Acronis Advanced Security + Endpoint Detection and Response (EDR)

Für Service Provider

Vereinfachte Endpunktsicherheit

Da bei mehr als 60 % aller Angriffe eine Form von Hacking genutzt wird[1], benötigen Unternehmen fortschrittliche Sicherheitslösungen von Anbietern, die sie bei der Abwehr aktueller hochentwickelter Bedrohungen unterstützen. Die meisten marktführenden EDR-Lösungen, die solcher Bedrohungen Herr werden können, sind mit folgenden Nachteilen verbunden:

- Hohe Kosten und Komplexität, sodass sie sich nicht für den Massenmarkt eignen
- Unvollständiger Schutz, sodass zur Gewährleistung der Geschäftskontinuität zusätzliche Integrationen erforderlich sind
- Langer Zeitraum bis zur Amortisierung, großer Schulungs- und Onboarding-Aufwand
- Schwierige Skalierung, sodass für den Betrieb große Sicherheitsexpertenteams benötigt werden

Leider verfügen Service Provider, die erst neu auf dem Markt sind, nur selten über die Expertise und die finanzielle Ausstattung, um einen eigenen EDR-basierten Service anzubieten. Anbieter mit etablierter Sicherheitsspezialisierung stellen häufig fest, dass der Aufbau eigener Erkennungs- und Reaktionsservices mit marktführenden Lösungen für mittelständische oder KMU-Kunden zu teuer ist – und müssen zudem erkennen, dass sie gleichzeitig mit den MDR-Services ihres Lösungsanbieters konkurrieren.

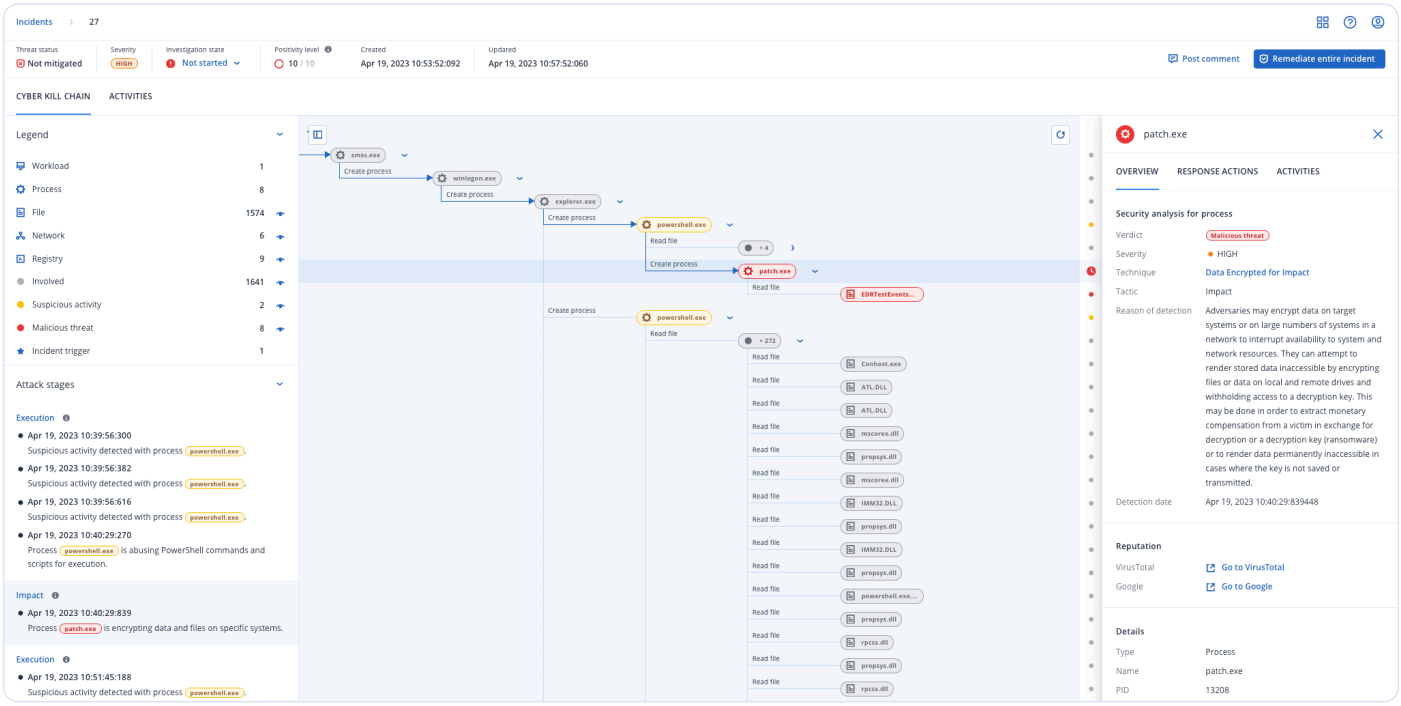
Acronis Advanced Security + EDR, speziell für Service Provider entwickelt

