8 casi d'uso di Acronis XDR per gli MSP

Introduzione

Le minacce diventano sempre più complesse e gli attacchi superano le misure di difesa degli endpoint. Quasi il 40% delle violazioni è causato dalla compromissione delle credenziali e oltre il 30% avviene tramite phishing.[1] A fronte di un phishing tradizionale piuttosto semplice, esiste un phishing rivolto alle applicazioni web molto più elaborato. Si è inoltre registrata un'intensificazione degli attacchi agli account di posta elettronica e collaborazione su cloud. Con il 29% delle aziende che segnala perdite di dati causate da violazioni della sicurezza,[2] una protezione olistica non può limitarsi a fermare le minacce informatiche.

Per contrastare questi attacchi ormai così sofisticati, è imprescindibile una soluzione di Extended Detection and Response (XDR). Il mercato dei prodotti XDR offre però agli MSP poche opzioni convenienti, facili da usare e integrate. Inoltre, molti sistemi XDR non garantiscono il ripristino e la continuità operativa. Questi ostacoli impediscono agli MSP di individuare la soluzione XDR adatta alle risorse IT, ai servizi e alle esigenze dei clienti che gestiscono.

Acronis XDR è stato progettato specificamente per gli MSP con l'intento di aiutare i Partner di ogni dimensione a offrire servizi XDR competitivi per proteggere le superfici di attacco a rischio, eseguire ripristini dopo gli attacchi e garantire la resilienza digitale.

Di seguito 8 casi d'uso di Acronis XDR per gli MSP:

1 Espandi la protezione e la visibilità a tutti gli endpoint e alle superfici di attacco più vulnerabili.

Mantenere la visibilità è una sfida costante per gli MSP, perché gli ambienti IT dei clienti crescono e diventano sempre più complessi. Con Acronis XDR, gli MSP possono rafforzare la telemetria oltre gli endpoint e proteggere le e-mail, le identità e le applicazioni Microsoft 365. Gli esperti della sicurezza possono così acquisire informazioni importanti sugli attacchi e potenziare le azioni di risposta, sia che la minaccia sia originata da un endpoint o si sia diffusa oltre.

2 Rileva e blocca gli attacchi avanzati prima che diventino violazioni.

Le più recenti minacce informatiche sono in grado di eludere i tradizionali sistemi di rilevamento. Acronis XDR monitora e mette in relazione gli eventi che interessano endpoint, e-mail, identità e ambienti Microsoft 365. In pochi minuti, la soluzione rileva e analizza le minacce complesse. Inoltre, MSP e clienti possono dormire sonni tranquilli sapendo che le minacce comuni vengono bloccate dalla pluripremiata protezione basata sul comportamento di Acronis.

3 Rispondi rapidamente alle minacce prima che creino danni.

A differenza di altri XDR di punta, Acronis XDR integra il ripristino per garantire la continuità operativa. Ridurre le conseguenze di un attacco è fondamentale per limitare al massimo le ripercussioni finanziarie, di reputazione e operative sui clienti. Prima che le minacce causino danni, Acronis XDR consente al team IT di mettere in quarantena i processi dannosi, isolare i workload, rimuovere gli URL e i file pericolosi e sospendere gli account compromessi.

[1] Verizon, "2024 Data Breach Investigations Report".
[2] InfoSecurity Magazine, 2024.

Inoltre, considerata la pressione che grava sulle aziende per la riduzione dei rischi informatici, Acronis XDR consente agli MSP di contenere le superfici di attacco dei clienti, prevenendo gli attacchi futuri con misure di sicurezza proattive e attive, come le patch delle vulnerabilità, il blocco degli indirizzi e-mail dannosi e il reset forzato delle password.

