COHESITY

WHITEPAPER

# Verbesserung der Cyber-Resilienz mit einer Digital Jump Bag™

## Schnelle Wiederherstellung der Minimum Viable Response Capability und Stärkung der Vorfallsreaktion

# INHALTSVERZEICHNIS

# Vorwort

**James Blake**
VP Cyber Resiliency Strategy

Seit über 30 Jahren stehe ich an vorderster Front bei destruktiven Cyberangriffen und Datendiebstahl. Ich habe Erfahrungen mit der Reaktion auf Wiper-Angriffe von Staaten und als Leitung des Cyberrisikomanagements bei der größten Bank der Welt sammeln können.

Während dieser Zeit habe ich den Wert einer „Jump Back" zu schätzen gelernt. Der Begriff bezog sich ursprünglich auf einen physischen Behälter mit wichtiger Hardware und Software, der zu einem physischen, von einem Angriff betroffenen Standort mitgenommen werden musste. Diese Jump Back enthielt alle wesentlichen Hilfsmittel, um den Vorfall schnell zu untersuchen, Beweise zu sammeln und Bedrohungen zu entschärfen. Neben Hard- und Software war darin auch eine ausgedruckte Kontaktliste mit den wichtigsten Stakeholdern innerhalb des Unternehmens sowie externen Ansprechpartnern, der Krisenmanagementplan, Workflows für die möglichen Arten von Vorfällen und ein Mobiltelefon zu finden. Der Gedanke dahinter war, sofort reagieren zu können: Denn wenn man erst unter dem Druck eines Vorfalls alles Nötige zusammensucht, vergeudet man wertvolle Zeit und vergisst leicht etwas Wichtiges. Die Jump Back enthielt eine Mischung aus Tools, Details zu Prozessen und einer Kommunikationsmethode.

Heute leben wir in einer Welt der Remote-Erfassung, der Endpunkte und Extended Detection & Response (EDR/XDR), der virtuellen Maschinen und Cloud-Instanzen. Jump Bags können noch immer physische Behälter sein, die wir an den Einsatzort mitnehmen. Der größte Nutzen liegt jedoch in der Vorbereitung einer Digital Jump Bag™. Dieses geschützte und verlässliche Repository ermöglicht nicht nur den schnellen Zugriff auf die für die Remote-Erfassung und -Analyse erforderlichen Tools, sondern auch auf alle anderen digitalen Daten, die für eine erfolgreiche Vorfallsreaktion und Wiederherstellung erforderlich sind.

# Zusammenfassung

Die Digital Jump Bag™ ist die Grundlage eines Reinraums (engl. Clean Room) – einer sicheren und isolierten Umgebung, in der das SecOps-Team die notwendigen Untersuchungsschritte durchführen kann, um zu verstehen, wie es zu einem Angriff kam. Außerdem werden in einem Reinraum vor der Wiederherstellung Abhilfemaßnahmen durchgeführt, um die Bedrohung zu beseitigen und ein erneutes Auftreten zu verhindern. Was in die Digital Jump Bag gehört, hängt von der Reife, der Struktur, den Prozessen und den Tools eines Unternehmens ab.

Im Kern ermöglicht die Digital Jump Bag einem Unternehmen die rasche Wiederherstellung einer Minimum Viable Response Capability (MVRC). Dabei handelt es sich um eine optimierte Zusammenstellung wesentlicher Tools, Dokumente und Prozesse, die für eine effektive Reaktion auf einen Cyberangriff erforderlich sind. Die MVRC stellt sicher, dass Unternehmen Sicherheitsverletzungen schnell eindämmen, wichtige Geschäftsabläufe wiederherstellen und Ausfallzeiten während eines Cybervorfalls minimieren können.

Die **Cohesity Clean Room-Lösung** unterstützt diesen modernen Ansatz, um Unternehmen bei der Bekämpfung destruktiver Cyberangriffe zu helfen. Sie lässt sich flexibel an unterschiedliche Bedürfnisse anpassen und trägt zur kontinuierlichen Verbesserung der operativen Cyber-Resilienz bei.

In diesem Whitepaper geben wir Empfehlungen, was Unternehmen beim Aufbau einer robusteren und flexibleren Strategie zur Reaktion auf Vorfälle in ihre Digital Jump Bag aufnehmen sollten.

# Häufig unbehandelte Probleme im Bereich der Cyber-Resilienz

Bei destruktiven Cyberangriffen werden häufig die Sicherheitstools der betroffenen Unternehmen umgangen, wobei EDR/XDR-Funktionen in viele der gängigen RaaS-Plattformen (Ransomware-as-a-Service) integriert sind, die für die große Mehrheit der heutigen Ransomware-Angriffe verantwortlich sind. EDR/XDR-Lösungen befinden sich naturgemäß auf dem Endgerät und sie bieten, sofern sie nicht umgangen werden, einen hervorragenden Einblick in Prozesse, Netzwerkverbindungen und Dateisysteme.

Viele Best Practices für die Vorfallsreaktion empfehlen, die Ausbreitung eines Vorfalls durch Isolation der infizierten Netzwerke und Hosts einzudämmen. Beispiele dafür sind der SANS Institute Six Step Incident Response Lifecycle, der NIST SP800-61 Computer Security Incident Handling Guide oder das RE&CT Framework und MITRE D3FEND. Im Bereich der Endpunktkontrollen bleiben einem Unternehmen bestenfalls die Informationen, die es bereits zur Untersuchung des Vorfalls gesammelt hat.

Da wir es jedoch mit Gegnern zu tun haben, die sich ständig anpassen, wissen wir nicht immer, welche Informationen wir sammeln müssen, um Angriffe im Voraus zu verstehen. Wir können uns von der Tatsache blenden lassen, dass unsere Untersuchungs- und Reaktionsfähigkeit inzwischen zu einer unerreichbaren Insel geworden ist. Ebenso ist ein forensisches Remote-Imaging von Datenträgern auf einem betroffenen Host unmöglich, wenn wir die Verbindung unterbrochen haben.

