Stato attuale del backup e del ripristino nel settore manifatturiero

RAPPORTO DI RIFERIMENTO 2026

Macrium Software | NewtonX®

Indice

Lo studio di riferimento Macrium 2026, condotto in collaborazione con NewtonX, esamina l'approccio alla protezione dei sistemi, al backup e alle strategie di continuità operativa delle aziende manifatturiere.

La ricerca ha coinvolto 100 responsabili delle decisioni nel settore IT e OT, la cui identità è stata verificata, provenienti da aziende manifatturiere di medie e grandi dimensioni con almeno 2.500 dipendenti in Nord America e nel Regno Unito.

1 Ambito della ricerca

2 Stato attuale del backup e del ripristino

3 Rischi resilienza e prestazioni di ripristino

4 Dinamiche organizzative e sfide

5 Priorità di investimento e orientamenti futuri

Macrium Software | NewtonX®

Ambito della ricerca

L'importanza strategica della protezione dei sistemi nella moderna manifattura

In un'epoca in cui le attività manifatturiere sono sempre più digitalizzate e interconnesse, la capacità di proteggere e ripristinare rapidamente le informazioni critiche si è trasformata da una questione tecnica in un imperativo strategico per l'azienda.

Le aziende manifatturiere operano all'incrocio tra processi tradizionali e tecnologie digitali all'avanguardia, creando contesti in cui un singolo punto di guasto può bloccare le linee di produzione, interrompere le catene di approvvigionamento e generare perdite che possono ammontare a centinaia di migliaia di euro.

Macrium Software NewtonX®

La complessità peculiare della protezione dei sistemi manifatturieri

A differenza di altri settori incentrati principalmente sulle infrastrutture IT tradizionali, il settore manifatturiero deve proteggere sistemi eterogenei e interdipendenti che abbracciano sia la tecnologia informatica (IT) che quella operativa (OT). I sistemi ERP, i sistemi di esecuzione della produzione, le piattaforme SCADA e i controllori logici programmabili generano tutti dati mission-critical, controllando al contempo i processi fisici di produzione.

Molte organizzazioni utilizzano sistemi legacy, alcuni dei quali risalgono a diversi decenni fa – affiancati da moderne infrastrutture cloud e dalle tecnologie emergenti dell'Industria 4.0.

Questi ambienti ibridi pongono sfide peculiari per l'implementazione di strategie complete di backup e ripristino che tengano conto di protocolli proprietari, requisiti operativi in tempo reale e siti produttivi distribuiti.

La posta in gioco sempre più alta

Per le aziende manifatturiere, i tempi di inattività rappresentano una minaccia diretta all'efficienza operativa e al posizionamento competitivo.

I tempi di inattività non pianificati possono costare alle aziende manifatturiere di medie dimensioni da decine a centinaia di migliaia di euro, compromettere al contempo la fiducia dei clienti, la reputazione del marchio e il rispetto degli impegni assunti nella catena di approvvigionamento.

Nonostante la posta in gioco sia così alta, molte aziende faticano a garantire adeguate capacità di backup e ripristino. I sistemi di backup rimangono non testati o vengono testati con scarsa frequenza, e le minacce informatiche in continua evoluzione, in particolare il ransomware che prende di mira le infrastrutture manifatturiere, hanno introdotto rischi che gli approcci tradizionali al backup non sono mai stati progettati per affrontare.

La strada da seguire

Affrontare queste sfide richiede un cambiamento radicale di approccio. Il backup e il ripristino devono essere riconosciuti come capacità strategiche che garantiscano direttamente la resilienza operativa, richiedendo investimenti in programmi di test completi e soluzioni appositamente progettate per la complessità del settore manifatturiero.

Questa ricerca illustra lo stato attuale delle pratiche di protezione dei sistemi nel settore manifatturiero, identifica le sfide comuni e le tendenze emergenti e offre indicazioni per guidare le organizzazioni verso una maggiore solidità verso queste evenienze.

I risultati rappresentano l'esperienza collettiva dei responsabili IT e delle attività operative, offrendo un punto di riferimento rispetto al quale le aziende manifatturiere possono valutare le proprie capacità e priorità.

Macrium Software | NewtonX®

Stato attuale del backup e del ripristino

Principali risultati

La frammentazione degli strumenti domina il panorama

Gli ambienti di backup nel settore manifatturiero sono caratterizzati da un'ampia varietà di piattaforme, con la stragrande maggioranza delle organizzazioni che utilizzano più soluzioni contemporaneamente. Le organizzazioni continuano ad aggiungere strumenti, considerando le diverse piattaforme come risposte a esigenze distinte.

Questo riflette la complessità intrinseca del settore manifatturiero, in cui la diversità dei sistemi rende difficile adottare approcci unificati.

Prevalgono le strategie ibride ma persistono carenze di fiducia

Tre quarti adottano approcci di backup ibridi che combinano soluzioni cloud e on-premise, dando priorità alla protezione di database, sistemi ERP e carichi di lavoro cloud.

Tuttavia, i sistemi di tecnologia operativa si collocano nettamente più in basso tra le priorità di protezione, nonostante la loro importanza critica.

Ancora più preoccupante, un terzo delle aziende manifatturiere non ha fiducia nella propria capacità di raggiungere gli obiettivi di ripristino e nelle capacità complessive di backup, evidenziando un divario tra implementazione e prontezza operativa.

Misurare senza convalidare crea punti ciechi

Le aziende manifatturiere si concentrano molto su metriche temporali come RTO e RPO, ma solo un quarto monitora la frequenza dei test di ripristino.

Questo crea pericolosi punti ciechi: le organizzazioni misurano i tassi di completamento dei backup senza convalidare la capacità effettiva di ripristino, una lacuna che potrebbe emergere solo al verificarsi di costose interruzioni della produzione.

Principali risultati e priorità attuali

Esistono opportunità di consolidamento per i fornitori in grado di soddisfare l'intera gamma delle esigenze delle esigenze produttive

I test e la convalida devono passare dall’essere attività periodiche a pratiche operative regolari

La protezione OT richiede una maggiore priorità, data l'importanza la criticità dei sistemi di produzione

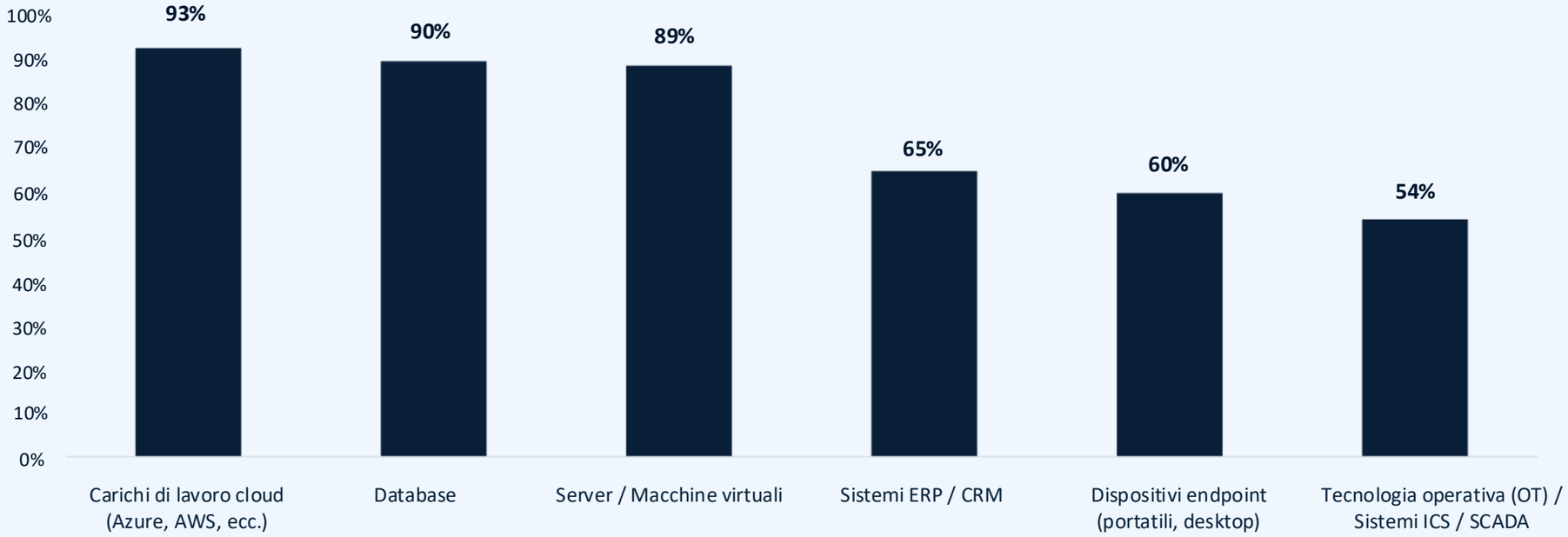
Rafforzare la fiducia attraverso capacità di ripristino comprovate, non solo attraverso metriche di completamento dei backup

Tre quarti delle aziende manifatturiere adottano strategie di backup ibride, che riflettono esigenze eterogenee di protezione dei sistemi. CI carichi di lavoro nel cloud, i database e i server sono in cima alle priorità di protezione, mentre i sistemi di tecnologia operativa (OT) occupano posizioni nettamente inferiori nella classifica per priorità, il che suggerisce l'esistenza di lacune nella protezione dell'OT nonostante la loro importanza critica per le operazioni di produzione.

