Acronis

WHITE PAPER

Oltre la Cyber Security: un modello pratico per trasformare la resilienza digitale e passare dalla prevenzione alla continuità operativa

Sintesi riepilogativa

Cyber Security e resilienza digitale sono due facce della stessa medaglia perché entrambe sono fondamentali per sostenere l'operatività aziendale e contrastare le minacce moderne. Mentre la Cyber Security tradizionale si concentra sulla prevenzione respingendo gli aggressori, la resilienza digitale rappresenta un cambiamento strategico che favorisce l'adattabilità e la continuità operativa dell'azienda. Non è quindi solo una funzione delle operazioni di sicurezza, ma è la capacità strategica di un'organizzazione di anticipare, resistere, riprendersi dalle minacce e adattarsi alle interruzioni operative informatiche.

Aspetto	Cyber Security	Resilienza digitale
Ambito	Tenere lontani gli aggressori	Operatività durante gli attacchi e successivo ripristino
Obiettivo primario	Prevenire gli attacchi/proteggere dati, infrastruttura	Adattabilità e continuità operativa
Presupposto di base	È possibile fermare gli attacchi	Gli attacchi sono inevitabili
Risultato	Evitare le violazioni	Minimizzare le interruzioni operative e garantire la continuità operativa
Attività principali	Firewall, antivirus, rilevamento/prevenzione delle intrusioni	Incident response, continuità operativa, disaster recovery
Approccio	Misure di difesa/perimetro	Agile/adattivo

Questo white paper presenta un modello di resilienza che supera i modelli di ridondanza tradizionali e guarda a un approccio unificato e basato sul rischio, Powered by Acronis. Questa trasformazione si colloca in un panorama delle minacce sempre più ostile, in cui il costo medio di una richiesta di risarcimento per ransomware è salito a oltre 1,18 milioni di dollari nel 2025.[1] Poiché affidarsi esclusivamente alle tattiche di prevenzione non è più sostenibile dal punto di vista finanziario, sempre più aziende adottano la piattaforma Acronis Cyber Protect per sostituire l'insieme di strumenti frammentari in uso con una struttura unificata e consolidata. In questo modo possono proteggere l'integrità delle risorse critiche e tornare rapidamente operative dopo qualsiasi interruzione operativa.

[1] Resilience Risk Operations Center, "Mid Year Cyber Risk Report", 2025. https://unlock.cyberresilience.com/hubfs/2025%20Cyber%20Risk%20Report.pdf

L'imperativo strategico: oltre la ridondanza

Da sempre, le organizzazioni adottano la ridondanza architettonica per ridurre al minimo le interruzioni operative, attraverso metodi come la doppia alimentazione, coppie di hardware ad alta disponibilità e data center ridondanti. Sebbene queste misure offrano protezione contro i guasti hardware fisici, sono state progettate per sopperire alle interruzioni accidentali e non agli avversari intelligenti.

Di fronte al ransomware di oggi, la resilienza basata sulla deduplicazione spesso non funziona. Un data center ridondante può anche replicare l'infezione dal sito primario mentre un attacco si propaga attraverso l'infrastruttura di rete. Inoltre, questi approcci frammentari sono spesso causa della proliferazione degli strumenti, che impone ai team IT la gestione di console non integrate per le attività di backup, disaster recovery e sicurezza. Questo crea un insieme di tecnologie caotico, il cosiddetto "Franken-Stack" che ostacola la produttività, aumenta il costo totale di proprietà e genera pericolosi punti ciechi di vulnerabilità.

La differenza di Acronis

La vera resilienza richiede una piattaforma capace e non una semplice collezione di strumenti. Acronis si differenzia offrendo una cyber protection nativamente integrata che include backup, sicurezza e disaster recovery (DR) all'interno di un unico agente e di un'unica console di gestione. In questo modo vengono eliminate le lentezze operative del passaggio da un'interfaccia all'altra, garantendo ripristini rapidi, verificati e affidabili.

Fase 1 Classificazione e priorità delle risorse

La base di qualsiasi strategia di resilienza è riconoscere che la protezione deve essere commisurata al valore della risorsa. Poiché non tutti i dati richiedono lo stesso livello di resilienza, il primo passo è la classificazione delle risorse.

