
- Rollenbasierte Zugriffskontrolle (RBAC) 7
- Quorum 7
- Prüfung 7
- Kontinuierliche Überwachung 7

Erkennung und Analyse: KI und ML zur Erkennung böswilliger Aktivitäten 7
- Anomalieerkennung 7
- Erkennung von Bedrohungen nahezu in Echtzeit 8
- Datenklassifikation 8
- Adaptive Verhaltensanalyse 8

Sicherheitsintegrationen: Nutzen Sie vorhandene Tools zur Erkennung, Reaktion und Behebung 8
- Sicherheitsinformations- und Ereignisverwaltung (SIEM) 9
- Sicherheits-Orchestrierung und automatisierte Reaktion (SOAR) 9
- Identitätsverwaltungslösungen 9
- Bedrohungserkennungslösungen 9
- Schwachstellenmanagement 9
- Anwendungsprogrammierschnittstelle (API) 10

Wiederherstellen: Sofortige Wiederherstellung kritischer Geschäftsprozesse und Dateien 10
- Skalierbare Wiederherstellung: Beschleunigen Sie die Wiederherstellung, gewährleisten Sie den Betrieb rund um die Uhr und erfüllen Sie SLAs 10
- Moderne Isolierung: Bei katastrophalem Verlust lokaler Backup-Daten 11

Fazit: Keine Option 11
Über Cohesity 12

Schützen, Erkennen und Wiederherstellen mit Cohesity

Die Cohesity-Plattform bietet Unternehmen einen außergewöhnlichen Mehrwert, um riesige Unternehmensdatenspeicher zu schützen und zu verwalten. Cyberkriminelle zielen jedoch auf Datenspeicher für verschiedene schändliche Aktivitäten ab, insbesondere Ransomware und Datendiebstahl. Ransomware ist nach wie vor die häufigste Bedrohung, da mit ihr leicht Geld gemacht werden kann. Cyberkriminelle versuchen daher ununterbrochen, Unternehmen zu kompromittieren.

Bei Ransomware-Angriffen ist kein Rückgang zu verzeichnen. Im Jahr 2021 kam es zu schätzungsweise 714 Millionen Angriffen[1], wobei alle 11 Sekunden ein Unternehmen Opfer eines Angriffs wurde[2]. Cyberkriminelle sind hochgradig organisiert und haben Tools und Dienste für verschiedene Phasen eines Ransomware-Angriffs entwickelt. Ein fehlgeleiteter Benutzerklick, eine einfache Fehlkonfiguration des Systems und das Einschleusen neuer, nicht erkennbarer Malware können für Unternehmen katastrophale Folgen haben. Ransomware-Angriffe können zu Kundenmisstrauen, Umsatzeinbußen und der Unterbrechung aktueller und zukünftiger Betriebsabläufe führen.

Zusammen mit Ransomware haben globale Konflikte das Risiko nationalstaatlich gesponserter Angriffe erhöht. Wie in der Shields Up-Warnung der US-amerikanischen Bundesbehörde CISA (Cybersecurity and Infrastructure Security Agency) und in den Warnungen anderer Nationen angemerkt, müssen alle Unternehmen besondere Sorgfalt walten lassen, um sicherzustellen, dass ihre Informationssysteme ausgeklügelten und hartnäckigen Angriffen widerstehen können.

Diese Herausforderungen erfordern umfassende Sicherheitslösungen für das Datenmanagement, bei dem die Datenmanagement-Plattform datenzentrierten Bedrohungen standhalten und sich aktiv dagegen wehren kann. Kernsicherheitsfunktionen, die sicherstellen, dass Daten nicht durch Ransomware-Angriffe beschädigt oder gelöscht bzw. von Datendieben oder böswilligen Insidern gestohlen werden können und die Erkennung laufender Angriffe sind wichtiger denn je.

Die letzte Verteidigungslinie gegen Ransomware

Gegen Ransomware-Angriffe, Datenschutzverletzungen oder Insider-Bedrohungen sind hinsichtlich Schutzes, Erkennung und Wiederherstellung mehrere Schlüsselfähigkeiten und -funktionen erforderlich.

Zum Schutz und zur Erkennung bieten die Sicherungs- und Erkennungsfunktionen Datenresilienz, um die absichtliche oder versehentliche Zerstörung von Daten zu verhindern. Zu den Sicherheitsvorkehrungen gehören strenge Zugriffskontrollen, um Einstellungen vor unbefugtem Zugriff oder Änderungen zu schützen und die Vertraulichkeit der Daten zu sichern und zu gewährleisten. Außerdem werden durch eine kontinuierliche Überwachung mit Erkennung und Analyse Angriffe und ungewöhnliche Aktivitäten identifiziert. Unterstützt werden diese Funktionen durch Integrationen mit führenden Sicherheitsanwendungen zur Automatisierung der Reaktion auf Vorfälle und zur Nutzung vorhandener Sicherheitsdienste für Unternehmen wie Schlüsselmanagement, Identitäts- und Zugriffsverwaltung, Multifaktor-Authentifizierung sowie Bedrohungs- und Schwachstellen-Scans. Diese Funktionen arbeiten zusammen, um eine solide Datenmanagement-Plattform bereitzustellen, die die Möglichkeit eines Angriffs, Daten zu manipulieren oder zu zerstören, verhindert und Unternehmen dabei hilft, Angriffe auf die laufenden Daten besser zu erkennen.