Neben den Sicherheitstools sind viele weitere Systeme an der Untersuchung und Eindämmung von Vorfällen sowie der Wiederherstellung beteiligt. Diese können von destruktiven Cyberangriffen wie Ransomware und Wipern betroffen sein, werden aber in vielen Business-Impact-Analysen nicht als kritisch angesehen. Ich war an Vorfallsreaktionen beteiligt, bei denen das dafür zuständige Personal nicht in die Gebäude gelangen konnte, weil die physischen Zugangskontrollen beeinträchtigt waren. Zahlreiche Unternehmen waren nicht in der Lage, mit der Presse, den Aufsichts- oder Strafverfolgungsbehörden, den Cyberversicherungen oder betroffenen Personen zu kommunizieren, da ihre Voice-over-IP- und E-Mail-Server betroffen waren. Viele von Unternehmen durchgeführte Tabletop-Übungen für Ransomware erfassen diese Auswirkungen, die durch die gezielten Methoden des Gegners entstehen, nicht ausreichend. Schließlich wollen Angreifer, dass Unternehmen Schwierigkeiten haben, auf Vorfälle zu reagieren und sich davon zu erholen.

Angesichts der Tatsache, dass RaaS-Plattformen innerhalb von nur fünf Tagen Exploits für kürzlich gepatchte Schwachstellen einschleusen, müssen wir diese in den Systemen identifizieren und sie patchen, bevor wir die Systeme wieder in Betrieb nehmen. Andernfalls wird derselbe Angreifer oder ein anderer, der dieselbe RaaS-Plattform nutzt, erneut eindringen.

Wir müssen auch den ursprünglichen Zugriffsvektor identifizieren, um das erste betroffene System (den so genannten „Patient Zero“) zu ermitteln, und uns dann weiter vorarbeiten. Es gilt zu verstehen, wie der Angreifer die Persistenz aufrechterhält, Privilegien ausweitet und andere Artefakte des Angriffs findet, damit eine Wiederherstellung in einem sicheren Zustand erfolgen kann. Reaktionsteams müssen auch die Art der Daten einordnen, die möglicherweise kompromittiert wurden, um die gesetzlichen Meldepflichten zu erfüllen.

Die Analyse verschlüsselter Systeme reicht nicht aus. In der Regel setzen Ransomware-Banden Verschlüsselungsprogramme ganz am Ende ihres Angriffszyklus ein. Oft ist das in den letzten Minuten oder Stunden eines Angriffs, der in unserer Infrastruktur bereits Hunderte von Tagen gedauert haben kann. Eine Verschlüsselung ist sehr auffällig. Sie löst wahrscheinlich

Sicherheitskontrollen aus und wird von Benutzern bemerkt. Zu diesem Zeitpunkt ist es dann aber bereits zu spät. Da schnell vorgegangen werden muss, sind Verschlüsselungsprogramme oft nicht auf Integrität ausgelegt. Dies führt zu großen Datenverlusten für diejenigen, die Geld für die Entschlüsselung zahlen. Wenn sich Unternehmen bei der Untersuchung auf verschlüsselte Systeme beschränken, ohne zu ermitteln, wie der Angreifer ins Netzwerk gelangt ist und dort verbleibt, ist der Weg in die Katastrophe vorprogrammiert.

Unternehmen mit solch einem Ansatz müssen oft Dutzende Wiederherstellungen durchführen und infizieren sich immer wieder. Dieser Teufelskreis kann nur durch die ordnungsgemäße Untersuchung von Vorfällen und die Nutzung der gewonnenen Erkenntnisse zur Beseitigung der Bedrohungen durchbrochen werden.

**Stellen Sie sich einmal folgende Fragen: Wie hätte das Ergebnis Ihrer letzten Tabletop-Übung ausgesehen, wenn Sie zu deren Beginn keine Telefone oder E-Mails gehabt hätten, aus Ihren Gebäuden ausgesperrt gewesen wären und nicht auf Identitäts- und Zugangsmanagementsysteme hätten zugreifen können?**

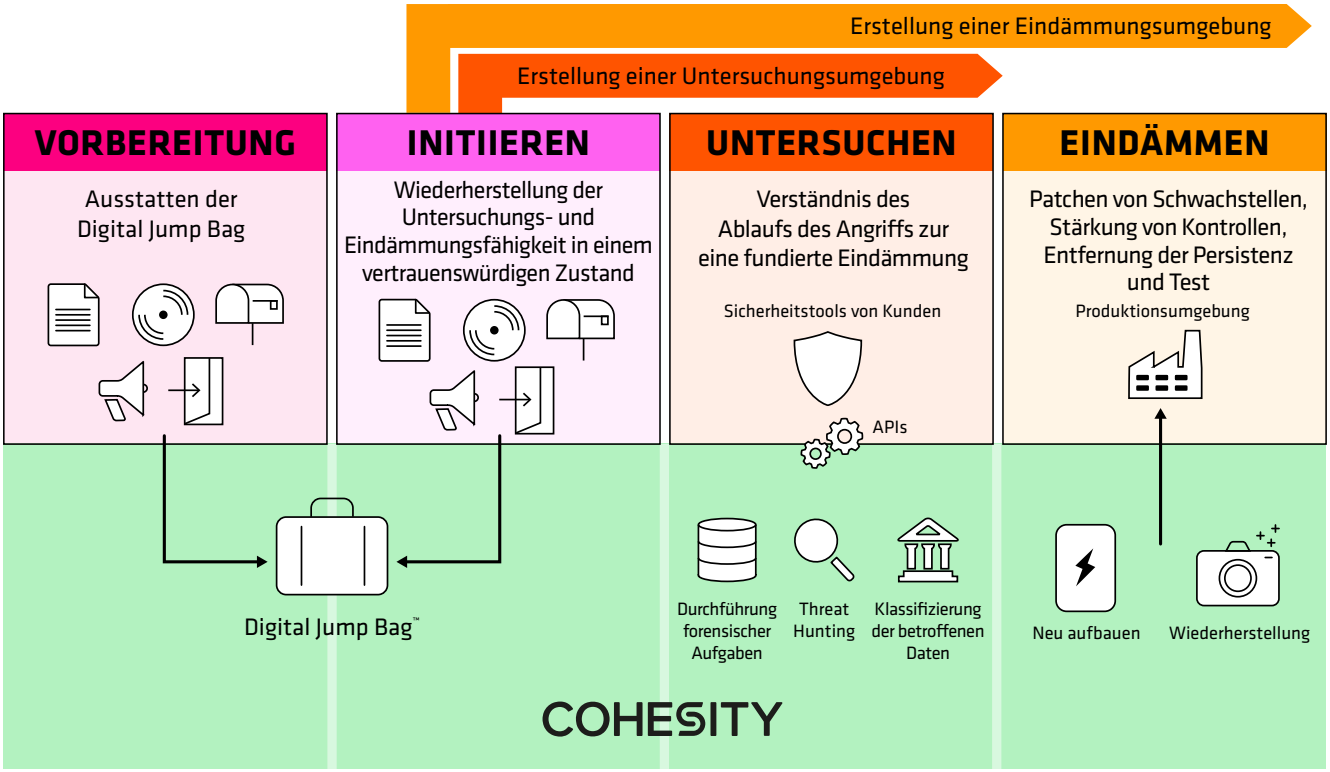
# Zusammenspiel von Digital Jump Bag und Cohesity Clean Room

