Acronis MDR provided by Acronis TRU

Service Definition

Version 1.1

Acronis



Table of Contents

1 Purpose and motivation 3

2 Features 4

3 Phases and interactions 5

3.1 Enablement 5

3.2 Learning Phase 5

3.3 Service 6

3.3.1 Incident Detected 6

3.3.2 Monthly reports 6

3.3.3 Communication Channels 6

4 Service components 7

4.1 Monitoring 7

4.2 Isolation 7

4.3 Response 7

4.3.1 Advanced Response Actions 8

4.3.2 Critical Endpoints 9

4.4 Threat Hunting 10

4.5 Reporting 10

4.5.1 Standard Monthly Reports 10

4.5.2 Advanced Monthly Reports 11

4.5.3 Root Cause Analysis Reports 11

4.5.4 Threat Hunting Reports 11

4.6 On-demand Incident Investigation Requests 13

5 RACI Matrix 14

6 Service Level Agreement (SLAs) 15

7 Extended Detection and Response (XDR) 16

1 Purpose and motivation

The primary goal of the MDR service is to enable Acronis partners to fully leverage the Acronis Cyber Protect platform without requiring a dedicated security incident management team.

The MDR service is offered on top of Acronis Advanced Security + EDR/XDR product. Acronis agent is used to collect and provide incident telemetry to the MDR vendor.

The intention of the current document is to provide the Acronis Partner with detailed information about the expectations for the service.

The MDR (Managed Detection and Response) service is available in two levels to meet varying partner needs:

- **Standard:** Designed for partners who can engage in some interaction with the platform. This level includes monitoring and incident response; however, mitigation actions are not implemented as part of the service. Instead, detailed mitigation recommendations are provided as comments within each incident report, allowing partners to address them according to their own processes.
- **Advanced:** A fully managed, hands-off service in which all mitigation actions are carried out as part of the service. This level includes advanced capabilities such as proactive Threat Hunting and comprehensive root cause analysis, delivering a robust and seamless security solution that requires minimal intervention from the MSP.

2 Features

Features	Standard	Advanced
24x7 monitoring	YES	YES
24x7 automated mitigation	YES	YES
24x7 response (isolation)	YES	YES
Incident analysis and verdict with response recommendations	YES	YES
Service Portal access	YES	YES
In-console MDR Menu	YES	YES
24x7 manual advanced mitigation and response using Acronis Capabilities	NO	YES
Root cause analysis and incident report for new critical true positive incidents	NO	YES
Threat Intelligence News and IOCs	NO	YES
Monthly Report	BASIC	ADVANCED
Threat Hunting	NO	YES
On demand incident investigation	NO	YES

3 Phases and interactions

3.1 Enablement

Service enablement will be performed in the MDR Menu of the Protection page within the Acronis Cyber Protect Cloud Console, using the "**Acronis MDR by Acronis TRU**" integration. When enabled at partner-level, it will ask for the following:

- **Escalation Contacts**: Up to four (minimum of two) partner contacts that need to be notified whenever an incident happens. These contacts will also be created in the Service Portal to access and interact in real-time with ongoing incidents. The primary contact will be used as the main stakeholder for the incidents and registered as the "reporter" in the Service Portal. Primary contact will also be the first to be contacted for approval whenever a mitigation action is required on a Critical Endpoint (see Critical Endpoints section for more information).
- **Multi Data Center toggle**: If you plan to enable the Acronis MDR by Acronis TRU service in multiple data centers, this toggle needs to be enabled.

After successfully enabling the integration at partner-level, specific customers need to be added to the service, specifying the desired Service Level.

3.2 Learning Phase

The first two weeks of the service will be dedicated to the learning phase, during which the Acronis MDR team will analyze and familiarize themselves with the customer's environment.

During this period, the primary objective is to understand the normal operational behavior of the systems and endpoints, allowing the detection logic to better distinguish between legitimate activities and potential threats.

As part of this process, the team will:

- **Review and assess security events and alerts** generated during the initial monitoring period.
- Identify and classify **potential false positives** that may arise due to environment-specific configurations, applications, or legitimate administrative activities.
- Request the necessary **configuration adjustments or exclusions** from the partner to fine-tune detections and ensure accuracy.
- Establish a **baseline of normal activity** to improve detection fidelity and reduce alert noise going forward.

