Enterprise Strategy Group | Getting to the bigger truth.™

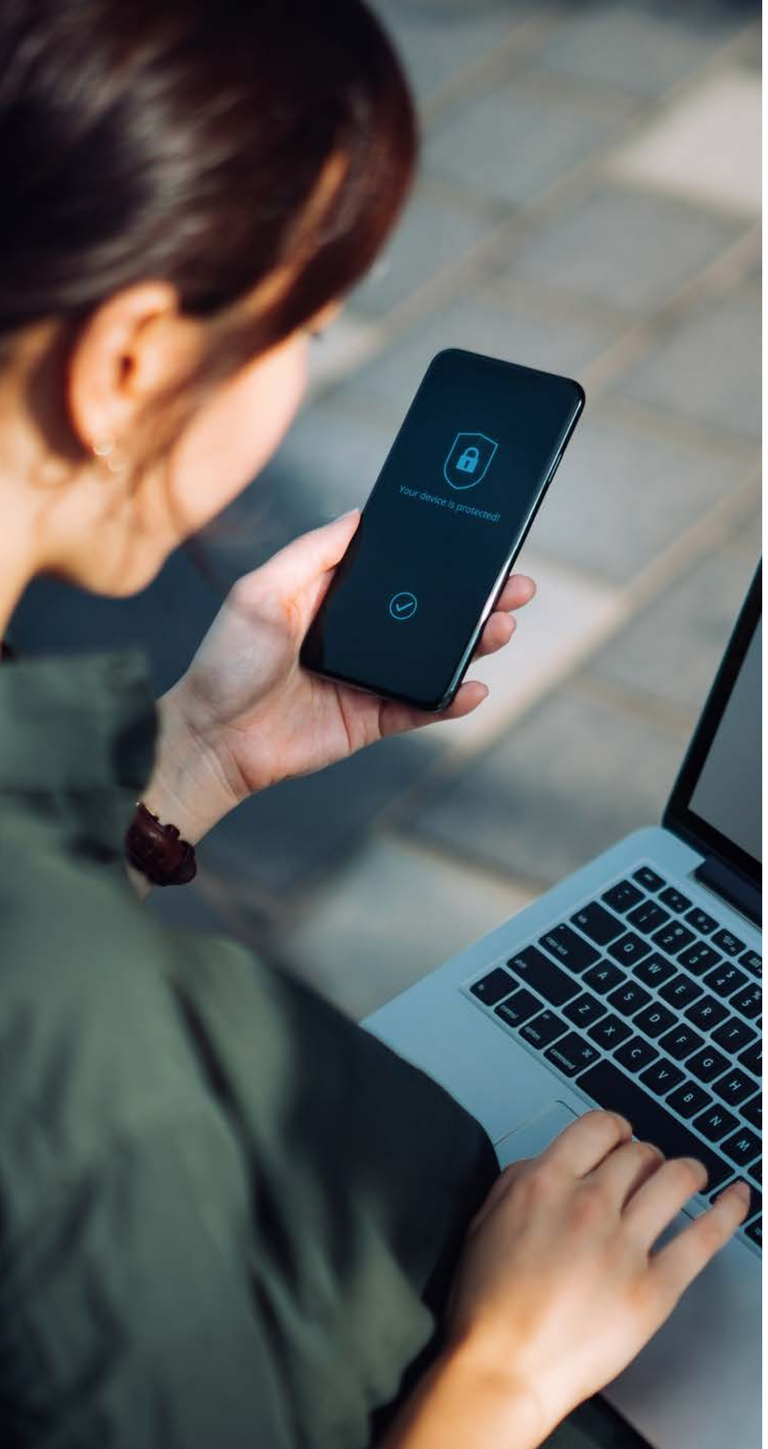
# Come creare un business cyber-resiliente pronto all'innovazione e alla crescita

**Adam Demattia,** Senior Director, Custom Research

MARZO 2022

# SOMMARIO






# Obiettivi e metodologia della ricerca

## OBIETTIVI:

Questo eBook esamina se e in che misura l'adozione di una solida strategia di cyber-resilienza da parte di un'organizzazione sia correlata alla prevedibilità IT, all'innovazione del business e al successo. Queste relazioni verranno individuate sulla base dei dati ottenuti dal confronto tra le organizzazioni della survey. Al termine della lettura di questo eBook sarà possibile:

- Comprendere come definiamo e misuriamo la cyber-resilienza e lo stato attuale della propria organizzazione.
- Quantificare i vantaggi delle organizzazioni altamente resilienti rispetto alle altre, in termini di prestazioni IT e di business.
- Infine, esaminando le misure messe in atto dalle organizzazioni cyber-resilienti, scoprire in che modo la propria organizzazione deve evolvere procedure e priorità per raggiungere prestazioni da leader di mercato.

## METODOLOGIA:

Nel primo trimestre del 2022, ESG ha condotto una survey in doppio cieco[1] su 750 responsabili delle decisioni IT e di sicurezza a conoscenza delle tecnologie di sicurezza informatica e resilienza adottate per proteggere il data center e gli ambienti dei dispositivi degli utenti finali.

Le organizzazioni rappresentate hanno incluso aziende del mercato di fascia media e grandi imprese e il campione è stato costituito da una combinazione orizzontale di settori verticali. La ricerca è stata anche di natura globale, coprendo Nord America (N=187), Europa occidentale (N=185), Asia Pacifico (N=179) e America latina (N=199).

[1] Intervistati anonimi e non informati che la survey veniva condotta da ESG né che era stata commissionata da Dell Technologies.



Torna a Sommario

## Risultati in evidenza

In questo eBook, le organizzazioni Preparate sono quelle con un livello ottimale di investimenti in tecnologie di sicurezza, dotazione di personale e rigorosi controlli dei rischi provenienti da terze parti. In base alla nostra ricerca, attualmente solo il 10% delle organizzazioni intervistate ha raggiunto questo livello di resilienza, evidenziando la necessità di maggiore focus e miglioramento da parte delle aziende.

Le organizzazioni cyber-resilienti riducono al minimo le interruzioni. Le organizzazioni Preparate presentano i seguenti risultati:

**Probabilità 7,3 volte maggiore**

di valutare eccellente il proprio livello di resilienza.

**Probabilità 2,5 volte maggiore**

di offrire un uptime pari o superiore al 99,99% per le proprie applicazioni business-critical, con un vantaggio stimato in termini di costo del downtime pari a $ 33,3 milioni.

**Agilità molto maggiore**

in termini di rilevamento degli incidenti (tempo medio di rilevamento [MTTD] più veloce del 20%) e di risposte agli incidenti (tempo medio di ripristino [MTTR] più veloce del 35%).

La cyber-resilienza è correlata al miglioramento delle prestazioni di business. Le organizzazioni Preparate presentano i seguenti risultati:

**Probabilità 8,5 volte maggiore**

di affermare che i punteggi di soddisfazione degli utenti finali superano in genere gli obiettivi, favoriti da un'assistenza e da un'esperienza dell'utente finale migliori.

**Probabilità 7,7 volte maggiore**

rispetto alle organizzazioni Esposte di immettere sul mercato nuove offerte prima della concorrenza.

Prevedono una crescita del fatturato dell'organizzazione

**2 volte superiore**

rispetto alle altre.



