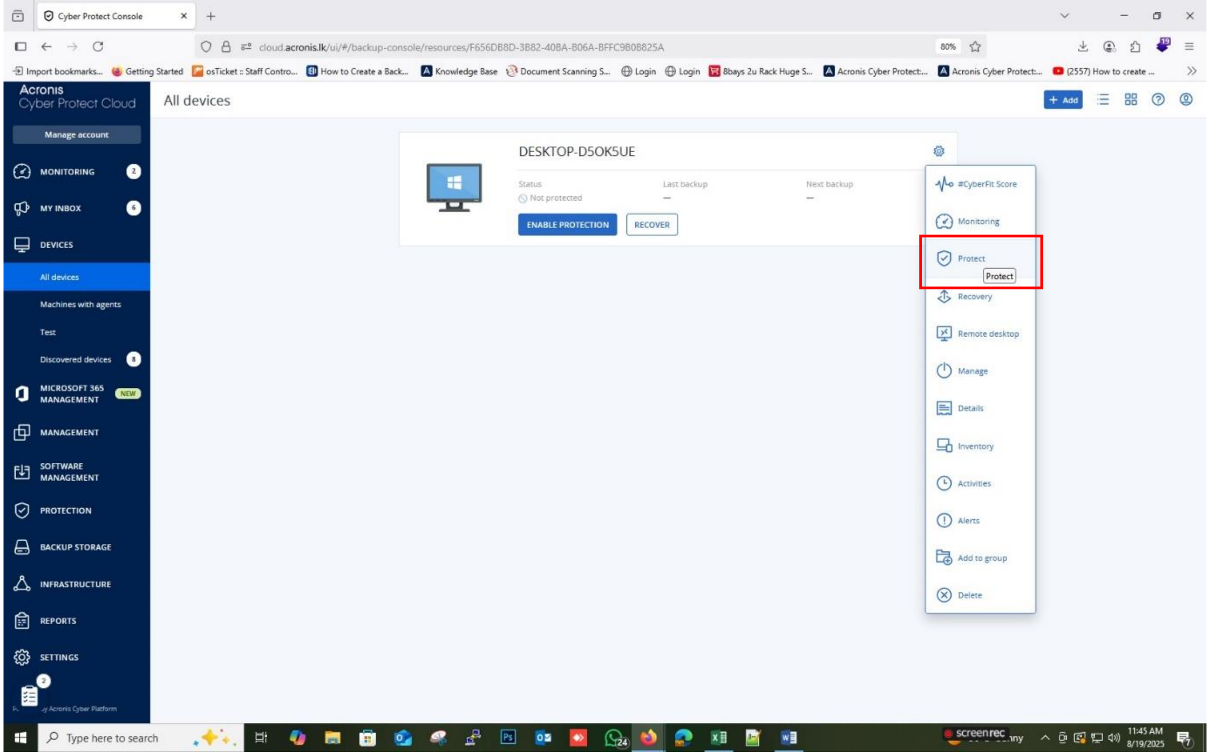
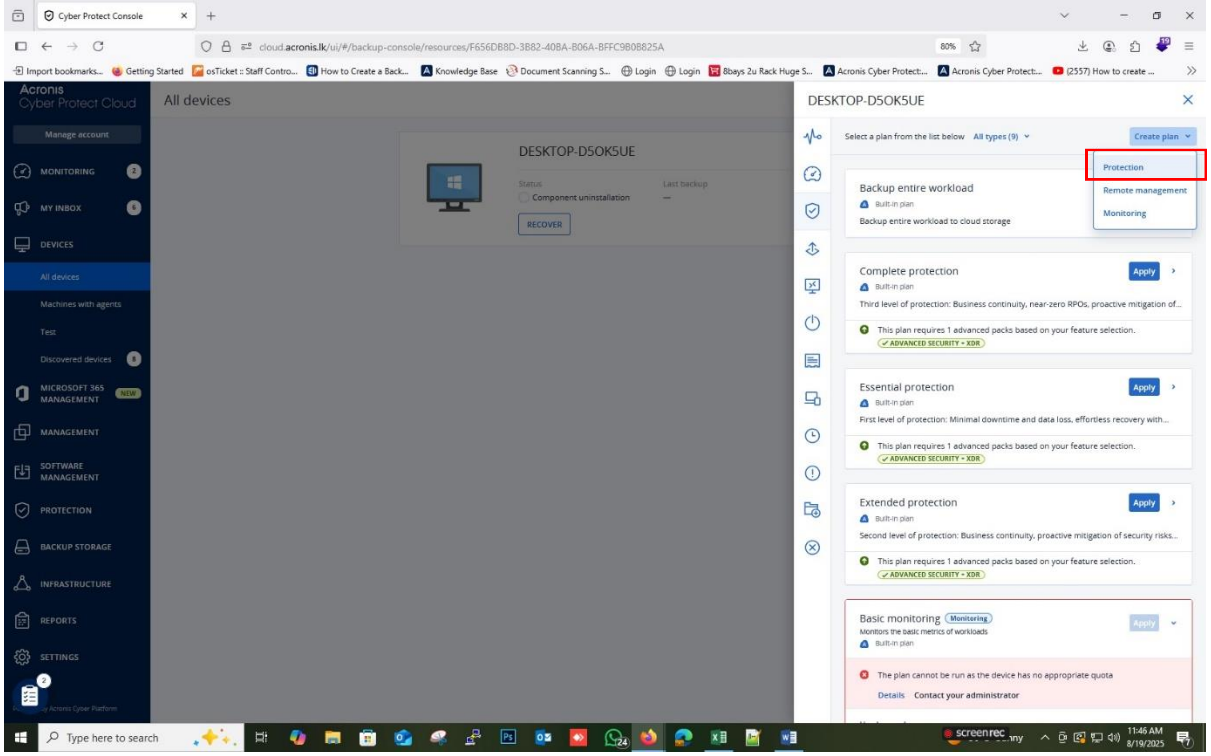
Steps to Create a protection plan