By the end of the learning phase, the MDR service will be better adapted to the customer's specific operational context, allowing for more effective and efficient threat detection and response in subsequent phases.

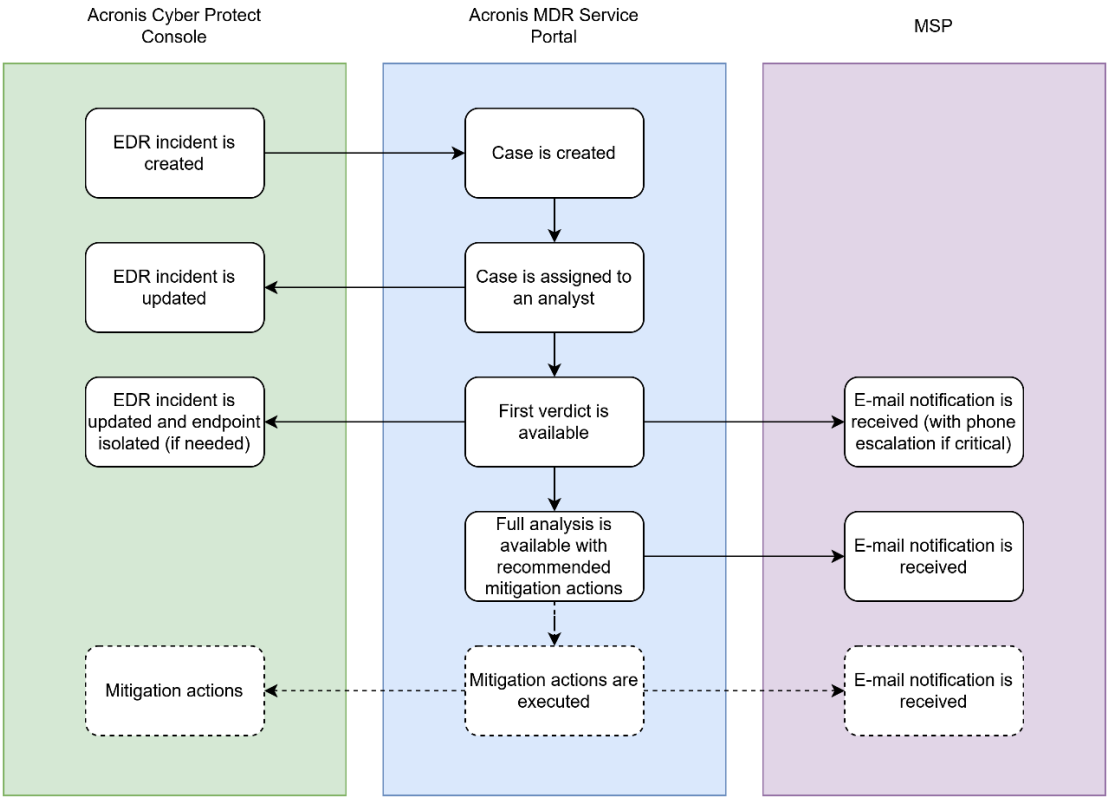
3.3 Service

3.3.1 Incident Detected

Once the Acronis EDR agent detects any suspicious or malicious activity and an incident is generated, the MDR Team will receive all the information and will start analyzing the activity. Once this happens and the incident is confirmed to be a true positive, all MSP's contacts defined in the Escalation Contacts will be notified via e-mail. In this notification, a link will be provided to access the incident in the Service Portal, with real-time visibility on any comment added by the analysts.

Once the investigation is concluded, a new notification will be sent, together with the conclusions about the incident, including all the recommended actions for remediation.

If the customer has the Advanced Service Level, those mitigation actions will be conducted with the necessary approvals in place.



3.3.2 Monthly reports

As part of the service, monthly reports will be provided and sent via e-mail to all the escalation contacts. Details of the report can be found in Regular Monthly Reports.

3.3.3 Communication Channels

Official communications channels are:

- E-mail to acronis.mdr@acronis.com. For general questions about the service, feedback, escalations.
- Service Portal https://acronismdr.atlassian.net/servicedesk. For incident-related questions, providing additional context and re-openings (by requesting it in a comment).