Torna a Sommario

# Definizione e misurazione della cyber-resilienza

# Quattro caratteristiche di un'organizzazione Preparata (o altamente resiliente)

Per stabilire se l'organizzazione di un intervistato poteva essere classificata come Preparata, abbiamo esaminato le loro risposte a quattro domande chiave riguardanti i livelli di personale addetto alla resilienza, le carenze di competenze, gli investimenti tecnologici e i processi di assessment dei rischi:

## PERSONE

**Come descriverebbe il livello di personale nel suo team di sicurezza informatica?**

- ☑ Nessuna posizione aperta
- ☐ Personale insufficiente, a corto di personale o adeguato

**Come descriverebbe il livello di competenze nel team di sicurezza informatica della sua organizzazione?**

- ☑ Nessuna carenza di competenze
- ☐ Molte carenze di competenze, varie carenze di competenze o adeguato

## TECNOLOGIA DI RESILIENZA

**Come definirebbe l'investimento della sua organizzazione in prodotti e servizi per proteggere sistemi, applicazioni e dati?**

- ☑ Soluzione ottimale
- ☐ Scarso, necessita di miglioramento o adeguato

## RISCHI PROVENIENTI DA TERZE PARTI

**L'organizzazione controlla o verifica la sicurezza dei suoi partner/vendor IT?**

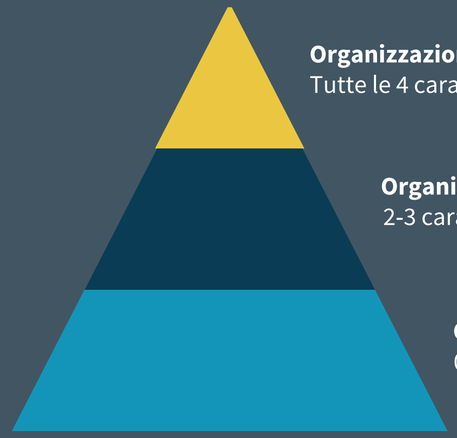
- ☑ In modo formale e rigoroso
- ☐ In modo informale, in modo occasionale o mai

## Ripartizione delle organizzazioni in base alla resilienza

(percentuale di intervistati, N=750)

ESG ha creato un modello basato sui dati che segmenta le organizzazioni degli intervistati in tre livelli di resilienza: **organizzazioni Preparate, organizzazioni Vulnerabili e organizzazioni Esposte.**

Il modello utilizza le quattro domande della survey riportate a sinistra come input per determinare lo stato di un'organizzazione. Ognuna di queste domande rappresenta una caratteristica delle organizzazioni Preparate (ovvero un attributo di un'organizzazione altamente resiliente) che si traduce in team in grado di assicurarne la protezione, finanziamenti alle tecnologie per la riduzione dei rischi o iniziative dell'organizzazione concentrate sul limitare il più possibile i rischi provenienti da terze parti. Quante più sono le caratteristiche di cui l'organizzazione dispone, tanto maggiore è la sua resilienza, come indicato di seguito:



**Organizzazioni Preparate:**
Tutte le 4 caratteristiche; 10% del mercato

**Organizzazioni Vulnerabili:**
2-3 caratteristiche; 26% del mercato

**Organizzazioni Esposte:**
0-1 caratteristica; 64% del mercato



Torna a Sommario

# Le organizzazioni cyber-resilienti riducono al minimo le interruzioni

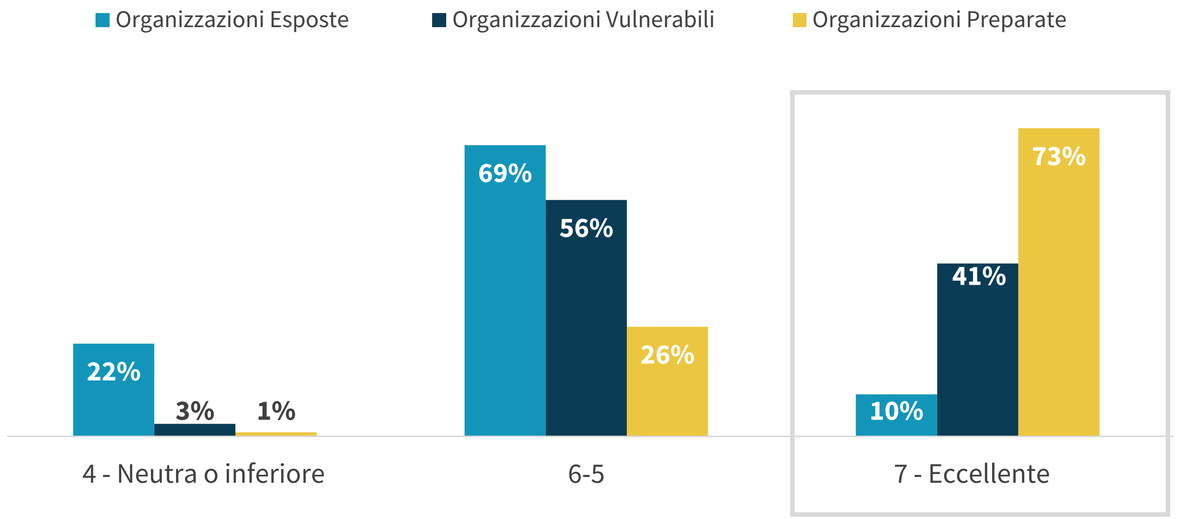
# Le organizzazioni Preparate sono molto più sicure della propria cyber-resilienza rispetto alle altre

A livello qualitativo, è importante misurare la fiducia dei leader IT e della sicurezza informatica nel livello di resilienza delle loro organizzazioni. Questi soggetti modellano e indirizzano le strategie delle proprie organizzazioni e sono nella posizione migliore per valutare il successo nell'attuazione di tali strategie.

Per misurare la fiducia, abbiamo chiesto agli intervistati di valutare la loro cyber-resilienza con un punteggio da 7 (eccellente) a 1 (scarsa). Gli intervistati hanno espresso una valutazione generalmente positiva, ma solo il 24% delle organizzazioni ha valutato eccellente la propria cyber-resilienza, segno di un tono nel complesso cautamente ottimistico.

In ogni caso, la fiducia varia notevolmente in base al livello di resilienza delle organizzazioni. Circa tre quarti delle organizzazioni Preparate (73%) valutano eccellente la propria resilienza.

Come valuterebbe la cyber-resilienza complessiva della sua organizzazione (ovvero la capacità di resistere a un attacco informatico e continuare le operazioni aziendali)? (Percentuale di intervistati)




Le organizzazioni Preparate hanno una

**probabilità 7,3 volte maggiore**

rispetto alle organizzazioni Esposte di valutare "eccellente" il proprio livello di resilienza.



Torna a Sommario

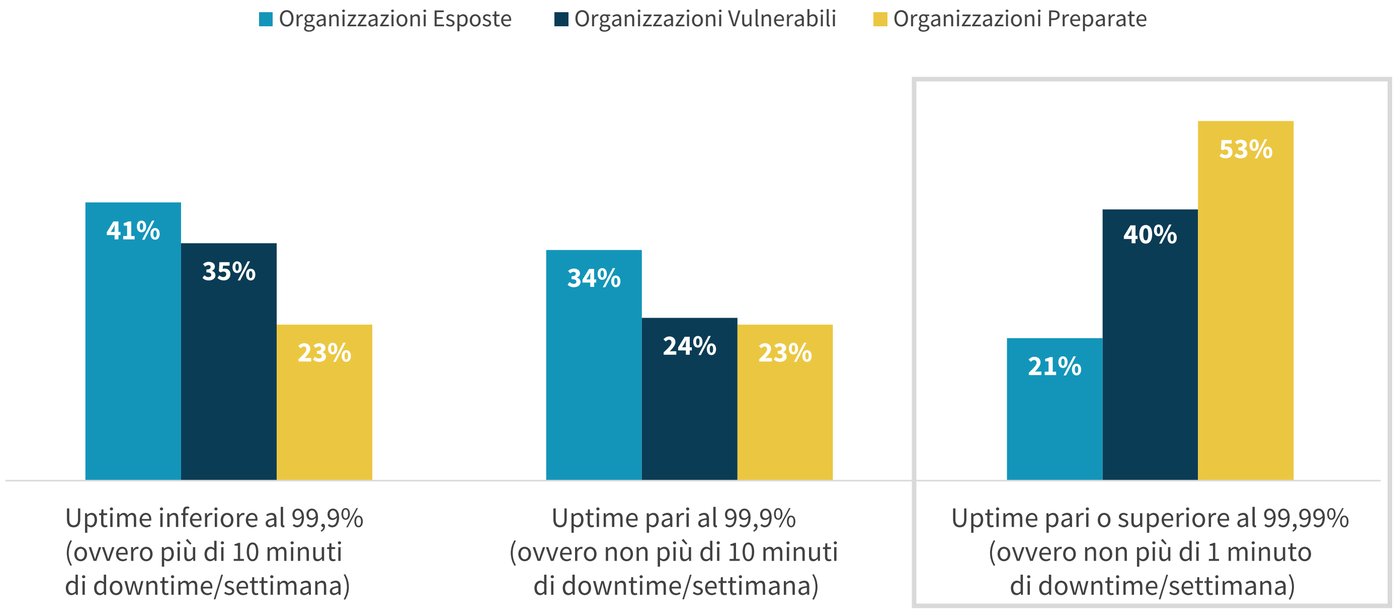
# Confronto dell'uptime delle applicazioni business-critical raggiunto a seconda dei vari livelli di cyber-resilienza

Oltre alle misurazioni qualitative della resilienza, altrettanto importanti, se non di più, sono le misurazioni quantitative riguardanti ad esempio uptime, tempo medio di rilevamento (MTTD) degli incidenti e tempo medio di ripristino (MTTR) dopo gli incidenti. Ciascuna di esse è stata sottoposta a benchmarking dalla ricerca.

