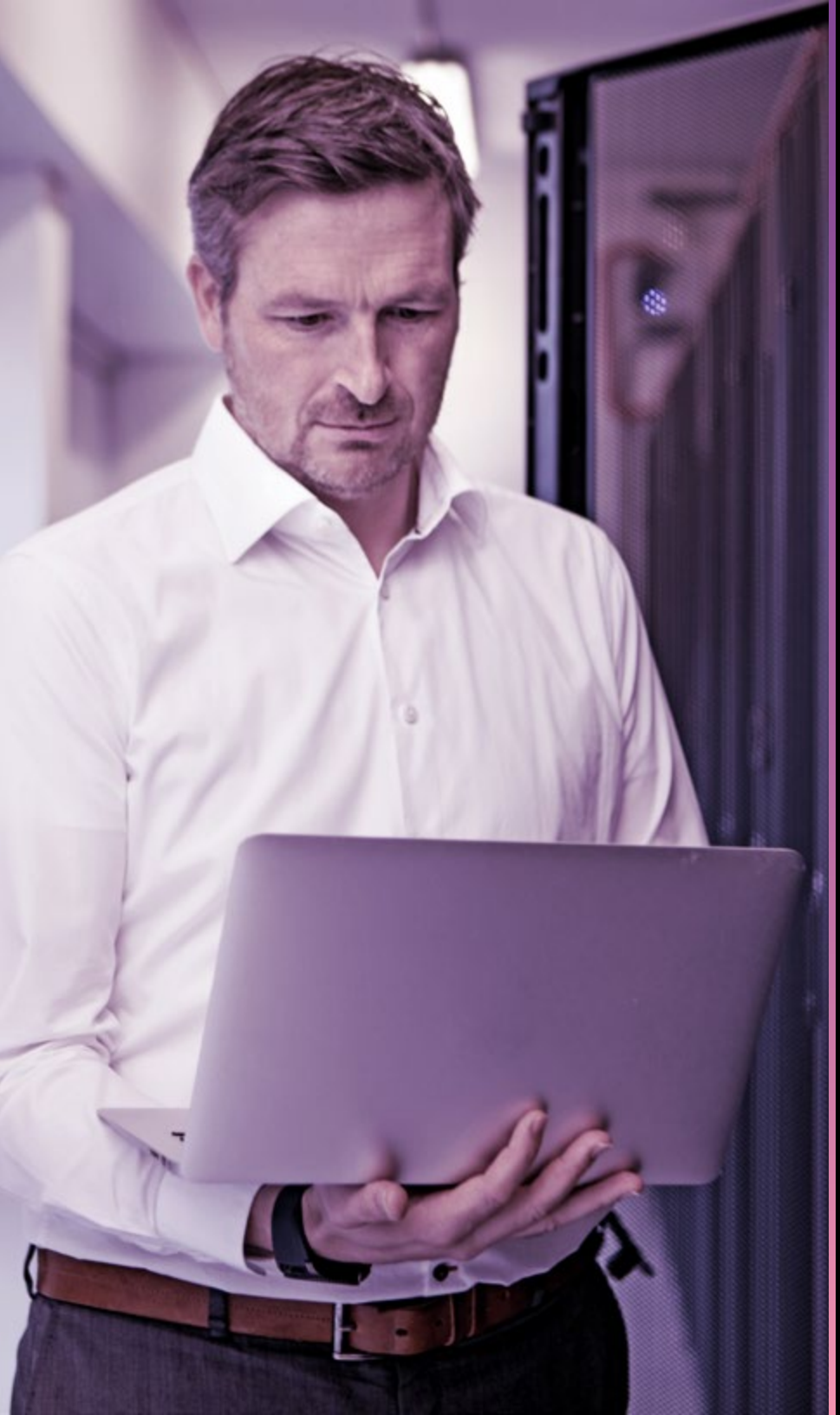


Commvault

eBOOK

Leitfaden zur Cyber-Bereitschaft und Recovery-Fähigkeit

ERFAHREN SIE, WIE SICH IHR UNTERNEHMEN FÜR DIE HERAUSFORDERUNGEN RÜSTEN KANN, DIE DAMIT EINHERGEHEN.