4 Offri ai clienti gli strumenti per la conformità normativa e la protezione dei dati sensibili.

Spesso i requisiti di conformità normativa prevedono la dimostrazione delle misure messe in atto per ridurre i rischi informatici e proteggere i dati sensibili. In combinazione con Acronis Advanced Data Loss Prevention e Advanced Disaster Recovery, Acronis XDR protegge i clienti dalle perdite di dati, dagli accessi non autorizzati e dai trasferimenti di dati sensibili, aiutando le aziende a mantenere la conformità, a essere idonee per la copertura di una cyber assicurazione e a soddisfare le normative del settore. Dai backup vengono acquisiti dati forensi che possono agevolare le indagini future. Acronis XDR classifica e assegna la priorità ai problemi relativi ai dati sensibili, offrendo ai tecnici IT una visibilità migliorata sulle risorse di maggior valore.

5 Consolida le soluzioni e centralizza la gestione.

Gestire una molteplicità di soluzioni puntuali è costoso e stressante per gli MSP. Di fatto, una gestione degli strumenti di sicurezza particolarmente gravosa contribuisce all'esaurimento delle risorse e all'affaticamento del personale tecnico. Acronis XDR fa parte di Acronis Cyber Protect Cloud, un consolidato ecosistema di soluzioni pensato per aiutare gli MSP a lanciare, espandere e personalizzare rapidamente l'offerta di servizi con una piattaforma specifica per la loro attività. Grazie a un approccio collaudato nel tempo e a un servizio unificato, gli MSP possono migliorare l'efficienza dei costi e semplificare la gestione.

6 Accelera le indagini sugli incidenti.

L'eccesso di avvisi è un problema importante che contribuisce all'affaticamento dei tecnici. Acronis XDR offre al personale IT elenchi degli incidenti con priorità generati dall'intelligenza artificiale per garantire che vengano risolti gli incidenti legittimi, oltre a riepiloghi degli attacchi, anch'essi basati su AI, che consentono all'IT di agire e comprendere rapidamente il contesto delle minacce. Infine, grazie alle interpretazioni degli attacchi generate dall'AI e basate sul framework MITRE ATT&CK, i tecnici degli MSP possono ridurre il tempo necessario per l'analisi da ore a minuti.

7 Garantisci la continuità aziendale anche durante gli attacchi.

Le soluzioni XDR con funzionalità di ripristino pensate per gli MSP sono una rarità nel mercato. Il ripristino e il disaster recovery integrati inclusi nelle funzionalità di risposta di Acronis XDR si distinguono rispetto alle soluzioni XDR tradizionali. Grazie al ripristino integrato, la soluzione garantisce la continuità operativa dell'azienda e protegge dalla perdita di dati. Dopo un attacco, gli MSP possono eseguire un rollback specifico in base all'attacco o un ripristino completo.

8 Dimostra il valore concorrenziale dei servizi forniti.

Le soluzioni specifiche sono costose e spesso non offrono agli MSP la flessibilità necessaria per effettuare il provisioning della protezione in modo pratico o efficiente, ostacolando la scalabilità. Acronis XDR include widget personalizzabili che permettono al reparto IT di realizzare un'offerta di sicurezza su misura del cliente o per tutti i servizi MSP. Il reparto IT può pianificare la creazione e l'invio automatico dei report ai clienti, nel formato desiderato.

Informazioni su Acronis

Acronis, leader globale nella Cyber Protection, fornisce soluzioni che integrano nativamente Cyber Security, protezione dei dati e gestione degli endpoint, progettate per i Managed Service Provider (MSP). Le soluzioni Acronis consentono di identificare, prevenire, rilevare, rispondere e correggere le minacce informatiche più recenti e di avviare il ripristino, garantendo la continuità operativa. Acronis Cyber Protect Cloud è disponibile in 26 lingue e in più di 150 paesi, ed è utilizzato da oltre 20.000 Service Provider per proteggere più di 750.000 aziende. Maggiori informazioni su www.acronis.com.

Non hai le risorse per implementare XDR autonomamente? Esternalizza la sicurezza con Acronis MDR

SCOPRI DI PIÙ

Vuoi saperne di più su Acronis XDR? Fissa una demo individuale.

REGISTRATI ORA

Acronis

Maggiori informazioni su www.acronis.com