Il fulcro della resilienza di un'organizzazione è la protezione dei processi business-critical. Per i team IT e di sicurezza, ciò significa mantenere operativi i carichi di lavoro delle applicazioni business-critical alla base di tali processi.

Mettendo a confronto il successo delle organizzazioni in quest'area, il divario appare evidente: le organizzazioni Preparate hanno una probabilità 2,5 volte maggiore rispetto alle organizzazioni Esposte di offrire un uptime del 99,99% o superiore per le app business-critical (pari a non più di 1 minuto di downtime a settimana, il 53% contro il 21%).

Qual è il tipico SLA che la sua organizzazione offre in termini di uptime per i carichi di lavoro business-critical?




Le organizzazioni Preparate hanno una

**probabilità 2,5 volte maggiore**

di offrire un uptime del 99,99% o superiore per le applicazioni business-critical.

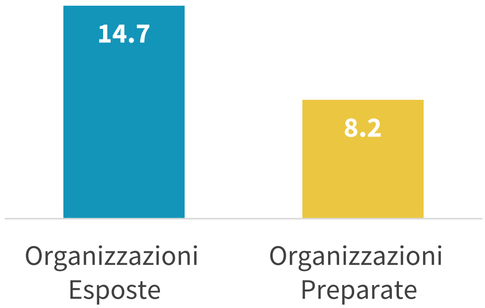


Torna a Sommario

# Qual è il vantaggio in termini di costo del downtime ottenuto dalle organizzazioni Preparate?

La ricerca ci consente di rispondere a questa domanda chiave. È ovvio che l'adozione di personale, l'investimento in tecnologie di resilienza e il controllo rigoroso dei rischi provenienti da terze parti comportano dei costi. Tuttavia, i dati ci mostrano la presenza di un notevole ritorno sul tale capitale investito: le organizzazioni Preparate riducono il downtime delle applicazioni business-critical del 44%. Combinando questi dati con il costo orario medio del downtime indicato dagli intervistati della ricerca e moltiplicando tale impatto economico per il numero totale di applicazioni business-critical, i dati mostrano che le organizzazioni Preparate ottengono un vantaggio in termini di costo del downtime di $ 33,3 milioni rispetto alle organizzazioni Esposte.

**DOWNTIME**
Ore medie di downtime per app all'anno




×

**COSTO ORARIO MEDIO DEL DOWNTIME [1]**

×

**NUMERO TOTALE MEDIO DI APPLICAZIONI BUSINESS-CRITICAL [2]**

=

**VANTAGGIO**
in termini di costo del downtime per le organizzazioni Preparate:

**$ 33,3 milioni/anno**



[1] Costo orario medio del downtime indicato dagli intervistati = $ 205.000, [2] Numero medio ipotizzato di applicazioni business-critical supportate: 25 (ipotesi conservativa)

Torna a Sommario

# Agilità di gestione degli avvisi e di risposta agli incidenti a seconda dei vari livelli di cyber-resilienza

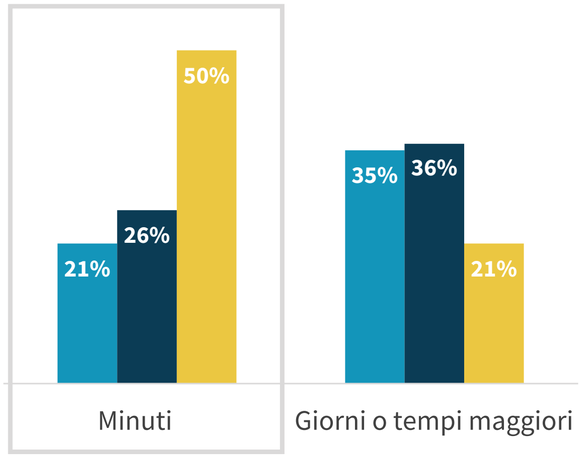
Per quanto riguarda il modo in cui le organizzazioni Preparate offrono uptime e disponibilità superiori, i dati sono ancora una volta chiari: la loro agilità è di gran lunga maggiore rispetto alle altre quando si tratta di analizzare, identificare gli incidenti e fornire loro risposta.

In tema di analisi e identificazione degli incidenti informatici, abbiamo definito l'MTTD come la quantità di tempo che intercorre tra il momento in cui viene generato un avviso e il momento in cui l'organizzazione esegue un'analisi completa per stabilire se si sia verificato un incidente di sicurezza. Le organizzazioni Preparate hanno una probabilità 2,4 volte maggiore rispetto alle organizzazioni Esposte di riuscire ad analizzare gli avvisi in pochi minuti (con un MTTD in media più veloce del 20%).

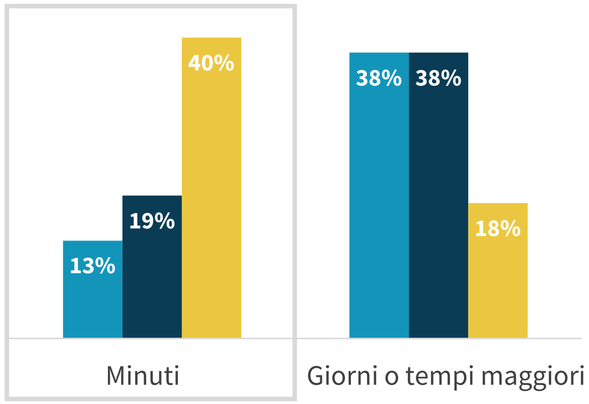
Per misurare l'agilità di risposta, abbiamo definito l'MTTR come la quantità media di tempo che intercorre tra la notifica di un incidente informatico e il ripristino completo delle operazioni del sistema informatico. Sulla base di questa misurazione, le organizzazioni Preparate hanno una probabilità 3,1 volte maggiore rispetto a quelle Esposte di eseguire il ripristino dopo gli incidenti solitamente in pochi minuti (con un MTTR in media più veloce del 35%).



Qual è il tempo medio di rilevamento (MTTD) degli incidenti della sua organizzazione per i carichi di lavoro business-critical? (Percentuale di intervistati)




Qual è il tempo medio di ripristino (MTTR) dopo gli incidenti della sua organizzazione per i carichi di lavoro business-critical? (Percentuale di intervistati)




Le organizzazioni Preparate hanno una

**probabilità 2,4 volte maggiore**

di analizzare gli avvisi solitamente in pochi minuti.

Le organizzazioni Preparate hanno una

**probabilità 3,1 volte maggiore**

di eseguire il ripristino dopo gli incidenti solitamente in pochi minuti.

Torna a Sommario


# Le organizzazioni cyber-resilienti superano le altre in termini di risultati di business

# Le organizzazioni resilienti forniscono un'esperienza degli utenti finali da leader di mercato

La resilienza, come molti aspetti dell'IT, ha l'obiettivo di essere invisibile agli utenti finali. È quando si verifica un evento imprevisto che si avvertono le carenze di resilienza.

