RIEPILOGO DELLA RICERCA ESG

Cyber-resilienza e prestazioni degli utenti finali

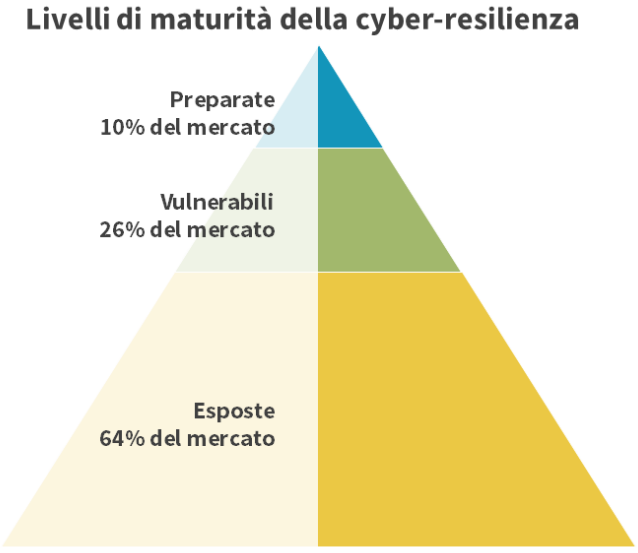
Data: marzo 2022 **Autore:** Dave Gruber, Principal ESG Analyst

ABSTRACT: la cyber-resilienza è un requisito essenziale per qualsiasi azienda. Ora che gli utenti lavorano da qualsiasi luogo, le organizzazioni devono gestire l'aumento delle superfici di attacco e investire in strategie consolidate per ridurre i rischi e agevolare i lavoratori. Dalla nuova ricerca di ESG emerge che gli investimenti in cyber-resilienza sono ancora più preziosi di quanto si pensasse in precedenza: oltre a ridurre al minimo il rischio, sono cruciali per innovare e crescere in un mondo basato sulla capacità di lavorare ovunque.

Panoramica della ricerca

Migliori capacità di cyber-resilienza contribuiscono a ridurre i rischi. Ma il livello di maturità della cyber-resilienza di un'organizzazione contribuisce anche a promuovere l'innovazione e ad accrescere il successo aziendale?

Per rispondere a questa domanda, ESG ha intervistato 750 responsabili delle decisioni IT, quindi ha assegnato gli intervistati alle diverse fasi della cyber-resilienza vedere il grafico a destra). Questa classificazione si è basata sulle risposte degli intervistati a quattro domande relative alla propria 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.



- Come descriverebbe il livello del personale nel suo team di sicurezza informatica?
- Come descriverebbe il livello delle competenze nel suo team di sicurezza informatica?
- Come definirebbe l'investimento della sua organizzazione in prodotti e servizi per proteggere sistemi, applicazioni e dati?
- L'organizzazione controlla o verifica la sicurezza dei suoi partner/vendor IT?

Per essere considerate Preparate, le organizzazioni devono dichiarare di non avere posizioni aperte da coprire nel loro team di sicurezza, di non avere team di sicurezza con lacune problematiche delle competenze, di finanziare in modo ottimale le tecnologie di sicurezza *e* di tenere formalmente e rigorosamente sotto controllo i rischi provenienti da terze parti. Le aziende con solo 2 o 3 di questi attributi sono state considerate Vulnerabili, mentre quelle con 0 o 1 Esposte.

Secondo i dati, solo il 10% delle organizzazioni rappresentate ha raggiunto lo stato Preparate, che corrisponde al più alto livello di maturità della cyber-resilienza.

Grazie al confronto delle prestazioni tecnologiche e aziendali in queste coorti, sia dal punto di vista quantitativo che qualitativo, la ricerca ha confermato la correlazione tra una maggiore cyber-resilienza e il miglioramento dell'uptime dei servizi IT, il rilevamento e la risposta più veloci agli incidenti, un aumento della soddisfazione degli utenti finali, livelli più alti di agilità nell'innovazione organizzativa e un outlook aziendale più positivo. La ricerca fornisce anche una roadmap empirica che le organizzazioni dovrebbero seguire per migliorare le proprie capacità e i propri risultati. Questo documento di riepilogo della ricerca si concentra sulle procedure per migliorare la maturità della cyber-resilienza che le organizzazioni dovrebbero applicare agli ambienti dei dispositivi per gli utenti finali.

