

Protected Infrastructure

Cyber protection integrata in modo nativo per server e VM

La resilienza digitale va oltre la tradizionale Cyber Security. Non è solo in grado di prevenire gli attacchi, ma permette alle aziende di continuare a operare anche quando si verificano gli incidenti. Secondo la definizione del NIST: "La resilienza digitale è la capacità di anticipare, affrontare, riprendersi e adattarsi a condizioni avverse, situazioni di stress, attacchi o compromissioni dei sistemi."

"Con quale velocità è in grado di riprendersi la tua azienda?" Se non sono stati predisposti playbook di incident response, strumenti e obiettivi RTO (Recovery Time Objective) e RPO (Recovery Point Objective) chiari e trasparenti, ogni interruzione rischia di trasformarsi per le aziende in perdite di fatturato, minore fiducia dei clienti e danni alla reputazione duraturi.

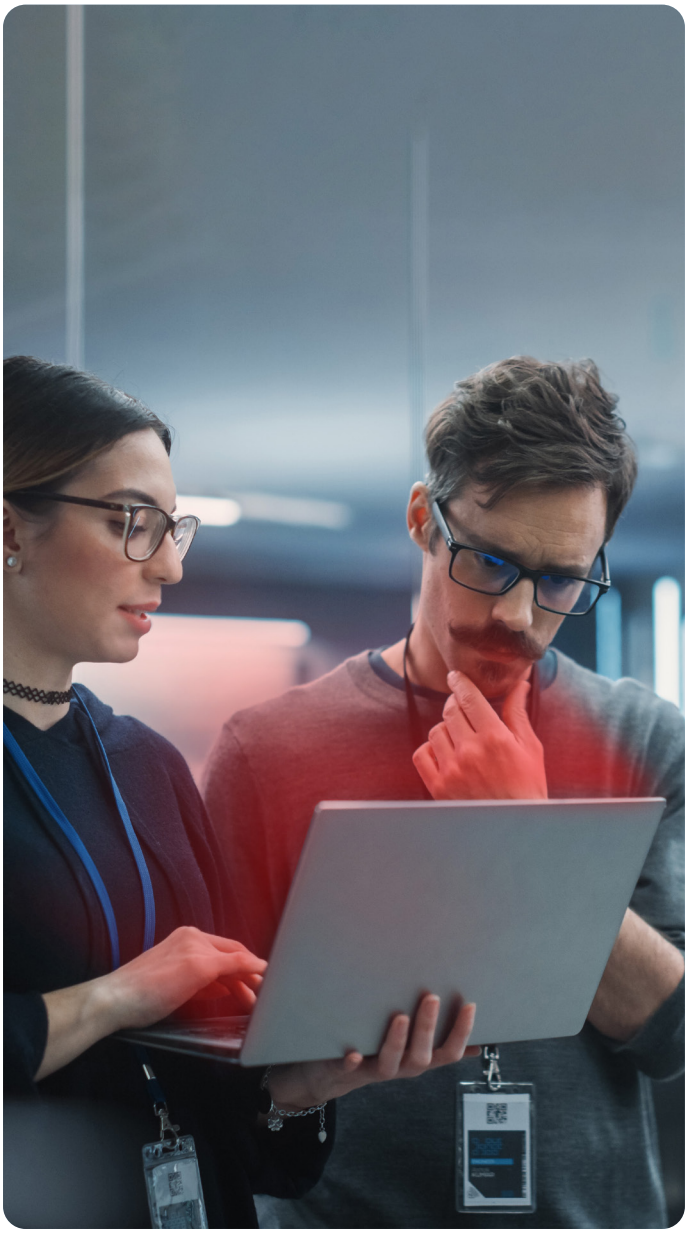


Aspetti critici della resilienza digitale

A prescindere dalla loro dimensione, le aziende si rendono conto che i costi delle interruzioni operative superano di molto quelli delle perdite di dati. Affrontano crescenti pressioni di conformità e controllo normativo perché eventuali falle nella preparazione espongono a sanzioni e a rischi di reputazione.

