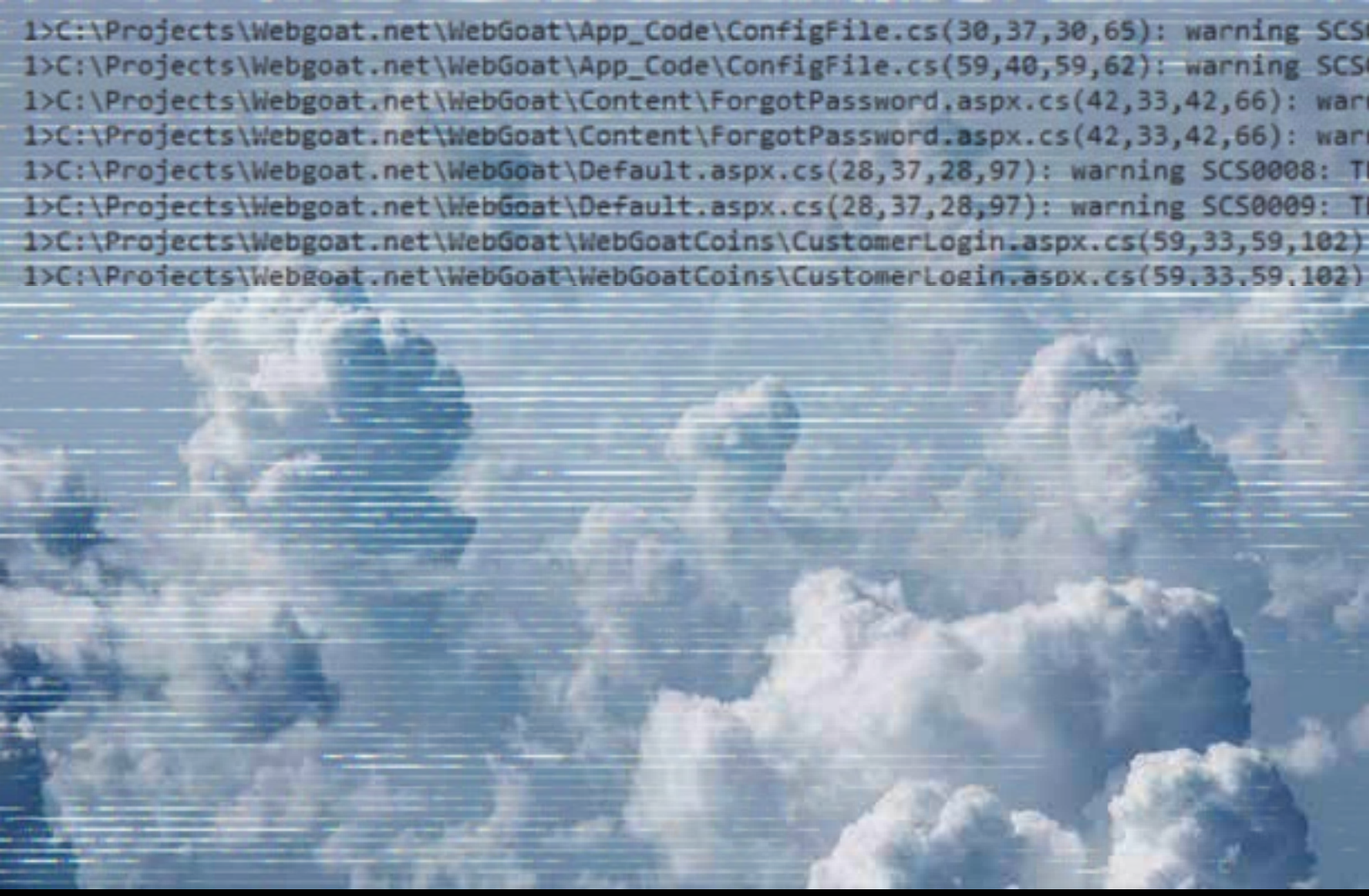

Guida

Commvault®

La soluzione per il ransomware che piacerà al tuo CISO

IL NUOVO PANORAMA DELLE MINACCE

In un panorama di minacce in continua evoluzione, gli attacchi informatici sono diventati più diffusi e costosi che mai. Per i responsabili della sicurezza e della tecnologia, lo sviluppo di una solida strategia per la resilienza e il recovery non è solo essenziale, ma è una questione urgente. Le violazioni **sono** una realtà. Disponi dei mezzi e delle risorse per rilevare una violazione e di un piano di risposta?

Potresti affidarti a soluzioni tradizionali per la sicurezza dei dati che utilizzano un mosaico di soluzioni di sicurezza poco integrate. In tal caso, i tuoi team di sicurezza si troveranno in una posizione di svantaggio nel momento in cui cercheranno di comprendere l'intera portata dell'attacco.

