

Checklist:
Five signs you need to add EDR to your MSP tech stack

Be prepared: Advanced attacks are on the rise

Protecting endpoints shouldn't be complicated and expensive. But today's endpoint detection and response tools force MSPs to resort to costly, advanced security expertise and require multiple point products for complete protection — including business continuity. Long time to value and resource-intensive services support are often needed, putting market-leading endpoint protection out of reach of all but the very largest organizations. With Acronis, there's a better way.

Taking advantage of trends like solution consolidation and AI-based guided incident analysis and remediation, Acronis has reduced the cost and complexity associated with EDR, democratizing the technology downmarket. Now is a great time for service providers to expand their services with comprehensive endpoint security that's easy to use, deploy and manage — unlocking a unique level of business continuity for your clients.

"More than 60% of breaches now involve some form of hacking."

Source: Verizon Data Breach Investigation Report, 2022.



Check the five signs that you need to add EDR to your tech stack

1 Clients' employees have access to valuable data through their endpoints

Even if your clients store their sensitive data in the cloud, if that data is accessible via employees' workstations, it can easily be exfiltrated by attackers who gain access through the endpoint. You need to ensure data is protected from unauthorized parties to save clients from severe financial, regulatory and reputational risks.

The data targeted by hackers tends to be of high value, such as data that is subject to regulations and trade secrets or intellectual property that can be leveraged for financial gain. The Acronis Cyber Protection Operation Center Report says that the average cost of a data breach is $5 million.

With Acronis, you can detect attacks that target sensitive data, allowing you to rapidly analyze and remediate the damage and report to clients. A single-click response ensures business continuity and integrated recovery.

Copyright © 2002–2023 Acr

2 You are looking for new revenue sources to grow your practice

Canalys reports that 27% of MSPs surveyed expect their cybersecurity revenue to grow by more than 20% in 2023. However, with the majority of service providers offering some form of managed security services, competition is a challenge.

Acronis is a great partner to launch and scale your security portfolio with ease — from anti-malware and email security, to EDR and DLP — integrated in a single platform and agent, and designed specifically for MSPs. With Acronis EDR, you don't need to resort to high budgets, complex point solutions, costly training sessions and large security teams.

3 You have clients in high-requirement security or compliance industries

Industries with high security and regulatory requirements require advanced protection like EDR. These organizations are usually at high risk due to attackers' motivation to acquire sensitive, valuable data. Most regulations, such as GDPR, HIPAA and PCI-DSS, require reporting within a strict time frame (e.g., 72 hours for GDPR) and can lead to severe fines in the event of a data leak.

Acronis Advanced Security + EDR enables you to not only detect advanced attacks with speed but also to prioritize incident alerts. The solution provides visibility into sensitive data affected by attacks and streamlines analysis with guided interpretation of incidents mapped to industry best practices (MITRE ATT&CK framework). The result is rapid response and reporting for compliance. Ensure regulatory compliance for your clients by reducing risks, tracking whether attacks target sensitive data, remediating and rolling back any damage, and reporting with ease and speed.

4 You or your clients are considering cyber insurance

To limit data breach liability, clients are increasingly turning to cyber insurers. Most insurers require that EDR be part of a customer's cybersecurity program. Acronis enables you to launch EDR in an easy, scalable and simple way, with fast time to value to protect clients. And, we enable you to reduce cyber insurance rates through integration with technologies like DLP and disaster recovery (DR).

The cost of cyber insurance depends upon several factors, including annual revenue, industry, type and amount of data held, and level of security. You should consider adding EDR to your service stack to cover data safeguard requirements for cyber insurance and enable clients to limit the risks for their business.

5 You want to increase your competitiveness

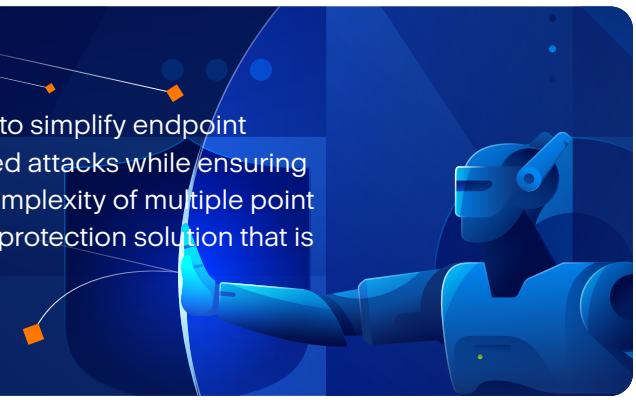
MSSPs and large security vendors are already providing advanced security controls to counter modern threats through managed detection and response (MDR) services. But due to their cost and operational complexity, EDR and MDR services based upon them remain out of reach for most SMB and mid-market clients.

With Acronis, you can differentiate yourself by offering endpoint detection and response services that are accessible and scalable for clients of all sizes and can be rightsized to your team's capabilities and expertise. You not only can detect and remediate attacks, but also ensure business continuity with pre-integrated backup and recovery capabilities — all with a single click.

Advanced Security + EDR

Designed for service providers, Acronis EDR enables you to simplify endpoint security — rapidly detect, analyze and remediate advanced attacks while ensuring unmatched business continuity. Eliminate the cost and complexity of multiple point products and enable your team with one complete cyber protection solution that is simple to manage and deploy.

→ Learn more



Acronis

Learn more at
www.acronis.com

Copyright © 2002-2023 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2023-05