INHALT

Die Sicherheits-, IT- und Operations-Teams vieler Unternehmen unterscheiden nicht zwischen Cyber Recovery und Disaster Recovery. Während des Cyber-Recovery-Prozesses nach aktuellen Vorfällen haben sich jedoch im Vergleich zu einer herkömmlichen Disaster Recovery einige spezielle Schwierigkeiten ergeben. Die unterschiedlichen Taktiken, Techniken und Vorgehensweisen der Angreifer haben gezeigt, dass bei Cyber- Recovery-Plänen folgendes berücksichtigt werden muss:

- **Unvorhersehbarkeit und sich ständig weiterentwickelnde Bedrohungen:** Im Gegensatz zu Naturkatastrophen sind Cyberangriffe arglistig und Angreifer bemühen sich sehr, ihre Handlungen und Bewegungen zu verschleiern. Aus diesem Grund kann es schwierig sein, festzustellen, wann genau der Angriff begonnen hat, welche Systeme betroffen sind oder wie hoch der Schaden ist.
- **Sekundäre Angriffe:** In einigen Fällen haben Angreifer während des Wiederherstellungsprozesses Code zum Starten sekundärer Angriffe oder zum Erstellen dauerhafter Hintertüren eingeschleust, die bei einer Wiederherstellungsaktion automatisch geöffnet werden.
- **Kompromittierte Backups:** Oft haben es Angreifer gezielt auf Backups abgesehen, um sicherzustellen, dass Wiederherstellungsversuche wirkungslos bleiben. Das steigert die Notwendigkeit, ein Lösegeld zu zahlen, um Betriebsdaten wiederherzustellen.
- **Zeitdruck:** Unternehmen stehen oft unter einem enormen Druck, nach einem Cyberangriff schnell wieder online zu gehen. Ausfallzeiten kosten ein Unternehmen nachweislich bis zu 12 Millionen US-Dollar pro Tag1. Und zu allem Übel kann eine rasche Wiederherstellung dazu führen, dass bereits kompromittierte Systeme wiederhergestellt werden und den Schaden noch verstärken.
- **Ressourcenabfluss:** Cyber Recovery kann ein ressourcenintensiver Prozess sein, der die Expertise von IT-, Sicherheits- sowie Rechtsabteilungen und manchmal sogar der Strafverfolgungsbehörden erfordert. Dies kann ohnehin knappe Ressourcen in einem Unternehmen belasten und Sicherheits- und Operations-Teams von anderen möglichen Cyberbedrohungen ablenken.

Indem Unternehmen ein Verständnis für diese Herausforderungen entwickeln, können sie einige grundlegende Elemente der Disaster Recovery nutzen, um einen Cyber- Recovery-Plan zu erstellen, der diese Schwierigkeiten antizipiert und ihnen hilft, nach einem Angriff schneller wieder auf die Beine zu kommen.

Dieser Leitfaden hilft Ihnen dabei, die Basis dafür zu legen, Ihr Unternehmen cyber-bereit zu machen. Wir geben Ihnen, unter Berücksichtigung einiger der gängigsten Richtlinien, Konzepte, Ideen und Prozesse an die Hand, die Sie für die Entwicklung Ihres eigenen Plans benötigen.