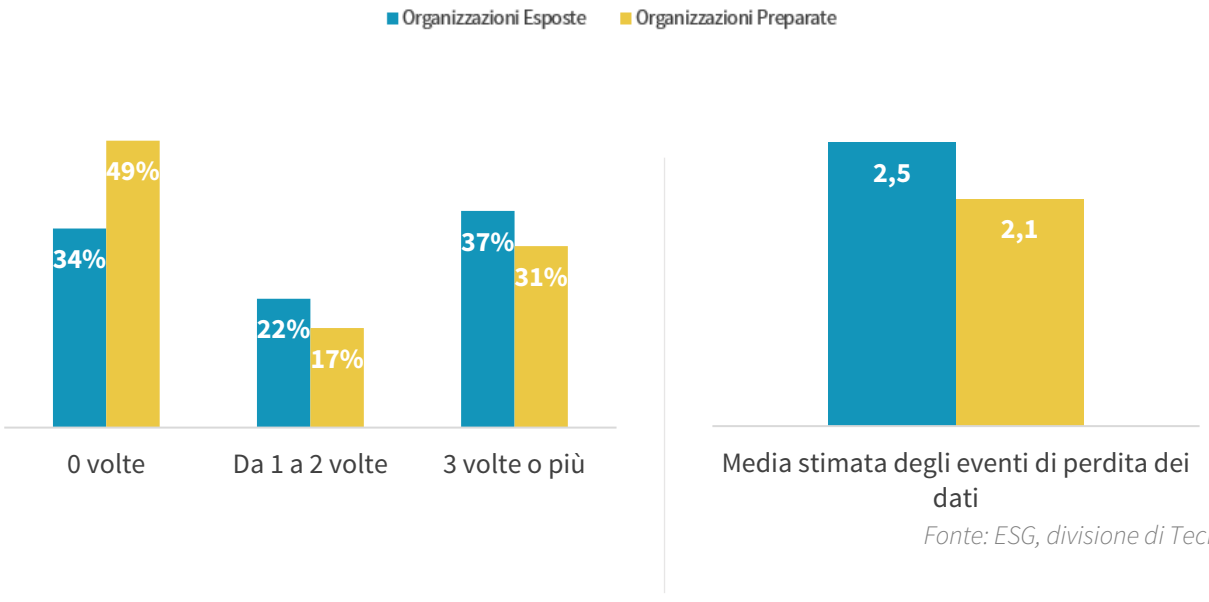
Sicurezza dei dispositivi degli utenti finali ed effetti correlati sulle organizzazioni cyber-resilienti

ESG ha riscontrato diverse differenze importanti tra le organizzazioni Preparate e le organizzazioni con livelli inferiori di maturità della cyber-resilienza, collegate al valore aziendale e all'utilizzo delle misure di sicurezza per i dispositivi degli utenti finali nella forza lavoro moderna e ibrida. In particolare, ESG ha rilevato che:

- Le organizzazioni Preparate **hanno una probabilità maggiore del 44%** di non incorrere in perdite di dati dovute a una compromissione dei dispositivi negli ultimi 12 mesi (vedere la Figura 1).
- Con una **probabilità quasi doppia** rispetto alle organizzazioni Esposte, meno dell'1% degli utenti delle organizzazioni Preparate ha affrontato un problema di sicurezza che ha richiesto la ricreazione dell'immagine del dispositivo. Ciò comporta che le organizzazioni Preparate **hanno una probabilità maggiore del 44%** di non incorrere in perdite di dati dovute a una compromissione dei dispositivi negli ultimi 12 mesi.
- Le organizzazioni Preparate, in media, **riducono la presenza di dispositivi non protetti del 33%.**

Figura 1. Le organizzazioni cyber-resilienti subiscono meno perdite di dati dovute a una compromissione dei dispositivi

Quante volte negli ultimi 12 mesi la sua organizzazione ha subito una perdita o una fuoriuscita di dati sensibili, in particolare in seguito a un'infezione da malware o a un altro tipo di compromissione di un notebook/PC desktop? (Percentuale di intervistati e media stimata degli eventi di perdita dei dati)

