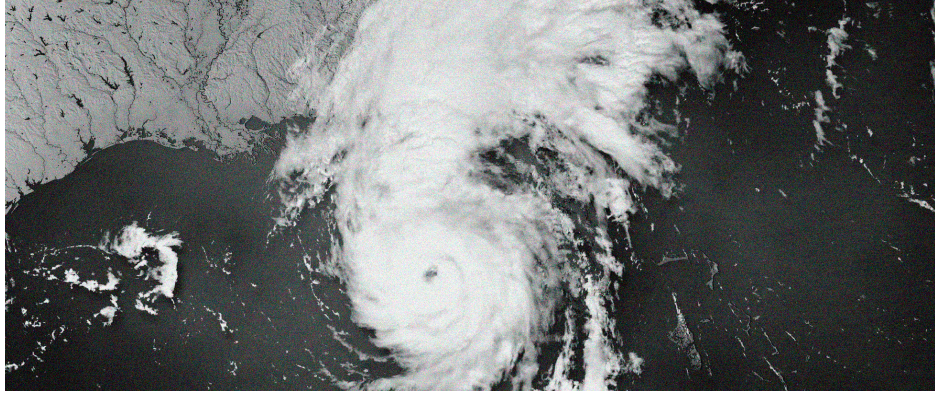
eBOOK

OLTRE IL DISASTER RECOVERY

Perché hai bisogno di una **strategia differente** quando avvengono gli attacchi cyber

Commvault®



Il Tuo Approccio al Recovery → Inizia Qui

Da eventi meteorologici ad attacchi cibernetici maliziosi, non mancano eventi distruttivi che minacciano tutti i giorni le tue operazioni aziendali. I giornali sono pieni di notizie di danni, causati da uragani e da ransomware.

Una buona pratica di business continuity aziendale include necessariamente avere un piano per riprendersi velocemente in caso di un incidente. Questo piano dovrebbe concentrarsi sulla protezione di dipendenti, clienti e dati, riducendo al contempo i danni a beni, finanze e reputazione. In questo modo, l'organizzazione può minimizzare gli impatti negativi e tornare a operare efficientemente nel più breve tempo possibile. Ma rimanere resilienti di fronte a queste minacce richiede costante vigilanza. Il recupero da disastri e il recupero cibernetico non sono la stessa cosa, quindi è cruciale comprendere le differenze. Leggi il seguito per scoprire perché è necessario avere entrambi i piani di recovery – e per capire come la minimum viability (operatività minima) nella tua organizzazione rappresenti un aspetto chiave del recupero cibernetico.

Con una preparazione accurata, una strategia di test comprensiva condotta regolarmente e soluzioni per un rapido recupero e ricostruzione di tutte le tue applicazioni e dati – sarai in grado di superare le sfide del recovery.

Perché Hai Bisogno di un Piano di Disaster Recovery

Hai bisogno di un piano di disaster recovery per gestire eventi prevedibili come guasti hardware o disastri naturali come incendi e inondazioni. In generale, questi incidenti non sono intenzionali e non mirano attivamente ai tuoi dati.

Il recupero da disastri di solito segue un piano predefinito con passaggi stabiliti per ripristinare rapidamente i sistemi. Il ripristino da backup ti aiuta a tornare online anche se alcuni dati vengono persi. Questo processo mira a mantenere la continuità aziendale, minimizzare l'impatto a lungo termine e proteggere i dati critici.

Perché Hai Bisogno di un Piano di

Cyber Recovery

Commvault®

Di contro, il recupero cibernetico affronta attacchi maliziosi come il ransomware o le violazioni dei dati, dove gli attaccanti cercano attivamente di danneggiare i tuoi sistemi e corrompere i tuoi dati. Questo potrebbe riguardare un sottoinsieme di dati o l'intera infrastruttura, inclusi i siti di failover per il recupero da disastri.

Gli attacchi cibernetici spesso richiedono investigazioni e attività di remediation prima del recupero, il che può allungare i tempi di ripristino.

Per evitare possibili attacchi e assicurarsi che non vi siano exploit residui, è fondamentale esaminare attentamente ogni componente dell'ambiente, compresi hardware, dati e backup, prima di procedere al ripristino. Questo perché i criminali informatici potrebbero aver celato malware o manipolato i file di backup. L'obiettivo è limitare i danni, prevenire la perdita di dati e mantenere un alto livello di sicurezza.

