Acronis
Advanced Security + Endpoint Detection and Response (EDR)
For service providers

Simplify endpoint security

With more than 60% of breaches now involving some form of hacking[1], businesses must now turn to advanced security solutions and providers to help them combat today's sophisticated threat landscape. However, most market-leading EDR solutions capable of countering these threats introduce:

- High costs and complexity, making them inaccessible downmarket

- A long time to value, high training and onboarding requirements

- Incomplete protection, requiring additional integration for business continuity

- Scalability challenges requiring large teams of security professionals to operate

Unfortunately for service providers just starting a practice, the skills and expenses required to run their own EDR-based service may be out of reach. For providers with established security specialization, they may find trying to build their detection and response services with market-leading solutions prices them out of their midmarket or SMB customers — only to find themselves also competing with the MDR services of their solution vendor.

Acronis Advanced Security + EDR, designed for service providers

Acronis understands that service providers need to balance offering effective services with meeting different client requirements and budgets.

We also know that they need an advanced security solution that can rightsize margins and in-house skills, is multitenant, SaaS based, offers better security outcomes — and — focuses on the right amount of automation and ease of use for rapid turn up and scale across multiple clients and their unique environments.

Designed for service providers, **Acronis Advanced Security + EDR** enables you to simplify endpoint protection — 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.

Streamline your detection and response services with Acronis
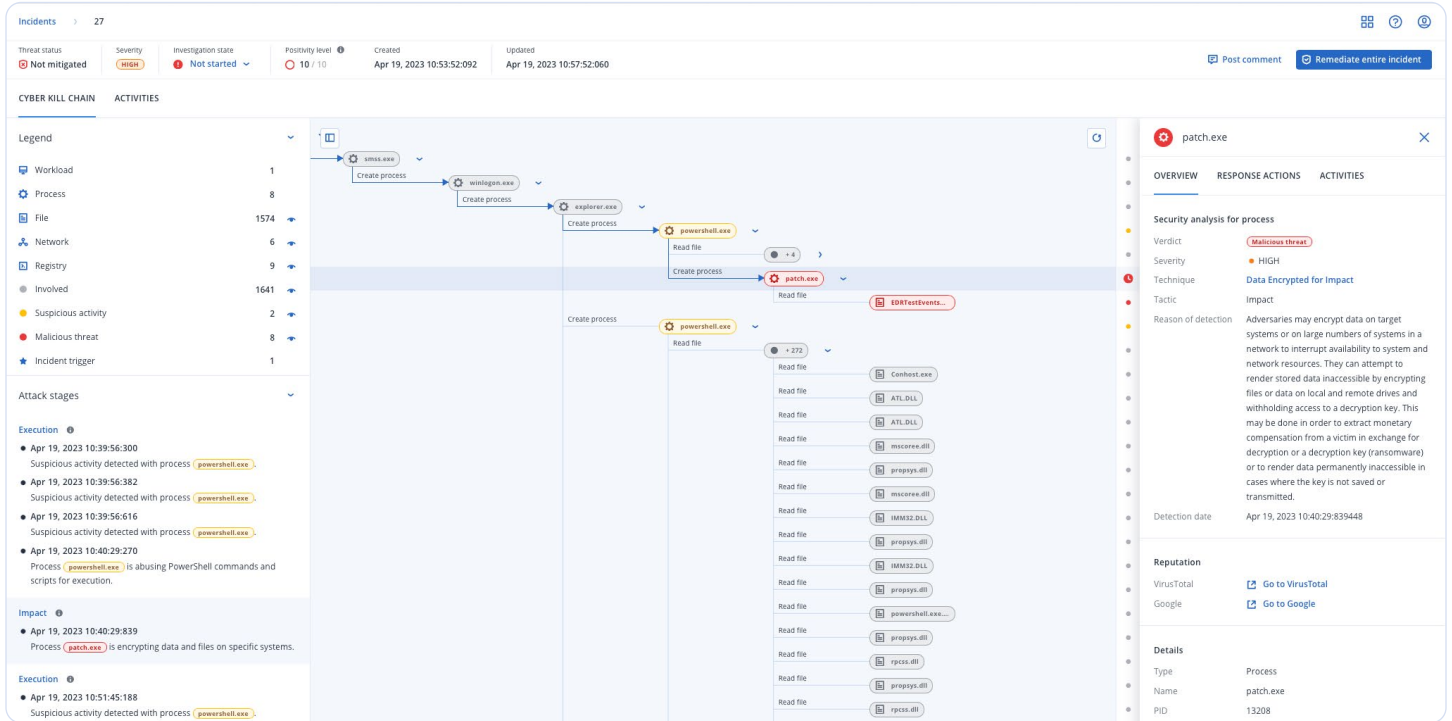
Optimized attack prioritization and analysis for rapid response	Integrated backup and recovery capabilities for unmatched business continuity	Complete cyber protection solution — designed for MSPs — in a single agent
• Streamline investigations with prioritization of potential incidents and reduced alert fatigue • Unlock minutes-not-hours analysis at scale, with automated correlation and AI-based guided attack interpretations • Increase visibility across MITRE ATT&CK® to rapidly grasp attack analysis and impact, including how an attack got in, what harm it caused, and how it potentially spread	• Integrated backup and recovery capabilities, providing unmatched business continuity where point-security solutions fail • Streamlined single-click remediation and recovery • Complete, integrated protection across the NIST Cybersecurity Framework — Identify, Protect, Detect, Respond, and Recover — all from a single solution.	• Quickly and easily launch new services using a single Acronis agent and console — to deploy, manage and scale • Easily scale across multiple clients while preserving healthy margins and minimizing OpEx — no need for a large team of highly skilled people to operate • Partner with a vendor focused on your success and enablement — not competing with you for business.