Die Digital Jump Bag bildet die Grundlage für die gesamte Cohesity Clean Room-Lösung. Sie unterstützt die kritischen Phasen der Vorfallsreaktion und Wiederherstellung, damit Unternehmen saubere Daten in die Produktion zurückbringen können (siehe unten).

Lassen Sie und die einzelnen Phasen etwas näher ansehen.

## Vorbereiten

In dieser Phase wählen wir aus, was in die Digital Jump Bag kommt, z. B. Netzwerk- oder Hypervisor-Konfigurationen, die mehrere voneinander abhängige Systeme unterstützen, die in der Eindämmungsumgebung wiederhergestellt werden. Im Abschnitt „Mögliche Komponenten Ihrer Digital Jump Bag“ finden Sie Anregungen für die nachfolgenden Phasen.



## Initiieren

In dieser Phase stellen wir die MVRC wieder her. Dabei werden die für die Kommunikation, Zusammenarbeit und Untersuchung von Vorfällen erforderlichen Tools aus der Digital Jump Bag in einen vertrauenswürdigen Zustand innerhalb der isolierten Clean-Room-Umgebung zurückversetzt. Mit der Digital Jump Bag werden auch die Umgebungen für die Untersuchung und Eindämmung geschaffen.

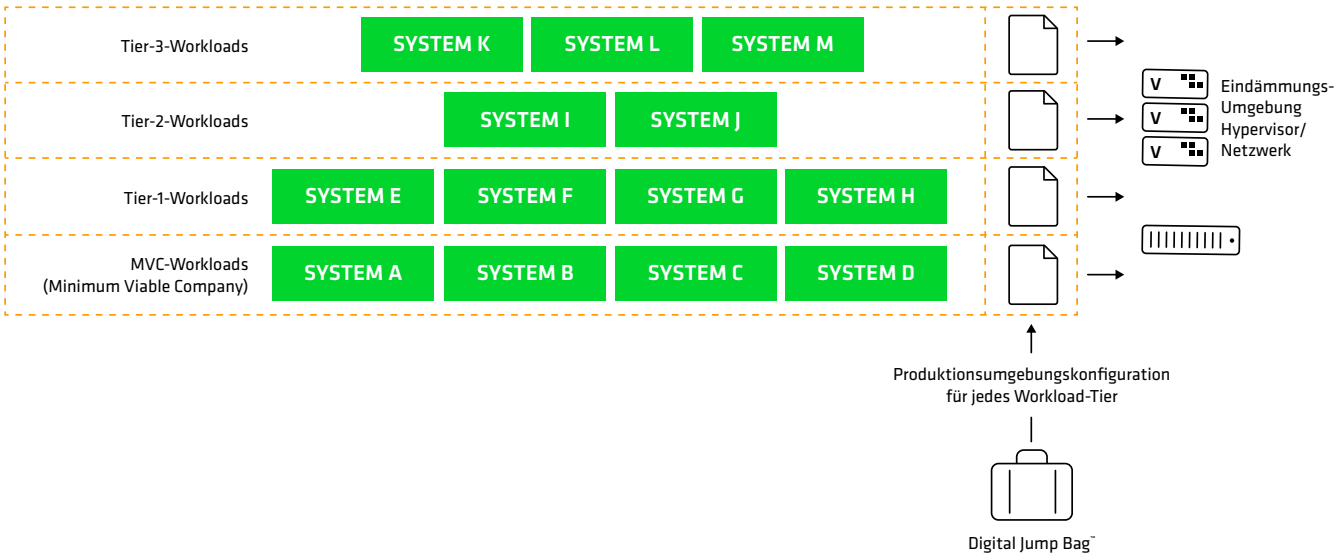
## Untersuchen

Das SecOps-Team nutzt die vertrauenswürdigen Sicherheitstools im isolierten Clean Room zusammen mit den nativen Funktionen von Cohesity für Datenklassifizierung, Threat Hunting und Dateisystemforensik, um den gesamten Ablauf eines Vorfalls von Anfang bis Ende zu verstehen. Da die Sicherheitstools innerhalb des Reinraums vertrauenswürdig sind und die Sicherheitsfunktionen von Cohesity nicht den Defense-Evasion-Methoden unterliegen, die gegen Endpunktkontrollen eingesetzt werden, können die Herausforderungen der Umgehung und Isolation aufgrund der Abriegelung überwunden werden. Die Data Security Alliance von Cohesity bietet eine Vielzahl an Sicherheitstools von Anbietern, die in meinen Security Operations Centres vorhanden und für die Arbeit mit Lösungen von Cohesity vorkonfiguriert sind.

## Eindämmen

Die IT-Abteilung nutzt die Erkenntnisse, die das Security Operations-Team über den Vorfall gewonnen hat, um die Systeme entweder wiederherzustellen und zu bereinigen oder sie in einen vertrauenswürdigen Zustand zurückzuversetzen. Die Untersuchungsphase beinhaltet keine vollständige Wiederherstellung von Systemen mit gegenseitigen Abhängigkeiten, in der Eindämmungsphase ist dies jedoch der Fall.