Im Bereich Recovery bietet Cohesity eine beispiellose skalierbare Wiederherstellung und moderne Isolierung. Die skalierbare Wiederherstellung ermöglicht es Unternehmen, ihren besten Wiederherstellungspunkt zu identifizieren, den Status bestimmter Daten zu verstehen, sofort Zugriff auf Dateien und Objekte zu gewähren und Tausende von VMs innerhalb von Minuten wiederherzustellen. Die moderne Isolierung bietet eine vertrauenswürdige Wiederherstellung für Worst-Case-Szenarien, bei denen der primäre Standort des Unternehmens vollständig deaktiviert wurde und für die Wiederherstellung nicht verfügbar oder geeignet ist.

Daten und Plattform sichern, Daten und Benutzer im Auge behalten

Datenresilienz besteht aus drei wesentlichen Faktoren. Zunächst müssen Daten unveränderlich sein und eine konfigurierbare Lebensdauer haben. Das heißt, dass die Daten nach dem Schreiben nicht mehr geändert werden können und bestimmte Kopien solange aufbewahrt werden, bis sie gemäß den Richtlinien des Unternehmens gelöscht werden. Als Nächstes müssen Daten, die von der Datenmanagement-Plattform eines Unternehmens gespeichert und übertragen werden, eine starke Verschlüsselung verwenden, um die unbefugte Einsicht in Daten zu verhindern. Datenschutz- und Branchenvorschriften wie DSGVO, PCI und HIPAA verlangen von Unternehmen, dass sie personenbezogene Daten (PII), Daten der Zahlungskartenindustrie (PCI) und geschützte Gesundheitsinformationen (PHI) verschlüsseln – und dies ist nur ein kleiner Teil der globalen Gesetze und Vorschriften, die diesen Schutz vorschreiben. Diese Funktionalitäten schützen die Daten vor böswilligen Aktionen, die von Ransomware verursacht werden, und stellen sicher, dass die Vertraulichkeit und Integrität der Daten gewahrt bleibt. Und schließlich muss die Datenmanagement-Plattform fehlertolerant sein und über Redundanz verfügen, damit gewährleistet ist, dass die Plattform für Backup-Zeitpläne gemäß den Unternehmenszielen für die Wiederherstellungspunkte verfügbar ist und kein einzelner Fehlerpunkt auftritt.

Zugriffskontrollen ermöglichen es Unternehmen, unter Einhaltung der Zero-Trust-Prinzipien genau zu steuern, wer auf die Datenmanagement-Plattform zugreifen und diese ändern kann. Mit der Multifaktor-Authentifizierung (MFA) können sich nur verifizierte Benutzer auf der Plattform anmelden. Dies ist wichtig, um die Übernahme von Administratorkonten und unbefugte Änderungen an Daten und Einstellungen zu verhindern. In Verbindung mit granularen rollenbasierten Zugriffskontrollen (RBAC) können Unternehmen streng kontrollieren, auf welche Funktionen Benutzer zugreifen dürfen, um das Prinzip der geringsten Rechte zu unterstützen. Zur weiteren Kontrolle von Änderungen an den Plattformeinstellungen verhindert das Quorum unbefugte Aktualisierungen, indem zwei oder mehr Genehmigungen erforderlich sind, um Konfigurationen oder Einstellungen zu ändern.

Erkennung und Analyse bieten Funktionen zum Analysieren und Überwachen von Plattformdaten auf Hinweise für laufende Angriffe, kompromittierte Workloads sowie Informationen über die Daten, um den Einsatz geeigneter Schutzmaßnahmen für sensible Daten sicherzustellen. Die Erkennungs- und Analysefunktionen umfassen neben der Überwachung der Daten auf ungewöhnliche Änderungen, die auf Ransomware oder andere böswillige Aktivitäten hindeuten können, auch die Überwachung des Benutzerverhaltens auf ungewöhnliche Datenzugriffe. Wird Kontext zu den Daten (z. B. Benutzerzugriffsaktivitäten) in fortschrittliche KI/ML-Modelle eingespeist, können Benutzerverhaltensanalysen wichtige frühe Einblicke in einen aufkommenden Ransomware-Angriff oder eine Insider-Bedrohung liefern.

Eine entscheidende Komponente der Erkennung und Analyse ist Datenintelligenz. Sie liefert Details über die Datenlandschaft des Unternehmens wie beispielsweise Standort, Klassifizierung, Nutzung und Volumen. Diese Informationen helfen dem Unternehmen zu verstehen, welche Daten es hat, und die angemessenen Schutzmaßnahmen und Kontrollen basierend auf ihrer Sensibilität sicherzustellen. Für eine schnelle Reaktion und Wiederherstellung können Ransomware-Erkennungswarnungen sowohl an IT- als auch an Sicherheitsbetriebsteams weitergeleitet und somit eine koordinierte Reaktion auf Vorfälle ermöglicht werden.