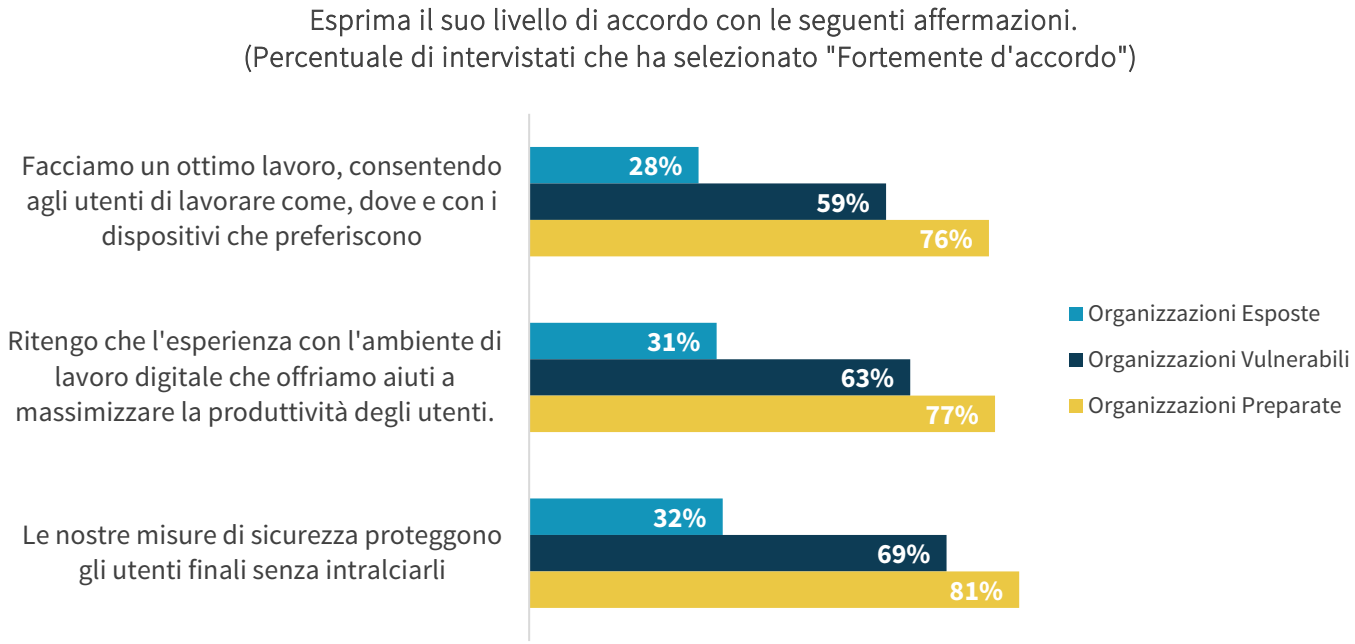


Fonte: ESG, divisione di TechTarget, Inc.

La soddisfazione dei lavoratori delle organizzazioni Preparate è maggiore

Le organizzazioni Preparate sottolineano il vantaggio di consentire ai lavoratori di scegliere dove e come lavorare, che produce punteggi di soddisfazione più alti per le esperienze di lavoro digitali. Nello specifico, ESG ha rilevato che le organizzazioni Preparate hanno una probabilità 2,7 volte superiore di percepire come un vantaggio la possibilità che offrono ai lavoratori di svolgere il proprio lavoro dove e con i dispositivi che preferiscono (vedere la Figura 2).

Figura 2. La cyber-resilienza rende più produttivi i lavoratori



Fonte: ESG, divisione di TechTarget, Inc.