Riparti con la Minimum Viability (operatività minima)

Quando un attacco cibernetico mette la tua organizzazione offline, la pressione per ripristinare le operazioni il più rapidamente possibile è altissima, al fine di minimizzare i danni finanziari e alla reputazione. Pertanto, un aspetto importante del recupero cibernetico è definire l'operatività minima necessaria alla tua azienda – cioè, l'insieme minimo di sistemi, dati e processi che devi ripristinare per rimanere operativo dopo una interruzione.

01 Identificare gli asset critici

Include **sistemi** (infrastruttura, applicazioni mission-critical, strumenti di comunicazione); **dati** (operativi, di conformità, di backup); e **processi** (operazioni aziendali, IT e sicurezza, coinvolgimento del cliente).

02 Valutare l'impatto di un'interruzione

Quanto costa alla tua organizzazione non essere operativi? Comprendere gli effetti dei tempi di inattività su ciascuno degli asset critici è fondamentale per il processo decisionale e per aiutare a dare priorità al loro ripristino.

03 Creare un piano

Successivamente, è necessario creare un piano per ripristinare gli asset più critici in caso di interruzione - e testare, testare, testare. Assicurarsi che i dipendenti siano formati sul loro ruolo nel ripristino.

04 Concentrarsi su un ripristino pulito e validato

È importante sottolineare che è necessario validare il ripristino di una copia pulita dei dati; avere copie isolate (air-gapped) aiuterà a consentire un ripristino più rapido di quei dati. E si dovrebbero condurre analisi forensi in una sala di ripristino isolata per trovare la causa principale e aiutare a prevenire futuri attacchi.

Conoscere l'impatto di un'interruzione:

$4.88M
Il costo medio di una violazione[1]

$14,056
Il costo medio di ogni minuto di downtime[2]

24 GIORNI
Il downtime medio dopo un attacco di ransomware[3]

1 Cost of a Data Breach Report 2024, IBM
2 IT outages: 2024 costs and containment, Enterprise Management Associates
3 Statista

PRONTI AL CYBER RECOVERY

SCENARI

Il ripristino da cyberattacchi generalmente determina un insieme diverso di esigenze rispetto ai piani di ripristino da disastro/continuità aziendale. Queste strategie possono essere combinate per convergere risorse e processi.

ELEMENTI	RIPRISTINO DA DISASTRO / CONTINUITÀ AZIENDALE	RIPRISTINO CYBER
COMPROMESSO	Perdita totale delle operazioni del sito	Dati, reti, sicurezza
RIPRISTINO	Ripristino/backup RTO, ricostruzione	Ripristino selettivo per la riparazione
RISORSE	Disponibilità totale dello stack	Validazione, ripristino, ricostruzione
PIANIFICAZIONE	Persistente	Elastico

ORGANIZZAZIONE

Il ripristino cyber richiede una responsabilità condivisa e collaborativa tra tutti i dipartimenti dell'organizzazione (persone, processi).

L'integrazione e l'automazione delle notifiche, delle azioni informate e dei flussi di lavoro tra i team possono accelerare i risultati.

CAPACITÀ

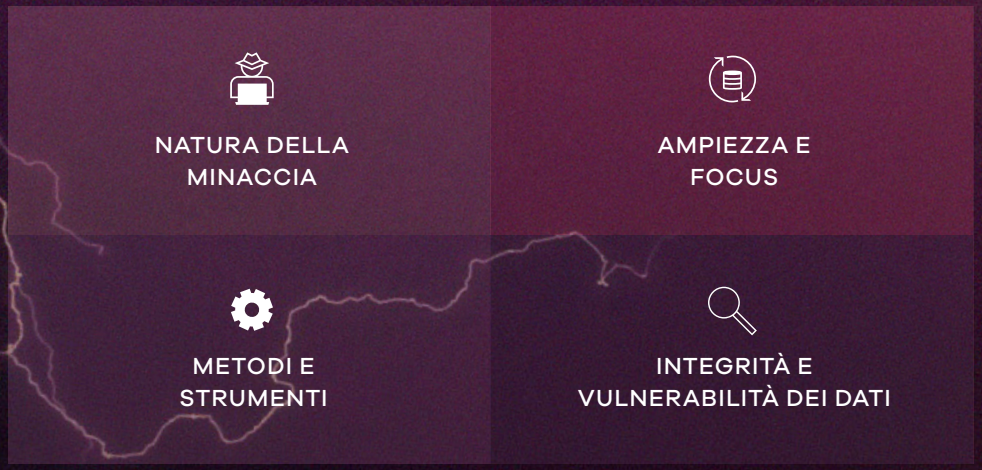
I requisiti di recupero cyber dipendono dagli obiettivi dell'organizzazione.