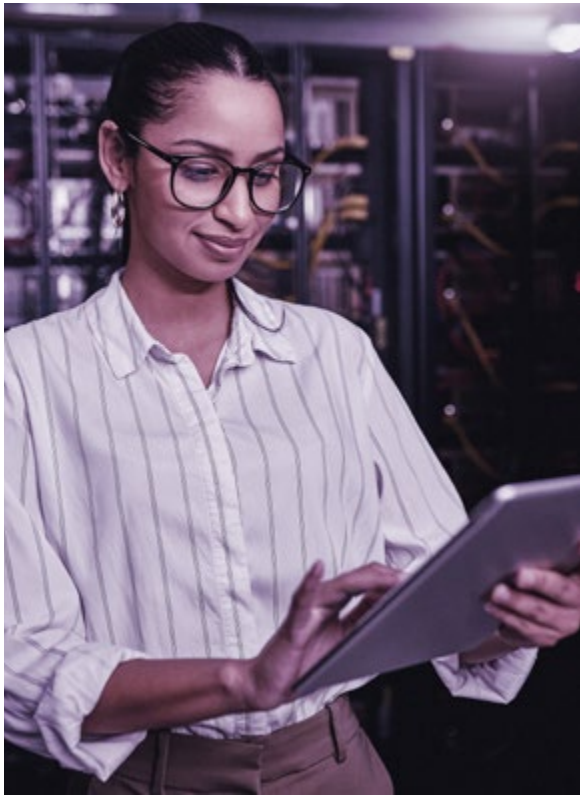
[1] SolarWinds: Pingdom Team, Average Cost of Downtime per Industry, Jan 9, 2023.

DAS NIST CYBER SECURITY FRAMEWORK ALS WEGWEISER

Das Cyber Security Framework des National Institute of Standards and Technology (NIST CSF) ist seit langem ein Wegweiser für Sicherheitsteams zur Entwicklung und Ausrichtung ihrer Sicherheitsprogramme und zum Schutz vor neuen und sich weiterentwickelnden Cyberbedrohungen.

Anhand der Kategorien Identifizieren, Erkennen, Schützen, Reagieren und Wiederherstellen, wird erklärt, wie man jeden Bereich für eine erfolgreiche Cyber Recovery weiter ausbaut.

1. **Identifizieren.** Analysieren Sie Ihre Daten, auch sensible/kritische Daten, und finden Sie heraus, wo sie sich befinden und wer dafür verantwortlich ist.
2. **Erkennen.** Nutzen Sie Sicherheitsfunktionen und -technologien, um zu überwachen, was mit Ihrer Umgebung und Ihren Daten geschieht.
3. **Schützen.** Implementieren Sie Mechanismen, um Ihre sensiblen oder kritischen Daten zu sichern und sie für die Wiederherstellung vorzubereiten.
4. **Reagieren.** Entfernen Sie den Angreifer aus Ihrer Umgebung, und entfernen oder schützen Sie den Angriffsvektor, über den Ihr Unternehmen infiltriert wurde. Wenn sich das nicht schnell erledigen lässt, bereiten Sie eine neue, intakte und nicht kompromittierte Arbeitsumgebung für die Wiederherstellung vor, die zur Fortsetzung des Geschäftsbetriebs verwendet werden kann.
5. **Wiederherstellen** Erstellen Sie eine nicht kompromittierte Version Ihrer gesamten Umgebung, einschließlich aller Daten, Anwendungen und der Infrastruktur.



VORBEREITUNG AUF DAS UNVORSEHBARE

Cyber-Vorfälle sind naturgemäß oft versteckte Angriffe, die Tage oder Wochen hinter den Kulissen vorbereitet werden, bevor es zu verheerenden Schäden kommt. Studien haben gezeigt, dass die durchschnittliche Verweildauer – die Zeit, die ein Angreifer während eines Angriffs tatsächlich innerhalb eines Unternehmens verbringt – 204 Tage oder fast 7 Monate beträgt[1].

> **204 Tage oder fast 7 Monate**
> **beträgt die durchschnittliche Verweildauer – die Zeit, die ein Angreifer während eines Angriffs tatsächlich innerhalb eines Unternehmens verbringt.**

Unternehmen führen seit langem Penetrationstests durch, um Bereiche mit schwacher Abwehr zu identifizieren, sowie Tabletop-Übungen, um die Disaster Recovery-Fähigkeit zu testen. Doch angesichts der Vielfalt an Cyberangriffen, ist in der Praxis zu berücksichtigt, dass in einem echten Cyber-Recovery-Szenario nahezu nichts als vertrauenswürdig gilt. Backups müssen auf permanente Malware gescannt werden. Die Infrastruktur muss bereinigt werden, um sicherzustellen, dass nur autorisierte Benutzer anwesend sind. Und Anwendungen und Daten müssen auf Backdoors überprüft und in einen Zustand vor dem Angriff (oder vor der Infiltration) versetzt werden.