Approccio attuale al backup e al ripristino

- Approccio ibrido (75%)
- Cloud (23%)
- Soluzione on-premise (2%)

Sistemi e tipi di dati gestiti per il backup



Macrium Software | NewtonX®

Base: tutti gli intervistati n=100

Soluzioni di backup e ripristino in uso

Le aziende manifatturiere operano in ambienti di backup fortemente frammentati: quasi due terzi (64%) utilizzano 2-3 soluzioni diverse e oltre un quarto (26%) impiega quattro o più strumenti per proteggere i propri sistemi IT e OT.

64%

2-3 soluzioni diverse

26%

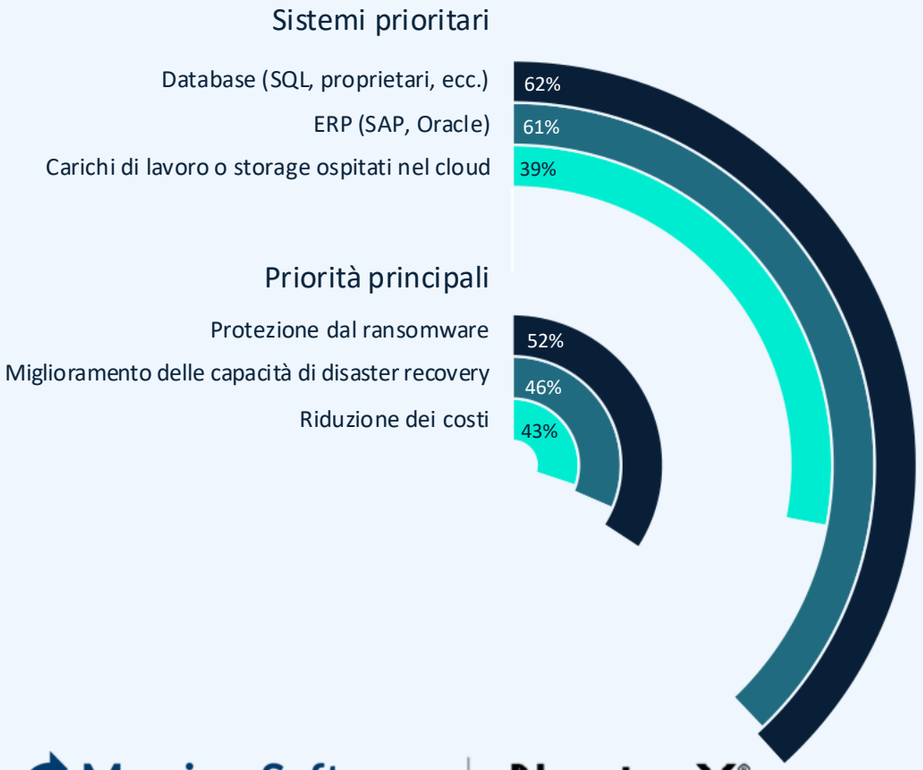
4 o più strumenti

Macrium Software | NewtonX®

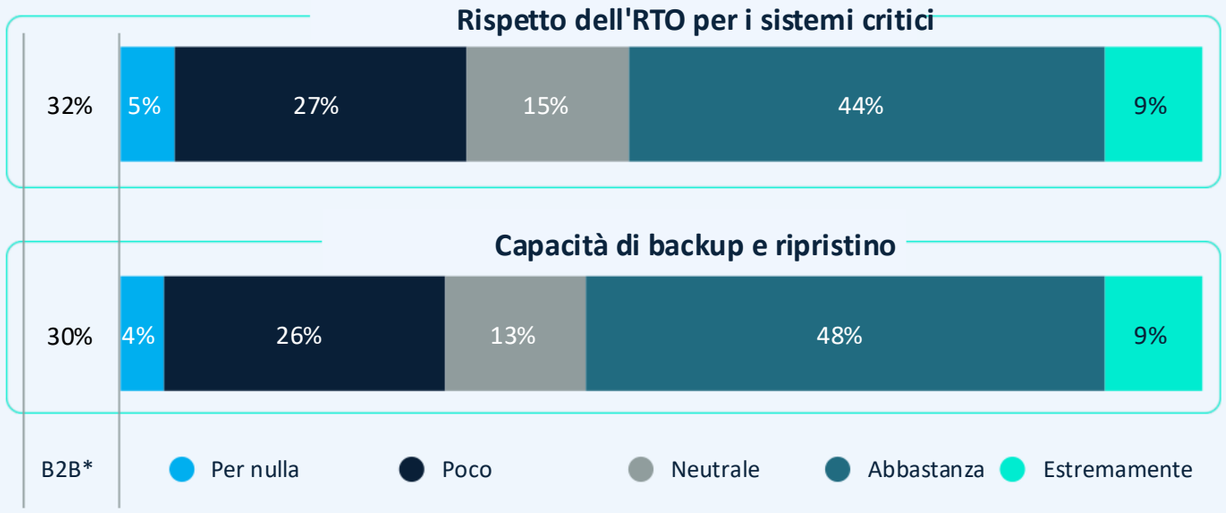
Base: tutti gli intervistati n=100

Le aziende manifatturiere concentrano il backup sui sistemi aziendali fondamentali, come database, ERP e i dati delle procedure in cloud, dando al contempo priorità alla difesa dal ransomware e al disaster recovery. Tuttavia, un terzo non ha fiducia nella propria capacità di rispettare gli RTO per i sistemi critici e nelle capacità complessive di backup. Questo divario tra investimento e fiducia suggerisce che l'implementazione di soluzioni di backup non garantisce la prontezza operativa quando occorre ripristinare i sistemi.

Strategia di backup e ripristino



Fiducia in...



Nel Regno Unito la fiducia nelle capacità di backup e ripristino è inferiore rispetto al Nord America (B2B* 46% contro 27%)

Base: tutti gli intervistati n=100

* B2B = Bottom 2 box (le due categorie inferiori: chi ha selezionato “Per nulla fiducioso” o “Poco fiducioso”

Monitoraggio dei KPI per il backup e il ripristino

Le aziende manifatturiere danno priorità alle metriche temporali di ripristino: il 73% monitora l'RTO e il 63% l'RPO, a conferma dell'importanza cruciale di ridurre al minimo i tempi di inattività. Tuttavia, emerge una lacuna preoccupante nelle pratiche di convalida: solo il 25% monitora la frequenza dei test di ripristino e appena il 44% la quantità di dati ripristinati correttamente.

Ciò dimostra che le organizzazioni si limitano a misurare ciò che è facile monitorare come i tassi di completamento dei backup e i tempi teorici di ripristino, anziché verificare se i sistemi possano effettivamente essere ripristinati quando necessario, creando così pericolosi punti ciechi che potrebbero emergere solo durante reali interruzioni della produzione.

73%
monitora l'RTO

63%
monitora l'RPO

25%
monitora la frequenza dei test di ripristino

44%
monitora la quantità di dati ripristinati

Base: tutti gli intervistati n=100

Le aziende manifatturiere operano prevalentemente in ambienti ibridi, in cui si affiancano sistemi moderni e sistemi legacy. La connettività cloud nei sistemi di produzione è in aumento e molti produttori stanno ormai integrando i servizi cloud in una parte consistente dei propri ambienti. Tuttavia, i recenti episodi di interruzione del servizio da parte di fornitori di grande rilievo e gli incidenti nella catena di approvvigionamento stanno sollevando interrogativi su come le operazioni OT possano mantenere la propria resilienza quando le interruzioni hanno origine al di fuori dello stabilimento.