Inoltre, la mancanza di collaborazione tra IT e sicurezza durante un incidente farà sì che la tua azienda rimanga ancora più indietro rispetto a un avversario che si muove velocemente.

Il prezzo di un piano di risposta mal implementato è rappresentato da costosi tempi di inattività, sanzioni per la conformità, violazioni della sicurezza e, in definitiva, danni alla reputazione dell'azienda.

$ 365.000

è il costo orario dei tempi di inattività.[1]

IL CAOS RICHIEDE UN APPROCCIO UNIFICATO

Purtroppo, il caos e le ore di lavoro che seguono una violazione della sicurezza possono rendere difficile decidere chi deve rispondere e come. Non c'è tempo per i conflitti interni. I team di sicurezza e IT devono lavorare fianco a fianco, dal punto di vista strategico e tattico. Questa collaborazione è vitale per una gestione del rischio efficiente ed efficace.

Tuttavia, solo il 30% dei team SecOps comprende appieno il ruolo degli ITOps.

e solo il 29% dei team ITOps comprende appieno le SecOps.[2]

La cyber resilience può fungere da ponte tra IT e sicurezza, migliorando il livello di sicurezza generale della tua organizzazione. I responsabili della sicurezza e della tecnologia devono dotare i propri team degli strumenti e delle strategie giuste per ridurre i rischi e proteggere i dati e la reputazione. Questi strumenti devono essere integrati per fornire contesto e una comprensione completa di attacchi, incidenti o violazioni.

61%

dei CISO concorda sul fatto che la propria azienda non è preparata ad affrontare un attacco informatico mirato.[3]

Inizia oggi stesso a costruire un'organizzazione più resiliente dal punto di vista informatico colmando il divario tra ITOps e SecOps. Preparati ad affrontare qualsiasi minaccia, incluso il ransomware, con una soluzione unificata che offre allarmi precoci, disponibilità al recovery continuo e scalabile automaticamente. Adotta un approccio che protegga i dati in tutta l'infrastruttura cloud ibrida e che renda più semplice il ripristino sia nel cloud che negli ambienti on-premise.

Naturalmente, il ransomware è sempre il sintomo di una violazione più ampia, ed è miope affrontare solo il meccanismo di distribuzione del ransomware senza affrontare i problemi sottostanti di messa in sicurezza della violazione e di eliminazione dell'accesso dell'aggressore. Di fatto, l'80% delle aziende che hanno subito un attacco ransomware ha subito un secondo o un terzo attacco. La tua azienda è preparata?

1 Splunk, "**Digital Resilience Pays Off Report**", febbraio 2023.
2 IDC, "**The Cyber-Resilient Organization: Maximum Preparedness with Bulletproof Recovery**", settembre 2023.
3 Proofpoint, "**2023 Voice of the CISO Report**", maggio 2023.

SONO TUTTI COINVOLTI

Sebbene l'obiettivo di tutti coloro che sono coinvolti nella cyber resilience sia quello di proteggere l'azienda da eventuali danni, IT e SecOps possono farlo in modi diversi che possono lasciare una potenziale esposizione a minacce esterne. La chiave è stabilire un terreno comune. Ecco alcuni esempi:

1. **Obiettivi condivisi:** i team IT e di sicurezza mirano a proteggere le risorse, i sistemi e i dati dell'organizzazione. Lavorano per mantenere la riservatezza, l'integrità e la disponibilità delle informazioni.

2. **Collaborazione:** i team IT e di sicurezza spesso collaborano strettamente per implementare e mantenere le misure di sicurezza. Lavorano insieme per individuare le vulnerabilità, implementare i controlli di sicurezza e rispondere agli incidenti.

3. **Gestione del rischio:** entrambi i team sono coinvolti nella valutazione e nella gestione dei rischi. I team IT si concentrano sui rischi operativi legati alla disponibilità e alle prestazioni del sistema, mentre i team di sicurezza si concentrano sulla riduzione dei rischi associati ad accessi non autorizzati, violazioni dei dati e altri incidenti di sicurezza.

4. **Conformità:** i team IT e di sicurezza collaborano per garantire la conformità alle normative e agli standard pertinenti. Collaborano per implementare controlli e processi che soddisfino i requisiti legali e di settore.

5. **Risposta rapida in caso di incidenti:** in caso di incidente di sicurezza, i team IT e di sicurezza collaborano per indagare, contenere e risolvere il problema. Collaborano insieme per ridurre al minimo l'impatto e ripristinare le normali operazioni.

6. **Consapevolezza e formazione:** entrambi i team svolgono un ruolo di promozione della consapevolezza della sicurezza e di formazione dei dipendenti. I team IT istruiscono gli utenti su pratiche informatiche sicure, mentre i team di sicurezza forniscono indicazioni per identificare e segnalare potenziali minacce alla sicurezza.