Kunden verwenden ihre Entwicklungsumgebungen häufig als Eindämmungsumgebung für die Dauer der Wiederherstellung nach einem Vorfall. Voneinander abhängige Systeme werden in der Eindämmungsumgebung mit Netzwerkkonfigurationen bereitgestellt, die den Produktionsumgebungen entsprechen. Diese Netzwerk- oder Hypervisor-Konfigurationen werden für jedes Tier voneinander abhängiger Systeme in der Digital Jump Bag gespeichert. Dies wird hier unten dargestellt.



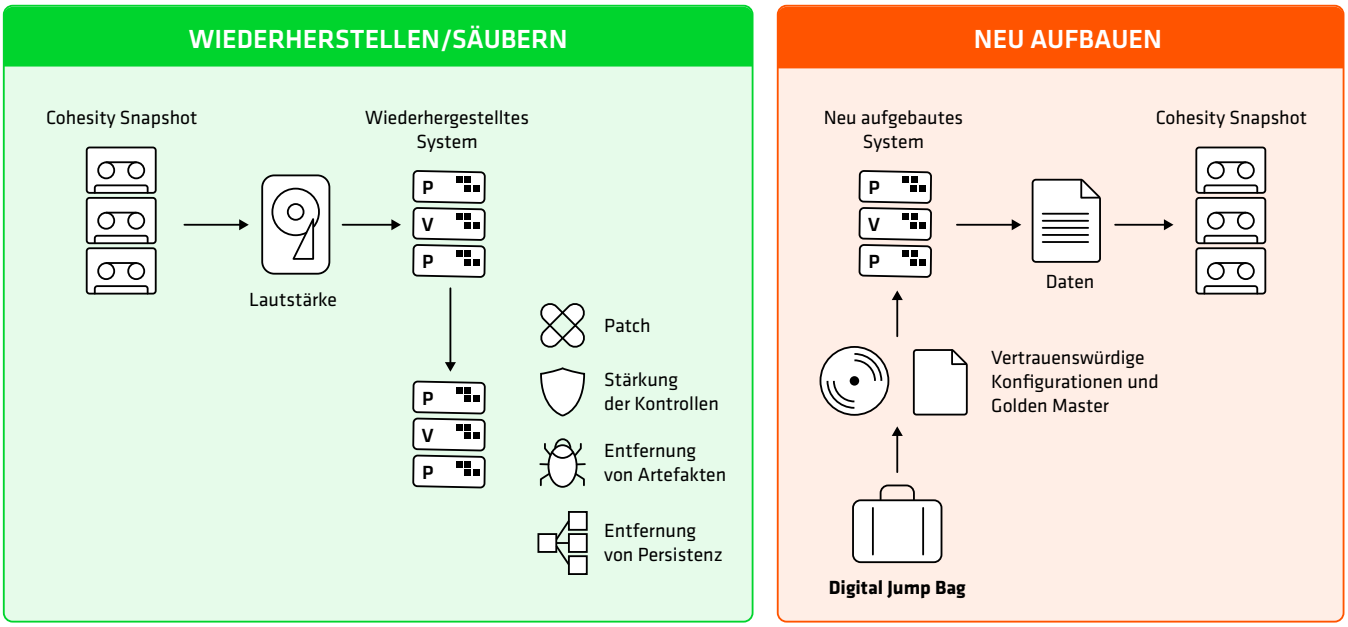

*Anpassung des Cohesity Clean Room an die Best Practices zur Vorfallsreaktion*

Mit der Cohesity Clean Room-Lösung können die Strategien „Wiederherstellen und bereinigen“ oder „In einen vertrauenswürdigen Zustand zurückversetzen“ universell angewandt oder während eines Vorfalls für jedes einzelne System ausgewählt werden, je nach Aufwand für die Behebung und des verbleibenden Risikos der Bedrohungen. Hier finden Sie eine kurze Beschreibung der beiden Optionen:

- **Wiederherstellen und bereinigen**: Die Systeme werden aus ihrem Snapshot wiederhergestellt und die vom SecOps-Team in der Untersuchungsphase beschriebenen Eindämmungsmaßnahmen werden durchgeführt. Da Daten in der Regel nicht als Träger schädlicher Payloads verwendet werden, kann die Datenwiederherstellung oft parallel zur Wiederherstellung des Systems erfolgen, was die letztendlich benötigte Zeit weiter verkürzt.
- **In einen vertrauenswürdigen Zustand zurückversetzen**: Die Digital Jump Bag enthält bekannte Konfigurationen, Installationsskripte und Golden Master Install Images. Nach dem Neuaufbau werden die Daten aus Snapshots in den neu aufgebauten Systemen wiederhergestellt.

Im Abschnitt **Verwendung der Jump Bag zur Wiederherstellung der Minimum Viable Response Capability** finden Sie einen genauen Vergleich der beiden Ansätze.

**Damit Unternehmen ein effektives und angemessenes Modell der geteilten Verantwortung für Cyber-Resilienz schaffen können, werden zwei Dinge benötigt: eine Umgebung, die den Untersuchungsanforderungen des SecOps-Teams gerecht wird, und eine Umgebung, die es dem IT-Team ermöglicht, durch die Umsetzung von Eindämmungsmaßnahmen eine sichere Recovery zu gewährleisten. Dieser Ansatz beschleunigt eine sichere Wiederherstellung, indem die Ressourcen von IT und SecOps optimal genutzt werden können.**