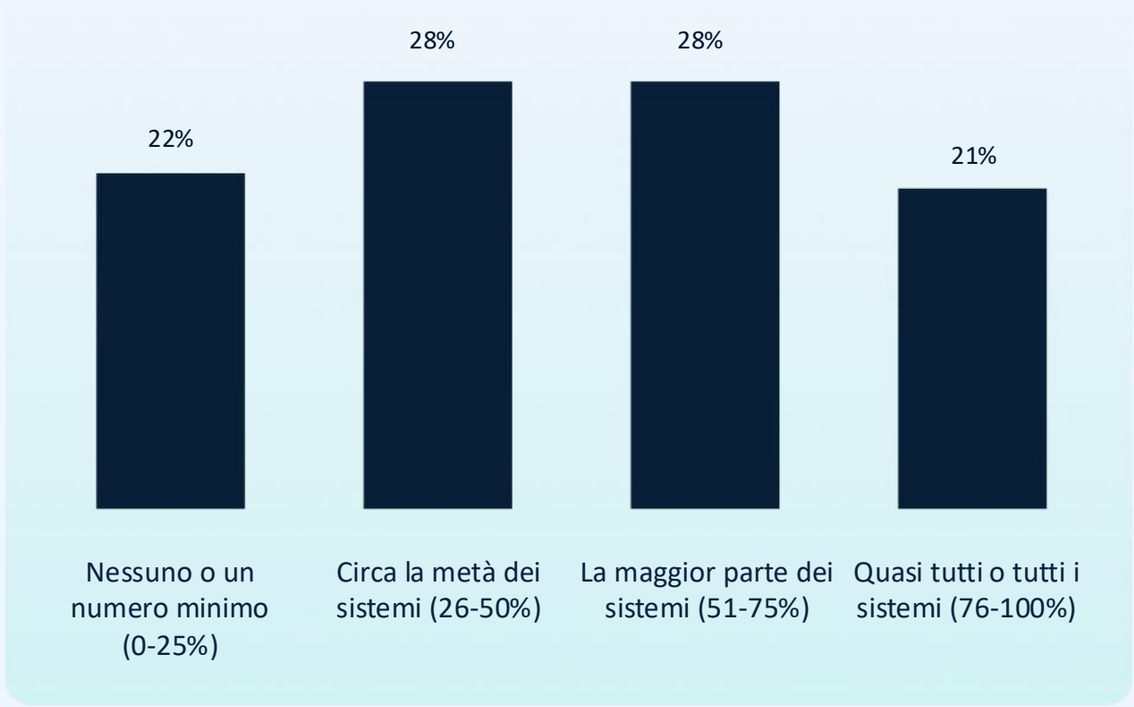
Infrastruttura IT e OT

47% Combinazione equilibrata - Presenza approssimativamente equivalente di sistemi moderni e legacy

42% Prevalentemente moderna - Maggioranza di sistemi attuali con alcuni sistemi legacy ancora in funzione

6% Completamente moderna - Tutti sistemi di ultima generazione e infrastrutture cloud

Sistemi manifatturieri e di produzione connessi al cloud



Base: tutti gli intervistati n=100

Rischi, resilienza e prestazioni di ripristino

Principali risultati

Le attività interne causano tempi di inattività con gravi conseguenze finanziarie

La maggior parte delle aziende manifatturiere subisce regolarmente tempi di inattività non pianificati dovuti a errori operativi e non da attacchi informatici. Tra le cause principali figurano mancanze nella manutenzione, errori di configurazione e guasti alle infrastrutture. La posta in gioco finanziaria è elevata, con molte aziende che subiscono perdite orarie importanti, eppure i tempi di ripristino superano costantemente le soglie accettabili. I test rivelano divari critici tra piani e prestazioni.

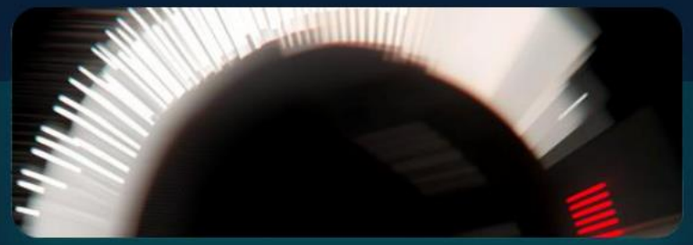
I test rivelano lacune critiche tra piani e prestazioni

Solo una piccola parte raggiunge gli obiettivi di ripristino dichiarati durante le esercitazioni di validazione; molte aziende registrano prestazioni significativamente più lente e alcune non effettuano mai test completi. Le organizzazioni monitorano regolarmente le metriche operative, ma conducono esercitazioni su larga scala solo una o due volte all'anno. Il completamento del backup viene monitorato continuamente, mentre la capacità di ripristino rimane non comprovata fino fino al verificarsi di guasti reali.

Dipendenze conformità e vicinanza dei fornitori orientano la strategia

Le aziende manifatturiere esprimono una diffusa preoccupazione riguardo alle le dipendenze da terze parti, e la maggior parte considera strategicamente importante l'ubicazione dei fornitori. La conformità aggiunge complessità attraverso molteplici quadri normativi con divergenze a livello regionale. Le recenti interruzioni hanno elevato la priorità del backup, sebbene molte aziende continuano a considerare la protezione dei sistemi in un'ottica di sicurezza informatica anziché da una prospettiva più ampia di resilienza operativa.

Principali risultati e priorità attuali



Spostare l'attenzione dalla prevenzione alla velocità di ripristino, poiché i problemi operativi interni causano la maggior parte dei tempi di inattività

Test regolari e completi devono sostituire le esercitazioni di disaster recovery poco frequenti per convalidare le capacità effettive

Dare priorità alla riduzione dei tempi di ripristino, considerando il notevole impatto finanziario delle interruzioni prolungate

La direzione IT guida il ripristino in quasi la metà delle aziende manifatturiere, mentre i team congiunti di coordinamento IT/OT se ne occupano in due quinti dei casi.

Tuttavia, i test evidenziano un divario preoccupante: solo il 18% rispetta o migliora i tempi di ripristino previsti, mentre il 48% impiega tempi leggermente più lunghi e il 26% si discosta significativamente dai propri RTO. Un ulteriore 6% non ha mai effettuato alcun test completo di ripristino, il che significa che opera senza una conoscenza comprovata delle proprie effettive capacità di ripristino.

18%

rispetta o migliora i tempi di ripristino previsti

48%

impiega tempi leggermente più lunghi

26%

non rispetta gli RTO

6%

non ha condotto test di ripristino completi

Responsabile del processo di ripristino in caso di inattività

Più elevato in Nord America (54%) rispetto al Regno Unito (27%)

Base: tutti gli intervistati n=100

Sebbene due terzi delle aziende manifatturiere esaminino le metriche di prestazione mensilmente o trimestralmente, le pratiche di convalida restano indietro. La metà testa i backup con una frequenza simile, ma il 60% conduce esercitazioni complete di disaster recovery solo due volte l'anno o una volta l'anno. Questo divario tra monitoraggio e convalida comporta che le organizzazioni controllino il completamento dei backup senza verificare regolarmente l'effettiva capacità di ripristino in caso di guasto dei sistemi.

Frequenza di...