Zusätzliche **Sicherheitsintegrationen** in die vorhandene Sicherheitsinfrastruktur bieten einen Kraftmultiplikator für die Sicherung und den Schutz der Datenmanagement-Plattform. Durch die Integration von Lösungen zum Schwachstellenmanagement und zur Bedrohungserkennung können Risiken und Bedrohungen identifiziert werden, während Identitäts- und Zugriffsmanagement-Integrationen es Unternehmen ermöglichen, vorhandene Zugriffskontrollen zu nutzen. SIEM- und SOAR-Integrationen erleichtern die Reaktion auf Vorfälle sowie das Ticketmanagement und bieten die Umgebungsunterstützung, die zum Sichern der Plattform erforderlich ist. Außerdem ermöglichen sie eine nahtlose Zusammenarbeit von Sicherheits- und IT-Betrieb.

Die Cohesity-Plattform verwendet eine Zero-Trust-Architektur, Analysen und Plattformschutzmaßnahmen, damit diese sicher und solide ist. Sie bietet mehrere bedeutende Vorteile zur Reduzierung von Risiken und zur Verbesserung der Cyber-Resilienz. Zu diesen Vorteilen gehören die Sicherheit und Widerstandsfähigkeit von Daten gegen Ransomware-Angriffe und Datenschutzverletzungen, Datensicherheit bei Betriebsausfällen und Naturkatastrophen, die Sicherung archivierter Daten sowie Datenintelligenz zur Unterstützung von Datenverwaltung und Compliance.

Im Detail

Im Folgenden finden Sie einen detaillierten Überblick über die Fähigkeiten und Funktionen der Cohesity-Plattform. Jede Hauptkomponente der Architektur wird nach Kategorien überprüft, die aus Folgendem bestehen:

Datenresilienz: Verschlüsselung von Daten im Ruhezustand und in Bewegung, Fehlertoleranz und unveränderliche Datenspeicherung

Zugriffskontrollen: Multifaktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrollen (RBAC), Quorum, Prüfung und kontinuierliche Überwachung

Erkennung und Analyse: Anomalieerkennung, Bedrohungserkennung nahezu in Echtzeit, Datenklassifizierung und adaptive Verhaltensanalyse

Sicherheitsintegrationen: Sicherheitsinformations- und Ereignisverwaltung (SIEM), Sicherheits-Orchestrierung und automatisierte Reaktion (SOAR), Identitätsverwaltung, Bedrohungserkennungslösungen, Schwachstellenmanagement und Anwendungsprogrammierschnittstelle (API)

Datenresilienz: Stellen Sie die Integrität und Verfügbarkeit von Plattformdaten sicher

Verschlüsselung von Daten im Ruhezustand und in Bewegung

Cohesity verschlüsselt alle Daten und Datenflüsse innerhalb der Plattform. Die Verschlüsselung verhindert, dass unbefugte Benutzer Daten außerhalb der Plattform einsehen. In der Plattform gespeicherte Daten sind unverständlich, es sei denn, sie werden von einem autorisierten Benutzer abgerufen und entschlüsselt. Die meisten Datenschutz- und Branchenvorschriften, insbesondere DSGVO, CCPA, PCI und HIPAA, verlangen von Unternehmen, PII, PCI und PHI mit Verschlüsselung zu schützen. Plattformdaten werden im Ruhezustand mit AES-256-Verschlüsselung gespeichert. Die Plattform bietet mehrere Optionen für die sichere Verwaltung von

Verschlüsselungsschlüsseln – entweder mit dem von Cohesity gestellten Key Management Service (KMS) oder über Drittanbieter wie z. B. Amazon Web Services KMS, Thales, Fortanix oder Entrust.

Für Daten während der Übertragung verwendet die Datenmanagement-Plattform von Cohesity den TLS-Standard. TLS verschlüsselt Daten, um sicherzustellen, dass Lauscher und Hacker den Datenfluss zur und von der Plattform nicht sehen können. Dies ist entscheidend, um private und sensible Daten im Hinblick auf Sicherheit und Compliance zu schützen. Cohesity verwendet bei der Übertragung die Protokolle TLS 1.2 und mTLS mit ausschließlich FIPS-geprüften Verschlüsselungssuiten mit Perfect Forward Secrecy (PFS)-Schutz.

Fehlertoleranz

Die Datenmanagement-Plattform von Cohesity bietet Toleranz für mehrere Systemfehler, damit eine hohe Verfügbarkeit der Plattform gewährleistet ist. Dadurch werden Ausfälle an einem einzelnen Fehlerpunkt verhindert, um SLA- und Geschäftskontinuitätsanforderungen zu erfüllen. Cluster können den Betrieb bei mehreren Ausfällen von HDDs und SDDs sowie Knoten, Gehäusen und Racks fortsetzen. Darüber hinaus können die Cluster Fehler an Netzteilen, Lüftern und Netzwerken auffangen.