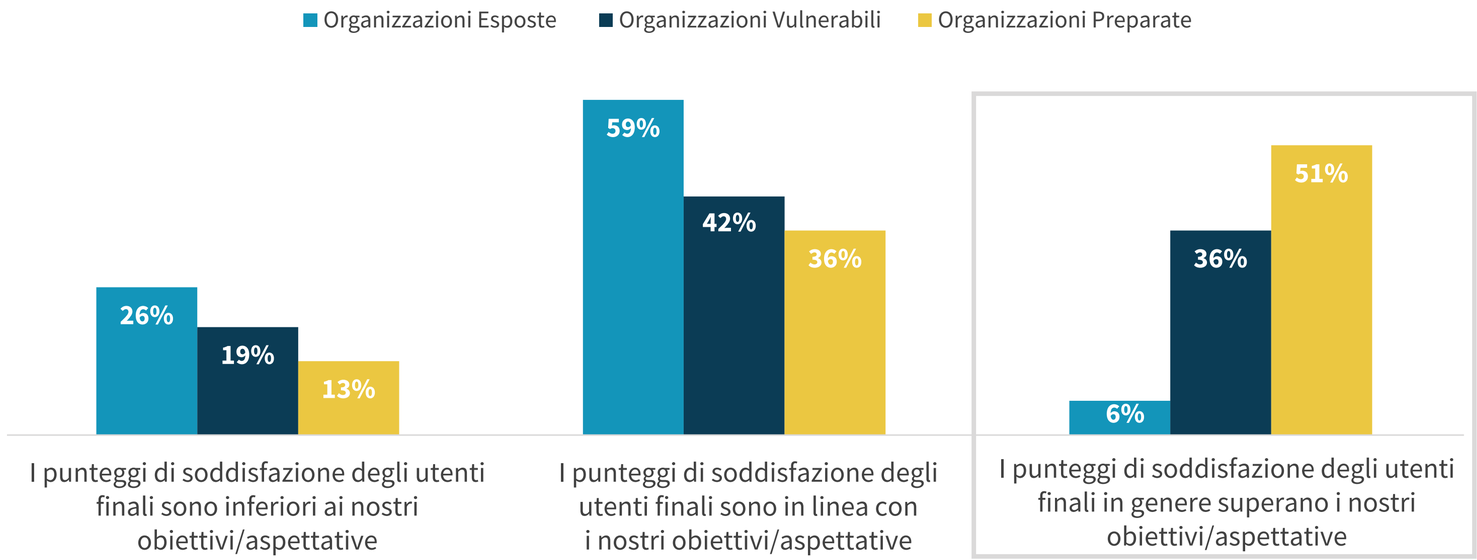
I dati mostrano che le organizzazioni Preparate operano a un livello superiore (rispetto alle altre) per quanto riguarda la limitazione delle interruzioni e che ciò si traduce in una maggiore soddisfazione degli utenti finali.

Abbiamo chiesto agli intervistati quali siano le prestazioni dell'organizzazione IT per quanto riguarda gli obiettivi di soddisfazione degli utenti finali. La maggior parte delle organizzazioni Preparate riferisce di superare in genere i propri obiettivi. Di fatto, le organizzazioni Preparate hanno una probabilità 8,5 volte maggiore rispetto alle organizzazioni Esposte di affermare che i punteggi di soddisfazione degli utenti finali superano in genere gli obiettivi.

Esiste una chiara correlazione tra il livello di resilienza e la capacità dell'IT di fornire l'esperienza degli utenti finali che i componenti delle linee di business richiedono.



Quali sono le prestazioni complessive della sua organizzazione IT in termini di obiettivi formali di soddisfazione degli utenti finali? (Percentuale di intervistati)




Le organizzazioni Preparate hanno una

**probabilità 8,5 volte maggiore**

di affermare che i punteggi di soddisfazione degli utenti finali superano in genere gli obiettivi.

Torna a Sommario

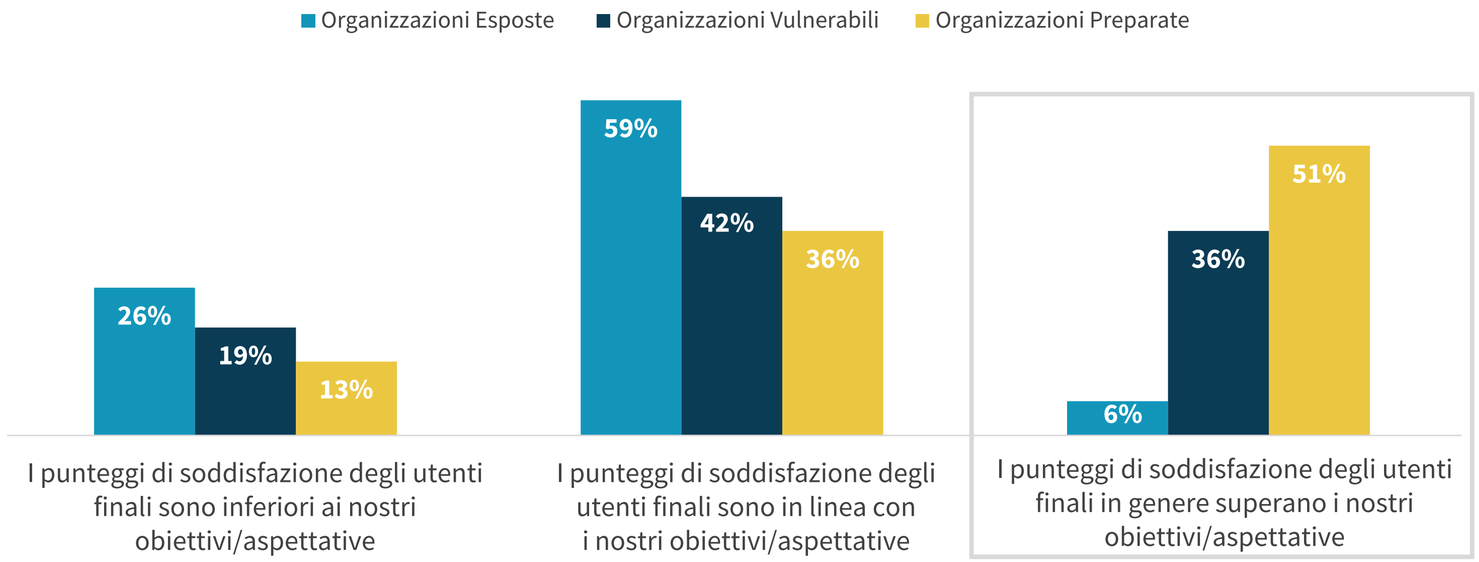
# Più che una semplice correlazione, la resilienza favorisce il miglioramento dell'esperienza degli utenti finali

Naturalmente, la correlazione non equivale a un rapporto di causalità, ma la ricerca fornisce la prova di un legame causale inequivocabile tra investimenti in resilienza e miglioramento dell'esperienza degli utenti finali.

Abbiamo chiesto agli intervistati se ritenessero che gli investimenti in resilienza delle loro organizzazioni avessero avuto un impatto positivo, neutro o negativo su aspetti quali l'agilità, l'innovazione e l'esperienza degli utenti finali. Alla domanda, l'87% ha indicato un impatto positivo.

Andando più a fondo ed esaminando i dati in base al livello di resilienza, le organizzazioni Preparate hanno una probabilità 3,2 volte maggiore rispetto alle organizzazioni Esposte di affermare che gli investimenti in resilienza hanno migliorato molto positivamente l'esperienza degli utenti finali, l'agilità e l'innovazione.

Gli investimenti in resilienza della sua organizzazione hanno avuto un impatto positivo/neutro/negativo sull'agilità, sull'innovazione e sull'esperienza degli utenti finali? (Percentuale di intervistati)




Le organizzazioni Preparate hanno una

**probabilità 3,2 volte maggiore**

di affermare che gli investimenti in resilienza hanno un impatto molto positivo.