Wir bei **Acronis** wissen, dass Service Provider effektive Services für sehr unterschiedliche Kundenanforderungen und Budgets anbieten müssen.

Wir wissen auch, dass sie eine fortschrittliche Sicherheitslösung benötigen, die Margen und Kompetenzen optimiert, mandantenfähig und SaaS-basiert ist sowie bessere Sicherheit und Automatisierung bietet. Gleichzeitig soll sie benutzerfreundlich sein und sich schnell einrichten sowie für mehrere Kund:innen und ihre individuellen Umgebungen skalieren lassen.

Acronis Advanced Security + EDR wurde speziell für Service Provider entwickelt und macht die Bereitstellung von Endpunktsicherheit ganz einfach. Erkennen, analysieren und beheben Sie hochentwickelte Angriffe in kürzester Zeit und bieten Sie Ihren Kund:innen Geschäftskontinuität der Spitzenklasse. Befreien Sie sich von den Kosten und der Komplexität parallel implementierter Punktprodukte und unterstützen Sie Ihr Team durch eine umfassende Cyber Protection-Lösung, die sich einfach verwalten und bereitstellen lässt.

Optimierung Ihrer Services für Erkennung und Vorfallreaktion mit Acronis



Optimierte Priorisierung und Analyse von Angriffen für schnelle Reaktionen

- Vereinfachen Sie die Untersuchung durch die Priorisierung potenzieller Zwischenfälle. Dadurch wird auch die Warnmeldungmüdigkeit verringert.
- Analysen können im großen Maßstab innerhalb von Minuten statt Stunden durchgeführt werden – mit automatischer Korrelation sowie geführten, Maschinenintelligenz-gestützten Angriffsinterpretationen.
- Sie erhalten einen verbesserten Überblick über MITRE ATT&CK®-Ereignisse und können dadurch die Ergebnisse der Angriffsanalyse und die Auswirkungen schneller verstehen, zum Beispiel: Wie erfolgte der Erstzugriff, welcher Schaden ist entstanden und hat sich der Angriff ausgebreitet.

Integrierte Backup- und Recovery-Funktionen für einzigartige Geschäftskontinuität

- Nutzen Sie integrierte Backup- und Recovery-Funktionen, die einzigartige Geschäftskontinuität bieten, wo Sicherheits-Einzellösungen keine Chance haben.
- Profitieren Sie von Behebung und Wiederherstellung mit einem Klick.
- Mit einer einzigen Lösung können Sie vollständigen, integrierten Schutz für alle Bereiche des NIST Cybersecurity Frameworks – IDENTIFY, PROTECT, DETECT, RESPOND und RECOVER (Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung) – anbieten.

Umfassende Cyber Protection-Lösung mit nur einem Agenten – speziell für MSPs entwickelt

- Der Launch neuer Services ist schnell und einfach möglich – mit einem einzigen Acronis Agenten über nur eine Konsole für Bereitstellung, Verwaltung und Skalierung.
- Durch minimale Betriebskosten (OPEX) lassen sich Services leicht unter Beibehaltung angemessener Margen für mehrere Kund:innen skalieren, da für den Betrieb kein großes Expertenteam erforderlich ist.
- Arbeiten Sie mit einem vertrauens-würdigen Anbieter zusammen, der sich auf Ihren Erfolg und Ihre Unterstützung konzentriert – und nicht mit Ihnen konkurriert.