Unveränderliche Daten

Daten, die von Cohesity gesichert werden, ändern niemals ihren gespeicherten Zustand, bis die Daten ablaufen. SpanFS™ von Cohesity bietet unveränderliche Datensicherungs-Snapshots, um das Ändern oder Löschen von Daten zu verhindern. Basierend auf der Hyperscale-Architektur kann SpanFS von Cohesity Backup-Daten in seinem gesicherten Dateisystem in unveränderlichen Snapshots speichern, die von außerhalb eines Cohesity-Clusters nicht gemountet oder direkt aufgerufen werden können. Die Datensicherungs-Snapshots werden in einem schreibgeschützten Zustand gespeichert. Externe Anwendungen oder unbefugte Benutzer können den Snapshot nicht ändern.

Alle Versuche, in einen unveränderlichen Datensicherungs-Snapshot zu schreiben, werden auf (kostenlose) Klone geschrieben, die nach Abschluss jedes Schutzlaufs auch als schreibgeschützt markiert werden. Für alle Mount-basierten Wiederherstellungen, die während des sofortigen Massenwiederherstellungsprozesses von Cohesity verwendet werden, wird die interne Ansicht zuerst geklont und dann der externen Umgebung ausgesetzt, wobei die interne Ansicht immer extern unzugänglich bleibt. Schreibvorgänge in interne Ansichten während der Datensicherung sind nur über vertrauenswürdige interne Dienste und authentifizierte APIs zulässig. Für zusätzliche Sicherheit kann DataLock (die WORM-Funktionalität von Cohesity) auf Cohesity-Snapshots angewendet werden. Wenn DataLock aktiviert ist, kann der Datensicherungs-Snapshot von niemandem, auch nicht von Administratoren, gelöscht werden, bis DataLock abläuft.

Zugriffskontrolle: Zero-Trust-Architektur

Gemäß des National Institute of Standards and Technology (NIST) ist Zero Trust wie folgt definiert: „Zero Trust (ZT) ist der Begriff für eine sich entwickelnde Reihe von Cybersicherheitsparadigmen, die die Verteidigung von statischen, netzwerkbasierten Perimetern verlagern, um sich auf Benutzer, Vermögenswerte und Ressourcen zu konzentrieren.“ Zero Trust konzentriert sich auf die Validierung der Authentizität und Autorisierung von Benutzern für jeden Zugriff oder jede Änderung an der Plattform.

Multifaktor-Authentifizierung (MFA)

Die Multifaktor-Authentifizierung (MFA) bietet eine starke Authentifizierung von Benutzern, um unbefugte Änderungen an den Plattformeinstellungen oder Daten zu verhindern. MFA verbessert die Plattformsicherheit, indem Benutzer aufgefordert werden, sich durch mehr als nur einen Benutzernamen und ein Passwort zu identifizieren. Passwörter und Benutzernamen sind anfällig für Brute-Force-Angriffe und können gestohlen werden. MFA erfordert, dass der Benutzer Login-Anfragen mit einer Antwort authentifiziert, die nur er selbst

geben kann (z. B. eine Handy-Challenge), oder mit einem zeitbasierten Einmalkennwort (TOTP). Cohesity unterstützt native MFA oder MFA-Drittanbieter wie Ping, Duo, Okta und mehr.

Rollenbasierte Zugriffskontrolle (RBAC)

Die granulare rollenbasierte Zugriffskontrolle ermöglicht es einem Unternehmen, Benutzern die geringsten Berechtigungen zu gewähren, die erforderlich sind, um ihre Arbeitsanforderungen auszuführen, Risiken zu minimieren und Bereiche außerhalb ihrer Verantwortlichkeiten unerreichbar zu halten. Unternehmen können Cohesity-Benutzerrollen auf bestimmte Anwendungen, Funktionen oder Arbeitsabläufe in der Plattform beschränken und dadurch die Aktivitäten eines Benutzers basierend auf seiner Rolle und seinen Verantwortlichkeiten einschränken. So können bestimmte Benutzer beispielsweise auf die Durchführung von Datensicherungen oder die Datenermittlung beschränkt werden.

Quorum

Cohesity nutzt Quorum-Genehmigungen (verfügbar in Version 6.8), um Unternehmen in die Lage zu versetzen, einseitige Änderungen an der Plattform innerhalb von Administratorkonten zu verhindern – eine entscheidende Kontrolle zum Schutz vor unbeabsichtigten Benutzerfehlern, betrügerischen Administratoren oder kompromittierten Konten. Mit Quorum erfordern Benutzeranfragen zum Ändern von Einstellungen oder Verwaltungsfunktionen mehrere Genehmigungen, um die Anfrage zu autorisieren.

Prüfung

Die Cohesity-Plattform verfügt über einen Benutzerprüfpfad für alle Aktionen, die auf dem Cohesity-Cluster durchgeführt werden. Diese Aufzeichnungen belegen die Einhaltung von Vorschriften und Betriebsintegrität. Prüfpfade können auch Bereiche der Nichteinhaltung identifizieren, indem sie Informationen für Audit-Untersuchungen bereitstellen. Prüfprotokolle erfassen Benutzeraktivitäten für Anmeldung/Abmeldung, Änderungen an Daten oder Dateneigenschaften und Auftragsplanung. Die Plattform organisiert Protokolle nach Kategorien, wie z. B. Active Directory oder Cluster, für eine schnelle Analyse.

