DATA SHEET

Acronis
Advanced Security + Endpoint Detection and Response (EDR)

For service providers

An EDR that's effective and efficient

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/XDR solutions capable of countering these threats introduce:

- High costs
- Complexity
- A long time to value
- Scalability challenges

Unfortunately for service providers just starting a practice, the skills and expenses required to run their own MDR service may be out of reach. For providers with established security specialization, they may find trying to build their MDR 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

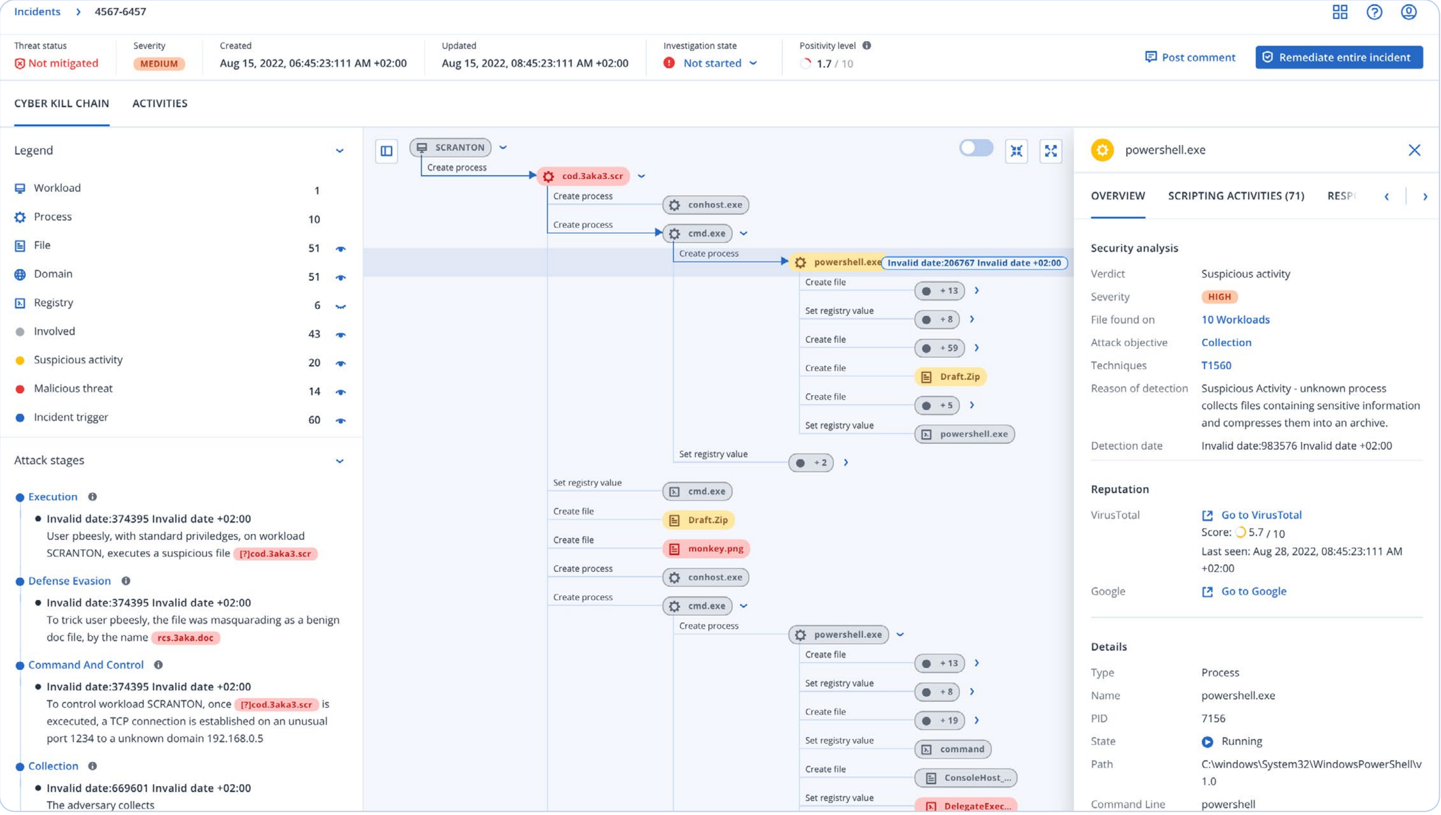
Acronis understands that service providers need to balance offering effective services with meeting different customer requirements and budgets.

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 customers and their unique environments.