Copyright © 2003-2026 Acronis International GmbH.

La gestione degli incidenti con strumenti eterogenei crea inoltre inutili complessità. Senza una strategia unificata, i team IT sperimentano il caos operativo e si ritrovano a dover necessariamente coordinare le attività di rilevamento, risposta e ripristino utilizzando più console e agenti. Si generano così inefficienze che aumentano i costi, rallentano i tempi di risposta e ampliano le responsabilità. L'aumento dei premi delle polizze contro i rischi informatici aggiunge un ulteriore motivo di preoccupazione perché una resilienza non sufficiente può portare al rifiuto della copertura assicurativa.



Ostacoli tecnologici alla resilienza

Con l'accelerazione della trasformazione digitale, la resilienza sembra un obiettivo più difficile da raggiungere. La superficie di attacco è in continua espansione, perché gli ambienti IT ibridi si ampliano per integrare i sistemi in sede, le piattaforme cloud e gli endpoint remoti, generando sempre più interdipendenze e potenziali punti di errore. Al contempo, le minacce diventano sempre più sofisticate. Ransomware, compromissioni della supply chain e rischi legati al personale interno sfruttano le vulnerabilità prodotte dalle singole soluzioni mirate, che possono sì contrastare rischi specifici, ma creano anche punti ciechi, procedure manuali e lacune in cui gli attaccanti si infiltrano rapidamente.

Il percorso verso la resilienza digitale

Per ottenere un'autentica resilienza, le sole difese digitali non bastano più. Occorre anche garantire la continuità operativa, indipendentemente dai motivi dell'interruzione. Per diventare resilienti, le aziende possono adottare un approccio strutturato che inizia con la **previsione** dei rischi tramite la mappatura delle risorse, la valutazione delle vulnerabilità e la gestione delle correzioni. Devono quindi essere in grado di **resistere** alle minacce rilevandole e contenendole in tempo reale con funzionalità avanzate come la protezione degli endpoint alimentata dall'AI e il monitoraggio basato su machine learning. Queste misure proattive sono efficaci solo se affiancate da una solida strategia di ripristino.

Il ripristino è infatti il passaggio critico successivo. Essere in grado di eseguire un ripristino rapido, affidabile e privo di malware dei dati e dei sistemi consente di ridurre al minimo i tempi di inattività. In presenza di un guasto grave, è prioritario garantire la continuità aziendale. Con Acronis Cloud Disaster Recovery, le aziende possono eseguire il failover immediato dei workload direttamente su Acronis Cloud o su Microsoft Azure. Il failover immediato garantisce la continuità anche durante le interruzioni più serie perché funge da ambiente di failback sicuro fino al completo ripristino dei sistemi primari.

Infine, la resilienza non è statica. Le organizzazioni devono sapersi **adattare** imparando dagli incidenti, formando i propri team e perfezionando le difese nel tempo.

Copyright © 2003-2026 Acronis International GmbH.

Disaster recovery di qualità

In definitiva, queste strategie non riguardano solo il ripristino dopo un'emergenza, ma anche la resilienza operativa che permette di continuare a svolgere le funzioni aziendali essenziali in qualsiasi circostanza. La capacità di ripristinare i servizi in pochi minuti anziché in giorni è la chiave per ridurre al minimo le perdite finanziarie e mantenere la fiducia dei clienti.

In genere, le strategie di disaster recovery vengono classificate in base agli RPO e agli RTO che permettono di raggiungere. Le due strategie più adottate sono:

Warm DR

Questo approccio offre un buon equilibrio tra costi e velocità di ripristino. Per farlo, utilizza sistemi pre-installati che possono essere attivati rapidamente, in linea con l'obiettivo di "ripristino" che prevede di ridurre al minimo i tempi di inattività pur avendo un RPO e un RTO definiti.