- Backup sicuri, isolati e immutabili
- Rilevamento precoce di schemi sospetti
- Analisi cyber e sanificazione dei dati
- Validazione del recupero automatizzata
- Recupero rapido e pianificato

DISASTER RECOVERY I TEST NON SONO SUFFICIENTI

Il test di ripristino da disastro è importante, ma il ripristino da cyberattacchi è molto più completo. Sebbene entrambi mirino a ripristinare la funzionalità operativa dopo le interruzioni, le differenze fondamentali richiedono risposte distinte. I piani tradizionali di ripristino da disastro faticano a gestire efficacemente le minacce complesse e sfaccettate che i cyberattacchi presentano.

Ecco perché:



Pertanto, sebbene i piani di ripristino da disastro forniscano una base preziosa per la risposta agli incidenti, farvi affidamento in caso di cyberattacco può essere pericoloso. Un piano di ripristino da cyberattacchi dedicato, supportato da strumenti specializzati, personale e test frequenti, è essenziale per mitigare i rischi e le complessità specifici di questi attacchi maliziosi.

CYBER RECOVERY

I TEST SONO FONDAMENTALI

Il test di ripristino da cyberattacchi è una vera e propria esercitazione (o test operativo) per ripristinare un'applicazione e i suoi dati da un backup. Questo è il tipo di processo di ripristino che avverrà in caso di incidente cyber, ed è il processo che NIST raccomanda.[1] I test di ripristino da disastro e quelli di ripristino da cyberattacchi hanno entrambi il loro ruolo, ma il ripristino da cyberattacchi è molto più completo.

Il test di ripristino da cyberattacchi permette di garantire la resilienza dei tuoi sistemi e dati, nonché la continuità aziendale. Il ripristino di applicazioni e dati critici è un processo complesso e pieno di sfide. Testare il ripristino da cyberattacchi aiuta a scoprire errori e a risolverli quando le posta in gioco è bassa.

I test daranno ai team coinvolti la pratica e la fiducia necessarie per ripristinare le applicazioni e i dati critici quando si verifica un incidente cyber.

Infatti, NIST raccomanda che "i backup dei dati siano eseguiti, protetti, mantenuti e testati," perché "è meglio identificare un problema inaspettato durante i test che durante un vero evento cyber."[1] Tuttavia, la realtà è che poche organizzazioni testano in modo completo, frequente e con successo.

NUMERI CRITICI

194 GIORNI
Tempo medio di permanenza di un attaccante in un'azienda[2]

Gli attaccanti iniziano a muoversi lateralmente nei

48 MINUTI
dall'attacco[3]

82% delle aziende
che pagano il riscatto non recuperano tutti i loro dati[4]

1 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf
2 https://www.ibm.com/reports/data-breach
3 https://go.crowdstrike.com/2025-global-threat-report.html
4 https://www.hiscoxgroup.com/news/blog/hiscox-cyber-readiness-report-2024

Come Commvault Aiuta

CON COMMVAULT, PUOI:

- Mettere in sicurezza i dati critici con copie isolate (air-gapped)
- Testare frequentemente per confermare che il tuo piano funzioni e che i tuoi dipendenti sappiano cosa fare
- Verificare che stai ripristinando una copia pulita dei tuoi dati
- Condurre analisi forensi in un ambiente di ripristino isolato e sicuro

COMMVAULT SOLUTIONS:

