Checkliste: Fünf Gründe, warum EDR in Ihrem MSP-Portfolio nicht fehlen darf

Vorbereitung ist alles: Hochentwickelte Angriffe nehmen zu

Der Schutz von Endpunkten sollte weder kompliziert noch teuer sein. Aktuelle Tools für Endpoint Detection & Response (EDR) zwingen MSPs jedoch, auf kostspielige Sicherheitsfachleute zurückzugreifen. Zudem erfordern sie den Einsatz mehrerer Punktlösungen, um vollständigen Schutz einschließlich Geschäftskontinuität sicherstellen zu können. Bis zur Wertschöpfung ist es oft ein langer Weg – oder es ist ressourcenintensiver Service-Support notwendig. Daher kam marktführender Endpunktschutz häufig nur für sehr große Unternehmen in Frage. Acronis bietet einen besseren Ansatz.

Durch Trends wie Lösungskonsolidierung und KI-basierte, geführte Vorfallanalyse und Behebung kann Acronis die Kosten und die Komplexität reduzieren, die üblicherweise mit EDR einhergehen, und dadurch den Technologie-Massenmarkt demokratisieren. Das ist eine hervorragende Gelegenheit für Service Provider, ihre Services mit umfassender Endpunktsicherheit zu ergänzen, die sich leicht einsetzen, bereitstellen und verwalten lässt. Dadurch erhalten Ihre Kund:innen bislang unerreichte Geschäftskontinuität.

„Mehr als 60 % aller Daten-kompromittierungen gehen auf die eine oder andere Form von Hacking zurück.“

Quelle: Verizon Data Breach Investigation Report, 2022.

Fünf Gründe, warum EDR in Ihrem Angebot nicht fehlen darf

1 Die Angestellten Ihrer Kund:innen haben über ihre Endpunkte Zugriff auf wertvolle Daten

Selbst wenn Ihre Kund:innen ihre sensiblen Daten in der Cloud speichern, können diese Daten, sofern sie über die Workstations der Angestellten zugänglich sind, von Cyberkriminellen exfiltriert werden, die sich über den Endpunkt Zugriff verschaffen. Sie müssen den Schutz der Daten vor nicht autorisierten Zugriffen gewährleisten, um schwerwiegende Finanz-, Compliance- und Reputationsrisiken zu vermeiden.

Die von Hackern ins Visier genommenen Daten sind in der Regel von hohem Wert. Dazu zählen etwa stark regulierte Informationen, Handelsgeheimnisse oder geistiges Eigentum, mit dem sich viel Geld verdienen lässt. Laut dem Acronis Cyber Protection Operation Center Report belaufen sich die Kosten je Datenschutzverletzung auf durchschnittlich 5 Millionen US-Dollar.

Mit Acronis können Sie Angriffe auf sensible Daten erkennen, sodass Sie den Schaden schnell analysieren und beheben und Ihre Kund:innen benachrichtigen können. Durch schnelle Reaktionen mit nur einem Klick wird die Geschäftskontinuität gewährleistet und die integrierte Recovery ausgelöst.

Copyright © 2002-2023 Acronis International GmbH.

2 Sie suchen nach neuen Einnahmequellen für Ihr Geschäft

Wie Canalys berichtet, gehen 27 % der befragten MSPs davon aus, dass ihr Cyber Security-Umsatz im Jahr 2023 um mehr als 20 % steigen wird. Da jedoch die meisten Service Provider in irgendeiner Form Managed Security Services anbieten, bleibt der Wettbewerb eine Herausforderung.

Acronis ist der ideale Partner für ein Sicherheitsportfolio, das sich mühelos launchen und skalieren lässt. Dabei sind alle Funktionen – einschließlich Malware-Schutz, E-Mail-Sicherheit, EDR und DLP – speziell für MSPs konzipiert und werden mit nur einem Agenten in einer einzigen Plattform integriert. Mit Acronis EDR sind Sie nicht auf große Budgets, komplexe Punktlösungen, kostspielige Schulungen und umfangreiche Sicherheitsteams angewiesen.