Torna a Sommario

# Come gli investimenti in resilienza fanno la differenza per le aziende

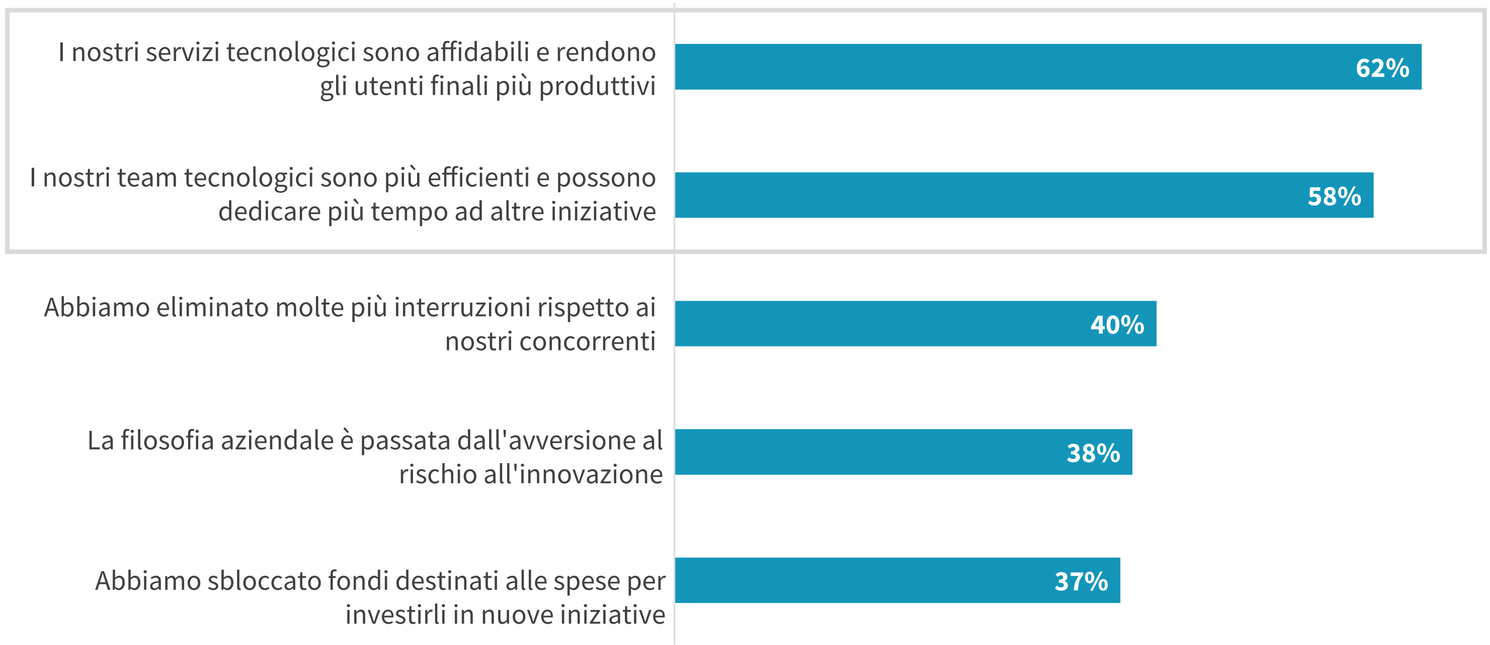
La ricerca ha dato risposta all'interessante domanda su come la resilienza migliori le capacità aziendali.

Si distinguono due effetti chiave complementari. Innanzi tutto, la resilienza diventa un'opportunità per le entità interessate e i centri di profitto dell'azienda: il 62% degli intervistati afferma che i propri investimenti contribuiscono a garantire la disponibilità e le prestazioni dei servizi tecnologici su cui gli utenti finali fanno affidamento per operare in modo efficace ed efficiente.

In secondo luogo, il 58% degli intervistati afferma che investire in una solida base di resilienza significa per i team tecnologici meno problemi da affrontare, consentendo loro di dedicarsi al supporto e all'accelerazione di iniziative e progetti innovativi che forniranno alle loro organizzazioni un vantaggio competitivo.

## "Si distinguono due effetti chiave complementari."

In che modo gli investimenti in resilienza contribuiscono al successo della sua azienda? (Percentuale di intervistati)





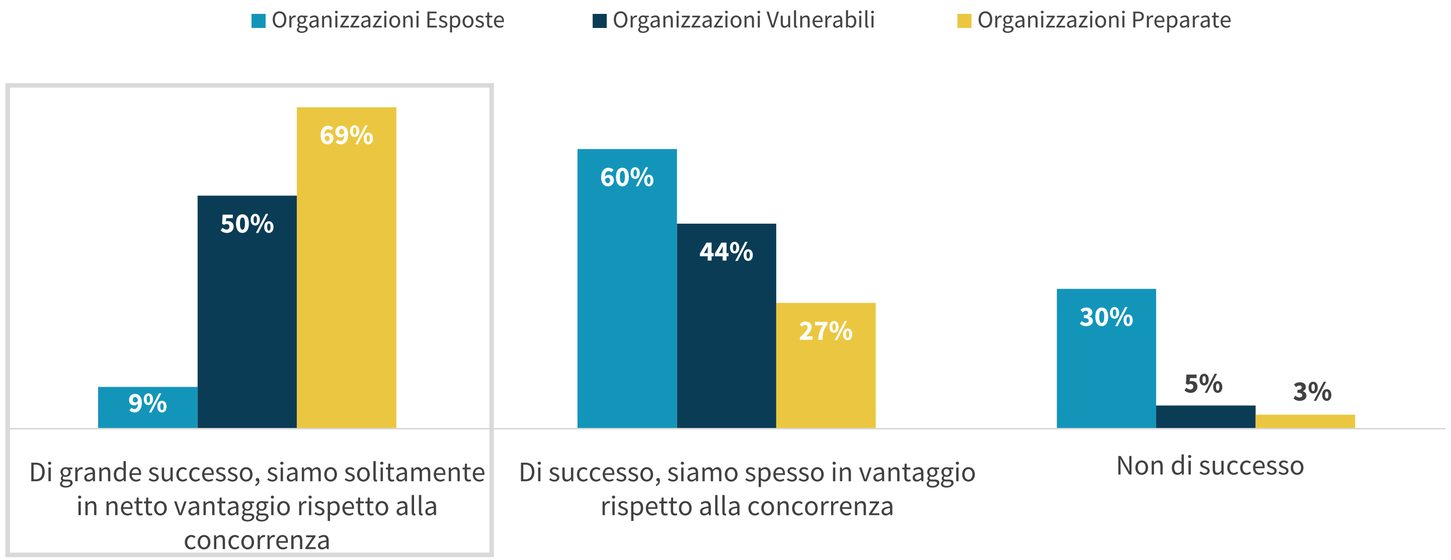

Torna a Sommario

# Le organizzazioni resilienti riescono a supportare meglio l'innovazione

I dati che indicano la capacità della resilienza di supportare l'innovazione delle organizzazioni sono evidenti. Le organizzazioni Preparate hanno una probabilità 7,7 volte maggiore rispetto alle organizzazioni Esposte di introdurre nuove offerte sul mercato solitamente prima della concorrenza.

Quando viene chiesto di esaminare più a fondo questo vantaggio, le organizzazioni Preparate riferiscono nel complesso che le loro organizzazioni sono in genere in anticipo di oltre 8 mesi rispetto ai concorrenti per quanto riguarda il time-to-market, ponendosi in una condizione di notevole vantaggio.

Con quale livello di successo la sua organizzazione sviluppa e lancia nuovi prodotti e servizi rispetto alla concorrenza? (Percentuale di intervistati)




Le organizzazioni Preparate hanno una

**probabilità 7,7 volte maggiore**

di immettere sul mercato nuove offerte prima della concorrenza.