Esame delle metriche di prestazione di backup e ripristino

68%

Mensile o trimestrale

Esercitazioni teoriche di backup o disaster recovery a livello aziendale

60%

Due volte l'anno o annuale

Test o convalida dei backup per garantire che i sistemi possano essere ripristinati correttamente

50%

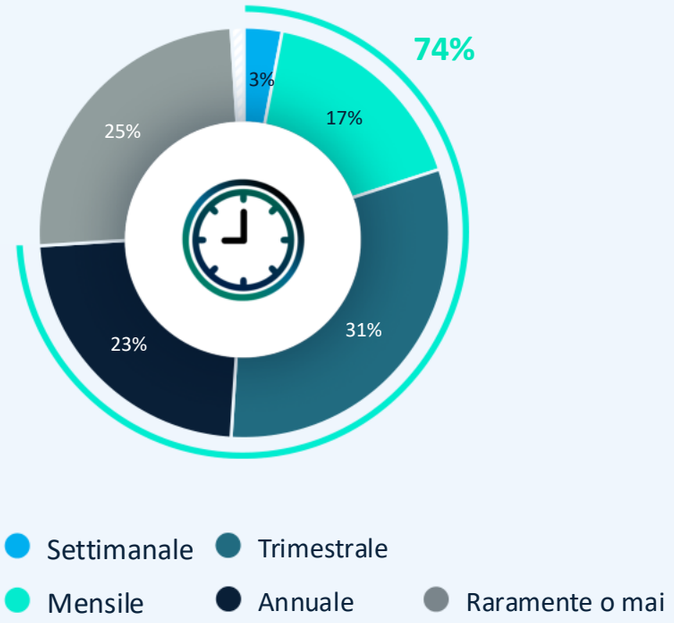
Mensile o trimestrale

Macrium Software | NewtonX®

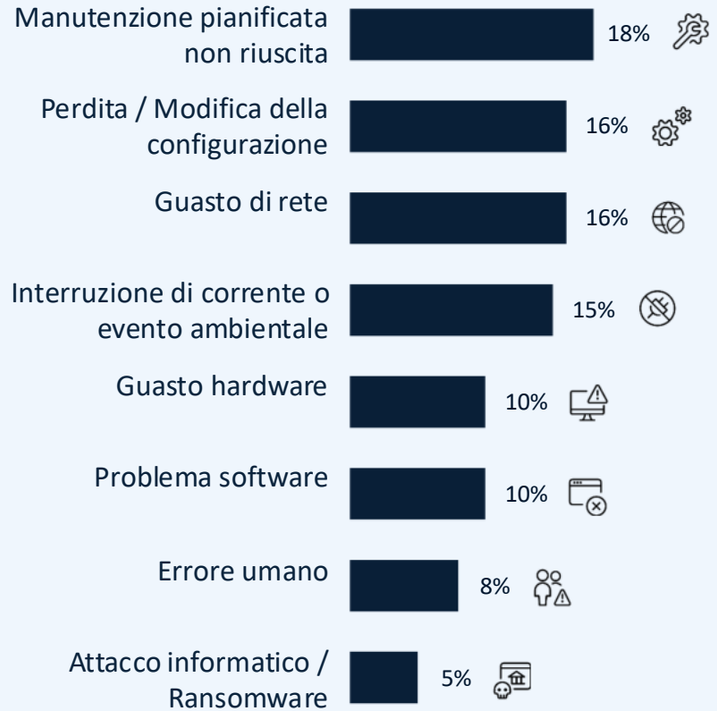
Base: tutti gli intervistati n=100

Tre quarti delle aziende manifatturiere subiscono tempi di inattività almeno una volta l'anno; la causa principale è la manutenzione non riuscita, seguita dalla perdita di configurazione e dai guasti di rete. Questo rivela che la maggior parte delle interruzioni deriva dalle attività interne piuttosto che da attacchi esterni. Quasi la metà delle aziende in Nord America e oltre un terzo di quelle nel Regno Unito stimano costi di inattività superiori a 100.000 dollari all'ora.

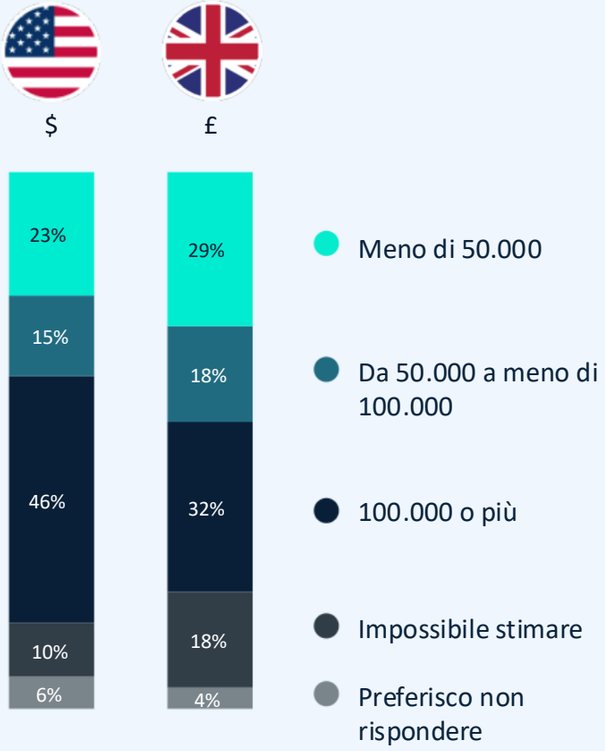
Frequenza dei tempi di inattività



Principali cause dei tempi di inattività



Costo orario dei tempi di inattività



Base: tutti gli intervistati n=100

Oltre la metà (55%) delle aziende del settore manifatturiero ha subito un attacco ransomware nell'ultimo anno, sebbene nella maggior parte dei casi sia stato possibile prevenirlo o contenerlo con successo: il 36% è stato bloccato completamente e l'11% è stato colpito con un impatto minimo. Tuttavia, l'8% ha subito significativi tempi di inattività operativa, a dimostrazione del fatto che le difese rimangono imperfette.

Ancora più preoccupante è la realtà dei tempi di ripristino: tre quarti delle organizzazioni richiedono oltre due ore per riprendere le attività.

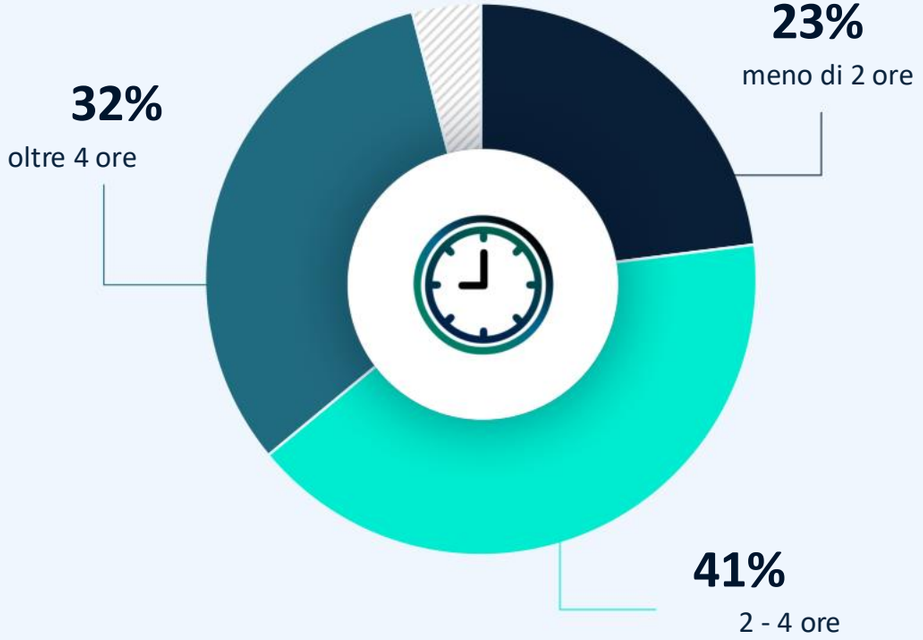
55%
ha subito un incidente ransomware nell'ultimo anno

36%
bloccato completamente

11%
rilevato con un impatto minimo

8%
tempi di inattività operativa significativi

Tempo di ripristino tipico durante l'inattività

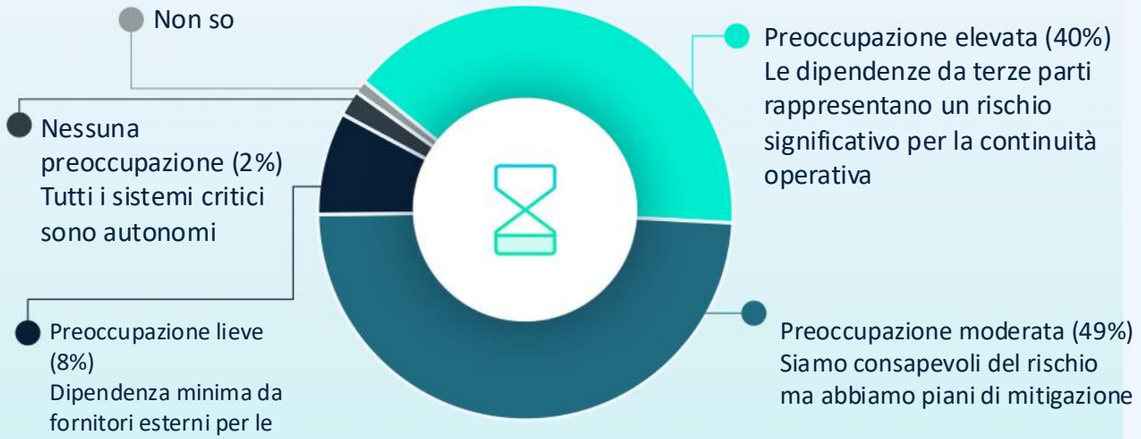


Il tempo di ripristino è più lungo in Nord America rispetto al Regno Unito (oltre 4 ore: 39% contro 12%)