Preisgekrönter Endpunktschutz

PC EDITORS' CHOICE

Editors' Choice

AV-TEST The Independent IT-Security Institute

AV-TEST-Teilnehmer und Testgewinner

VB 100 VIRUS virusbtn.com

VB100-zertifiziert

ICSA labs

Malware-Schutz von ICSA Labs zertifiziert

AV comparatives

Von AV-Comparatives zertifiziert

Einzigartige geschäftliche Resilienz durch Acronis

Bei Acronis benötigen Sie nur eine Plattform für umfassenden Endpunktschutz und Geschäftskontinuität. Diese Plattform ist mit etablierten Branchenstandards wie NIST abgestimmt, sodass Sie gefährdete Ressourcen und Daten erkennen und proaktiv schützen können und zudem alle Bedrohungen stoppen, Angriffe abwehren und Angriffsschäden beheben können.

Acronis: Geschäftskontinuität für alle Bereiche des NIST-Frameworks

Identifizierung	Schutz	Erkennung	Reaktion	Wieder-herstellung
Advanced Security + EDR				
• Hardware-Inventarisierung • Erkennung ungeschützter Endpunkte	• Schwachstellen-Bewertungen • Exploit-Prävention • Gerätekontrolle • Sicherheits-konfiguration	• Feed zu neuen Bedrohungen • Suche nach Kompromittierungs-indikatoren neuer Bedrohungen • Malware- und Ransomware-Schutz • KI- und ML-basierte Verhaltenserkennung • URL-Filterung	• Schnelle Vorfallanalyse • Workload-Behebung mit Isolierung • Forensische Backups	• Schnelles Rollback von Angriffen • Massenwieder-herstellungen per Mausklick • Self-Service-Recovery
Acronis Cyber Protect Cloud				
• Software-Inventarisierung • Datenklassifizierung	• Patch-Verwaltung • DLP • Backup-Integration • Cyber Scripting	• E-Mail-Schutz	• Untersuchungen per Remote-Verbindung	• Vorab mit Disaster Recovery integriert

Wichtige EDR-Funktionen

Priorisierung von Vorfällen

Überwachen und korrelieren Sie automatisch Endpunktereignisse, wobei verdächtige Ereignisketten als Vorfallwarnungen priorisiert werden.

Automatisierte Interpretation von Vorfällen entsprechend MITRE ATT&CK®

Vereinfachen Sie die Reaktion und steigern Sie die Reaktionsmöglichkeiten auf Bedrohungen mithilfe KI-basierter Angriffsinterpretationen entsprechend MITRE ATT&CK®, um innerhalb von Minuten Folgendes zu erfahren:

- Wie erfolgte der Erstzugriff?
- Wie haben die Angreifer ihre Spuren verwischt?
- Welchen Schaden hat der Angriff verursacht – und wie ist er entstanden?
- Wie hat sich der Angriff ausgebreitet?

Reaktionen mit nur einem Klick für hervorragende Geschäftskontinuität

Lassen Sie Einzellösungen hinter sich und profitieren Sie von der Integration von Cyber Security, Data Protection und Endpunktschutz-Verwaltung und der Möglichkeit, mit nur einem Klick auf Vorfälle zu reagieren.

- **Behebung** durch Isolierung von Endpunkten und Bedrohungen
- **Weitere Untersuchungen** mithilfe von Remote-Verbindungen und forensischen Backups
- **Verhinderung zukünftiger Angriffe** durch das Schließen von Sicherheitslücken
- **Gewährleistung der Geschäftskontinuität** durch Rollback-Fähigkeiten bei Angriffen und integrierte Funktionen für Backup und Recovery

Vereinfachen Sie Endpunktsicherheit noch heute

Verzichten Sie auf den Einsatz mehrerer Tools und setzen Sie beim Endpunktschutz auf eine einzige Lösung sowie umfassende Sicherheitskompetenzen. Vereinfachen Sie Endpunktsicherheit mit Acronis EDR.

→ Mehr erfahren

1. Quelle: „Data Breach Investigation Report“, Verizon, 2022.

Acronis

Weitere Informationen unter
www.acronis.com