4 Service components

4.1 Monitoring

Acronis monitors security alerts and notifications from the customer's endpoints as detected through the Acronis EDR/XDR agent and platform. Acronis correlates and prioritizes security alerts with common threats, threat intelligence, and third-party threat intelligence, leveraging analytics, security orchestration, and response to help determine whether events or notifications represent a breach or compromise.

Any detected security events that Acronis believes may pose a potential security threat will be escalated into a customer-facing security incident ("Security Incident"), accessible in the Acronis Cyber Protect EDR portal and in the Service Portal. Security Incidents will be reported promptly in accordance with the Service Level Agreement (SLA). Acronis will provide context on the severity of the threat and recommended remediation actions (including any action already taken).

4.2 Isolation

Acronis analysts will leverage predefined playbooks to initiate a response in the form of endpoint isolation. Any response actions by Acronis will be reflected in the body of the appropriate security incident. The decision to isolate an endpoint will be made based on data from the endpoint, with further enrichment from threat intelligence and threat research. For critical endpoints, isolation will only be done after explicit approval by the MSP. MDR Analysts are authorized to isolate non-critical endpoints based on their situational evaluation, with implied customer consent.

4.3 Response

Acronis will analyze events, alerts, and data to identify potential threats and respond appropriately. Response and remediation activities will occur after the initial monitoring and isolation activities have been completed. After a security incident has been detected, Acronis will initiate responses aligned with the nature of the security incident. Responses and remediation activities include:

- Guidance on how to mitigate, stop, or prevent a security incident based on the data, intelligence, and advisories provided.
- Analysis and investigation of security events to determine the root cause and extent of compromise.
- Approved workflows (taking the Critical Endpoints group into account) to isolate machines, quarantine threats, or fully remediate the threat.
- A detailed security escalation, citing the customer-facing security incident, threat intelligence, and advisories.
- Incident escalation through various channels, including creating a security incident, email notifications, and phone calls (in critical situations), using the contact details provided by the MSP.
- Communication with the MSP until the threat has been remediated, providing timely updates as new information arises.

Where response actions are outside the scope of the MDR tooling or agreement, Acronis will provide recommendations on areas to focus. This may include recommendations for additional services such as incident response.

4.3.1 Advanced Response Actions

The following response actions will be used on top of isolation for the Advanced Service Level customers:

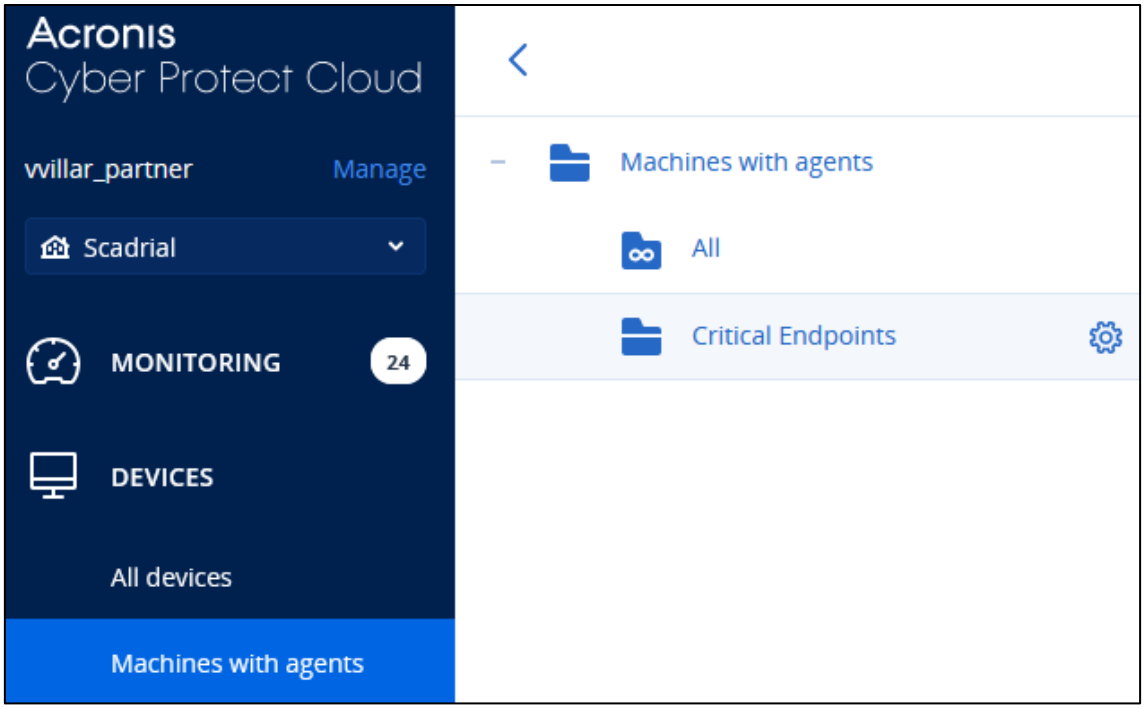
Action	Additional License Required
Stop threat (process)	None
Quarantine file	None
Add to block/allowlist	None
Rollback	None
Recover from backup*	Backup
Recover with DR*	Disaster Recovery
Execute custom script	RMM
Manual access through remote shell	RMM
Patch vulnerability	RMM
Suspend user*	XDR + M365 Integration
Force password reset*	XDR + M365 Integration
Terminate user sessions*	XDR + M365 Integration
Block network resource on Firewall*	XDR + Fortinet Firewall Integration
Block sender's email address*	XDR + FortiMail Integration