[1] 2023 IBM Ponemon Cost of a Data Breach Report, p14
Cost of a Data Breach Report 2023.pdf

REDUNDANZ KANN SEHR KOSTSPIELIG SEIN

Zusätzliche Darksites zum Schaffen von Redundanz sind eine wertvolle Methode zum Schutz Ihrer Daten, da Sie Ihnen Übungsmöglichkeiten bieten und Sie sich auf Cyberangriffe vorbereiten können. Aber natürlich ist die zusätzliche Infrastruktur mit immensen Kosten verbunden.

Jeder physische Standort erfordert Ausgaben für Planung, Immobilien, Aufbau, Ausstattung, Energiekosten, Steuern, Personal und laufende Wartung. Diese Kosten summieren sich schnell und können sich je nach Größe des Unternehmens auf mehrere zehn oder Hunderte Millionen Dollar pro Jahr belaufen, was für viele Unternehmen nicht leistbar ist und somit nicht in Frage kommt.

BEDARFSGERECHTE CLEANROOM RECOVERY

Mit der Einführung von Commvault® Cloud Cleanroom™ Recovery können Unternehmen die Kosten und die Komplexität für die Verwaltung von Reinräumen vor Ort vermeiden. Der erste und einzige Reinraum zur Cyber Recovery ermöglicht schnelle Tests und Wiederherstellungen in einer sicheren, Cloud-basierten Umgebung.

Cleanroom Recovery ist eine praktische und kostengünstige Lösung, die Tests und Wiederherstellungen für eine größere Anzahl an Unternehmen leichter zugänglich macht. Außerdem lässt sie sich bei Bedarf schnell einrichten und ganz nach Belieben testen, was sehr praktisch ist, wenn Sie Änderungen vornehmen oder verschiedene Szenarien testen möchten.

Sie können Anwendungen und Daten problemlos wiederherstellen und nach einem Ereignis forensische Untersuchungen durchführen. Sie verfügen über eine isolierte Wiederherstellungsumgebung, die im Fall eines Angriffs für Geschäftskontinuität sorgt. Cleanroom Recovery umfasst auch eine Integration mit Microsoft Defender, die die Überprüfung auf Bedrohungen automatisiert, um festzustellen, ob die Daten sauber sind.

WIE CLEANROOM RECOVERY EINE MALWARE-FREIE CLOUD-UMGEBUNG SCHAFFT

Air-Gapping
Isolierte Datenkopien, getrennt von den Quellumgebungen.