Classificare la criticità dei server in base al valore aziendale e non al numero di server

Un malinteso comune nella pianificazione della resilienza è equiparare il volume tecnico e il valore aziendale. È invece necessario comprendere che il requisito per la resilienza digitale è dettato dalla criticità del server, non dal numero di server o dalle specifiche di prestazione.

Come indicato nelle metodologie di valutazione del rischio, un singolo server critico sul quale risiedono informazioni proprietarie o proprietà intellettuale top-secret ha un valore maggiore rispetto a 100 server che ospitano dati non sensibili.

La perdita di una singola risorsa critica può causare gravi responsabilità finanziarie, sanzioni normative o danni alla reputazione.

Pertanto le risorse per la resilienza, come gli obiettivi RTO prossimi allo zero e i failover ad alta disponibilità, non dovrebbero essere applicate in modo omogeneo all'intero ambiente, ma concentrate invece sui workload specifici che generano il fatturato e supportano l'immagine aziendale.

Applicare etichette efficaci alle risorse per automatizzare le policy di protezione

Per concretizzare questo concetto, è necessario passare dalla classificazione teorica cartacea alla classificazione digitale nelle console di gestione. Applicare etichette efficienti alle risorse significa assegnare ai workload tag di metadati che ne definiscono le policy di protezione automatizzate.

Tra le più comuni etichette di classificazione troviamo:

Riservato o proprietario
Il livello più alto, la cui compromissione causa gravi perdite per l'azienda. Per queste risorse è necessario Acronis Disaster Recovery con funzionalità di failover immediato.

Sensibile
La violazione provoca danni tangibili alla mission o alla reputazione aziendale. Sono necessari backup immutabili frequenti e obiettivi RPO ottimizzati.

Privato
Dati interni come i registri del personale, a cui si applicano le pianificazioni di backup standard.

Pubblico
Dati che possono essere divulgati. Priorità più bassa per le risorse di ripristino.

Applicando le etichette alle risorse nella console Acronis, i team IT possono automatizzare l'applicazione dei piani di protezione, garantendo che un server riservato erediti automaticamente una policy di backup immutabile e una macchina virtuale in standby nel cloud, mentre per un server pubblico verrà eseguito un backup giornaliero standard.

Fase 2 Analisi dell'impatto sull'attività aziendale e quantificazione finanziaria

Una volta classificate le risorse, l'analisi di impatto sull'operatività aziendale (BIA, Business Impact Analysis) identifica le operazioni critiche e quantifica le conseguenze di una loro interruzione operativa.

Principali metriche di ripristino

La BIA definisce le metriche essenziali che la piattaforma Acronis deve soddisfare:

- **RTO**: tempo massimo tollerabile prima dell'esecuzione del ripristino.
- **RPO**: perdita di dati massima tollerabile.
- **MTD**: periodo massimo di interruzione operativa tollerabile durante il quale un sistema può rimanere non disponibile prima che ciò causi danni irreversibili. Il superamento del valore MTD segna il passaggio dall'interruzione operativa al potenziale fallimento dell'azienda.
- **MTCR**: tempo medio per il ripristino pulito; è una metrica moderna per il ransomware che misura il tempo necessario per tornare a una condizione verificata e priva di malware.

Acronis si occupa dell'obiettivo MTCR integrando la scansione di sicurezza nel processo di ripristino e impedendo il ripristino di file infetti.

Analisi quantitativa del rischio

Per giustificare l'investimento in un'architettura di resilienza, è bene avvalersi dell'analisi quantitativa del rischio per calcolare il valore previsto delle perdite annuali (ALE, Annual Loss Expectancy). Tale valore viene calcolato moltiplicando il valore della risorsa, il fattore di esposizione e la frequenza annua prevista. Acronis supporta questo modello economico con opzioni di licensing flessibili, che permettono di allineare la spesa aziendale direttamente al valore delle risorse derivato dai calcoli sul rischio.