Torna a Sommario

# Le organizzazioni resilienti sono più ottimiste in termini di futura crescita del fatturato

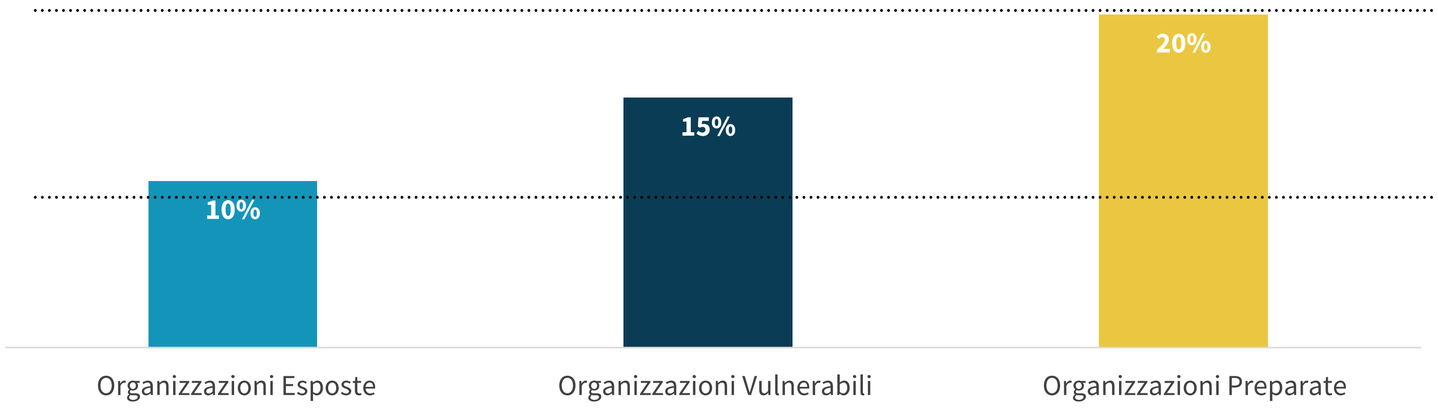
Oltre che con l'innovazione, la resilienza è in evidente correlazione con la crescita.

Abbiamo chiesto agli intervistati di prevedere a quale tasso si aspettano che il fatturato delle proprie organizzazioni cambierà nei prossimi anni.

In media (mediana), gli intervistati delle organizzazioni Preparate prevedono una crescita del fatturato a un tasso due volte maggiore rispetto alle organizzazioni Esposte.

La capacità di queste organizzazioni di eliminare le interruzioni, mantenere la produttività del personale e contribuire all'innovazione svolge un ruolo importante nel migliorare l'ottimismo aziendale degli intervistati.

A quale tasso annuo si aspetta che la sua organizzazione aumenti (o riduca) il fatturato di alto livello nei prossimi anni? (Mediana del tasso di crescita annuale)




Le organizzazioni Preparate prevedono una

**crescita del fatturato a un tasso 2 volte maggiore**

rispetto alle organizzazioni Esposte.



Torna a Sommario

# Come diventare un'azienda cyber-resiliente

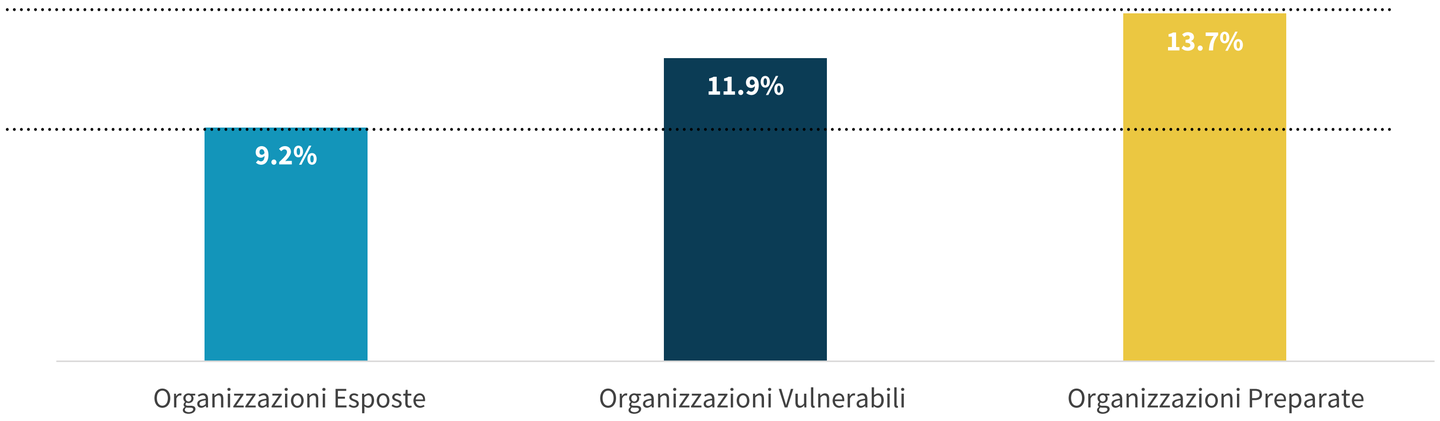
# Le organizzazioni Preparate assegnano più fondi alla sicurezza informatica rispetto alle altre

Sulla base dei nostri criteri di segmentazione, sappiamo che le organizzazioni Preparate finanziano le tecnologie di sicurezza informatica e resilienza a quello che ritengono sia un livello "ottimale", mentre le organizzazioni Vulnerabili ed Esposte ritengono che esistano margini di miglioramento.

Tuttavia, questi dati fuori da un contesto non sono utili per i leader IT e della sicurezza. Per approfondire l'argomento, abbiamo chiesto agli intervistati quale percentuale della loro spesa tecnologica viene assegnata alla sicurezza informatica. Ciò che abbiamo osservato è che le organizzazioni Preparate spendono circa il 14% del budget tecnologico per la sicurezza informatica, il 49% in più rispetto alle organizzazioni Esposte.

Le organizzazioni che spendono al di sotto di questa soglia dovrebbero ridistribuire i finanziamenti per allinearsi ai leader di mercato.

Quale percentuale del budget IT della sua organizzazione viene assegnata alla sicurezza informatica? (Media stimata)





In media, le organizzazioni Preparate investono il

**49% in più**

del budget tecnologico nelle aree della sicurezza informatica/resilienza.



Torna a Sommario

# Le organizzazioni Preparate dedicano più capitale umano alla sicurezza e alla resilienza

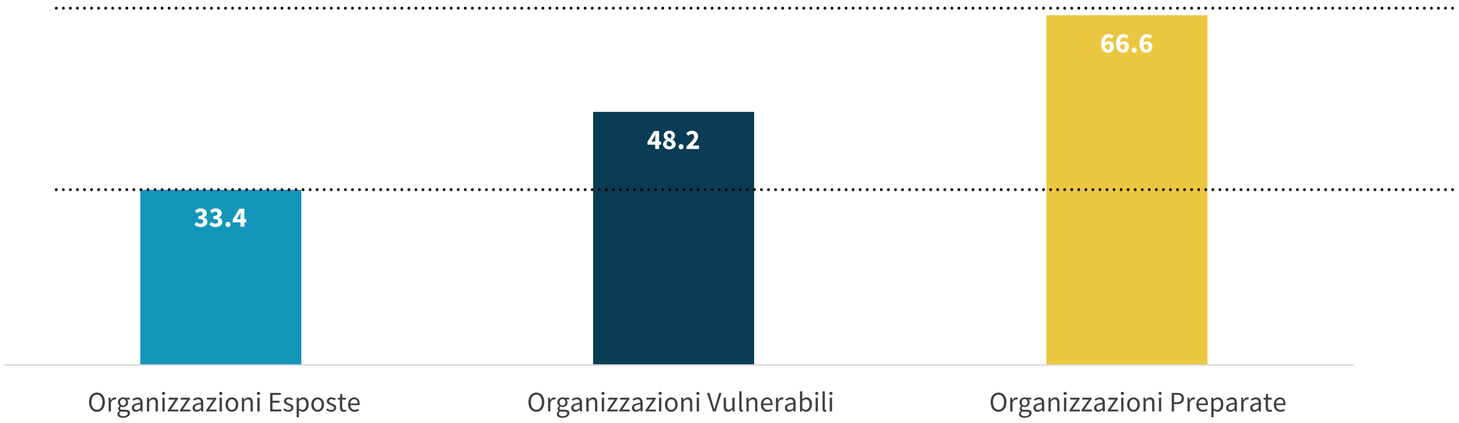
Come per i finanziamenti, sappiamo che le organizzazioni Preparate ritengono i propri team di sicurezza (inclusi i professionisti IT incentrati sulla sicurezza) ben dotati di personale. Tuttavia, osservando il numero medio di ETP assegnati in base al livello di resilienza, notiamo quanto la disparità sia ampia.