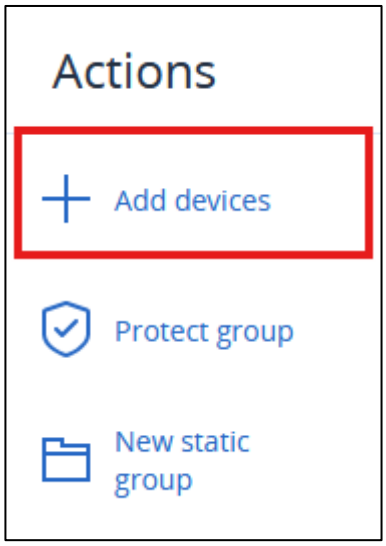
*Will always require approval

4.3.2 Critical Endpoints

MDR partners can configure a list of critical endpoints to exclude from response actions (including isolation), using the “Critical Endpoints” group that will be created upon enablement.

It can be done by accessing the “Devices” page in Acronis Cyber Protect Cloud:





Before running any kind of response action on these devices, the contacts defined upon enablement will be asked for approval (including a phone call if the incident is critical).

4.4 Threat Hunting

As part of the Advanced Service level, Acronis MDR will conduct monthly Threat Hunting exercises. These exercises will include:

- An **in-depth investigation** into the most critical threat(s) that may affect end customers. These investigations can cover topics such as new vulnerabilities, new advanced malware families, TTPs recently used by APT groups, and other related issues.
- A **hypothesis** about the types of behaviors that could be observed on an endpoint but may go undetected by traditional security solutions. This hypothesis can be supported by practical exercises carried out in virtualization labs to confirm the telemetry events that the Acronis agent would be able to collect.
- Based on the previous hypothesis, a **modelling** process should be developed to translate the observed behaviors into Acronis Event Search QL.
- This **search** should be conducted for all customers using MDR Advanced, treating any confirmed findings as **incidents** to be handled by the service, in accordance with established SLAs.

The methodology will be as follows:

- The hypothesis will be the same for all Advanced customers. This means that the query executed for each partner will be identical. During the initial phase of the service, these searches will be conducted manually, with API support planned for Q3 2026.
- All details of the investigation and research will be included as part of the Advanced monthly reporting package, delivered as a separate document. This will encompass the rationale behind the investigation, relevant technical details (including the modeled behaviors to monitor), and the query used for detection.
- If a finding is detected, it will be treated as a new incident, investigated and remediated through the standard incident response process, and summarized in the monthly report for the affected customer.