Acronis Advanced Security + EDR is an MSP-class solution delivered as part of a single, integrated platform. As a part of Acronis Cyber Protect Cloud, you can build modular security services while supporting your customers across the NIST framework of IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER stages for true business resilience.

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

Streamline your detection and response services with Acronis



Threat status	Severity	Created	Updated	Investigation state	Positivity level
Not mitigated	MEDIUM	Aug 15, 2022, 06:45:23:111 AM +02:00	Aug 15, 2022, 08:45:23:111 AM +02:00	Not started	1.7 / 10

Legend

Workload	1
Process	10
File	51
Domain	51
Registry	6
Involved	43
Suspicious activity	20
Malicious threat	14
Incident trigger	60

Attack stages

- Execution
  - **Invalid date:374395 Invalid date +02:00**
    User pbeesly, with standard priviledges, on workload SCRANTON, executes a suspicious file [?]cod.3aka3.scr
- Defense Evasion
  - **Invalid date:374395 Invalid date +02:00**
    To trick user pbeesly, the file was masquarading as a benign doc file, by the name rcs.3aka.doc
- Command And Control
  - **Invalid date:374395 Invalid date +02:00**
    To control workload SCRANTON, once [?]cod.3aka3.scr is excecuted, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5
- Collection
  - **Invalid date:669601 Invalid date +02:00**
    The adversary collects

Security analysis

Verdict	Suspicious activity
Severity	HIGH
File found on	10 Workloads
Attack objective	Collection
Techniques	T1560
Reason of detection	Suspicious Activity - unknown process collects files containing sensitive information and compresses them into an archive.
Detection date	Invalid date:983576 Invalid date +02:00

Reputation

VirusTotal	Go to VirusTotal Score: 5.7 / 10 Last seen: Aug 28, 2022, 08:45:23:111 AM +02:00
Google	Go to Google

Details

Type	Process
Name	powershell.exe
PID	7156
State	Running
Path	C:\windows\System32\WindowsPowerShell\v1.0
Command Line	powershell

Rapid detection and incident analysis

- Increase visibility across **MITRE ATT&CK®**
- Streamline analysis with automated correlation and **human-friendly interpretation**
- Get better outcomes and fewer false positives with **prioritization of suspicious activities**

MSP-class solution

- **Turn up services rapidly** on an existing Acronis agent and console
- Benefit from easy-to-use **single-click response** to guided interpretations
- **Focus on what matters** like true indicators-of-compromise (IoCs) – not scanning logs
- Work with a vendor ally focused on your success and positive customer outcomes – **not competing with you for your customer business.**

Continuity at the speed of business

- Protect across the **NIST** framework
- Remediate with **centralized response management**
- **Go proactive** before threats become breaches
- **Count on pre-integrated recovery** capabilities where point-security solutions fail

Key capabilities

Prioritization of suspicious activities

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

Automated MITRE ATT&CK® attack chain visualization and interpretation

Unlock minutes-not-months incident investigation guided by an automated visualization and interpretation of the attack chain. Mapped to the MITRE ATT&CK® framework (from Reconnaissance to Discovery), explains in an easy-to-understand way how the threat got in, spread, what damage it caused, and how it hid its tracks.

Intelligent search for Indicators of Compromise (IoCs)

Automated threat hunting capabilities help service providers streamline and focus efforts on highly prioritized IoCs of emerging threats based on an actionable threat intelligence feed.

Single-click, holistic response

Unlike pure-play cybersecurity solutions, Acronis Cyber Protect Cloud brings the full power of its platform with integrated capabilities across the NIST framework for real business continuity.

Identify

You need to know what you have to fully investigate into it and protect it. Our platform includes both **inventory** and **data classification** tools to help you better understand attack surfaces.

Protect

Close security vulnerabilities using our **threat feed, forensic insights**, and natively integrated tools like **data protection maps, patch management, blocking analyzed attacks,** and **policy management.**

Detect

Continuous monitoring using automated **behavioral- and signature-based engines**, URL filtering, an emerging **threat intelligence** feed, **event correlation** and **MITRE ATT&CK®**

Respond

Investigate threats and conduct follow-up audits using a secure, **remote connection** into workloads or reviewing automatically saved **forensic data in backups**. Then, remediate via **isolation, killing processes, quarantining,** and **attack-specific rollbacks.**

Recover

Ensure systems, data and the customer business are up and running using our fully-integrated, market-leading **backup and disaster recovery** solutions.

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

Availability

Acronis Advanced Security + EDR will be available in our Early Access Program starting December 2022.

Please contact your Acronis representative for more information.

Acronis

Learn more at
www.acronis.com