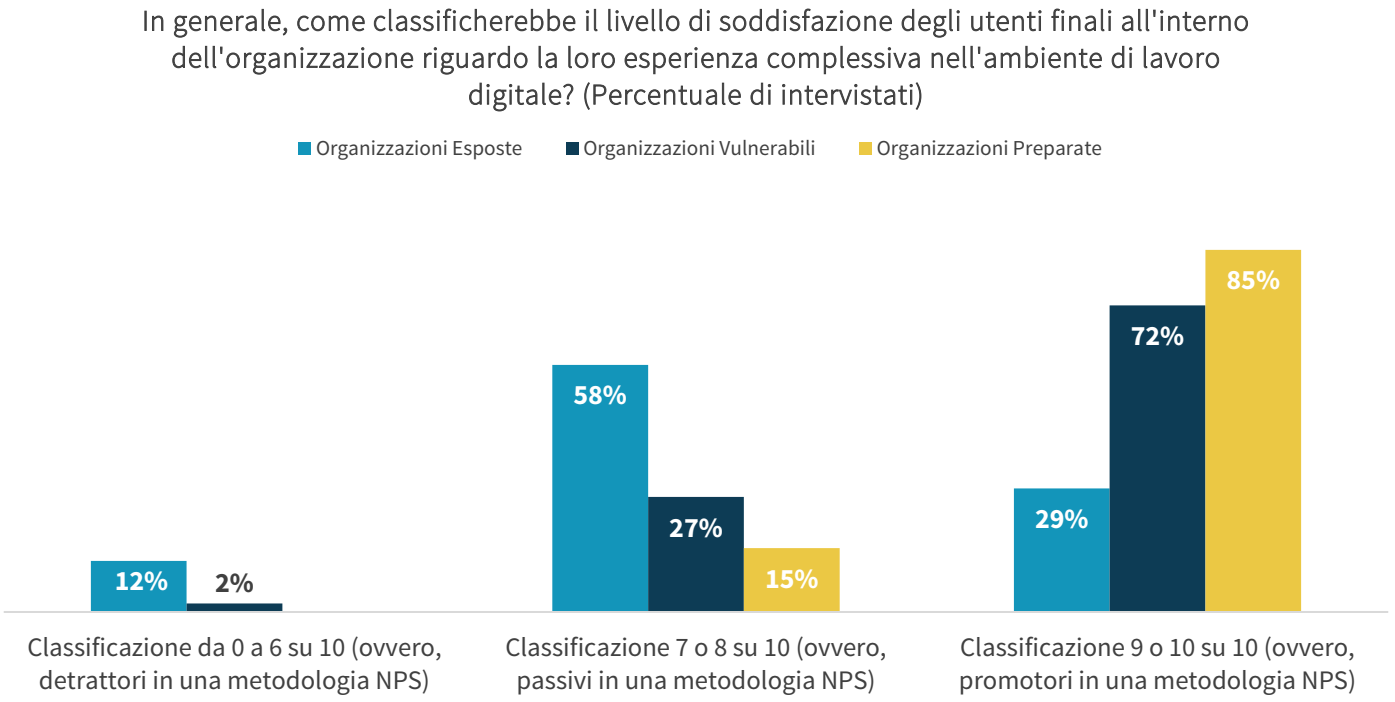
Il collegamento tra cyber-resilienza e soddisfazione degli utenti finali

Quando i lavoratori sono liberi di svolgere le proprie attività senza problemi dove e come preferiscono, possono rimanere concentrati sugli obiettivi aziendali principali. La ricerca mostra che i lavoratori delle organizzazioni Preparate assegnano ai loro team IT un punteggio di soddisfazione 5 volte maggiore rispetto agli utenti delle organizzazioni Esposte, relativamente alla possibilità di consentire il lavoro digitale (in base a una metodologia NPS) (vedere la figura 3).[1]

Gli utenti delle organizzazioni Preparate assegnano ai loro team IT un punteggio di soddisfazione 5 volte maggiore rispetto agli utenti delle organizzazioni Esposte.

1 L'85% delle organizzazioni Preparate descrive i propri utenti finali come "promotori", assegnando alla loro esperienza di lavoro digitale una valutazione di 9 o 10, mentre nessuno li descrive come "detrattori", con un risultato pari a +85 NPS per la coorte delle organizzazioni Preparate. Al contrario, solo il 29% delle organizzazioni Esposte descrive i propri utenti finali come "promotori", mentre il 12% li descrive come "detrattori", con un conseguente punteggio di +17 NPS per la coorte delle organizzazioni Esposte.

Figura 3. La cyber-resilienza aumenta la soddisfazione dei lavoratori



Fonte: ESG, divisione di TechTarget, Inc.

Conclusioni

Gli investimenti nella cyber-resilienza sono necessari, considerato il ruolo critico che i team IT e di sicurezza svolgono in tutta l'organizzazione. Di fronte al crescente volume delle minacce, la cyber-resilienza è già un aspetto prioritario all'interno di ogni organizzazione.

Da questa ricerca di ESG, tuttavia, si evince anche che il valore della cyber-resilienza fornita attraverso funzionalità di sicurezza intrinseca si estende ben oltre la semplice riduzione dei rischi operativi. Gli investimenti nella cyber-resilienza si traducono in un ambiente più favorevole e positivo per la produttività e l'innovazione. Quando i dipendenti possono lavorare ovunque in modo sicuro, sono liberi di concentrarsi maggiormente sull'innovazione.

Leggi l'eBook

Come ottenere l'aiuto di Dell Technologies

Informazioni su Dell Technologies

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.

Informazioni su Intel

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.

Informazioni su VMware

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.

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

www.esg-global.com contact@esg-global.com + 1 508.482.0188