Commvault® Cloud for AD: Enterprise Edition

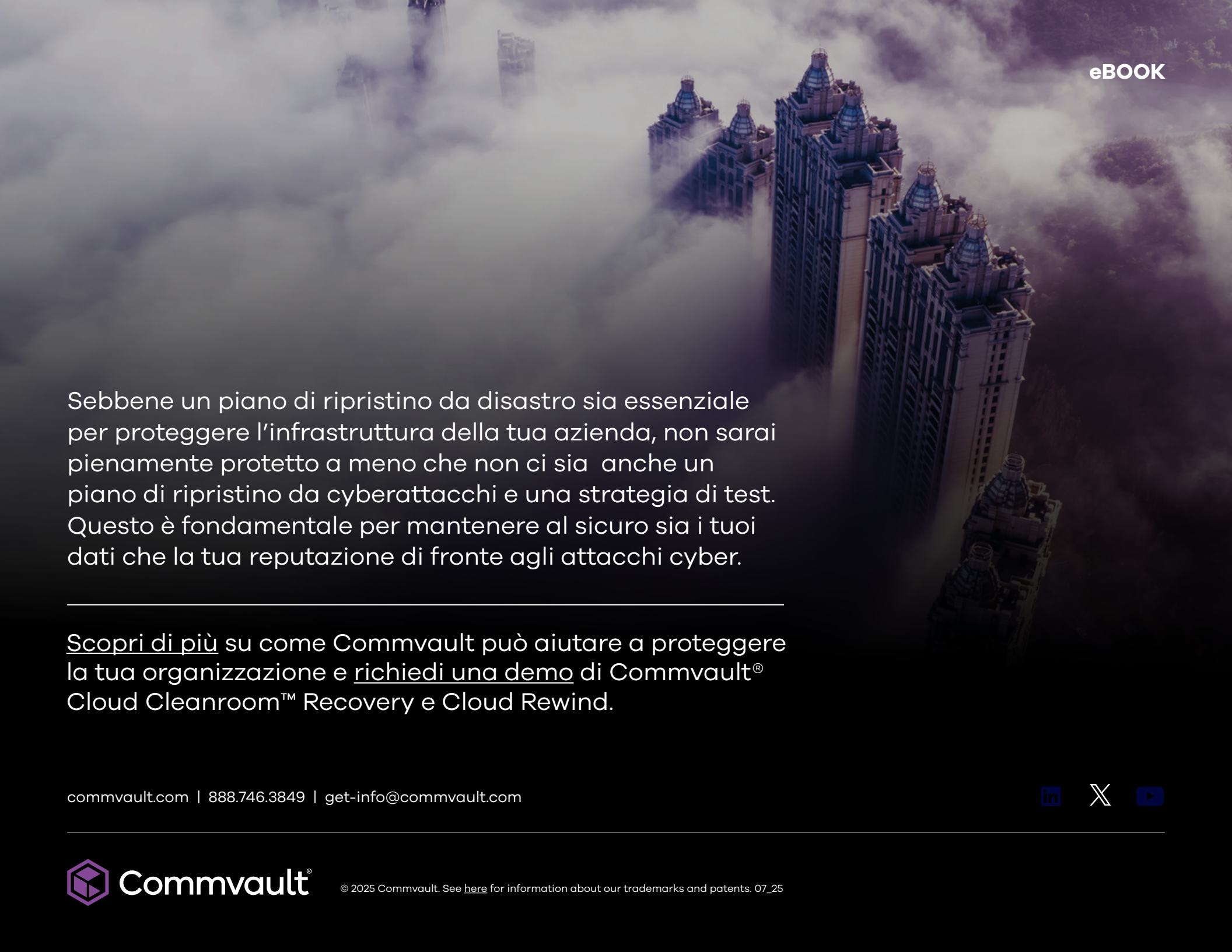
La gestione delle identità e degli accessi è fondamentale per ripristinare le tue operazioni dopo un attacco. Commvault Cloud for Active Directory Enterprise Edition ti permette di proteggere e accelerare il ripristino dei dati AD in caso di corruzione, cancellazione accidentale e attacchi ransomware, abilitando il ripristino automatico a livello di foresta.

Commvault® Cloud Cleanroom™ Recovery

Fornisce un ambiente di ripristino sicuro e isolato su richiesta. Questa soluzione è molto di più di uno spazio sicuro. Consente alle organizzazioni di testare l'efficacia dei piani di ripristino da cyberattacchi, di fornire un ripristino pulito e rapido delle tue applicazioni e dati, e di condurre analisi forensi sicure. Con archiviazione immutabile isolata, automazione integrata e ridimensionamento del ripristino potenziato dall'IA, Cleanroom Recovery ti aiuta a mantenere le operazioni aziendali attive, anche di fronte a minacce cyber sofisticate.

Commvault® Cloud Rewind™

Va oltre i tradizionali backup e ripristino da disastro – permettendoti di scoprire, proteggere, ripristinare e ricostruire continuamente per stabilire la resilienza cyber e mantenere le operazioni aziendali attive. Puoi tornare a un punto specifico nel tempo e ricostruire rapidamente applicazioni cloud dinamiche e distribuite da interruzioni e attacchi ransomware. Con una macchina temporale cloud puoi ripristinare rapidamente i tuoi dati, applicazioni e configurazioni.



eBOOK

Sebbene un piano di ripristino da disastro sia essenziale per proteggere l'infrastruttura della tua azienda, non sarai pienamente protetto a meno che non ci sia anche un piano di ripristino da cyberattacchi e una strategia di test. Questo è fondamentale per mantenere al sicuro sia i tuoi dati che la tua reputazione di fronte agli attacchi cyber.

Scopri di più su come Commvault può aiutare a proteggere la tua organizzazione e richiedi una demo di Commvault® Cloud Cleanroom™ Recovery e Cloud Rewind.

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

Commvault®