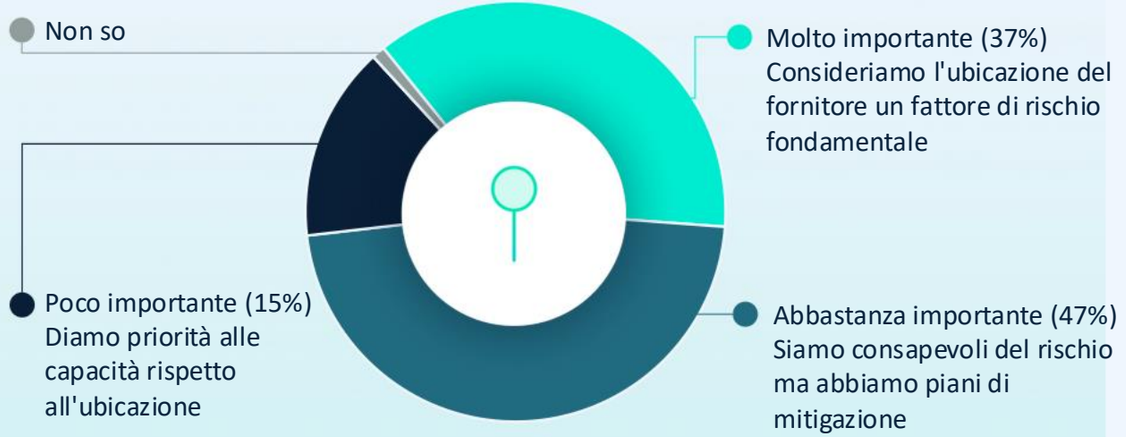
Base: tutti gli intervistati n=100

Quasi nove aziende manifatturiere su dieci esprimono preoccupazione per le dipendenze da terze parti, riflettendo una maggiore consapevolezza delle vulnerabilità della catena di approvvigionamento. Oltre quattro su cinque considerano inoltre importante l'ubicazione geografica del fornitore per la propria strategia di resilienza, suggerendo che l'efficacia del backup dipende non solo dalle capacità della soluzione, ma anche dalla vicinanza del fornitore, dalla sovranità dei dati e dal supporto locale negli scenari critici di ripristino.

Preoccupazioni per le dipendenze da terze parti e dalla catena di approvvigionamento durante l'inattività



Importanza dell'ubicazione del fornitore per la resilienza e la strategia dei dati



Le dipendenze da terze parti e dalla catena di approvvigionamento
Destano maggiore preoccupazione nel Regno Unito rispetto al Nord America (62% contro 32%)

Base: tutti gli intervistati n=100

Impatto delle recenti interruzioni sulle priorità di backup e ripristino

Le recenti interruzioni operative hanno determinato cambiamenti significativi nelle priorità relative al backup e al ripristino, con tre quarti delle aziende manifatturiere che segnalano un impatto di varia entità. Tra le organizzazioni colpite, il backup e il ripristino sono diventati una priorità di primo piano, con la metà che riferisce che i piani di resilienza sono attualmente in fase di revisione in risposta alle interruzioni di servizio.

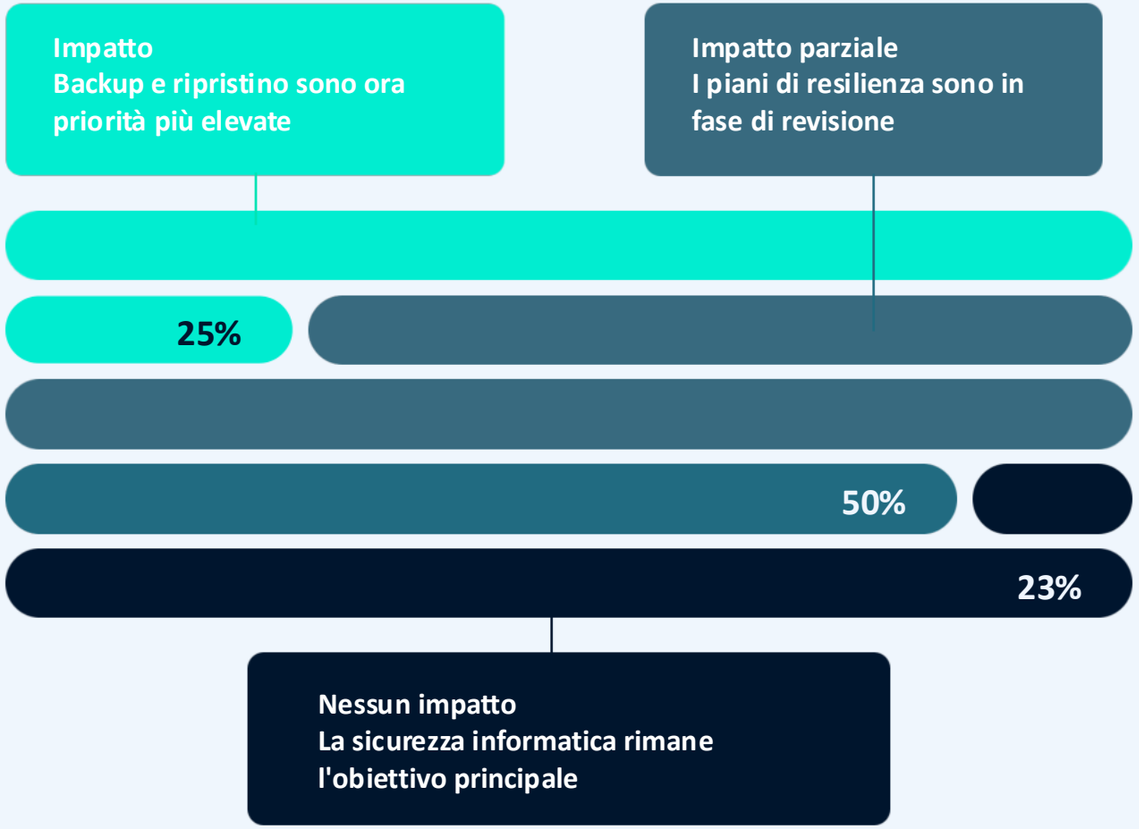
Solo il 23% indica che gli incidenti recenti non hanno influito sulle proprie priorità di backup, mentre la sicurezza informatica rimane il principale obiettivo strategico.