Open the customer's Cyber Protection console
Go to **Devices → All devices** for the tenant you're managing.



1. **Select endpoints → Protect → Create plan**
   Check the boxes next to the machines you want, then **Create plan** click **Protect**, (You can also go via **Management → Protection plans → Create plan**.)



Backup entire workload
Built-in plan
Backup entire workload to cloud storage

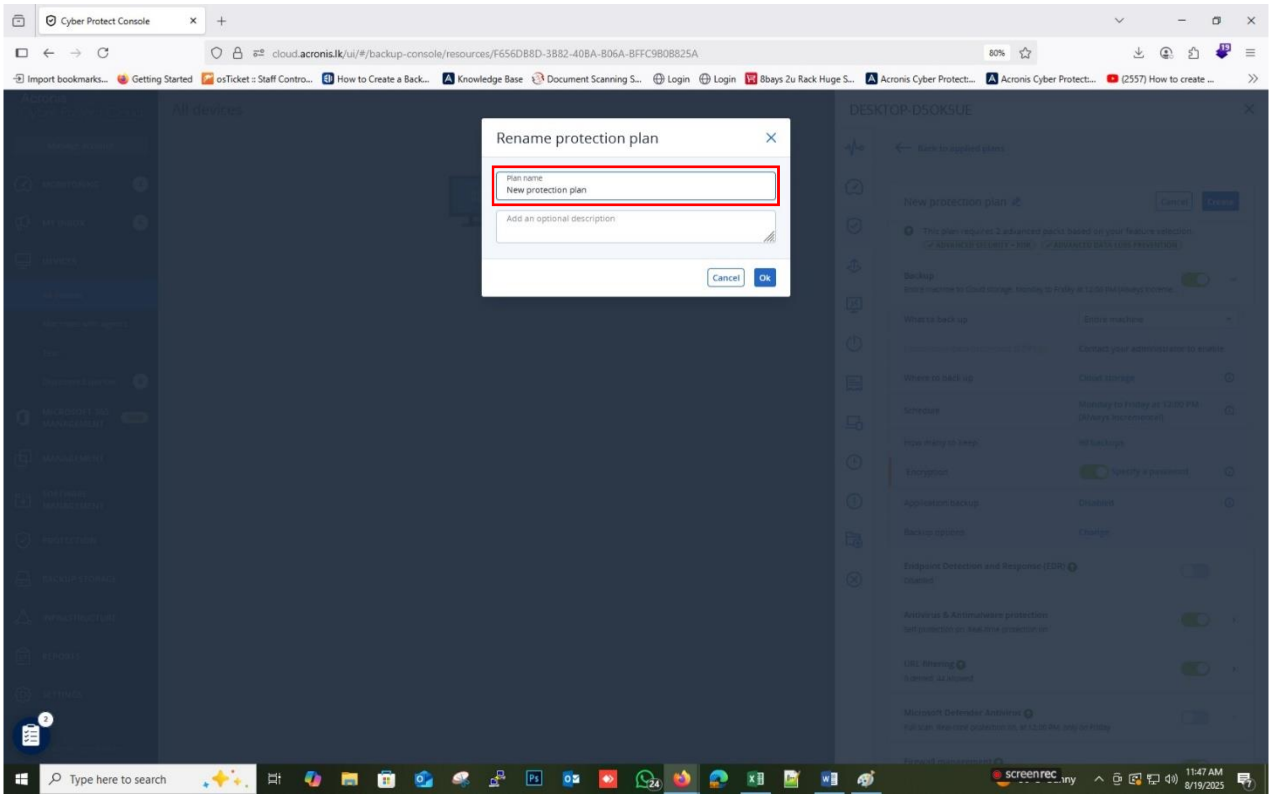
Complete protection
Built-in plan
Third level of protection: Business continuity, near-zero RPOs, proactive mitigation of...
This plan requires 1 advanced packs based on your feature selection.

Essential protection
Built-in plan
First level of protection: Minimal downtime and data loss, effortless recovery with...
This plan requires 1 advanced packs based on your feature selection.