Kontinuierliche Überwachung

Die Plattform von Cohesity bietet Umgebungsüberwachung, um das Risiko menschlicher Fehler und Fehlkonfigurationen zu verringern. Die Überwachung umfasst Scans der Cohesity-Umgebung, einschließlich einer Reihe von Sicherheitskonfigurationen, und berücksichtigt eine Vielzahl von Faktoren wie Zugriffskontrolle, Audit-Protokolle und Verschlüsselungs-Framework, die für den Schutz des Sicherheitsstatus des Daten-Clusters entscheidend sind.

Erkennung und Analyse: KI und ML zur Erkennung böswilliger Aktivitäten

Anomalieerkennung

Die Cohesity-Plattform analysiert die aus Produktionsumgebungen aufgenommenen Daten bei jeder einzelnen Datensicherung sofort auf verräterische Anzeichen ungewöhnlicher Aktivitäten oder Datenänderungen. Diese Aktivitäten können auf einen Ransomware-Angriff hindeuten. Ein zentrales Dashboard warnt bei Anomalien basierend auf dem Timing und der Häufigkeit des Lesens und Schreibens von Daten, der Zufälligkeit von Daten und der Änderung von Dateien, einschließlich hinzugefügter, gelöschter und geänderter Dateien. Mit der Anomalieerkennungsfunktion von Cohesity können Unternehmen Warnungen für Bedingungen festlegen, die auf Ransomware oder andere böswillige Aktivitäten hinweisen könnten.

Erkennung von Bedrohungen nahezu in Echtzeit

Bedrohungen des Datenschutzes und der Sicherheit können durch verschiedene Klassen von Malware entstehen. Zur Verringerung des Malware-Risikos können Unternehmen ihre Sicherheitskontrollen ergänzen, indem sie zusätzliche Datenscans einsetzen, um Viren, Trojaner und andere Malware zu erkennen. Cohesity unterstützt das Scannen unstrukturierter Daten, wodurch Unternehmen zahlreiche Scans durchführen und die Erkennung ohne Mehraufwand für die Produktion und andere Echtzeitdienste verbessern können.

Datenklassifikation

Der Begriff Datenverbreitung definiert die wachsende Anzahl an Standorten, das Volumen und die Vielfalt von Daten in Unternehmen, was auch als „Massendatenfragmentierung“ bezeichnet wird. Angesichts der zunehmenden Verbreitung benötigen Unternehmen Automatisierung, um die wachsenden Quellen kritischer und sensibler Daten zu verfolgen und sicherzustellen, dass Datensicherung, Sicherheit, Analytik, Governance und Datenschutz keine Lücken in ihrer Abdeckung aufweisen.

Ab dem 2. Halbjahr 2022 wird die Datenplattform von Cohesity eine automatisierte Datenklassifizierung bereitstellen, damit Unternehmen sensible Informationen ermitteln, klassifizieren, markieren und somit sicherstellen können, dass Schutzmaßnahmen und Sicherheitsvorkehrungen die Compliance- und SLA-Anforderungen erfüllen. Die KI-basierte Klassifizierung beleuchtet sensible Daten im gesamten Unternehmen. Sie ermöglicht die Erstellung von Karten mit Datenberechtigungen, die den Standort und die Klassifizierung sensibler Daten detailliert beschreiben.

Diese vordefinierten Richtlinien helfen Unternehmen, ihre globalen und regionalen Anforderungen für DSGVO, CCPA, HIPAA und andere Vorschriften zu erfüllen. Zudem können Unternehmen mehr als 100 vordefinierte Muster nutzen, um Richtlinien zu erstellen, die auf ihre spezifischen Herausforderungen und Bedürfnisse abgestimmt sind.

Adaptive Verhaltensanalyse

Anomales Benutzerverhalten und unangemessene Dateneinstellungen können das Risiko von Datenlecks erhöhen. Voraussichtlich in der ersten Hälfte des Jahres 2022 wird die Plattform den Datenzugriff und die Protokolle auf ungewöhnliche Datenaktivitäten und -nutzung überwachen, die auf böswillige Handlungen hindeuten könnten. Darüber hinaus können potenziell übermäßig gefährdete Daten durch die Analyse von Zugriffskontrolllisten (ACLs) identifiziert werden, bei denen sensible Daten wie PII keine ausreichenden Zugriffsbeschränkungen haben. Dies bietet Datenschutz- und Sicherheitsteams eine frühzeitige Warnung vor Verhaltensweisen, die auf einen Ransomware-Angriff oder andere böswillige Aktivitäten schließen lassen. Außerdem können so Datenrisiken, die durch schwache Zugriffseinstellungen verursacht werden, proaktiv gemindert werden.

