Acronis

Nuovi KPI per la resilienza digitale

Le tradizionali metriche di ripristino misurano la velocità e la perdita di dati ma per le minacce moderne servono KPI in grado di misurare la pulizia del ripristino e il livello di accettabilità delle interruzioni.

Perché i KPI tradizionali non bastano più

KPI tradizionali

RPO Recovery Point Objective
Il volume accettabile di perdita di dati.

RTO Recovery Time Objective
La velocità necessaria per il ripristino dei sistemi.

Un ripristino rapido che recupera un sistema infetto è un'operazione non riuscita.

Questi KPI sono stati creati per guasti hardware e interruzioni accidentali e non tengono conto degli attacchi che compromettono l'integrità dei sistemi.

I KPI moderni: MTCR e MTD

KPI	MTCR	MTD
Nome completo	Tempo medio per il ripristino pulito	Massima interruzione operativa tollerabile
Definizione	Il tempo necessario per ripristinare un ambiente verificato e privo di malware	Tempo massimo durante il quale un'azienda può essere offline o sostenere risorse degradate prima che le conseguenze siano inaccettabili
Perché è importante	Garantisce che il sistema ripristinato non sia compromesso e sia sicuro da usare	Allinea le decisioni di ripristino all'impatto sull'azienda

Modello tradizionale e modello di resilienza a confronto

Modello tradizionale	Modello di resilienza
RTO	RTO
RPO	RPO
	MTCR
	MTD

Un ripristino moderno richiede velocità e affidabilità.

Le interruzioni operative limitano la produttività

23 giorni
Tempo medio di inattività da ransomware[1]

76%
Percentuale di aziende che segnalano una perdita significativa di produttività dopo un incidente[2]

30%
Tempo dedicato annualmente alla risoluzione delle interruzioni IT[3]

1,5-3 ore
Produttività persa ogni giorno a causa della proliferazione degli strumenti[4]

Tempi di inattività e stack frammentari minano direttamente l'efficienza dei tecnici e la produttività aziendale.

Perché la metrica MTCR migliora l'efficienza dei tecnici

Un ripristino pulito riduce il carico di lavoro dei tecnici:

- ☑ Nessun ciclo di reinfezione
- ☑ Nessun ripristino ripetuto
- ☑ Meno tempo da dedicare a districarsi tra gli strumenti
- ☑ Indagini e triage più brevi
- ☑ Ritorno più rapido a operazioni stabili
- ☑ Maggior numero di endpoint gestito da ogni tecnico

La riduzione del MTCR moltiplica la produttività dei tecnici per ogni cliente e ambiente.

Come una piattaforma unificata può ridurre MTCR e MTD

Funzionalità che riducono il tempo di ripristino e le interruzioni:

- Difesa dal ransomware assistita da AI
- Convalida del backup potenziata da AI
- Verifiche di ripristino isolate
- Flussi di lavoro integrati di protezione, rilevamento e ripristino

L'architettura unificata velocizza il ripristino pulito e riduce le interruzioni operative.

Resilienza digitale non significa solo protezione

Ripristino più pulito → Meno rilavorazioni

Minor tempo di inattività → Maggiore produttività

Operazioni unificate → MTCR più veloce

Migliore continuità → Risultati più solidi per i clienti

Scopri come Acronis può aiutarti ad anticipare le minacce, resistere agli attacchi, riprenderti più velocemente e adattarti al futuro.

Scopri di più | Contattaci

---

[1] Statista: "Average duration of downtime during a ransomware attack". https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-us/

[2] Verizon. "Data Breach Investigation Report", Verizon, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

[3] DevOps.com. "Survey: IT Teams Spend About a Third of Time Responding to Disruptions". https://devops.com/survey-it-teams-spend-about-a-third-of-time-responding-to-disruptions/

[4] Level.io. "The MSP Tool Sprawl Problem, Why Fewer Tools Mean Better Productivity". https://level.io/blog/tool-sprawl

Acronis