75%

un qualche livello di impatto

23%

sicurezza informatica come principale obiettivo strategico

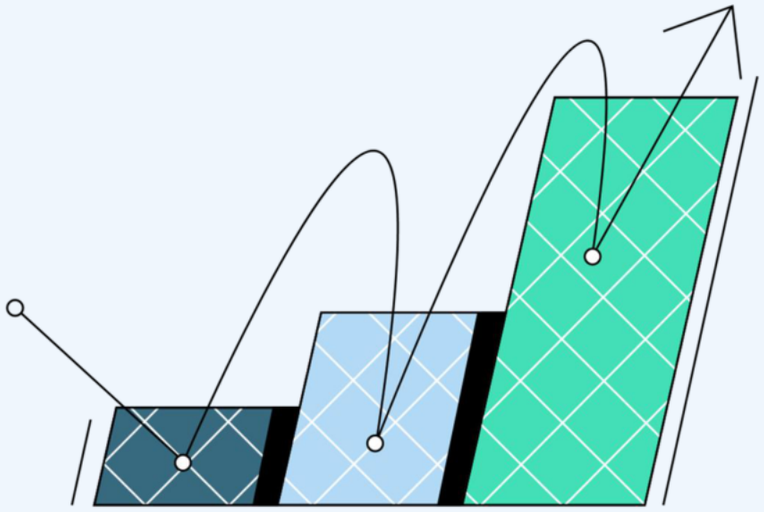


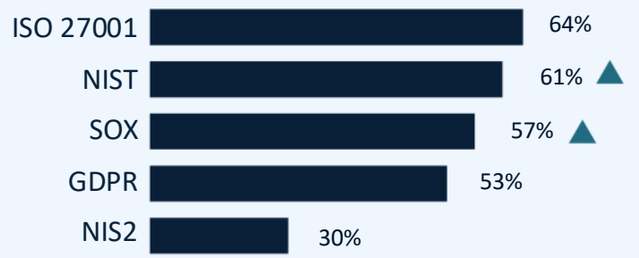
Base: tutti gli intervistati n=100

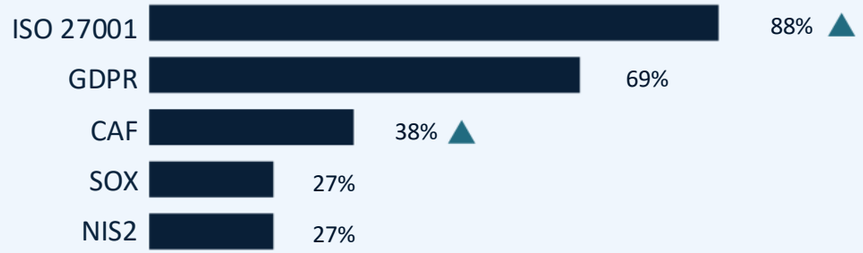
Framework di conformità rilevanti per le attività di backup e ripristino

ISO 27001 (gestione della sicurezza delle informazioni) è lo standard di conformità principale sia in Nord America sia nel Regno Unito. Il GDPR occupa una posizione di rilievo in entrambi i mercati a causa dei requisiti di protezione dei sistemi transfrontalieri.

Tuttavia, nelle normative secondarie emergono notevoli divergenze a livello regionale, il che suggerisce che i produttori debbano districarsi in un panorama normativo complesso e caratterizzato da molteplici quadri normativi, in cui standard universali come la norma ISO 27001 forniscono una copertura di base, ma le operazioni regionali richiedono misure di conformità aggiuntive e specifiche per il mercato che influenzano direttamente i requisiti in materia di backup e ripristino.







▲ ▲ = Più elevato per il mercato indicato

Base: tutti gli intervistati n=100 – Nord America = 74; Regno Unito = 26

Dinamiche organizzative e sfide

Principali risultati

Le attività interne causano tempi di inattività con gravi conseguenze finanziarie

La maggior parte delle aziende manifatturiere subisce regolarmente tempi di inattività non pianificati dovuti a errori operativi e non da attacchi informatici. Tra le cause principali figurano mancanze nella manutenzione, errori di configurazione e guasti alle infrastrutture. La posta in gioco finanziaria è elevata, con molte aziende che subiscono perdite orarie importanti, eppure i tempi di ripristino superano costantemente le soglie accettabili.
I test rivelano divari critici tra piani e prestazioni.

I test rivelano lacune critiche tra piani e prestazioni

Solo una piccola parte raggiunge gli obiettivi di ripristino dichiarati durante le esercitazioni di validazione; molte aziende registrano prestazioni significativamente più lente e alcune non effettuano mai test completi. Le organizzazioni monitorano regolarmente le metriche operative, ma conducono esercitazioni su larga scala solo una o due volte all'anno. Il completamento del backup viene monitorato continuamente, mentre la capacità di ripristino rimane non comprovata fino fino al verificarsi di guasti reali.

Dipendenze conformità e vicinanza dei fornitori orientano la strategia

Le aziende manifatturiere esprimono una diffusa preoccupazione riguardo alle le dipendenze da terze parti, e la maggior parte considera strategicamente importante l'ubicazione dei fornitori. La conformità aggiunge complessità attraverso molteplici quadri normativi con divergenze a livello regionale. Le recenti interruzioni hanno elevato la priorità del backup, sebbene molte aziende continuano a considerare la protezione dei sistemi in un'ottica di sicurezza informatica anziché da una prospettiva più ampia di resilienza operativa.

Principali risultati e priorità attuali

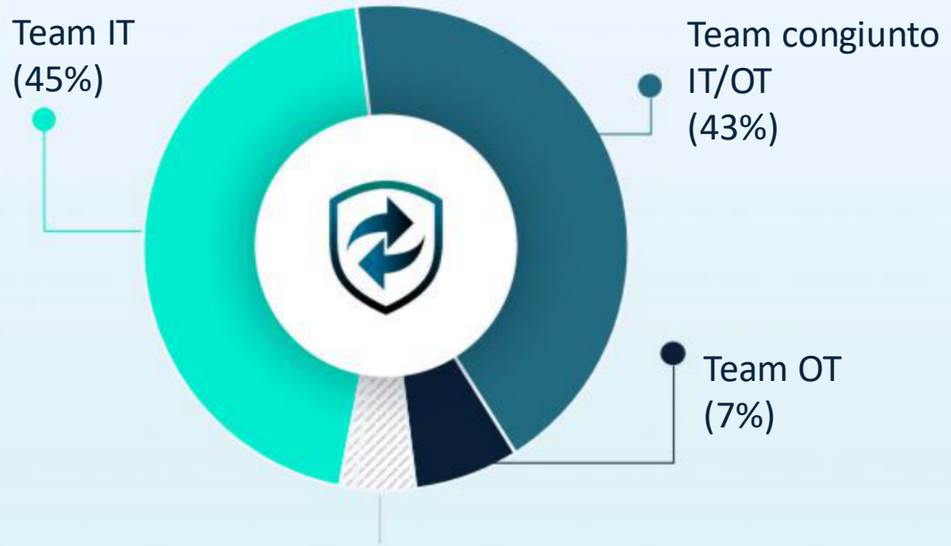
Affrontare la qualità delle attività operative interne come causa principale dei tempi di inattività

Aumentare la frequenza dei test per convalidare le capacità teoriche

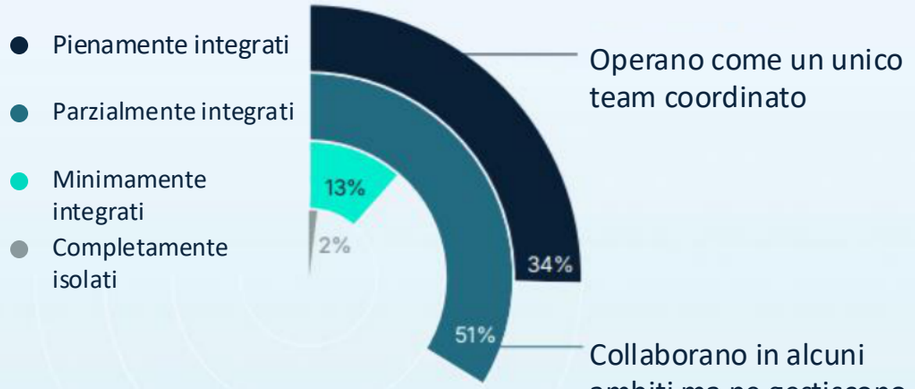
Adottare una mentalità orientata alla resilienza operativa, andando oltre gli approcci incentrati sulla sicurezza informatica

La responsabilità dei backup OT è ripartita in modo quasi equo tra i team IT e i team congiunti IT/OT, eppure solo un terzo di essi raggiunge una piena integrazione. La maggior parte delle organizzazioni opera con un coordinamento parziale, collaborando in alcuni ambiti mentre ne gestisce altri separatamente. Questa mancanza di coordinamento comporta un rischio significativo, poiché un backup OT efficace richiede una profonda conoscenza operativa che i team IT operanti in isolamento potrebbero non possedere.

Responsabili della gestione del backup e del ripristino OT



Integrazione dei team IT e OT per il backup e il ripristino



L'integrazione parziale / completa è più diffusa in Nord America (91%) rispetto al Regno Unito (69%)

Base: tutti gli intervistati n=100

Barriere culturali e complessità tecnica dominano le sfide della collaborazione IT/OT

45%
Barriere culturali e organizzative

Sfide legate alle dinamiche di gruppo, alla fiducia, alle priorità, alle mentalità e alla separazione tra i reparti IT e OT

20%
Integrazione tecnica e infrastruttura

Problemi relativi a sistemi legacy, strumenti incompatibili, segmentazione della rete e complessità tecnica dell'integrazione degli ambienti IT e OT

12%
Governance e chiarezza delle responsabilità

Mancanza di chiarezza nei ruoli, nelle responsabilità, nell'autorità decisionale e nella responsabilizzazione dei team IT e OT

8%
Vincoli di risorse e budget

Limitazioni finanziarie, priorità di budget concorrenti e risorse insufficienti per le iniziative di collaborazione

> "Lavoro isolato, scarsa comprensione delle integrazioni e delle dipendenze in un'architettura fortemente interconnessa."