Sicherheitsintegrationen: Nutzen Sie vorhandene Tools zur Erkennung, Reaktion und Behebung

Es braucht ein ganzes Dorf, um Bösewichter in Schach zu halten. Nahezu alle Unternehmen verfügen über Toolsets zur Erkennung von Malware, Viren und Schwachstellen und haben umfassende Verfahren und Richtlinien entwickelt, um zu überprüfen, ob Informationsressourcen sicher verwendet werden können. Daher ist die Cohesity-Plattform so konzipiert, dass sie sich in die bestehende Sicherheitsstruktur eines Unternehmens integrieren lässt, damit z. B. eine konsistente Implementierung der Benutzerauthentifizierung und Datenverschlüsselung gewährleistet, bestehende Lösungen und Prozesse für die Reaktion und das Management von Vorfällen ergänzt und bereits vorhandene Lösungen zur Erkennung von Bedrohungen und Schwachstellen genutzt werden können. Dadurch kann die Datenmanagement-Plattform von

Cohesity die Sicherheitsrichtlinien und -prozesse des Unternehmens unterstützen und erweitern. Integrationen umfassen mehrere Sicherheitskategorien, darunter SIEM und SOAR, Identitätsmanagement, Schwachstellenmanagement und Bedrohungserkennung. Diese werden im Folgenden näher beschrieben:

Sicherheitsinformations- und Ereignisverwaltung (SIEM)

Unternehmen nutzen SIEM, um eine Echtzeitanalyse von Sicherheitswarnungen zu erhalten, die von Anwendungen und Netzwerkhardware generiert werden. Die Datenmanagement-Plattform von Cohesity liefert Warnungen, die auf Ransomware-Angriffe oder andere böswillige Aktivitäten hinweisen. Mit der Integration von Cohesity und Cisco SecureX können Unternehmen ihre Reaktion auf diese Warnungen automatisieren. Auf diese Weise können Unternehmen die Untersuchung und Reaktion auf Ransomware-Bedrohungen beschleunigen, indem sie Einblicke in kompromittierte Daten mit anderen globalen Intelligenz- und Kontextinformationen auf einer einzigen Plattform aggregieren und korrelieren.

Sicherheits-Orchestrierung und automatisierte Reaktion (SOAR)

SOAR hilft Unternehmen beim Sicherheitsmanagement, der Automatisierung von Sicherheitsvorgängen und der Reaktion auf Sicherheitsvorfälle. Unternehmen sind dadurch in der Lage, schnell und effektiv auf Vorfälle zu reagieren, z. B. auf mutmaßliche Ransomware, die durch die Datenmanagement-Plattform von Cohesity erkannt wurde. Cohesity verfügt über eine Integration mit der Cortex XSOAR-Lösung von Palo Alto Networks. Diese Integration hilft Sicherheits- und IT-Teams, Ransomware-Angriffe zu erkennen und sich davon zu erholen. Datenanomalien werden von der Cohesity-Datenmanagement-Plattform erkannt und an XSOAR weitergeleitet, das eine automatisierte Vorfallverarbeitung und -verwaltung in Verbindung mit Bedrohungsinformationen und Malware-Erkennung bietet.

Identitätsverwaltungslösungen

Viele Unternehmen verwenden Identitätsverwaltungslösungen für eine gemeinsame, hochsichere Methode zur Authentifizierung von Benutzern. Die Datenmanagement-Plattform von Cohesity unterstützt native MFA oder MFA-Drittanbieter wie Ping, Duo, Okta und mehr.

Bedrohungserkennungslösungen

Die Bedrohungserkennung hilft bei der Identifizierung bösartiger Software, die von Angreifern verwendet werden könnte, um Ransomware oder Cyberangriffe zu starten, Daten zu stehlen oder die Kontrolle über die Systeme eines Unternehmens zu erlangen. Cohesity nutzt die Bedrohungserkennung, um die Plattform vor oder nach der Datenaufnahme zu scannen und so Malware zu erkennen. Cohesity bietet native Unterstützung über seine ClamAV-Lösung.

