

# Acronis Cyber Protection Week 2021

Acronis

Sondaggio deepdive regionale:  
Europa, Medio Oriente e Africa (EMEA)

**Paesi:** Germania, Svizzera, Regno Unito, Belgio, Paesi Bassi, Svezia, Francia, Italia, Spagna, Bulgaria, Emirati Arabi Uniti, Arabia Saudita, Sudafrica

**Intervistati:** 2.600 utenti e professionisti IT



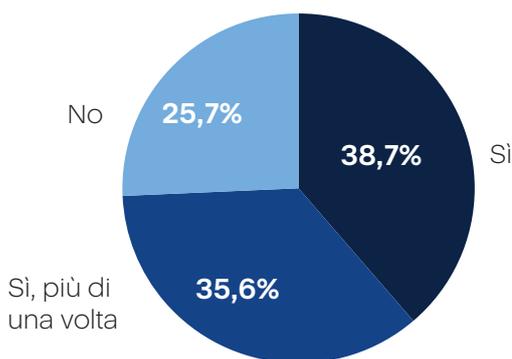
## UTENTI IT - CONCLUSIONI PRINCIPALI

Le sfide, le preoccupazioni e le vulnerabilità riferite dagli utenti di tecnologie IT ad uso personale in Europa, Medio Oriente e Africa sono condivise dal resto del mondo.

## LE MISURE DI PROTEZIONE DEI DATI SONO INADEGUATE

Nell'area EMEA, un allarmante 87% di utenti di IT ad uso personale ignora le best practice di backup, ad esempio la regola del 3-2-1. Quasi tre quarti degli intervistati hanno dovuto eseguire un ripristino avvalendosi di backup non ottimizzati e solo il 26% dichiara di non aver subito una perdita di dati irrecuperabile.

Avete mai sperimentato la perdita definitiva di dati o di un dispositivo?



## LE ESIGENZE AUMENTANO, LA CYBER SECURITY NON TIENE IL PASSO

Solo il 68% di utenti di IT ad uso personale installa le patch di sicurezza il giorno stesso in cui vengono diffuse. Al contempo, il 70% non utilizza affatto tecnologie antimalware oppure utilizza un antimalware che non previene gli attacchi zero-day; quasi altrettanti intervistati (circa il 66%) riferiscono di non essere in grado di capire se qualcuno ha avuto accesso o ha modificato i dati in modo insolito.

Queste lacune di sicurezza sono amplificate dall'utilizzo più intensivo dei dispositivi registrato nel corso dell'anno: l'84% segnala un uso più frequente rispetto al solito, con un raddoppio nell'11% dei casi. Ai criminali informatici si presenta quindi un'opportunità ancora più grande, con i dati e la privacy di questa fascia di utenti esposti a un rischio più elevato.

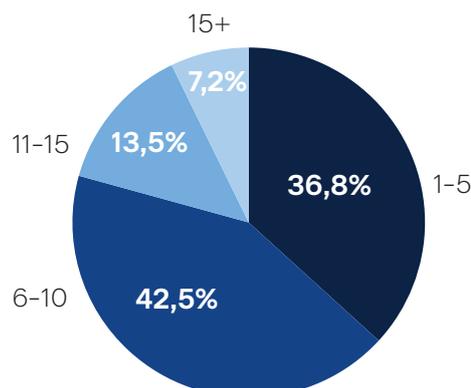
## PROFESSIONISTI IT - CONCLUSIONI PRINCIPALI

I professionisti dell'IT nell'area EMEA hanno predisposto i propri stack IT con soluzioni di Cyber Security e protezione dati, ma registrano ancora perdite di dati e interruzioni operative.

## LE RICHIESTE DI PROTEZIONE AFFIDABILE SONO SEMPRE PIÙ PRESSANTI

Quasi l'80% degli utenti di IT ad uso professionale nell'area EMEA è tenuto al rispetto di almeno una normativa sulla privacy dei dati. Per far fronte a questa esigenza, la maggior parte dei team IT si è dotata di tutte le funzionalità di Cyber Protection consigliate. Purtroppo, per il 73% delle aziende ciò implica l'esecuzione simultanea di oltre 5 soluzioni e agenti differenti; nel 21% di questi casi le soluzioni eseguite sono più di 10.

Quanti strumenti e agenti di sicurezza e protezione diversi sono attualmente in uso nella vostra azienda?



## IL MIX DI PROTEZIONE NON È FUNZIONALE

Malgrado l'adozione di tutte queste tecnologie, nell'anno passato la metà dei professionisti IT nell'area EMEA che abbiamo intervistato ha comunque subito perdite di dati e interruzioni operative, con potenziali perdite di profitto e di produttività e spese da affrontare, incluse quelle imputabili a eventuali sanzioni per la mancata conformità alle normative sulla privacy dei dati.

I risultati del report suggeriscono che i professionisti IT sono perfettamente consapevoli di questo limite. Tra le priorità segnalate per il 2021 in tutta la regione, troviamo infatti il miglioramento della privacy dei dati e della conformità, il rinnovo dello stack di Cyber Security e il supporto avanzato per gli ambienti di lavoro a distanza.

## I TIMORI PIÙ DIFFUSI RELATIVI ALLE MINACCE INFORMATICHE IN EMEA

I principali timori riferiti da tutti gli utenti intervistati nella regione EMEA sono in sintonia con i risultati del nostro report globale. Si registra tuttavia una carenza di attenzione e consapevolezza in relazione ad alcune minacce quali ransomware, cryptojacking, attacchi DDoS, attacchi IoT e attacchi dall'interno.

Utenti di IT ad uso personale	Utenti di IT ad uso professionale
1. Furto di dati	1. Malware
2. Malware	2. Furto di dati
3. Attacchi di phishing	3. Attacchi di phishing
4. Ransomware	4. Ransomware
5. Attacchi IoT	5. Attacchi DoS/DDoS

**Vuoi scoprire qual è l'approccio alla Cyber Protection scelto dai singoli e dalle organizzazioni di tutto il mondo?**

Richiedi la tua copia del Report globale per la Acronis Cyber Protection Week 2021

SCARICA

## Informazioni su Acronis

Acronis coniuga protezione dati e sicurezza informatica per offrire una [Cyber Protection](#) integrata e automatizzata in grado di risolvere i problemi di salvaguardia, accessibilità, privacy, autenticità e sicurezza (SAPAS) del mondo digitale di oggi. Grazie a modelli di deployment flessibili che si adattano alle esigenze dei service provider e dei professionisti IT, Acronis garantisce una Cyber Protection di livello superiore per dati, applicazioni e sistemi con soluzioni innovative di nuova generazione per antivirus, [backup](#), [disaster recovery](#) e [gestione della protezione degli endpoint](#). Con le sue [pluripremiate tecnologie anti-malware basate su IA](#) e di [autenticazione dei dati basate su blockchain](#), Acronis protegge qualsiasi tipo di ambiente – cloud, ibrido o in sede – a un costo contenuto e senza sorprese.

**Acronis**

Per saperne di più, visita  
[www.acronis.com](http://www.acronis.com)

Copyright © 2002–2021 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 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. 2021-04