Cold DR

Focalizzato esclusivamente sulla ricostruzione e sul ripristino dei dati, il cold DR esegue ripristini completi a partire dai backup, con tempi di ripristino più lunghi ma costi operativi inferiori.

Unificando rilevamento, protezione e ripristino, le aziende conquistano il vantaggio strategico dato non solo dal sopravvivere a una crisi, ma di uscirne più forti di prima. Acronis Cloud Disaster Recovery permette alle aziende di selezionare il giusto livello di resilienza per ogni workload, dalle opzioni di failover da warm a cold che ricostruiscono i servizi dopo un'interruzione, fino alla continuità immediata con l'Hot DR integrato. Questa flessibilità rafforza le difese in ogni fase del percorso verso la resilienza digitale.



Copyright © 2003-2026 Acronis International GmbH.

La soluzione Protected Infrastructure

La soluzione Acronis Protected Infrastructure unifica backup, disaster recovery, sicurezza degli endpoint, valutazione del rischio e prevenzione della perdita di dati in un'unica piattaforma di Cyber Protection nativamente integrata. Questo approccio elimina i silos, riduce la proliferazione degli strumenti e garantisce la resilienza senza aggiungere complessità. La piattaforma copre ogni fase del percorso di resilienza: anticipare, resistere, recuperare e adattarsi. Avvalendosi di un'unica piattaforma, di una sola console e di un singolo agente, le aziende possono velocizzare il rilevamento delle minacce, tornare operative senza interruzioni e adattarsi ai rischi in continua evoluzione.

PREVISIONE	RESISTENZA	RIPRISTINO	ADATTAMENTO
• Individuazione dei dispositivi • Mappa della protezione dati • Inventario delle risorse • Vulnerability assessment • Gestione delle patch	• Rilevamento delle minacce in tempo reale • Rilevamento e risposta degli endpoint (EDR) alimentati dall'AI. • Monitoraggio basato su machine learning • Contenimento rapido delle minacce attive	• Recupero sicuro e automatizzato dei dati • Disaster recovery in cloud • Backup immutabili • Mobilità dell'hypervisor • Ripristino su punti privi di malware	• Monitoraggio e gestione degli endpoint • Security Awareness Training (SAT) • Modelli con suggerimenti di incident response

Perché le aziende scelgono Acronis

In un ambiente in cui gli attacchi informatici sono inevitabili, Acronis potenzia la resilienza digitale unificando la protezione dalle minacce alimentata dall'AI con il disaster recovery orchestrato nel cloud in un'unica piattaforma. A differenza degli approcci frammentati di sola prevenzione, Acronis garantisce che i dati critici siano sia protetti che recuperabili attraverso backup immutabili, rilevamento del ransomware basato sull'AI e convalida del ripristino pulito.

Grazie a un disaster recovery completamente gestito dal cloud, al failover immediato verso Acronis Cloud, a un modello di calcolo a consumo e a test ed esecuzione controllati dal cliente, la soluzione Acronis Protected Infrastructure offre una cyber protection di livello enterprise senza i costi e la complessità delle infrastrutture legacy. Il risultato è un ripristino più veloce, un rischio operativo ridotto e una continuità operativa ininterrotta quando è più importante.

Pianifica una demo con un esperto Acronis

Per garantire la continuità aziendale, la sola protezione non basta più. Serve la resilienza. Scopri come Acronis può aiutarti ad anticipare le minacce, resistere agli attacchi, riprendersi più velocemente e adattarsi al futuro.

CONTATTACI



Acronis

Maggiori informazioni su www.acronis.com

Copyright © 2003-2026 Acronis International GmbH. Tutti i diritti riservati. Acronis e il logo Acronis sono marchi registrati di Acronis International GmbH negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali o marchi registrati sono proprietà dei rispettivi titolari. Soggetto a modifiche tecniche. Le immagini potrebbero non corrispondere al prodotto reale. Si declina qualsiasi responsabilità per possibili errori. 2026-11