Responsabile di reparto o di unità aziendale, produzione automobilistica, mezzi di trasporto e componenti, Regno Unito

> "La sfida principale è il contrasto tra priorità e culture. Per l'OT, la priorità principale è la continuità operativa e la sicurezza."

Responsabile di reparto o di unità aziendale, produzione per il settore sanitario e di dispositivi medici, Regno Unito

> "L'OT definisce la strategia, ma l'IT è responsabile dell'infrastruttura. Coordinarsi è quindi difficile."

Direttore senior o direttore, produzione alimentare, di bevande e di prodotti agricoli, Stati Uniti

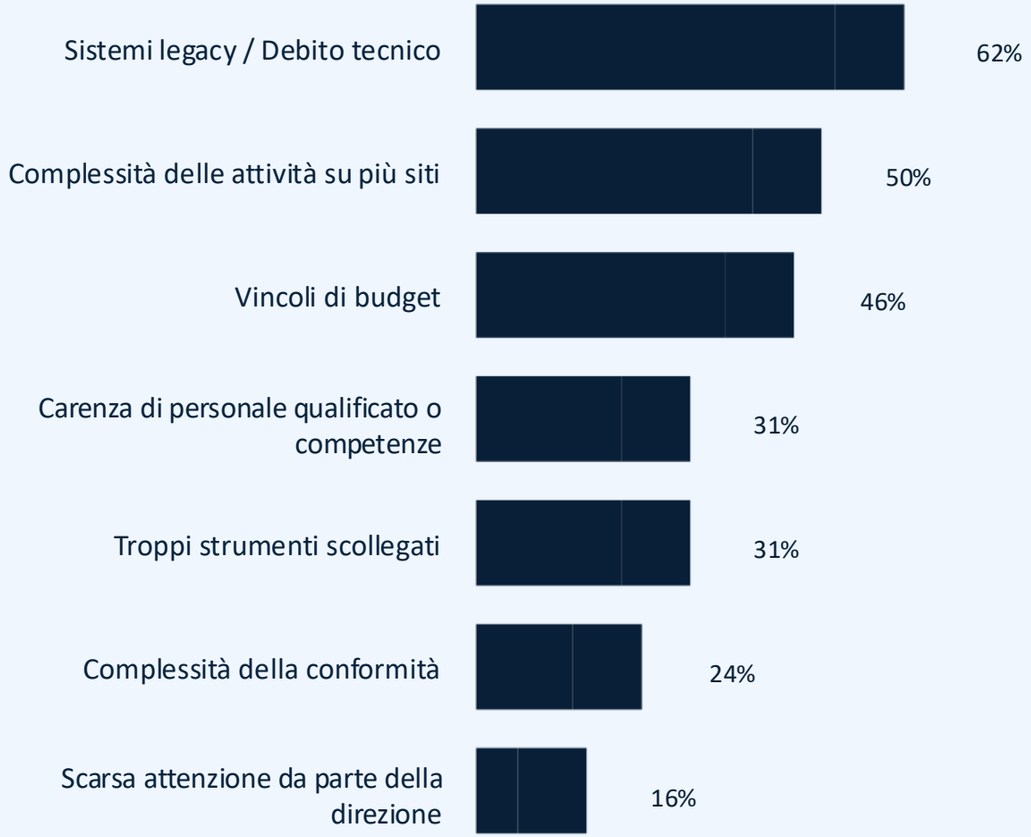
Macrium Software | NewtonX®

Base: tutti gli intervistati n=100

I sistemi legacy e il debito tecnico emergono come la sfida principale. A breve distanza seguono la complessità operativa legata alla presenza su più sedi e i vincoli di budget, delineando un trio di sfide strutturali che ostacolano in modo sostanziale il progresso.

È interessante notare come la carenza di personale qualificato e la frammentazione degli strumenti occupino posizioni di minor rilievo; ciò suggerisce che il problema non riguardi tanto le risorse o la proliferazione tecnologica, quanto piuttosto l'onere intrinseco di infrastrutture obsolete che resistono alla modernizzazione.

Principali sfide nel miglioramento del backup e del ripristino

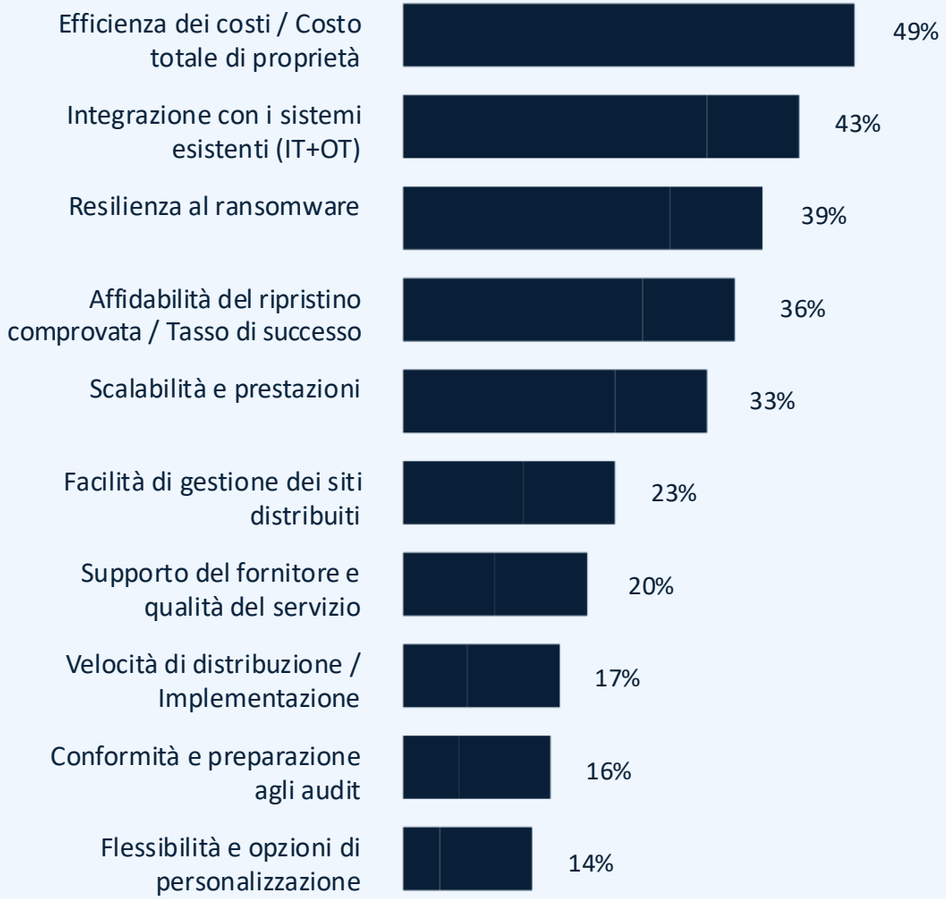


Base: tutti gli intervistati n=100

Nel valutare le soluzioni di backup e ripristino, le aziende privilegiano i risultati di business concreti rispetto alle funzionalità tecniche. L'efficienza dei costi (e il costo totale di proprietà) è il fattore predominante, seguito a breve distanza dall'integrazione con i sistemi IT e OT esistenti e dalla protezione contro i ransomware; si delinea così un chiaro podio che mette in risalto valore, compatibilità e sicurezza.

Le posizioni relativamente più basse della facilità di gestione, della qualità del supporto del fornitore e della preparazione alla conformità indicano che questi aspetti sono considerati requisiti di base piuttosto che elementi di differenziazione.