In media, le organizzazioni Preparate impiegano il doppio di ETP nei propri team di sicurezza rispetto alle organizzazioni Esposte (66,6 ETP contro 33,4).

L'analisi di questi dati in base alle dimensioni dell'azienda contribuisce a rendere queste informazioni ancora più utili.

- Le aziende Preparate del mercato di fascia media e di medie dimensioni (da 250 a 4.999 dipendenti) impiegano 62 ETP rispetto ai 27,7 ETP delle controparti Esposte.
- Le grandi imprese Preparate (oltre 5.000 dipendenti) impiegano 76,8 ETP rispetto ai 47,8 ETP delle controparti Esposte.

Approssimativamente, quanti ETP (equivalenti a tempo pieno) dedicati fanno parte del team di sicurezza informatica interno della sua organizzazione (contando i ruoli IT incentrati sulla sicurezza informatica)? (Media stimata)




In media, le organizzazioni Preparate impiegano un numero

**doppio di ETP**

nel loro team di sicurezza.



Torna a Sommario

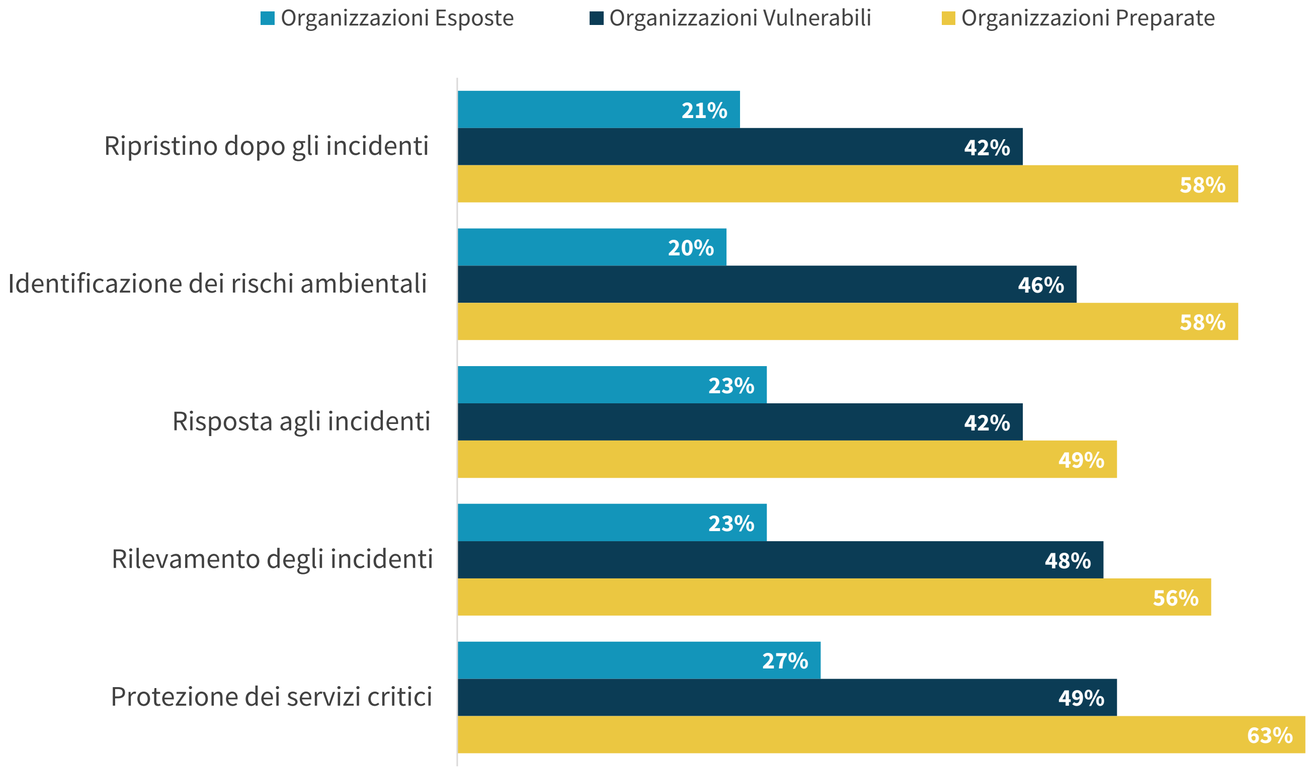
# Le organizzazioni Preparate hanno aumentato gli investimenti nell'intero ciclo di vita dei rischi

Nella survey è stato chiesto agli intervistati di pensare ai loro investimenti nell'intero ciclo di vita dei rischi (come definito da NIST CSF), dall'identificazione dei rischi fino al ripristino dopo gli incidenti.

Il tema comune? Le organizzazioni Preparate hanno una probabilità molto maggiore rispetto alle altre di avere aumentato gli investimenti in tutte le aree di oltre il 15% rispetto all'anno precedente.

Questo comportamento sottolinea la criticità di un approccio ai rischi di tipo "Defense in Depth", che fornisce alle organizzazioni le risorse necessarie per ridurre il rischio in ogni fase.

In quale delle seguenti aree di mitigazione dei rischi il livello dei nuovi investimenti della sua organizzazione negli ultimi 12-24 mesi ha superato il 15% rispetto all'anno precedente? (Percentuale di intervistati)






Torna a Sommario

# Le organizzazioni preparate rafforzano il proprio ambiente con tecnologie intrinsecamente sicure

Questo eBook si concentra sul concetto di resilienza aziendale e sui risultati associati a livello generale. La ricerca ha ulteriormente approfondito i vari aspetti degli ambienti delle organizzazioni, dallo storage ai server fino ai dispositivi client.

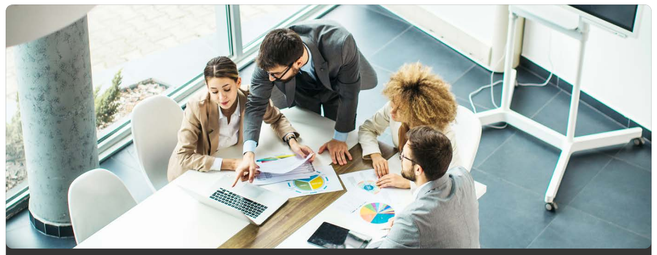
In ogni area, le organizzazioni Preparate sono leader di mercato in termini di adozione di tecnologie con funzionalità di sicurezza intrinseca e realizzano prestazioni superiori che vanno da riduzione del downtime a minori istanze di downtime fino al danneggiamento meno frequente dei dispositivi.

Le organizzazioni Preparate riducono le interruzioni dell'alimentazione e la perdita dei dati nel proprio ambiente di storage con soluzioni dotate di funzionalità intrinseche di protezione dei dati.

**LEGGI IL RIEPILOGO**

Le organizzazioni Preparate promuovono l'innovazione con l'automazione intelligente della sicurezza nel proprio ambiente di elaborazione.

**LEGGI IL RIEPILOGO**



Le organizzazioni Preparate riducono il danneggiamento dei dispositivi e limitano la perdita di dati con tecnologie client dotate di funzionalità di sicurezza intrinseca, con conseguenti risultati evidenti in termini di esperienza dei dipendenti.

**LEGGI IL RIEPILOGO**

Le organizzazioni Preparate danno priorità all'adozione di soluzioni tecnologiche dotate di sicurezza intrinseca. Ulteriori informazioni su questo concetto e sulle relative motivazioni.