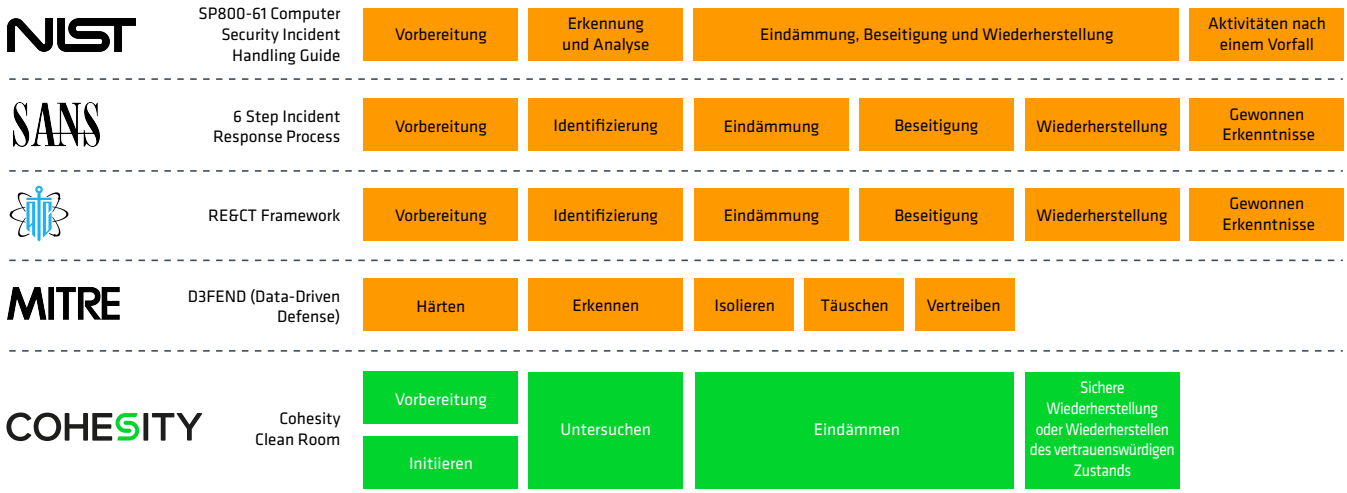

*Der Cohesity Clean Room bietet Kunden die Möglichkeit, Workloads wiederherzustellen und zu bereinigen oder Systeme schnell in einen vertrauenswürdigen Zustand zurückzuversetzen.*

Sobald die Systeme neu aufgebaut oder wiederhergestellt wurden, können Funktions- und Leistungstests in diesem Tier von Workloads durchgeführt werden. Dabei wird zunächst ein Snapshot erstellt, anschließend wird der gesamte Workload mit gegenseitiger Abhängigkeit in der Produktionsumgebung wiederhergestellt. Dies geschieht in der Gewissheit, dass der gesamte Umfang des Vorfalls untersucht, die Bedrohungen entschärft und die Leistung und Funktionalität wiederhergestellt wurden.

Diese Testfälle können in der Digital Jump Bag für jedes Recovery Tier von voneinander abhängigen Workloads gespeichert werden. Sollte bei der Untersuchung und Eindämmung etwas übersehen worden sein, muss nicht wieder von vorne begonnen werden, da der am Ende der Eindämmungsphase erstellte Snapshot als Grundlage für weitere Untersuchungen und Eindämmungen verwendet werden kann.

# Anpassung des Cohesity Clean Room an die Best Practices zur Vorfallsreaktion

Die Cohesity Digital Jump Bag und die Minimum Viable Response Capability entsprechen den Best Practices zur Reaktion auf Cybervorfälle, die im SANS Institute Six-Step Incident Response Lifecycle, NIST SP800-61 Computer Security Incident Handling Guide, RE&CT Framework und MITRE D3FEND beschrieben sind. Mit diesem Ansatz können Unternehmen, die diese Methoden bereits anwenden, die Cohesity Clean Room-Lösung problemlos in ihren bestehenden Workflow integrieren. Kunden, die ihre Reaktions- und Wiederherstellungsfähigkeit bei Vorfällen verbessern möchten, können die Cohesity Clean Room-Lösung übernehmen, um diese Best Practices zu nutzen.




*Anpassung des Cohesity Clean Room an die Best Practices zur Vorfallsreaktion*

# Zusammenführung von Sicherheit und IT-Betrieb für mehr Cyber-Resilienz

Cyber-Resilienz ist ein Teamsport: Sie kann weder vom IT- noch vom SecOps-Team im Alleingang erreicht werden. Beide Teams müssen über integrierte Prozesse und komplementäre Tools verfügen. Ebenso wenig kann ein einzelner Hersteller Cyber-Resilienz bieten. Die Cohesity Clean Room-Lösung ist so konzipiert, dass das SecOps-Team die Untersuchungsumgebung und das IT-Team die Eindämmungsumgebung übernimmt und nutzt. Diese Aufteilung und Zuständigkeiten zwischen den Teams tragen dazu bei, ein klares Modell der geteilten Verantwortung zu gewährleisten und keine Maßnahmen zu vergessen. Es besteht die Möglichkeit, bereits behobene Snapshots iterativ wieder in die Untersuchungsphase zurückzuversetzen, wenn ein Aspekt des Angriffs bei der anfänglichen Untersuchung und Eindämmung übersehen wurde. So muss nicht von vorn begonnen werden, was die Untersuchungszeit und die endgültige Wiederherstellung verkürzt.

Sobald SecOps die Untersuchung eines Workloads in der Untersuchungsumgebung abgeschlossen hat, kann diese an die IT und die Eindämmungsumgebung übergeben werden, um sie neu aufzubauen, wiederherzustellen und zu bereinigen. Dies gewährleistet die effizienteste Nutzung der IT- und SecOps-Ressourcen.

## Schneller reagieren, smarter wiederherstellen: Cohesity CERT (Cyber Event Response Team)

Vielen Unternehmen fehlt es an Fachwissen oder Ressourcen für eine wirksame Reaktion auf Cybervorfälle. Um die negativen Auswirkungen zu minimieren, haben wir unsere erstklassige Datensicherheitslösung um einen speziellen CERT-Service erweitert.

Cohesity CERT ermöglicht eine schnelle Recovery nach Cyberangriffen unter Anleitung von Experten. Das Team stellt sicher, dass Ihre Daten wiederhergestellt werden und Ihr Unternehmen den Betrieb mit minimaler Ausfallzeit wieder aufnehmen kann.


Cohesity CERT steht allen Kunden von Cohesity als Teil ihres bestehenden Abonnements zur Verfügung.