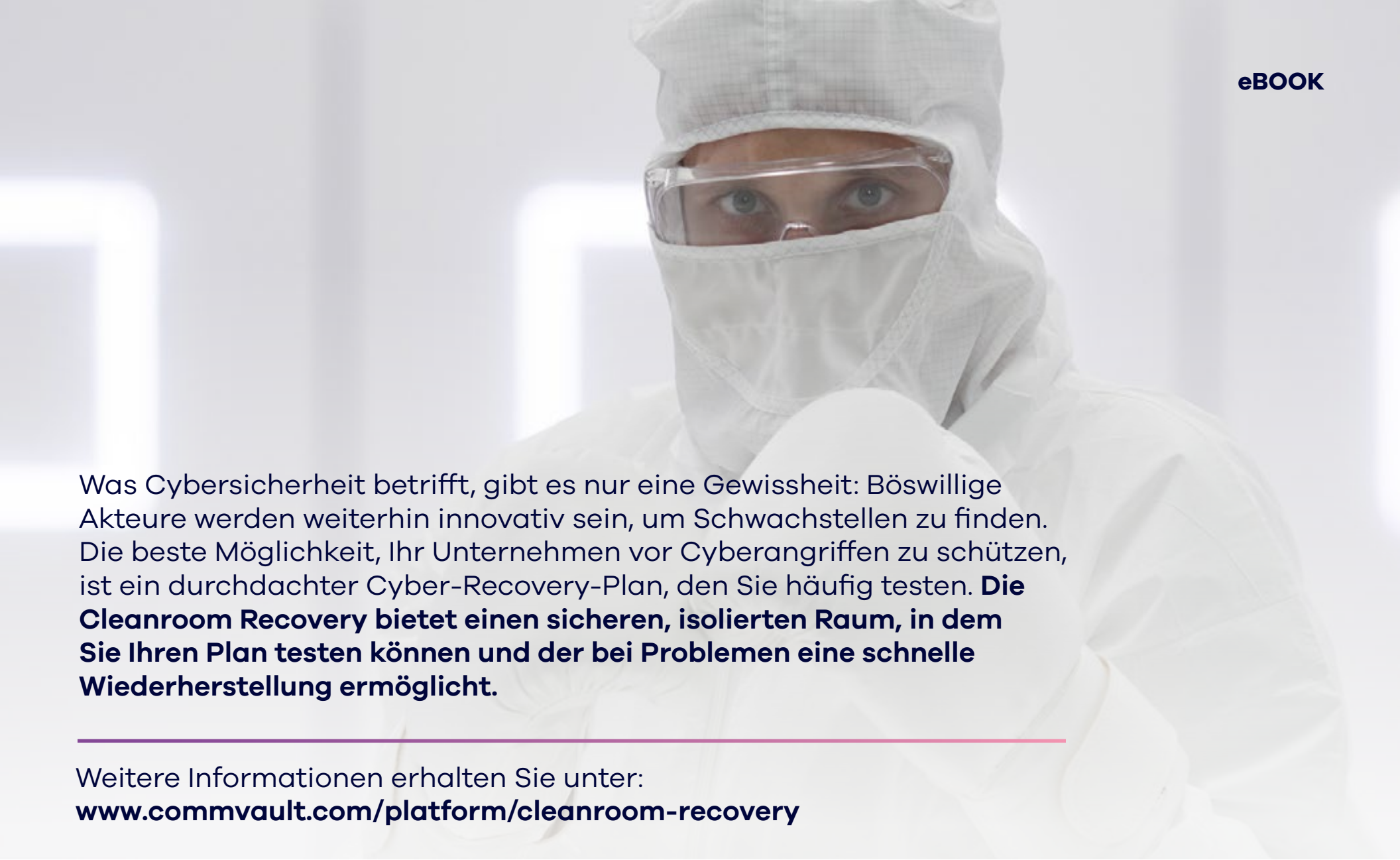
Unveränderliches Design
Backups mit mehrschichtigen, Zero-Trust-Zugriffskontrollen.

Integrierte Automatisierung
Nutzen Sie Automatisierung und Orchestrierung für eine unkomplizierte Implementierung und einfache Abläufe.

Robuster Ransomware-Schutz und End-to-End-Security
Integrierte Anomalie-Erkennung, Reporting und Verschlüsselung von Daten sowohl im Ruhezustand als auch während der Übertragung.

Automatisierte Recovery-Validierung
Datenwiederherstellbarkeit durch orchestrierte Validierung der Anwendungswiederherstellung. recovery validation.

Sichere forensische Analyse
Führen Sie sichere Analysen mit Malware-freier Hardware in isolierten Cloud-Umgebungen durch.



eBOOK

Was Cybersicherheit betrifft, gibt es nur eine Gewissheit: Böswillige Akteure werden weiterhin innovativ sein, um Schwachstellen zu finden. Die beste Möglichkeit, Ihr Unternehmen vor Cyberangriffen zu schützen, ist ein durchdachter Cyber-Recovery-Plan, den Sie häufig testen. **Die Cleanroom Recovery bietet einen sicheren, isolierten Raum, in dem Sie Ihren Plan testen können und der bei Problemen eine schnelle Wiederherstellung ermöglicht.**

Weitere Informationen erhalten Sie unter:
www.commvault.com/platform/cleanroom-recovery

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®