Acronis

Advanced Security + Endpoint Detection and Response (EDR) for **Acronis** Cyber Protect Cloud

Early-access: Q1 2022

THE ONLY EDR DESIGNED FOR MSPS, WITH NO SECURITY EXPERTISE REQUIRED

Current EDR solutions require extensive and costly security expertise, such as internal SOC team or MDR services. In addition, you need to have a suite of other solutions to respond to and remediate the threat fully.

Acronis Advanced Security + EDR enables you to quickly and easily detect, visualize and analyze advanced threats and hacking techniques that bypass other security layers. That's because its easy-to-understand interpretation of attacks empowers MSPs to rapidly investigate, respond, remediate and recover.

ENHANCE YOUR SECURITY SERVICE TECH STACK WITH STREAMLINED INCIDENT INVESTIGATION AND RESPONSE

Combine the power of threat prevention and detection	Analyze attacks within minutes	Recover business operations faster
Prevent most threats from becoming breaches while increasing the visibility of the attack flow. Empower your team to detect and respond to advanced attacks, which bypass other protection layers, such as advanced persistent threats (APTs).	Eliminate incident- analysis complexity with an automatic attack chain interpretation that every team member can understand. Automatically correlate events pertaining to an incident without needing to analyze hundreds of lines of logs.	Enable hyper-efficient remediation with centralized response management. Empower your team with an unmatched array of responses to investigate and remediate the threat, recover data and close existing security gaps.

*Advanced Security + EDR includes all the functionalities of <u>Acronis Cyber Protect Cloud</u> and <u>Advanced Security</u>.

Command a premium for your expertise

- Achieve higher revenue per client with advanced security services that are otherwise unavailable in the MSP market
- Control your TCO and enable better margins with easier service-tiering using a single, integrated platform for backup and disaster recovery, next-generation anti-malware, email security, workload management and EDR capabilities

Maintain your margins and prevent runaway costs

- Spend less time on incident investigation by unlocking minutesnot-hours threat analysis and response
- Eliminate the need for highly-skilled security personnel such as external SOC teams and MDR services
- Gain end-to-end visibility over all steps of the attack with automatic correlation of events

Minimize risks for clients and strengthen their security posture

- Provide faster remediation
 andrecovery centralize incident
 response through integrations with
 other cyber protection technologies
- Detect and respond to advanced threats – catch threats that bypass preventive security layers
- Prepare forensic and breach reports
 with ease pass more audits and
 simplify regulatory compliance

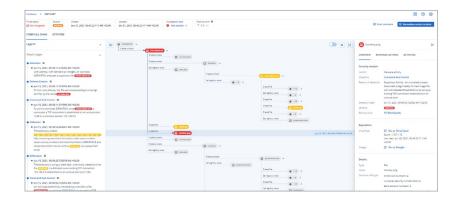
ACHIEVE RAPID INCIDENT ANALYSIS AND RESPONSE FOR CLIENTS WITH UNMATCHED SIMPLICITY

Easy-to- understand interpretation of attacks	Unmatched threat response capabilities	Multifaceted event correlation	Effortless deployment	Centralized cyber protection via a single console
Rely on your team regardless of its security expertise. Understanding incidents and how to respond to them is easy: the interpreted attack chain shortens incident analysis from hours to minutes.	Centralized management enables you to deliver an unmatched array of responses: investigation, threat remediation, data and system recovery and preventive measures against similar future threats.	Empower your team to see beyond standard events on client workloads. The unique integration of data protection, next-generation anti- malware, and EDR offers far greater visibility.	Enable the delivery of EDR services to your clients with just the flick of a switch. Once Acronis Cyber Protect Cloud agent is installed, you'll minimize provisioning overhead.	Control your TCO, reduce management overhead and boost margins using a single solution that integrates backup, disaster recovery, next-generation anti-malware, email security, workload managementand EDR.

Cut your average threat investigation and response time to a few minutes

- Embolden your team to effortlessly analyze attacks, regardless of their level of expertise
- · Narrated incidents are easy to interpret, emphasizing the objectives of each step and the artefacts targeted by the attacker

Analyst verdict	
True positive	
Remediation actions	
Step 1 – Stop threats	
Stops all processes related to the threat.	
Step 2 - Quarantine threats	
After being stopped, all malicious or suspicious processes and files are quarantined.	
Step 3 – Rollback changes	
Rollback first deletes any new registry entries, scheduled tasks or files created by the threat (and	any of its children
threats). Next, rollback reverts any modifications made by the threat (or its children) to the registr	
and/or files existing on the workload prior to the attack. To optimize speed, rollback tries to resto	re items from the
local cache. Items that fail to be restored will be restored by the system from backup images.	
Restore workload	
If any of the above selected remediation steps fail completely of partially	
Prevention actions	
Add to blocklist	
Adds all threats from the incident to the blocklist in the selected protection plans. This action will threats from future executions	prevent these
Protection plan	~
Patch workload	
Prevents further attacks by patching software that contains vulnerabilities used by attackers in or	der to get a
foothold on the workload	
Change Investigation state of the Incident to: Closed	



Mount a more comprehensive response than ever before

IInvestigate

• Investigate threats with a secure, • Recover lost or affected data remote connection to workloads and automatically save forensic data in backups for follow-up audits and investigations

Remediate

 Remediate the threat by isolating
 Prevent future breaches by the workload, killing malware processes, guarantining the threat and enabling fast rollback of any changes made to clients' workloads

Recover business operations

due to breaches and minimize downtime withintegrated bestof-breed backup and disaster recovery

Prevent

closing security vulnerabilities leveraged in the attack with patch management and blocking analyzed threads from being executed

Early-access to Advanced Security + EDR

Register to enjoy exclusive early access to materials and try the only EDR solution designed for MSPs - launching Q1 2022.

REGISTER FOR EARLY-ACCES

Acronis

Learn more at www.acronis.com Copyright © 2002-2021 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 othe trademarks or registered trademarks are the property of their respective owners. Technical changes and