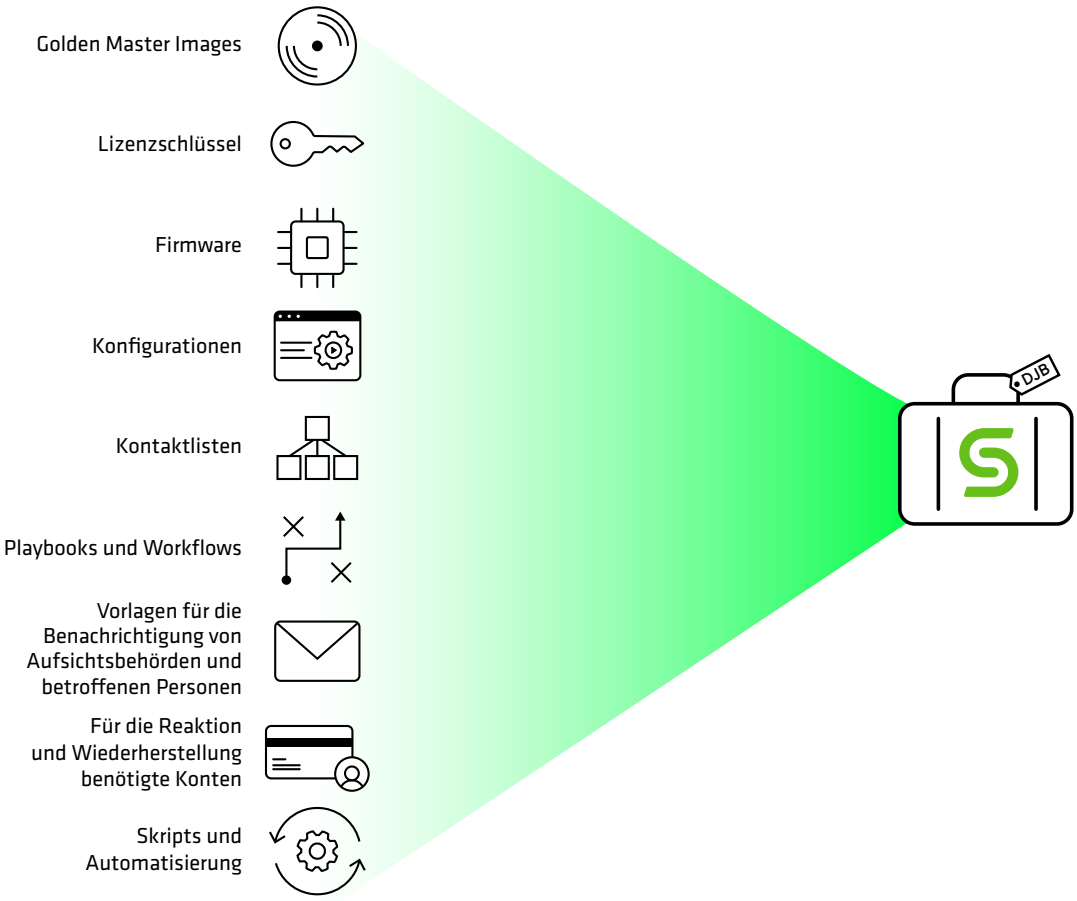
# Mögliche Komponenten Ihrer Digital Jump Bag

Der Inhalt Ihrer Digital Jump Bag hängt von Ihren individuellen Triage-, Untersuchungs- und Eindämmungsprozessen und den dafür verwendeten Tools ab.

Im Allgemeinen sehen wir die folgenden Elemente in den Digital Jump Bags unserer Kunden:

## Dokumentation

- Eine Kontaktliste mit internen und externen Stakeholdern wie Strafverfolgungsbehörden, Zentren für Informationsaustausch und -analyse, Versicherungsgesellschaften, Notfalleinsatzkräften und Aufsichtsbehörden
- Netzwerkdiagramme
- Möglicherweise ein Backup oder Dump der Konfigurationsmanagement-Datenbank des Unternehmens
- Eine Kopie des Runbooks/Workflows für die Reaktion auf Vorfälle
- Verträge und Richtliniendokumente über die Beauftragung von Incident-Response-Services und Cyberversicherungen
- Benutzerhandbücher für Anwendungen und Tools



## Ressourcen für die Initiierungsphase: Zusammenarbeit und Kommunikation

- Bei einem Vorfall ist es sehr wahrscheinlich, dass mit internen Stakeholdern und externen Drittparteien wie Strafverfolgungsbehörden, Informationsaustausch- und Analysezentren, Versicherungsgesellschaften, Ansprechpartnern für Vorfälle, Aufsichtsbehörden, der Presse und betroffenen Personen kommuniziert werden muss. Dafür sollte eine Digital Jump Bag Folgendes enthalten:
  - Als funktionierend bekannte Router- und Switch-Firmware und -Konfigurationen, um eine sichere Verbindung zu ermöglichen. Alternativ kann das Unternehmen auch vertrauenswürdige Stand-by-Geräte unterhalten.
  - Firewall-Software und -Konfigurationen zur Beschränkung der Ein- und Ausgänge auf die für die Reaktion und Wiederherstellung erforderlichen Ressourcen (einschließlich des Zugangs zu Cohesity Helios).
  - Die grundlegenden Installationsmedien und Lizenzschlüssel für das Betriebssystem, die als Grundlage für die Wiederherstellung anderer Systeme, einschließlich in den Untersuchung- und Eindämmungsumgebungen, verwendet werden.
  - Automatisierungs- und Orchestrierungsskripte, die von Windows Answerfiles für unbeaufsichtigte Installationen über Ansible Playbooks bis hin zu Terraform Infrastructure-as-a-Code reichen können.
  - VoIP-Serversoftware und -konfiguration (Voice-over-IP Management). Hier gilt es zu beachten, dass dies nicht die gesamte VoIP-Produktionsumgebung ist. Sie enthält nur Leitungen, die sich auf Reaktion und Wiederherstellung beziehen. Die VoIP-Produktionskonfiguration wird nach der Untersuchung und Behebung aller gefundenen Bedrohungen wieder online gestellt.
  - E-Mail-Serversoftware und -konfiguration. Wie beim VoIP-Server handelt es sich hierbei nicht um eine Funktionalität für die Produktion. Es ermöglicht lediglich die Kommunikation zwischen den an der Reaktion und Wiederherstellung beteiligten Ressourcen.
  - Andere vom Unternehmen verwendete Tools für die Zusammenarbeit, z. B. Ticketing, Conferencing-Tools usw., können in die Jump Bag aufgenommen werden.
  - Vorlagen für die Benachrichtigung von Aufsichtsbehörden und betroffenen Personen.

