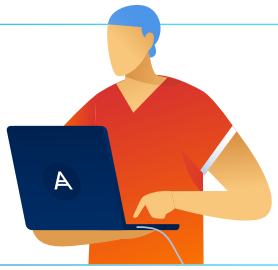
Acronis Advanced Security + Endpoint Detection and Response (EDR)

Per Service Provider

Semplifica la sicurezza degli endpoint

Oltre il 60% delle violazioni avviene oggi tramite una qualche forma di accesso non autorizzato[1], il che porta le aziende ad adottare soluzioni di sicurezza avanzate e i Service Provider ad aiutarle a difendersi da minacce sempre più sofisticate. La maggior parte delle soluzioni EDR leader di mercato in grado di contrastare queste minacce introduce però alcune problematiche:

- Complessità e costi elevati, che le rendono inaccessibili alle aziende con budget limitati
- Una protezione incompleta, che richiede ulteriori integrazioni per assicurare la continuità operativa
- Time-to-value di lungo periodo, necessità di formazione e onboarding elevate
- Problematiche di scalabilità, con la conseguente necessità di grandi team di professionisti della sicurezza



Per i Service Provider che avviano una propria attività, gli investimenti iniziali per la gestione di servizi propri basati su EDR possono essere inaccessibili. I provider con un'esperienza in sicurezza già consolidata che scelgono soluzioni leader di mercato su cui costruire l'offerta di servizi di rilevamento e risposta potrebbero invece essere tagliati fuori dal mercato dei clienti PMI e del mid-market per il costo troppo elevato, e ritrovarsi anche a competere con i servizi MDR del fornitore della soluzione scelta.

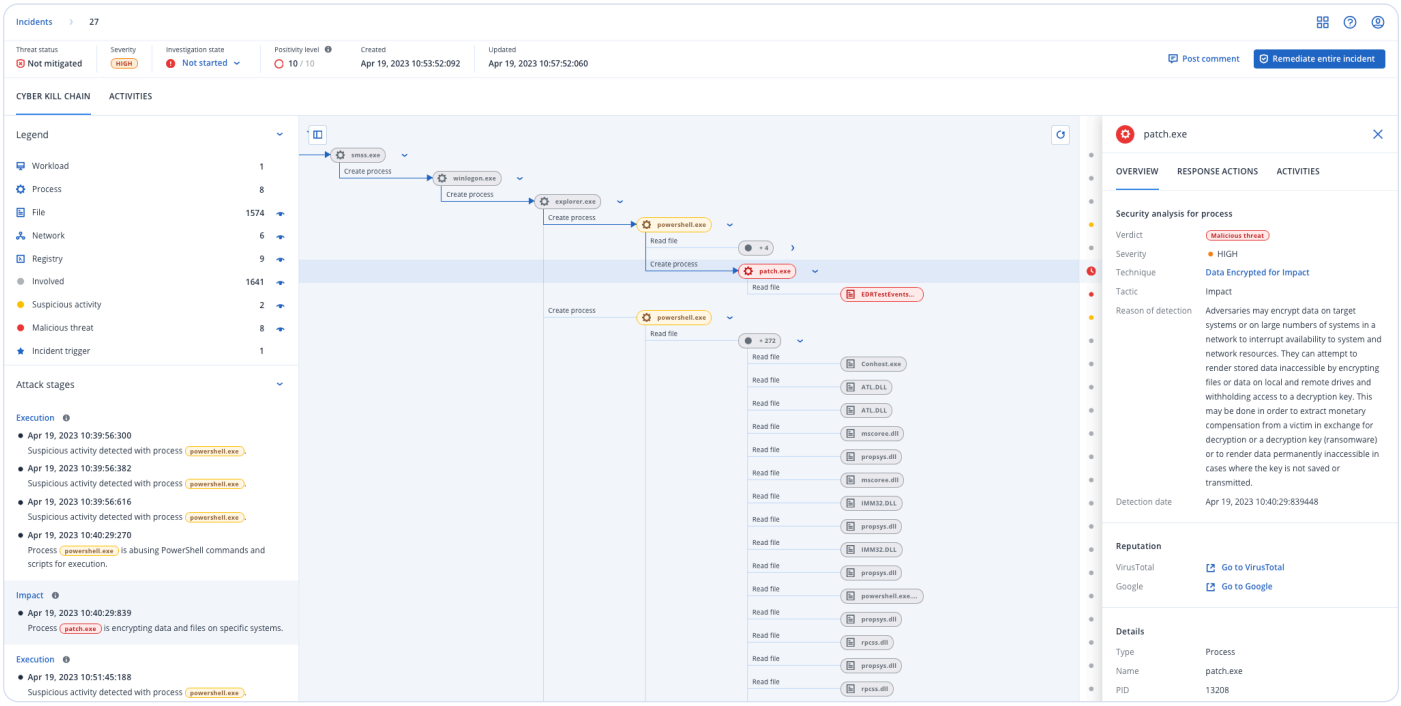
Acronis Advanced Security + EDR, progettato per i Service Provider

Acronis sa che i Service Provider devono bilanciare un'offerta di servizi efficienti con i diversi requisiti e budget dei loro clienti.

La soluzione di sicurezza avanzata ideale è in grado di razionalizzare margini e competenze interne, è multi-tenant, basata su SaaS, offre maggiore sicurezza e prevede la giusta quantità di automazione e di facilità d'uso, per accelerare l'adozione e la scalabilità presso più clienti nei loro ambienti esclusivi.