Calcolo dell'ALE:

Valore della risorsa ×

Fattore di esposizione ×

Frequenza annua prevista

Fase 3 Risposta strategica al rischio

In base all'analisi del rischio, le organizzazioni adotteranno una risposta strategica su misura per la criticità delle proprie risorse. Per i sistemi aziendali strategici, quando non è possibile evitare del tutto i rischi, la strategia necessaria è la mitigazione del rischio. Acronis svolge il ruolo di motore principale di questa strategia grazie a due livelli critici che puntano a fermare gli attacchi prima che possano devastare l'azienda.

Mitigazione del rischio: neutralizzare le minacce

La mitigazione si concentra sulla riduzione della probabilità e dell'impatto di una violazione. L'archiviazione immutabile e la difesa assistita dall'AI sono le misure applicate con la strategia Acronis. I backup vengono archiviati in modalità di governance, per garantire che anche qualora un attaccante ottenga l'accesso amministrativo, non sia in grado di eliminare i dati di backup. Intanto, i motori di rilevamento comportamentale potenziati dall'AI identificano in tempo reale le minacce zero-day analizzando i processi attivi e arrestando gli attacchi prima che possano causare danni.

Recupero da rischio: garantire la continuità

Quando la mitigazione viene aggirata, la strategia si sposta sul recupero dal rischio, per garantire che l'azienda resti operativa. Per i workload strategici, Acronis Cloud fornisce un ambiente di failover per il disaster recovery, che permette all'azienda di spostare immediatamente la produzione sul cloud, passando dalla fase critica alla continuità mentre il sito principale viene ripristinato.

Fase 4 Pianificazione della continuità operativa ed esecuzione

L'esecuzione della strategia di resilienza avviene attraverso un ciclo continuo di anticipazione, resistenza, recupero e adattamento. Per sostituire i processi legacy con un'efficienza moderna, Acronis offre un disaster recovery e una Cyber Protection a più livelli progettata per l'ambiente cloud aziendale.

Fase di recupero: disaster recovery integrato

Quando si verifica un'interruzione operativa, la fase di recupero diventa l'obiettivo primario. Integrato nella licenza di backup di base, Acronis Disaster Recovery offre un ripristino di livello enterprise a una frazione del costo dei siti legacy, pesanti in termini di hardware.

- **Infrastruttura gestita nel cloud:** l'ambiente cloud e la piattaforma di orchestrazione di base sono completamente gestiti da Acronis. La complessità per il cliente risulta così ridotta, perché si elimina la necessità di manutenzione di hardware off-site.
- **Esecuzione controllata dal cliente:** mentre l'infrastruttura è gestita da Acronis, i clienti mantengono il controllo totale su avvio, test e gestione delle operazioni di failover e failback tramite la console centralizzata.
- **Strategia di failover e test senza rischi:** la piattaforma supporta il failover diretto in Acronis Cloud. Per garantire che funzioni quando necessario, gli abbonamenti includono lo storage ad accesso frequente gratuito per consentire di eseguire il failover di prova dei workload critici senza costi aggiuntivi.
- **Convalida del ripristino pulito:** per evitare che venga ripristinato codice malevolo, la convalida del backup assistita da AI scansiona le minacce e verifica che i punti di ripristino siano puliti prima che entrino in produzione.

Fase di resistenza: Cyber Protection a più livelli

Per garantire che un'azienda possa resistere a un attacco il semplice ripristino non basta: serve la protezione attiva dei dati, che si realizza con backup completi a livello di immagine e backup immutabili a livello di file, archiviati in modalità di governance e combinati con una difesa dal ransomware basata su AI, in grado di rilevare e bloccare in tempo reale la crittografia comportamentale.

Punteggio di resilienza e modello DREAD

Per mantenere un'elevata resilienza, le organizzazioni possono utilizzare alcuni parametri che ne misurano la maturità. Un componente chiave di questa strategia è l'assegnazione della priorità alle minacce tramite il modello DREAD, che attribuisce un valore alle categorie seguenti: danno potenziale, riproducibilità, sfruttabilità, utenti interessati, rilevabilità.