# Ressourcen für die Untersuchungsumgebung

Das SecOps-Team ist in der Regel für die in der Untersuchungsphase verwendete Umgebung verantwortlich. Der Schwerpunkt liegt auf dem Verständnis des gesamten Angriffszeitraums, damit das Unternehmen fundierte Entscheidungen über die Wiederherstellung der Produktionsfähigkeit und den Schutz vor Neuinfektionen und erneuten Angriffen treffen kann. Die Systeme werden innerhalb des Unternehmens untersucht. Dabei kommt eine Mischung aus den nativen SecOps-Funktionen von Cohesity für Aufgaben wie Datenklassifizierung, Threat Hunting und Dateisystem-Forensik sowie andere mit Cohesity kompatible Sicherheitstools zum Einsatz. Die Bedrohungssuche mit Cohesity wird nicht durch die Eindämmung eines Vorfalls beeinträchtigt. Sie ist passiv, d. h., sie ist nicht für Angreifer sichtbar und unterliegt nicht den Umgehungsmethoden, die bei Endpunktsicherheitslösungen üblich sind. In der Untersuchungsphase werden die Systeme gewöhnlich isoliert betrachtet.

- Installationsmedien und -konfigurationen für Sicherheitssoftware. Dies ermöglicht die Neuinstallation von Tools in einem vertrauenswürdigen Zustand innerhalb des isolierten Clean Rooms und stellt sicher, dass die Tools und Reaktionen nicht umgangen oder gestört werden.
- Die Sicherheitstools können im Clean Room wieder in einen vertrauenswürdigen Zustand versetzt werden. Diese Tools hängen stark von den Vorlieben Ihres Incident Response Teams ab, enthalten jedoch in der Regel zumindest einige der folgenden Elemente:
  - Endpoint Detection & Response (EDR) und Extended Detection & Response (XDR) Tools wie Palo Alto Networks, Cisco XDR und CrowdStrike
  - Tools für die forensische Erfassung und Analyse wie

Dissect, Flare, Redline, Sleuth Kit, Autopsy, CyLR und Unix-like Artifacts Collector (UAC)

- Tools für Hinweise auf Kompromittierungen und das Teilen von Beweisen wie Cortex, Kuiper und MISP
- Analysetools für Ereignisprotokolle wie Event Log Explorer, Event Log Observer, Hayabusa, LogonTracer oder Windows Event Log Analyzer (WELA)
- Schwachstellen-Scanner wie Qualys, Rapid7 neXpose, Tenable Nessus oder OpenVAS
- Paketerfassungs- und Analysesoftware wie Wireshark
- Netflow/SFlow-Analysetools
- Speichererfassungs- und -analysetools wie Volatility, Memoryze, Orochi, Rekall und WindowsSCOPE
- Sandboxes, Malware-Reverse-Engineering- und Analysetools wie Cuckoo, CAPA, CAPE, Ghidra, Joe Sandbox, Mastiff, Radare 2 und Valkyrie Comodo
- Forensische Verlaufstools für Webbrowser wie Internet History Forensics
- Viele der oben genannten Tools sind in Sicherheitssoftware-Distributionen wie Kali Linux und SANS Institute SIFT Workstation enthalten. Diese können in der Digital Jump Bag aufbewahrt werden, anstatt jedes einzelne Tool installieren zu müssen.

# Ressourcen für die Eindämmungsumgebung

Das IT-Team ist normalerweise für die Eindämmungsumgebung verantwortlich. In der Eindämmungsumgebung werden Betriebssysteme und Anwendungen von vertrauenswürdigen Installationsmedien und Konfigurationen, die in der Digital Jump Bag enthalten sind, neu erstellt oder von Backup-Snapshots wiederhergestellt und mithilfe der Informationen, die durch die Sicherheitsmaßnahmen während der Untersuchungsphase gewonnen wurden, bereinigt. Es werden Abhilfemaßnahmen ergriffen, um Bedrohungen zu einzudämmen. Dazu gehören das Patchen von Schwachstellen, die Anwendung fehlender Kontrollen oder Regeln zur Verhinderung oder Erkennung künftiger Angriffe der gleichen Art und die Entfernung von Persistenzmechanismen, schädlichen Accounts oder anderen Angriffsartefakten. In der Eindämmungsumgebung werden voneinander abhängige Systeme, die ein Produkt oder einen Dienst bereitstellen sollen, zusammengeführt und neu aufgebaut oder bereinigt, bis schließlich Leistung und Funktionalität durch die Wiederherstellung von Daten aus einem Backup-Snapshot getestet werden können. Zu diesem Zeitpunkt wird ein Snapshot erstellt und die Systeme werden in der Produktionsumgebung wiederhergestellt.

- Wenn das Unternehmen einen Neuaufbau statt einer Wiederherstellung und Bereinigung anstrebt, enthält die Digital Jump Bag die erforderlichen Installationsmedien und Konfigurationen für den Application Stack.
- Die Netzwerk- oder Hypervisor-Konfiguration, die für den aktuell abhängigen Workload erforderlich ist. Dadurch kann die Eindämmungsumgebung die Produktionsumgebung nachbilden, in der der Workload letztendlich wiederhergestellt wird.
- Testfälle für Workloads.

# Verwendung der Jump Bag zur Wiederherstellung der Minimum Viable Response Capability

Bei der Einrichtung der Systeme innerhalb der MVRC mit der Digital Jump Bag haben Kunden zwei Möglichkeiten: Wiederherstellung eines vorgefertigten Systems oder Neuaufbau des Systems aus vertrauenswürdigen Quellen.

- **Bewahrung der Minimum Viable Response Capability:** Erstellen Sie die für die MVRC benötigten Systeme und führen Sie ein Backup auf Datenträgerebene durch. Speichern Sie diese in der Digital Jump Bag. Wenn ein Cyber-Sicherheitsvorfall vermutet wird, der sich auf Systeme auswirkt, die für die Reaktion und Wiederherstellung benötigt werden, oder wenn der Verdacht einer Umgehung der Sicherheitstools besteht, werden die Snapshots wiederhergestellt, um die Minimum Viable Response Capability zu etablieren.
- **Neuaufbau auf Grundlage von Ressourcen in der Digital Jump Bag**: Dabei werden vertrauenswürdige Konfigurationen und Golden Master Images für die Systeme, die für die MVRC benötigt werden, in der Digital Jump Bag aufbewahrt. Im Falle eines Cyber-Sicherheitsvorfalls, der sich auf Systeme auswirkt, die für die Reaktion und Wiederherstellung benötigt werden, oder bei dem der Verdacht besteht, dass Sicherheitstool umgangen werden, wird die Digital Jump Bag eingesetzt. Diese Systeme werden mithilfe von Skripten oder Orchestrierungstools neu aufgebaut.