4.5 Reporting

The following reports will be included as part of the service:

Report	Frequency	Service Level
Standard Monthly Report	Monthly	Standard
Advanced Monthly Report	Monthly	Advanced
Root Cause Analysis Report	Per confirmed incident	Advanced
Threat Hunting Report	Monthly	Advanced

4.5.1 Standard Monthly Reports

A monthly report will be created with the following information:

- **Deployment Status**: Drill-down on how many endpoints have been contacting the console each day for the last 30 days, with the purpose of detecting anomalies in the connectivity or installation status of the endpoints.
- **Incident List with Statistics and Graphs** for:
    - **Severity Breakdown**
    - **Most Impacted Endpoints**

- **State Breakdown**
- **SLA Breakdown**
- **False Positive Rates** as per the resolution status
- **Incident Details** with ticket number, summary, creation time, status and resolution
- **Detection Type Breakdown** (process, file, network, registry, script)

The report will be sent no later than the fifth working day of the month (Monday to Friday).

4.5.2 Advanced Monthly Reports

In addition to the information included in the Standard Monthly Reports, Advanced partners will also receive:

- **Human-written Executive Summary**: Including the highlights for the given month, protection status, relevant incidents and recommendations.
- **Threat Intelligence**: Context regarding the latest research conducted by the Acronis TRU (Threat Research Unit)

4.5.3 Root Cause Analysis Reports

For confirmed true positive MDR incidents, a report will be created, composed of the following information:

1. **Executive Summary**: A brief explanation of what happened, where it occurred, and the implications and impact of the incident.
2. **Source of the Incident**: An enumeration of the different detections and context about them (e.g., alerted processes, suspicious connections).
3. **Infection Vector**: An analysis of the origin of the infection (as much as possible) that provides context on how the threat reached the endpoint.
4. **Timeline of the Incident**: A step-by-step analysis of the actions performed by the threat (including those blocked by the EDR/XDR).
5. **Impact**: If the incident was not successfully mitigated, a detailed analysis of its implications.
6. **Response Actions Performed**: A record of actions done to stop the threat.
7. **Threat Intelligence**: Basic context on the detected threats (e.g., the malware family, the TTPs used, the associated Threat Actor).
8. **Recommendations**: Actions to be taken by the partner or end customer to avoid being impacted by the threat in the future.

This report will be delivered no later than seven days after a critical incident has been resolved.

4.5.4 Threat Hunting Reports

As part of the monthly Proactive Threat Hunting exercises performed for Advanced Customers, a formal report will be produced to document the analytical process, supporting intelligence, technical evidence reviewed, and conclusions reached. This report ensures transparency of the hunting activity, supports security posture improvements, and provides auditable documentation of proactive security operations.

The report will include the following components:

Hypothesis

The hypothesis defines the suspected threat scenario that the hunting activity is attempting to confirm or disprove. It serves as the foundation of the hunting exercise and guides data collection, query design, and analysis methodology.

A well-defined hypothesis should be intelligence-driven and environment-specific, considering the customer's technology stack, threat exposure, and current attack trends.

It will include:

- A clear description of the potential attack technique or adversary behavior.
- The assumed attacker objective (e.g., persistence, lateral movement, data exfiltration, credential access).
- The scope of systems, identities, networks, or workloads being evaluated.
- The risk rationale explaining why this scenario is relevant to the customer.

Example:

An attacker may be leveraging compromised credentials to maintain persistent access through cloud identity services while avoiding traditional endpoint detection mechanisms.

Threat Intelligence

This section provides the external and internal intelligence sources used to build and validate the hunting hypothesis. It demonstrates that the hunting activity is aligned with real-world adversary behaviors and current threat landscape trends.

Threat intelligence may include:

- Known adversary tactics, techniques, and procedures (TTPs).
- Industry or sector-specific threat campaigns.
- Intelligence from commercial, open-source, or internal research feeds.
- Recent vulnerabilities or exploit trends relevant to the customer environment.
- Mapping to frameworks such as MITRE ATT&CK (when applicable).

The goal is to justify why the hypothesis is realistic and worth investigating.

Indicators of Compromise (IOCs)

This section lists the technical artifacts used to detect signs of malicious activity associated with the hypothesis. IOCs are used as search pivots across logs, telemetry, and security tools.

IOCs may include:

- Malicious IP addresses or ASN ranges.
- Suspicious domains or URLs.
- File hashes (MD5, SHA1, SHA256).
- Registry keys, mutexes, or file paths.
- Email indicators such as sender domains or message patterns.
- Cloud indicators such as suspicious API calls or service principals.