Acronis rafforza ogni dimensione del punteggio DREAD:

Danno potenziale
Il rapido failover nel cloud preserva i ricavi e contiene l'impatto economico.

Riproducibilità
I backup immutabili interrompono i cicli di reinfezione e impediscono agli aggressori di ottenere nuovi successi.

Sfruttabilità
Le vulnerability assessment automatizzate chiudono i possibili varchi nella sicurezza che gli attaccanti possono sfruttare.

Utenti interessati
L'isolamento e l'etichettatura dettagliata dei workload minimizza il raggio d'azione, garantendo che la compromissione non si propaghi a tutti gli utenti.

Rilevabilità
Le analisi EDR riducono il tempo di permanenza degli attaccanti, impedendo alle minacce di rimanere nascoste a lungo.

Perché scegliere Acronis

In un contesto in cui la prevenzione da sola non è più sufficiente, Acronis colma il divario tra la sicurezza tradizionale e la continuità operativa totale dell'azienda. Unificando la difesa dalle minacce potenziata dall'AI con il rapido disaster recovery gestito nel cloud, Acronis garantisce che i dati critici non siano solo protetti in caso di attacco, ma anche organizzati per essere ripristinati in modo rapido e affidabile.

Disaster recovery integrato e garanzia di ripristino: Acronis Disaster Recovery è un componente aggiuntivo il cui funzionamento è legato a una licenza di backup di base attiva. La soluzione offre disaster recovery di livello enterprise a una frazione del costo dei siti legacy, pesanti in termini di hardware.

Infrastruttura di disaster recovery gestita nel cloud: l'ambiente cloud di base, la piattaforma di orchestrazione e l'infrastruttura necessaria sono completamente gestiti da Acronis, riducendo in questo modo la complessità per i clienti.

Failover immediato su Acronis Cloud con fatturazione a consumo: i carichi di lavoro critici dei server possono essere ripristinati in Acronis Cloud durante un'interruzione o un attacco, con fatturazione del processo solo all'attivazione del failover, eliminando così i costi di standby.

Esecuzione controllata dal cliente: mentre l'infrastruttura è gestita da Acronis, i clienti mantengono il controllo su avvio, test e gestione delle operazioni di failover e failback tramite la console.

Convalida del ripristino pulito: la convalida del backup assistita da AI esegue scansioni alla ricerca delle minacce e verifica che i punti di ripristino ne siano privi.

Test senza rischi: gli abbonamenti includono lo storage ad accesso frequente gratuito per consentire l'esecuzione di failover di prova e di produzione dei workload critici, senza costi aggiuntivi.

Protezione a più livelli: backup completi immutabili a livello di immagine e di file archiviati in modalità di governance. Le misure di difesa basate su AI contro il ransomware rilevano la crittografia comportamentale.

Conclusione: un percorso unificato per garantire la continuità operativa

L'attuale panorama delle minacce è caratterizzato da attacchi basati su AI e danni finanziari repentini, che per essere contrastati richiedono un sostanziale cambiamento dell'approccio alla protezione dell'operatività aziendale. Le aziende non possono più affidarsi alla speranza che le difese perimetrali reggano o che strumenti di ridondanza scollegati riescano a fermare la propagazione del ransomware.

La soluzione consiste in una transizione verso la piattaforma unificata di cyber protection di Acronis. Consolidando in un'unica soluzione backup, disaster recovery, Cyber Security e gestione degli endpoint, le aziende eliminano la complessità della proliferazione degli strumenti e ottengono tutte le potenzialità della protezione basata su AI.

In definitiva, la resilienza è una decisione economica. Allineando la protezione al valore delle risorse aziendali, con una classificazione rigorosa delle risorse e un'analisi di impatto, ed eseguendo questa strategia tramite i runbook di ripristino orchestrati nel cloud e convalidati dall'AI di Acronis, le organizzazioni si garantiscono la capacità di sopravvivere all'inevitabile. Con Acronis, le aziende non si limitano a recuperare, ma si riprendono in modo più efficace, proteggendo il loro futuro in un mondo digitale imprevedibile.

Acronis

Per saperne di più, visita acronis.com