7. **Stress test:** un team che si allena insieme crea legami e ottiene maggiori risultati. Lo stress test dei tuoi piani, delle tue politiche e della tua capacità di interagire individua le aree di potenziale miglioramento. È preferibile che tutto venga organizzato in condizioni ideali, senza lo stress di un attacco.

Nel complesso, la collaborazione e la comunicazione efficace tra i team IT e di sicurezza sono fondamentali per mantenere un'infrastruttura IT sicura e resiliente.

GLI ATTACCHI SONO UNA REALTÀ. ASSICURATI CHE I TUOI TEAM IT E DI SICUREZZA SIANO PRONTI.

I dirigenti IT e della sicurezza necessitano di funzionalità avanzate di sicurezza per affrontare i rischi informatici in modo efficace, ridurre al minimo le minacce e migliorare i risultati di recovery dei dati.

Ricorda, non è una questione del **SE** si verificherà una violazione, ma di **QUANDO** la **RILEVERAI**, di **COSA** hai fatto per prepararti e di **COME** risponderai.

Cominciamo a parlarne

Per stimolare una migliore collaborazione e individuare un terreno comune, ecco alcune domande da considerare:

- Quanto è preparata la tua organizzazione a rispondere alle minacce informatiche e a garantire la continuità aziendale in caso di incidente?
- Quali sono le risorse critiche e quali sono i tempi di inattività aziendale previsti?
- Quali sono le ipotesi sulla disponibilità: l'esercizio ha preso in considerazione l'interruzione di AD, l'interruzione di Vmware, l'interruzione dell'area cloud?
- I tuoi team comprendono i propri ruoli e le proprie responsabilità durante un attacco?
- Chi ha accesso e visibilità su cosa? Hai meccanismi di conversazione fuori banda?
- Come proteggere e gestire i dati quando si adottano ambienti cloud ibridi?
- Quanto costerebbe all'azienda e alla sua reputazione una violazione e un conseguente ransomware?

COMMVAULT CLOUD: CYBER RESILIENCE PER IL MONDO IBRIDO

È inoltre indispensabile disporre della tecnologia giusta per raggiungere questi obiettivi comuni. Commvault Cloud®, basato sull'AI di Metallic, è l'unica piattaforma di cyber resilience progettata per soddisfare le esigenze delle aziende ibride e per dotare i team SecOps e ITOps delle funzionalità di sicurezza e recovery dei dati di cui hanno bisogno di fronte all'evoluzione delle minacce basate sull'intelligenza artificiale.

In un mondo ibrido in continua espansione e ultra complesso, ci sono rischi intrinsechi da risolvere, mitigare e accettare. Riesci a identificare rapidamente le risorse create con poco o nessun preavviso? Sei a conoscenza di software, hardware e servizi esterni che potrebbero esporre i tuoi dati a minacce informatiche? Tutto questo costringe i CISO a fare scelte difficili su come dare priorità e allineare nel modo più efficace le risorse limitate, i rischi in continua espansione e le esigenze aziendali.

Per molte ragioni, le aziende cercano soluzioni a fornitore unico. Le normative, la conformità e le policy hanno spinto le aziende a voler saperne di più sulla sicurezza che un fornitore di servizi offre nelle rispettive sedi. I responsabili IT e della sicurezza chiedono ai fornitori dettagli sui loro pen-test, sul software development lifecycle (SDLC), sul bill of material (SBOM) e su altri documenti per dimostrare che non erediteranno la scarsa sicurezza informatica di un fornitore.

Commvault Cloud è progettato appositamente per proteggere, monitorare, creare report, gestire e recuperare i dati di qualsiasi workload, da qualsiasi luogo, il tutto da un **unico pannello di controllo**. Eliminando la necessità di pagare strumenti aggiuntivi che finiscono per creare lacune e vulnerabilità. Grazie a un motore dotato di intelligenza artificiale sempre attiva, Commvault Cloud offre una piattaforma unificata che protegge tutti i workload dalle minacce in evoluzione, garantendo al contempo un ripristino rapido e, soprattutto, pulito.

83%

delle aziende ritiene auspicabile il consolidamento dei sistemi con un unico fornitore.[4]

Total Cost of Ownership 5 volte più basso

Commvault vanta un TCO cinque volte inferiore rispetto ad altri strumenti di protezione cloud nativi.[5]

4 Forta, Digital Guardian Data Protection, "**Top Considerations for CISOs When Consolidating Information Security Solutions**", aprile 2023.
5 Analisi del TCO dei clienti Commvault.

AI avanzata, che abilita le funzionalità di nuova generazione

In qualità di dirigente, responsabile della sicurezza dei dati dell'azienda, devi combattere ad armi pari. Le minacce odierne basate sull'intelligenza artificiale ti impongono di agire rapidamente, di avviare per tempo le misure di sicurezza e di essere pronto a ripristinare su larga scala.