When possible, indicators will include:

- Source of the indicator.
- Confidence level.
- Last observed date.

- Context of malicious usage.

Findings

The findings section summarizes the results of the hunting exercise. It clearly states whether suspicious, malicious, or benign activity was observed and provides evidence supporting the conclusion.

Findings typically include:

- Summary of analyzed data sources.
- Description of suspicious or confirmed malicious activity (if found).
- Timeline of relevant events.
- Affected assets, users, or workloads.
- Risk assessment and potential business impact.
- Recommendations for remediation, detection improvements, or monitoring enhancements.

If no threats are identified, the report should still document:

- Data reviewed.
- Coverage achieved.
- Confidence level of the negative result.

Queries Used

This section documents the technical queries, scripts, or search logic used during the hunting activity. It ensures reproducibility, knowledge sharing, and continuous improvement of hunting methodologies.

This section enables future hunts to reuse proven detection logic and helps analysts validate or expand previous investigations.

4.6 On-demand Incident Investigation Requests

The service will allow Advanced partners and customers to submit the following requests:

- **Mitigated incident reopening (handled either automatically or manually).** This may occur when the MSP/customer believes more information is needed or when new evidence has emerged that could change the incident's assessment.
- **Investigation requests for detections made outside of the MDR service.** These investigations should be limited to the scope of the EDR/XDR telemetry and will only be available to Advanced customers. Threat Hunting methodology should be used to resolve such requests, utilizing the endpoint telemetry. Investigation requests must be opened through the Service Portal.

5 RACI Matrix

The RACI Matrix stands for:

- **R** - Responsible
- **A** - Accountable
- **C** - Consulted
- **I** - Informed

	Parties	
Action	**Acronis**	**MSP**
CyberApp enablement	C, I	R, A
Agent deployment on endpoints, including registration	I	R, A
Protection Plan configuration (for EDR)	I	R, A
Addition of endpoints to the Critical Endpoints Group	I	R, A
24x7 monitoring for new or updated alerts	R, A	I
Incident investigation and isolation	R, A	C, I
Root Cause analysis report generation	R, A	I
Incident updates	R, A	I
First verdict response through different communication channels	R, A	I
Incident recommendations generation	R, A	I
Application of incident recommendations (including rollback and recovery from backup)	Standard: C Advanced: R, A	Standard: R, A Advanced: C, I
Monthly reports generation	R, A	I
Proactive Threat Hunting execution and notification	R, A	I
On-demand incident investigations	A, C	R, C
Resolution of performance-related issues	A, C	R, C
Notification of exclusion requests	R, A	I
Resolution of exclusion requests	C, I	R, A

6 Service Level Agreement (SLAs)

Service Level Agreements (SLAs) establish the defined performance and response targets that Acronis commits to delivering as part of the service. These agreements are critical to ensure service consistency, operational transparency, and accountability. Clearly defined SLAs provide customers with assurance that security events will be addressed within agreed timeframes, helping to reduce risk exposure and limit potential business impact during security incidents.

METRIC	DEFINITION	OBJECTIVE
MEAN TIME TO REACT	The average amount of time measured from the time an alert is generated to the time an investigation is initiated.	15 minutes for high and critical severity alerts. 30 minutes for low and medium severity alerts.
MEAN TIME TO RESPOND	The average amount of time measured from the time an investigation is initiated to the time an analyst provides initial incident analysis or provides a response to the partner.	60 minutes.
MEAN TIME TO RESOLVE	The average amount of time measured from the time an investigation is initiated to the time the investigation is resolved.	24 hours (ad-hoc exceptions may apply if partner collaboration is needed).

7 Extended Detection and Response (XDR)

Acronis MDR will use all protection mechanisms included in the Acronis Advanced Security + XDR. This includes response and enrichment based on XDR integrations for customers using the feature.

Current situation: XDR integrations are only available in the Acronis Cyber Protect console. Therefore, if a specific response action using these integrations is needed, analysts will manually access the console. The same applies to enrichment: if an incident includes information that can be enriched via XDR integrations, this will be accessed directly from the console.

Coming soon: Acronis is working to include all these features in the public API to streamline incident management with related XDR information. In the future, these integrations will also be capable of generating external incidents, which will be accessible in the API and classified under a separate category to distinguish them from standard incidents.