Fattori chiave nella valutazione o nel rinnovo delle soluzioni di backup e ripristino



Base: tutti gli intervistati n=100

Priorità di investimento e prospettive future

Principali risultati

Crescita degli investimenti trainata da minacce informatiche efficienza e modernizzazione delle infrastrutture

La stragrande maggioranza delle aziende manifatturiere prevede di aumentare la spesa per il backup, con la difesa informatica che emerge come la priorità assoluta. L'automazione dei processi e gli aggiornamenti infrastrutturali seguono a ruota, rivelando tre imperativi critici: proteggersi dalle minacce in continua evoluzione, migliorare l'efficienza operativa e affrontare le vulnerabilità dei sistemi obsoleti.

La consapevolezza della trasformazione digitale supera l'attuazione

Sebbene la maggior parte delle aziende manifatturiere riconosca l'importanza strategica della trasformazione digitale, molte meno hanno destinato risorse significative alla sua attuazione. Questo divario nell'esecuzione rivela che l'Industria 4.0 rimane in larga parte un'aspirazione anziché una realtà operativa.

Le organizzazioni sembrano essere frenate dalle stesse barriere che ostacolano la modernizzazione del backup: dipendenze dai sistemi legacy, limitazioni finanziarie e priorità concorrenti. Con la crescente interconnessione degli ambienti, questo ritardo crea esigenze di protezione sempre maggiori senza i corrispondenti investimenti in capacità.

Principali risultati e priorità attuali

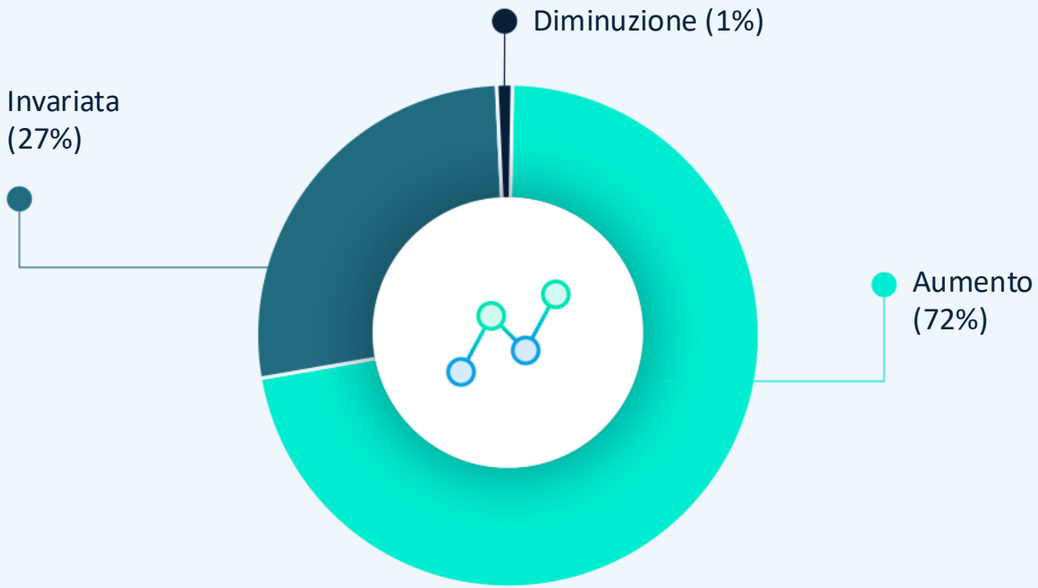
La resilienza informatica domina le decisioni di investimento e richiede soluzioni con capacità comprovate di difesa dalle minacce

La modernizzazione dei sistemi legacy crea opportunità di rinnovamento delle infrastrutture e potenziamento della protezione

La trasformazione digitale amplierà progressivamente i requisiti di protezione dei sistemi, ma i tempi degli investimenti rimangono incerti

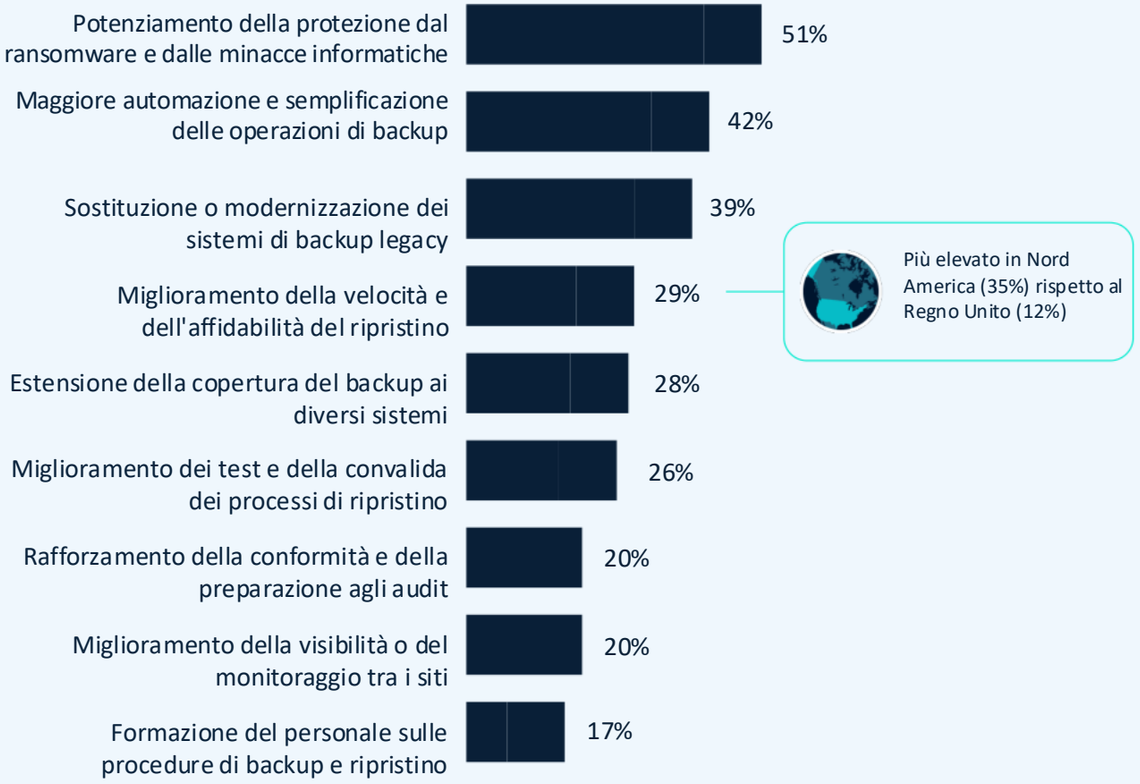
La stragrande maggioranza delle aziende manifatturiere sta aumentando gli investimenti nel backup, e quasi tre quarti prevedono una crescita del budget. La protezione dal ransomware domina le priorità di investimento, seguita da vicino dall'automazione e dalla modernizzazione dei sistemi legacy, riflettendo la triplice sfida dell'aumento delle minacce informatiche, delle esigenze di efficienza operativa e del debito tecnico.

Variazione prevista della spesa per backup e ripristino



Aumento medio della spesa del 12%

Ambiti prioritari di investimento



Base: tutti gli intervistati n=100

Attuale attenzione all'Industria 4.0 nelle organizzazioni

Sebbene il 51% delle aziende manifatturiere riconosca l'Industria 4.0 come un ambito importante, indicando una consapevolezza diffusa delle esigenze di trasformazione digitale, solo il 22% l'ha elevata a priorità strategica di primo piano, accompagnandola con investimenti concreti. Un ulteriore 20% la include nella pianificazione futura, mentre il 6% ne discute senza tuttavia disporre di piani definiti; ciò dimostra che, pur riconoscendone l'importanza, la stragrande maggioranza delle imprese non ha ancora stanziato risorse significative.

Questo significativo divario nell'esecuzione suggerisce che le organizzazioni incontrino ostacoli nel tradurre in pratica la visione della trasformazione digitale, frenate probabilmente dalla dipendenza da sistemi obsoleti, da vincoli di budget e da altre priorità operative concorrenti.

51%
la riconosce come ambito importante

22%
l'ha elevata a priorità strategica principale

20%
la considera per la pianificazione futura

6%
senza piani concreti

51%
L'Industria 4.0 è un ambito importante ma non ancora un investimento rilevante

22%
È una priorità strategica principale e un ambito di investimento attivo

Macrium Software | NewtonX®

Base: tutti gli intervistati n=100

Grazie

PER MAGGIORI INFORMAZIONI CONTATTARE:

Team marketing Macrium
channel@macrium.com

Macrium Software | NewtonX®