Jede Strategie hat ihre Vor- und Nachteile, die in der nachfolgenden Tabelle aufgeführt werden:

| **Bewahrung einer Minimum Viable Response Capability, Erstellung eines MVRC-Backups und Wiederherstellung des Snapshots nach einem Vorfall** | |
|---|---|
| **Vorteile** | **Nachteile** |
| Schneller Zugriff auf funktionierende Systeme während der Reaktion | Patches und Aktualisierungen erfordern weitere Schritte (Rebuild, Update/Patch, Backup), für die kontinuierlich Ressourcen benötigt werden. Bei diesen Schritten können Fehler auftreten, die sich negativ auf die Reaktion und Wiederherstellung auswirken. Angenommen, ein Unternehmen war nicht in der Lage, seine IT-Systeme zu schützen, und wurde angegriffen. Welche Garantie gibt es dafür, dass die bereits erstellten und gesicherten MVRC-Systeme nicht die gleichen Probleme haben werden? |
| Fähigkeit zur Wiederherstellung von ausschließlich erforderlichen Komponenten | Beansprucht exponentiell mehr Speicherplatz in der Digital Jump Bag und verursacht Lizenzkosten |
| | Muss möglicherweise während der Reaktion aktualisiert und gepatcht werden, was zu Verzögerungen führen kann |
| | Kann Abhängigkeiten der Infrastruktur erzeugen |
| **Voraussetzungen** | |
| Erfolgreicher Test des Aufbaus der MVRC aus der Digital Jump Bag | |
| Erstellung eines MVRC-Backups, Aktivierung der gesetzlichen Aufbewahrungspflichten für juristische Zwecke, Replizierung und Offsite-Archivierung | |

| Neuaufbau der Minimum Viable Response Capability aus vertrauenswürdigen Quellen nach einem Vorfall | |
|---|---|
| **Vorteile** | **Nachteile** |
| Relativ einfach zu pflegende Quellen, da neue Versionen von Betriebssystemen, Anwendungen oder Konfigurationen einfach in die Digital Jump Bag exportiert werden | Ein Neuaufbau der Infrastruktur ist sehr zeitintensiv |
| Sehr portabel dank Replikation und Archivierung | |
| Bessere Anpassungsfähigkeit an Hardware- und Plattformänderungen | |
| Der Backup-Footprint in der Digital Jump Bag ist deutlich geringer (d. h. ein Windows Server 2025 Image ist ca. 3,6 GB groß und kann von verschiedenen Systemen gemeinsam genutzt werden, während jeder Server mit Minimum Viable Response Capability, der dieses Image verwendet, ca. 35 GB benötigen würde). | |
| **Voraussetzungen** | |
| Festlegung eines Verfahrens für das Erstellen und Aktualisieren der Digital Jump Bag | |
| Einübung verschiedener Content-Nutzungsszenarien | |
| Bereithaltung der benötigten Hardware oder Festlegung eines Prozesses, um die vorhandene Hardware sicher zu entfernen | |

# Fazit

Angesichts immer raffinierterer und destruktiverer Cyberangriffe müssen Unternehmen von der reaktiven Wiederherstellung zur strategischen Resilienz übergehen. Dafür müssen sie eine umfassende Digital Jump Bag in ihre Strategie zur Vorfallsreaktion integrieren, um schneller auf Cyberangriffe reagieren zu können. Eine gut vorbereitete Digital Jump Bag ermöglicht die MVRC und dient als Grundlage für einen Clean Room. Sie stattet SecOps-Teams mit den nötigen Tools, Prozessen und Dokumenten aus, die für die Untersuchung von Vorfällen, die Eindämmung von Bedrohungen und die Wiederherstellung des Betriebs mit minimalen Ausfallzeiten erforderlich sind.

Der Cohesity Clean Room bietet eine vertrauenswürdige Umgebung, die die Vorfallsreaktion beschleunigt und Untersuchungen unterstützt, während das Risiko von Folgeangriffen minimiert wird.

Dank des modularen Aufbaus schafft Cohesity umgehend eine isolierte Umgebung, die Reaktion und Wiederherstellung unterstützt und es den Teams ermöglicht, bei der Bedrohungsbehebung schneller zusammenzuarbeiten.

# Über Cohesity

**Cohesity** ist führend im Bereich KI-gestützte Datensicherheit. Mehr als 12.000 Unternehmenskunden, darunter über 85 der Fortune 100 und fast 70 % der Global 500, verlassen sich auf Cohesity, um ihre Resilienz zu stärken und gleichzeitig Gen-AI-Einblicke in ihre riesigen Datenbestände zu bekommen. Die Lösungen des Unternehmens, das aus dem Zusammenschluss von Cohesity und dem Datenschutzgeschäft von Veritas hervorgegangen ist, sichern und schützen Daten On-Premises, in der Cloud und am Edge. Cohesity hat seinen Hauptsitz in San Jose, Kalifornien, betreibt Standorte auf der ganzen Welt und wird durch NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud und andere unterstützt. Folgen Sie Cohesity auf **LinkedIn**, **X** und **Facebook**, um weitere Informationen zu erhalten.

Auf **www.cohesity.com** erfahren Sie, wie Cohesity Ihren Weg zu moderner Datensicherheit beschleunigen kann.

# Empfohlene Lektüre

Die folgenden Whitepapers, Leitfäden und Blogs können ebenfalls hilfreich für Sie sein.

- Aufbau von Cyber-Resilienz in einer Zeit destruktiver Cyberangriffe
- Moderne Topologien für Datensicherheit und -management: Ein Leitfaden für IT-Führungskräfte
- Introducing the Cohesity clean room design
- A field guide for AI-powered data security: How to deliver breakthrough business outcomes
- An executive's guide to modern data security and management

## Erfahren Sie mehr bei Cohesity



COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000056-002-DE 4-2025