Powered by award-winning endpoint protection

↘ Editors' choice

↘ AV-TEST participant and test winner

↘ VB100 certified

↘ ICSA Labs endpoint anti-malware certified

↘ AV-Comparatives certified

Unmatched business resilience with Acronis

With Acronis you can count on a single platform for holistic endpoint protection and business continuity, aligned with established industry standards such as NIST, enabling you to identify vulnerable assets and data, proactively protect them, detect and stop any threats, and respond to and recover from attacks.

Acronis: Business continuity across NIST

Identify	Protect	Detect	Respond	Recover
Advanced Security + EDR				
• HW inventory • Unprotected endpoint discovery	• Vulnerability assessments • Exploit prevention • Device control • Security configuration	• Emerging threats feed • Search for IOCs of emerging threats • Anti-malware and anti-ransomware • AI- and ML-based behavioral detection • URL filtering	• Rapid incident analysis • Workload remediation with isolation • Forensic backups	• Rapid rollback of attacks • One-click mass recovery • Self-recovery
Acronis Cyber Protect Cloud				
• SW inventory • Data classification	• Patch management • DLP • Backup integration • Cyber scripting	• Email security	• Investigation via remote connection	• Pre-integrated with disaster recovery

EDR key capabilities

Prioritization of incidents

Monitor and automatically correlate endpoint events, with prioritization of suspicious event chains in the form of incident alerts.

Automated interpretation of incidents mapped to MITRE ATT&CK®

Streamline response and increase reactiveness to threats, leveraging AI-based interpretations of attacks

mapped to MITRE ATT&CK® to understand in minutes:

- How the attacker got in
- How they hid their tracks
- What harm the attack caused and how it caused it
- How the attack spread

Single-click response to attacks for unmatched business continuity

Prevail where point solutions fail — leverage the full power of integration among cybersecurity, data protection and endpoint security configuration management via a single-click response to incidents:

- **Remediate** by isolating endpoints and quarantining threats
- **Investigate further** using remote connections and forensic backups
- **Prevent future attacks** closing open vulnerabilities
- **Ensure business continuit**y with attack rollbacks and integrated backup and recovery

Simplify endpoint security today

Don't resort to multiple tools and advanced security expertise to protect endpoints. Simplify endpoint security with Acronis EDR.

→ **Learn more**

1. Source: **"2022 Data Breach Investigation Report", Verizon**