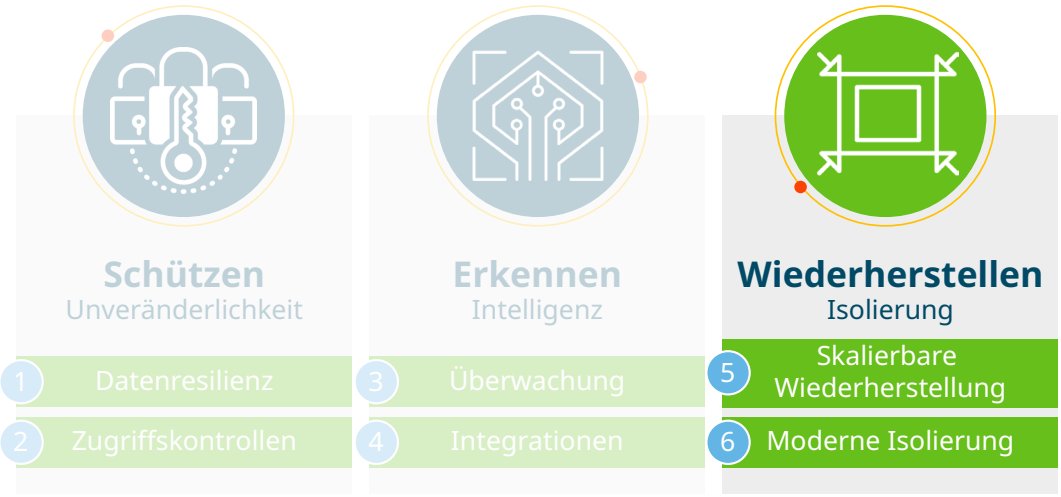
Schwachstellenmanagement

Das Schwachstellenmanagement gibt Einblick in potenzielle Risiken, die von Anwendungen, Browsern und Softwarediensten ausgehen. Die Lösungen kategorisieren und priorisieren diese Schwachstellen und helfen Unternehmen dabei, das Risiko von Datenschutzverletzungen und Malware wie Ransomware zu reduzieren. Unternehmen haben die Möglichkeit, die Technologie von Tenable zu nutzen, um Schwachstellen in den Daten und Umgebungen zu identifizieren, die von der Cohesity Datenmanagement-Plattform verwaltet werden. Cohesity CyberScan, powered by Tenable, stellt ein detailliertes Dashboard zur Verfügung und liefert einen globalen Überblick über alle Cybergefahren in einer Produktionsumgebung, um Risiken zu reduzieren. Durch die Ermittlung blinder Flecken in der Infrastruktur können Unternehmen kritische Cyberrisiken und Schwachstellen beheben, bevor sie ausgenutzt werden.

Anwendungsprogrammierschnittstelle (API)

Über die oben genannten vorgefertigten Integrationen hinaus kann die Datenmanagement-Plattform von Cohesity in jede Sicherheitslösung mit einer sicheren und dennoch offenen API integriert werden. Warnungen, Statusinformationen und andere Erkenntnisse von der Cohesity-Plattform können von Sicherheitsanwendungen Dritter genutzt werden, um die spezifischen Anforderungen und betrieblichen Herausforderungen von Unternehmen zu erfüllen. Die Liste der standardmäßigen Integrationen wird sich im Laufe der Zeit basierend auf der Kundennachfrage weiterentwickeln. Darüber hinaus gibt es bereits heute die Möglichkeit, maßgeschneiderte Integrationen zu erstellen, die den individuellen Anforderungen von Unternehmen entsprechen.

Wiederherstellen: Sofortige Wiederherstellung kritischer Geschäftsprozesse und Dateien



Skalierbare Wiederherstellung: Beschleunigen Sie die Wiederherstellung, unterstützen Sie den Betrieb rund um die Uhr und erfüllen Sie SLAs

Die skalierbare Wiederherstellung bietet Unternehmen sofortigen Zugriff auf kritische Geschäftsprozesse und Daten, um ihre anspruchsvollen Recovery Time Objectives (RTOs) zu erfüllen. Zunächst einmal liefert die Plattform basierend auf den ML-Modellen Unternehmen den letzten bekannten guten Wiederherstellungspunkt und eine leistungsstarke Suche, damit sie den Status bestimmter Dateninstanzen ermitteln können. Als Nächstes können Unternehmen mit vollständig hydratisierten Snapshots Hunderte von VMs, Dateien oder Datenbanken beliebiger Größe sofort wiederherstellen. Dieser Prozess ermöglicht es IT-Mitarbeitern, geschäftliche SLAs einzuhalten und gleichzeitig Zeit und Ressourcen zu sparen.

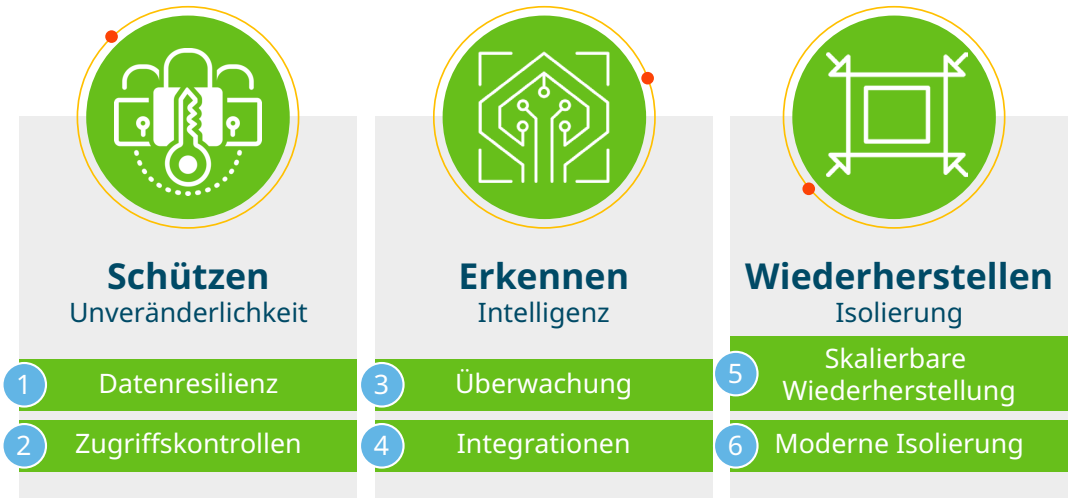
Und zu guter Letzt können Unternehmen sofort auf Dateien und Objekte zugreifen. Dieser schnelle Zugriff auf Dateien und Objekte ist dank Cohesity SmartFiles möglich. Unternehmen können sofort die letzte gute Datensicherung ihrer NAS-Freigaben klonen und diese Dateien direkt aus dem Cohesity Cluster bereitstellen – wodurch der Dienst für Benutzer wiederhergestellt wird, ohne dass Daten verschoben werden müssen. Sie können auch kritische Daten aus ActiveDirectory wiederherstellen, wenn Zugriffskontrolllisten betroffen sind.

