Acronis

I 5 motivi principali per cui la tua azienda deve essere protetta con l'EDR in questo momento

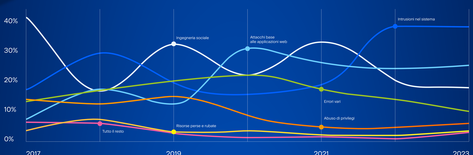
01.
L'aumento dei rischi digitali richiede un approccio basato sulla prevenzione

Il costo medio di una violazione dei dati ha raggiunto il suo massimo nel 2023 con 4,45 milioni di dollari. Ciò rappresenta un aumento del 2,3% rispetto al 2022.

Fonte: Cost of Data Breach Report, 2023, Ponemon Institute e IBM Security

02.
Garantire la difesa contro attacchi avanzati

Gli attacchi stanno diventando sempre più sofisticati e per essere protetti è necessario disporre di controlli di sicurezza più avanzati come l'EDR.



Fonte: Data Breach Investigation Report (DBIR) di Verizon 2023

03.
Accelera la risposta agli incidenti e arricchisci l'analisi

Il 51% delle organizzazioni, in seguito ad una violazione, prevede di aumentare gli investimenti per la sicurezza. Le principali aree individuate per ulteriori investimenti riguardano pianificazione e test di risposta agli incidenti (IR), formazione dei dipendenti e tecnologie di rilevamento e risposta alle minacce.

Tipi di investimento più comuni tra coloro che aumentano gli investimenti in sicurezza a seguito di una violazione

Fonte: Cost of Data Breach Report, 2023, Ponemon Institute e IBM Security

04.
Garantire la conformità ai requisiti normativi esistenti e a quelli futuri

Ciascuna azienda di classe A deve implementare, a meno che il CISO non abbia approvato per iscritto l'uso di controlli di compensazione ragionevolmente equivalenti o più sicuri: (1) una soluzione EDR (endpoint detection and response) per monitorare attività anomale, compresi, ma non solo, i movimenti laterali.

Fonte: Stato di New York DFS

I tre amplificatori del costo della violazione di maggiore impatto su 27 fattori.

Fonte: Cost of Data Breach Report, 2023, Ponemon Institute e IBM Security

05.
Requisiti assicurativi per la cyber security

Fonte: Federal Trade Comission https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

Le best practice includono

- Crittografia dei dati sensibili
- Vulnerability assessment e patch management
- EDR
- Backup programmatico e piano di DR
- Politiche rigorose di autenticazione (MFA) e autorizzazione (gestione dei privilegi minimi)
- Anti-malware basato sul comportamento
- Corso di sensibilizzazione alla sicurezza
- Piano di incident response IR

Prova la cyber protection olistica che garantisce la resilienza della tua azienda

Acquista ora | Provalo subito