**LEGGI IL RIEPILOGO**

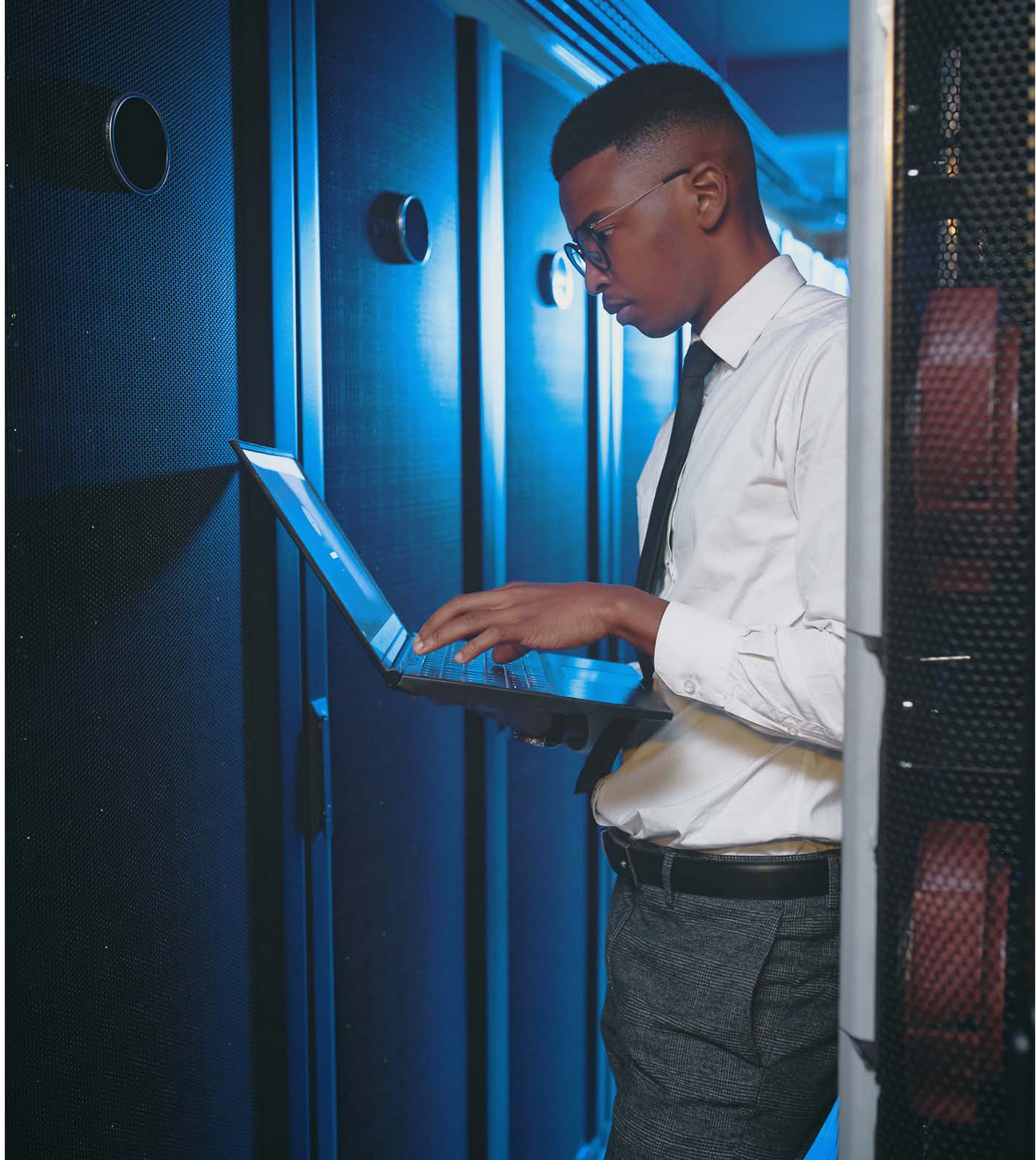


Torna a Sommario

# Conclusioni

Grazie alla loro capacità di mantenere produttivi gli utenti finali, rispondere rapidamente agli incidenti di sicurezza o consentire ai team tecnici di promuovere iniziative critiche di IT Transformation, le organizzazioni Preparate offrono un esempio interessante e basato sui dati a tutte le altre aziende per il raggiungimento di uno stato altamente resiliente. A seconda dello stadio in cui si trova oggi l'organizzazione, la strada da percorrere potrebbe apparire demoralizzante, ma questa ricerca può contribuire a creare il business case.

**In che modo Dell Technologies può essere d’aiuto**



# Dati demografici

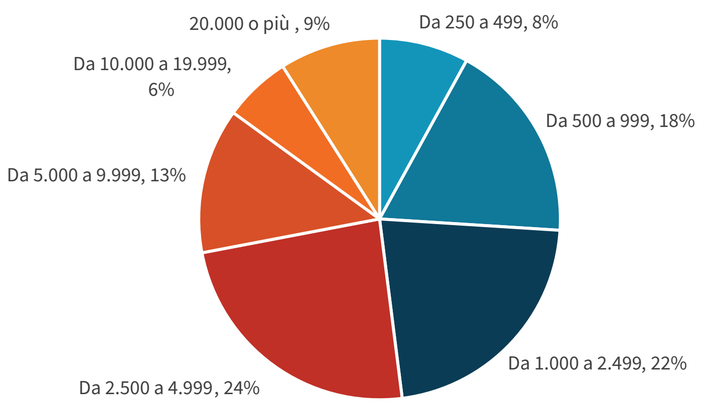
I dati contenuti in questo report derivano da una survey condotta tra l'11 gennaio e il 7 febbraio 2022. I grafici di seguito descrivono in dettaglio i dati demografici degli intervistati della survey situati in Nord America (N=187), Europa occidentale (N=185), Asia Pacifico (N=179) e America latina (N=199).

i totali nelle figure e nelle tabelle di questo report potrebbero non raggiungere il 100% per effetto dell'arrotondamento.

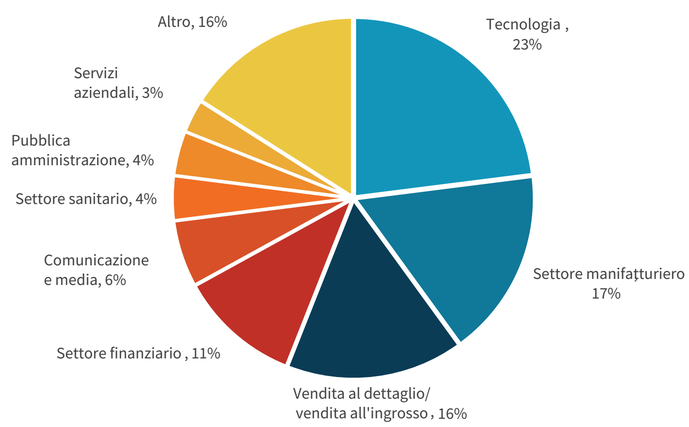
Il margine di errore per una dimensione del campione pari a 750 con livello di confidenza del 95% è di + o - 4 punti percentuali.

**INTERVISTATI PER MANSIONE**


**INTERVISTATI PER DIMENSIONE DELL'AZIENDA**




**INTERVISTATI PER SETTORE**






Torna a Sommario

## Informazioni su Dell Technologies, Intel e VMware

La tecnologia non è mai stata così importante come nell'attuale epoca basata sui dati e Dell crede che possa essere un'eccezionale forza propulsiva. Il nostro impegno è volto a salvaguardare il ruolo della tecnologia nel progresso umano e si traduce nel supporto alla pianificazione, alla preparazione e alla protezione dagli attacchi, che consente di promuovere l'innovazione con la massima sicurezza.


On-premise, nel public cloud o nell'edge, Dell Technologies e Intel collaborano per garantire prestazioni ottimali in un'ampia gamma di carichi di lavoro. Il portafoglio incentrato sui dati di Intel si basa su decenni di ottimizzazione delle applicazioni ed è progettato per aiutare le aziende a muoversi più velocemente, archiviare più dati ed elaborare di tutto dall'edge al cloud.


Insieme, VMware e Dell offrono un valore unico ai clienti condivisi. Le nostre soluzioni e piattaforme integrate, unite a una presenza su scala globale e al profondo coinvolgimento dei clienti, accelerano il percorso verso la Digital Transformation. Le innovative soluzioni VMware per la modernizzazione delle app, il multi-cloud e il software Anywhere Workspace si combinano con l'ampio portafoglio IT di Dell Technologies, che spazia dagli endpoint al cloud, per aiutare i clienti a realizzare operazioni protette e coerenti e un time-to-value più rapido.




Torna a Sommario


**Enterprise Strategy Group** è una società di analisi, ricerche e strategie integrate che offre alla community tecnologica globale servizi per contenuti Go-to-market, market intelligence e informazioni pratiche.