3 Ihre Kund:innen arbeiten in Branchen mit hohen Sicherheits- oder Compliance-Anforderungen

Branchen, die hohen Sicherheits- und Behördenanforderungen unterliegen, benötigen erweiterte Schutzmaßnahmen wie EDR. Diese Unternehmen sind in der Regel stark gefährdet, da es Hacker auf ihre sensiblen und wertvollen Daten abgesehen haben. Die meisten Vorschriften wie DSGVO, HIPAA und PCI-DSS verlangen, dass Meldungen innerhalb eines knappen Zeitraums erfolgen (bei der DSGVO sind es beispielsweise 72 Stunden). Im Falle eines Datenlecks drohen zudem empfindliche Geldstrafen.

Mit Acronis Advanced Security + EDR können Sie hochentwickelte Angriffe nicht nur schnell erkennen, sondern auch Vorfallwarnungen priorisieren. Die Lösung bietet Einblick in die von Angriffen betroffenen sensiblen Daten sowie geführte Vorfallanalysen basierend auf Branchen-Best Practices (MITRE ATT&CK-Framework). Dadurch können Sie schnell reagieren und Compliance-Auflagen gerecht werden. Unterstützen Sie Ihre Kund:innen bei der Einhaltung von Vorschriften, indem Sie Risiken reduzieren, prüfen, ob Angriffe auf sensible Daten ausgerichtet waren, Probleme beheben, Schäden per Rollback rückgängig machen sowie schnell und einfach Bericht erstatten.

4 Sie oder Ihre Kund:innen ziehen eine Cyberversicherung in Betracht

Um ihre Haftung im Falle einer Datenschutzverletzung zu begrenzen, wenden sich immer mehr Unternehmen an Cyberversicherungen. Die meisten Versicherungsgeber geben vor, dass EDR als Bestandteil des Cyber Security-Programms von Versicherten implementiert sein muss. Mit Acronis können Sie EDR einfach und skalierbar implementieren und Ihre Kund:innen schnell und zuverlässig schützen. Durch die Integration von Technologien wie DLP und Disaster Recovery lassen sich zudem die Beiträge zur Cyberversicherung senken.

Die Kosten dafür hängen unter anderem vom Jahresumsatz, der Branche, den Datentypen, der Datenmenge sowie den vorhandenen Sicherheitsmaßnahmen ab. Sie sollten das Hinzufügen von EDR zu Ihrem Service-Angebot in Betracht ziehen, um die Datensicherheitsanforderungen der Cyberversicherer zu erfüllen und Ihren Kund:innen dadurch die Möglichkeit zu bieten, die Risiken für ihr Unternehmen zu begrenzen.

5 Sie möchten wettbewerbsfähiger sein

MSSPs und große Sicherheitsanbieter bieten bereits erweiterte Sicherheitskontrollen an, um modernen Bedrohungen mit MDR-Services (Managed Detection and Response) zu begegnen. Aufgrund der hohen Kosten und Komplexität bleiben die damit verbundenen EDR- und MDR-Services für den Großteil der kleinen und mittleren Unternehmen jedoch unerreichbar.

Mit Acronis können Sie sich vom Wettbewerb abheben, indem Sie EDR-Services anbieten, die für Kund:innen jeder Größe zugänglich und skalierbar sind und die sich entsprechend den Fähigkeiten und Kompetenzen Ihres Teams dimensionieren lassen. Dadurch sind Sie nicht nur in der Lage, Angriffe zu erkennen und zu beheben, sondern gewährleisten dank integrierter Backup- und Recovery-Funktionen die Geschäftskontinuität Ihrer Kund:innen – und all das mit nur einem Klick.

Advanced Security + EDR

Acronis 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.

→ Mehr erfahren

Acronis

Weitere Informationen unter
www.acronis.com

Copyright © 2002-2023 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH in den Vereinigten Staaten und/oder in anderen Ländern. Alle anderen Marken oder eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber. Technische Änderungen, Abweichungen bei den Abbildungen sowie Irrtümer sind vorbehalten. 2023-05