Moderne Isolierung: Bei katastrophalem Verlust lokaler Backup-Daten

Wie von „Shields Up“ empfohlen, sollten Unternehmen die 3-2-1-Regel für Backup-Daten implementieren: 3 vollständige Backup-Datenkopien – 2 lokale und 1 isolierte. Die isolierte Kopie bietet eine weitere Offsite-Kopie der Backup-Daten im Falle eines katastrophalen Ereignisses, das die lokalen Kopien der Daten deaktiviert.

Die Isolierung kann auf verschiedene Weise erfolgen: Isolierung auf Band, eine vom Kunden verwaltete Isolierung in der Cloud oder eine SaaS-Isolierung. Für anspruchsvolle RTO- und RPO-Anforderungen würden die meisten Unternehmen die Isolierung in der Cloud oder über SaaS nutzen. Diese Optionen bieten das beste Gleichgewicht zwischen Wiederherstellung und Isolierung. Die Wahl der Isolierung ist allerdings keine Entweder-Oder-Entscheidung. Es können mehrere Optionen ausgewählt werden, um verschiedene Datentypen zu unterstützen, wie beispielsweise Transaktionsdaten oder vorwiegend statisches geistiges Eigentum, Quellcode oder Geschäftsgeheimnisse.

Fazit: Keine Option



Die Schutz-, Erkennungs- und Wiederherstellungsfunktionen von Cohesity zur Ransomware-Abwehr sind ein mehrschichtiger Ansatz zur Sicherung und Erhöhung der Widerstandsfähigkeit von Daten und zur Bereitstellung einer schnellen Wiederherstellung. Dabei kommen Verschlüsselung, Unveränderlichkeit und WORM-Funktionen zum Schutz von Backup-Daten vor unbefugten Änderungen zum Einsatz sowie Zero-Trust-Prinzipien zur Kontrolle und Verwaltung des Benutzerzugriffs auf die Plattform mit granularer RBAC, MFA und Sicherheit auf Bankenniveau mit Quorum. Die Erkennung bietet verwertbare Einblicke mit Analysen zu Datenanomalien und Benutzerverhalten sowie Bedrohungserkennung nahezu in Echtzeit und ist in bestehende Kontrollen integriert, um bestehende Ransomware-Abwehrmaßnahmen zu verstärken. Die letzte Phase, die Wiederherstellung, nutzt eine leistungsstarke sofortige Massenwiederherstellung und Dateizugriff, um kritische Geschäftsprozesse und Daten wieder online zu bringen.

Angesichts der sich ständig ändernden Bedrohungslandschaft wird die Plattform von KI und ML angetrieben, die entscheidende Funktionen bereitstellen, um neuen Sicherheitsbedrohungen einen Schritt voraus zu sein, die mit manuellen Prozessen nicht zu bewältigen sind.

Ransomware und andere Bedrohungen haben das Datenmanagement in den Vordergrund von Sicherheit und Cyber-Resilienz gerückt. Ohne eine solide, intelligente und integrierte Datenmanagement-Plattform zur

Abwehr und Vereitelung von Cyberangriffen und zur Wiederherstellung nach solchen Angriffen riskieren Unternehmen katastrophale Datenverluste und Geschäftsunterbrechungen.

Quellen:

1 https://blog.sonicwall.com/en-us/2021/10/cyber-threat-alert-ransomware-breaks-another-record/

2 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Über Cohesity

Cohesity vereinfacht das Datenmanagement extrem. Die Lösung erleichtert es, Daten zu sichern, zu verwalten und aus ihnen Wert zu schöpfen – über Rechenzentrum, Edge und Cloud hinweg. Wir bieten eine vollständige Suite von Services, die auf einer Multi-Cloud-Datenplattform konsolidiert sind: Datensicherung und Wiederherstellung, Notfallwiederherstellung, Datei- und Objektdienste, Entwicklung/Test sowie Daten-Compliance, Sicherheit und Analysen. Das reduziert die Komplexität und vermeidet die Fragmentierung der Massendaten. Cohesity kann als Service, als selbst verwaltete Lösung sowie über Cohesity-Partner bereitgestellt werden.

Besuchen Sie unsere Website und unseren Blog, folgen Sie uns auf Twitter und LinkedIn und liken Sie uns auf Facebook.

2000044-002-DE 8-2022