"La velocità di rilevamento è chiaramente la chiave per mitigare l'impatto delle intrusioni e il rilevamento, in particolare, richiede l'automazione per essere efficace. Tuttavia, la maggior parte delle organizzazioni è ancora sulla strada del rilevamento e del reporting completamente automatizzati[2]."
IDC: *The Cyber-resilient Organization: Maximum Preparedness with Bullet-proof Recovery*

Commvault Cloud, basato sull'A di Metallic, utilizza l'intelligenza artificiale, l'apprendimento automatico (ML) e l'automazione per offrire la più avanzata intelligence di protezione dei dati del settore. Prevede le minacce più rapidamente, garantisce ripristini più puliti e accelera i tempi di risposta.

Piattaforma di servizi innovativi

La piattaforma Commvault Cloud consente ai team SecOps e IT di gestire i processi in modo più efficiente ed economico.

Abbiamo rivoluzionato la sicurezza dei dati e il ripristino fornendo una difesa a più livelli attraverso un'esperienza semplice, unificata e simile al SaaS. Le comprovate capacità sono fornite attraverso i servizi della nostra piattaforma, che forniscono tutto, dagli allarmi tempestivi al ripristino rapido di tutti i dati, per qualsiasi workload, ovunque.

92%

delle organizzazioni prevede di utilizzare l'intelligenza artificiale e il machine learning per rafforzare la propria sicurezza informatica.[6]

Early Warning	Governance del rischio
Rileva le minacce più velocemente, riduci al minimo il loro l'impatto e limita la tua esposizione ai rischi.	Migliora la sicurezza dei tuoi dati individuando e correggendo in modo proattivo i rischi, nei dati di produzione e di backup.
Readiness & Response	**Cyber Recovery**
Garantisci la resilienza con preparazione avanzata, convalida automatizzata e recovery test continui.	Garantisci un recovery rapido, con la flessibilità di eseguire il ripristino da qualsiasi luogo, su larga scala.

6 Synchro Works Consulting, "**The Value of Danger of AI in Cybersecurity**", agosto 2023.

Commvault offre la giusta gamma di funzionalità di rilevamento, sicurezza e recovery per ridurre i rischi, minimizzare l'impatto degli attacchi e garantire una continuità aziendale incrollabile di fronte alle minacce. Proteggi il tuo ambiente in modo semplice e veloce con le seguenti funzionalità.

- **Air-gap e immutabilità:** salvaguarda i dati di backup in archivi sicuri con air-gap e con rigorosi controlli di accesso per evitare manomissioni.
- **Clean Restore Point Validation:** l'automazione basata sull'intelligenza artificiale verifica e assicura punti di ripristino puliti, previene le reinfezioni e fornisce set di dati incontaminati.
- **Gestione della postura della sicurezza dei dati:** individua, analizza e proteggi i file sensibili per ridurre i rischi di esfiltrazione dei dati, di produzione e di backup.
- **Early Warning:** rileva le minacce prima della crittografia, dell'esfiltrazione o del danneggiamento con la tecnologia brevettata di allarme precoce che scopre e devia le minacce zero-day e avanzate prima che raggiungano i tuoi dati. Proteggi inoltre le risorse e gli ambienti di backup da malintenzionati.
- **Resilience e Recovery:** elimina i rischi legati al malware, previeni le reinfezioni e orchestra i ripristini su larga scala con un ripristino rapido e affidabile.
- **Approfondimenti sulla sicurezza:** ottieni l'osservabilità end-to-end e gestisci i rischi relativi ai dati in modo efficiente. Reagisci per tempo e limita l'esposizione attraverso un unico pannello di controllo.
- **Architettura zero-trust:** approfondisci l'autenticazione multifattoriale e multipersona, la gestione degli accessi privilegiati (PAM) e gli strumenti di gestione dell'identità e degli accessi (IAM) come CyberArk, YubiKey e la biometria (come AAL3).

COMMVAULT CLOUD UNISCE IT E SECOPS:

Implementando Commvault Cloud, la tua azienda può trarre vantaggio dalla vera sicurezza e recovery dei dati nel cloud ibrido, consentendoti di vedere, gestire e recuperare i dati ovunque si trovino.

Commvault offre ai nostri clienti un vantaggio nel garantire la resilienza di fronte a un attacco informatico. Questo grazie ad anni di innovazione e di leadeship nel settore, con oltre 1.500 brevetti. Uno dei vantaggi più importanti offerti da Commvault Cloud è un'architettura unica creata per il mondo ibrido. Offre il recovery di massa più rapido e ottimizzato del mercato.

Sfrutta la potenza della cyber resilience

Per saperne di più, visita **www.commvault.com** o **richiedi una demo**.