Progettato per i Service Provider, **Acronis Advanced Security + EDR** consente di semplificare la protezione degli endpoint perché rileva, analizza e corregge all'istante gli attacchi avanzati, garantendo una continuità operativa senza confronti. Elimina il costo e la complessità della gestione di più prodotti dedicati e offri al tuo team una soluzione di Cyber Protection completa e semplice da gestire e distribuire.

Ottimizza i servizi di rilevamento e risposta con Acronis



Ottimizzazione dell'analisi e della prioritizzazione degli attacchi per una risposta tempestiva	Backup e ripristino integrati per una continuità operativa senza confronti	Cyber Protection completa con un unico agente, pensata per gli MSP
• Velocizza le indagini dando priorità ai potenziali rischi e riduci l'eccesso di avvisi • Analizza gli eventi in pochi minuti e su vasta scala grazie alla correlazione automatizzata e alle interpretazioni guidate e basate su AI degli attacchi • Ottieni più visibilità in tutte le fasi MITRE ATT&CK® con un'analisi rapida dell'attacco e del suo impatto e informazioni su come la minaccia si è infiltrata, sui danni che ha causato e su come può essersi diffusa	• Funzionalità di backup e ripristino integrate che garantiscono una continuità operativa senza confronti laddove le soluzioni di sicurezza dedicate non riescono • Correzione e ripristino ottimizzati e con un clic • In un'unica soluzione, ottieni una protezione integrata e completa in tutte le fasi del NIST Cybersecurity Framework: identificazione, protezione, rilevamento, risposta e ripristino.	• Avvia rapidamente nuovi servizi con un unico agente e una sola console Acronis, con la massima facilità di deployment, gestione e scalabilità • La scalabilità semplificata per più clienti consente di ottenere cospicui margini di profitto e contenere le spese di esercizio, senza richiedere personale altamente specializzato • Collabora con un fornitore interessato al tuo successo, che non entra in competizione con te per la tua clientela

Protezione degli endpoint premiata

PC EDITORS' CHOICE

Editors' choice

AV-TEST

Partecipante e vincitore del test AV-TEST

VB 100 VIRUS

Certificazione VB100

ICSA labs

Certificazione Endpoint Anti-Malware di ICSA Labs

AV comparatives

Certificazione AV-Comparatives

Resilienza aziendale senza confronti con Acronis

Con Acronis, puoi contare su un'unica piattaforma in grado di garantire una sicurezza olistica degli endpoint e la continuità operativa, in linea con gli standard di settore riconosciuti quali quelli del framework NIST, e che ti permette di identificare i dati e le risorse vulnerabili, proteggerli in modo proattivo, rilevare e bloccare qualsiasi minaccia, rispondere agli attacchi e ristabilire la normale operatività.

Acronis: continuità operativa secondo i principi NIST

Identificazione

Protezione

Rilevamento

Risposta

Ripristino

Advanced Security + EDR				
• Inventario hardware • Individuazione degli endpoint non protetti	• Vulnerability assessment • Prevenzione degli exploit • Controllo dei dispositivi • Configurazione della sicurezza	• Feed sulle minacce emergenti • Ricerca degli indicatori di compromissione delle minacce emergenti • Funzionalità anti-malware e anti-ransomware • Rilevamento comportamentale basato su AI e ML • Filtraggio degli URL	• Analisi rapida degli incidenti • Isolamento e correzione dei workload • Backup forensi	• Rollback rapido degli attacchi • Ripristino in blocco con un clic • Ripristino automatico
Acronis Cyber Protect Cloud				
• Inventario software • Classificazione dei dati	• Patch management • DLP • Integrazione dei backup • Cyber scripting	• Sicurezza e-mail	• Indagini tramite connessione remota	• Pre-integrazione con funzionalità di disaster recovery

Principali funzionalità di un sistema EDR

Prioritizzazione dei problemi di sicurezza

Monitora e metti in correlazione in modo automatico gli eventi che si verificano sugli endpoint, con l'assegnazione di priorità alle catene di eventi sospetti e la generazione di avvisi sugli incidenti.

Interpretazione automatizzata degli incidenti associata al framework MITRE ATT&CK®

Ottimizza la risposta e aumenta la reattività alle minacce sfruttando le interpretazioni degli attacchi basate su AI e associate al framework MITRE ATT&CK® per capire in pochi minuti:

- Come l'hacker si è infiltrato nel sistema
- Come ha nascosto le proprie tracce
- Che danni ha causato l'attacco e come
- Le modalità di diffusione dell'attacco

Un solo clic per rispondere agli attacchi e ottenere una continuità operativa senza confronti

Vinci dove le soluzioni puntuali non riescono: sfrutta tutte le potenzialità dell'integrazione tra Cyber Security, protezione dati e gestione della configurazione della sicurezza degli endpoint reagendo ai problemi con un solo clic:

- **Correzione** con isolamento degli endpoint e quarantena per le minacce
- **Indagini approfondite** con connessioni remote e backup forensi
- **Prevenzione degli attacchi futuri** con correzione delle vulnerabilità esistenti
- **Garanzia di continuità operativa** con rollback dopo gli attacchi, backup e ripristino integrati

1. Fonte: "2022 Data Breach Investigation Report", Verizon

Acronis

Per saperne di più, visita www.acronis.com