Extended protection
Built-in plan
Second level of protection: Business continuity, proactive mitigation of security risks...
This plan requires 1 advanced packs based on your feature selection.

Basic monitoring Monitoring
Monitors the basic metrics of workloads
Built-in plan
The plan cannot be run as the device has no appropriate quota
Details Contact your administrator

2. **Name your plan**
   Give it something clear like “Security-Only (EDR)”.



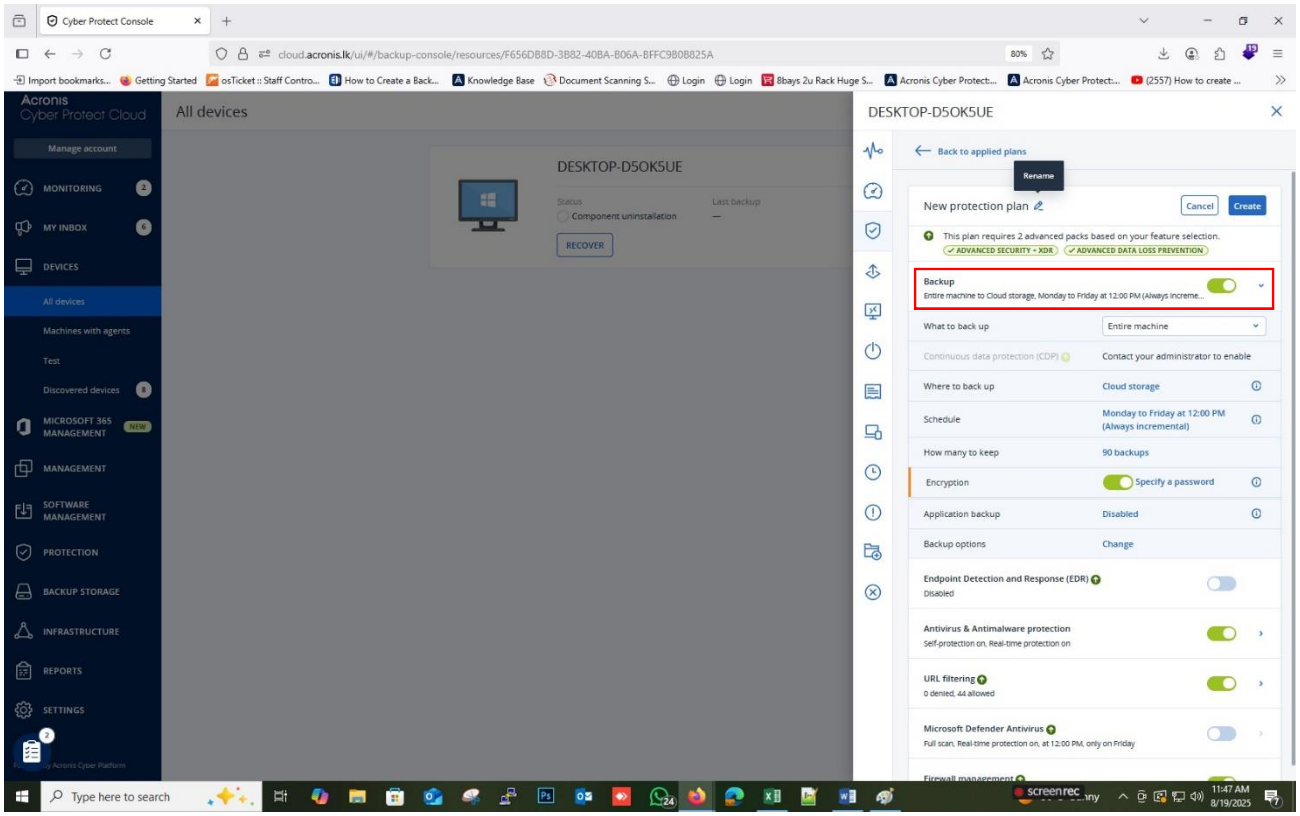
Rename protection plan

Plan name: New protection plan

Add an optional description

Cyber Protect Console
cloud.acronis.lk/ui/#/backup-console/resources/F656DB8D-3B82-40BA-B06A-BFFC9B08825A
Cancel
Ok
Type here to search
11:47 AM
8/19/2025

3. **Turn OFF the Backup module**
   In the plan editor, **disable** the **Backup** section (toggle it off / remove it). This ensures the plan is security-only. The Acronis UI supports enabling/disabling plan modules via toggles in this screen.



DESKTOP-D5OK5UE

New protection plan

This plan requires 2 advanced packs based on your feature selection.
✓ ADVANCED SECURITY + XDR ✓ ADVANCED DATA LOSS PREVENTION

Backup
Entire machine to Cloud storage, Monday to Friday at 12:00 PM (Always increme...

What to back up	Entire machine
Continuous data protection (CDP)	Contact your administrator to enable
Where to back up	Cloud storage
Schedule	Monday to Friday at 12:00 PM (Always incremental)
How many to keep	90 backups
Encryption	Specify a password
Application backup	Disabled
Backup options	Change

Endpoint Detection and Response (EDR)
Disabled

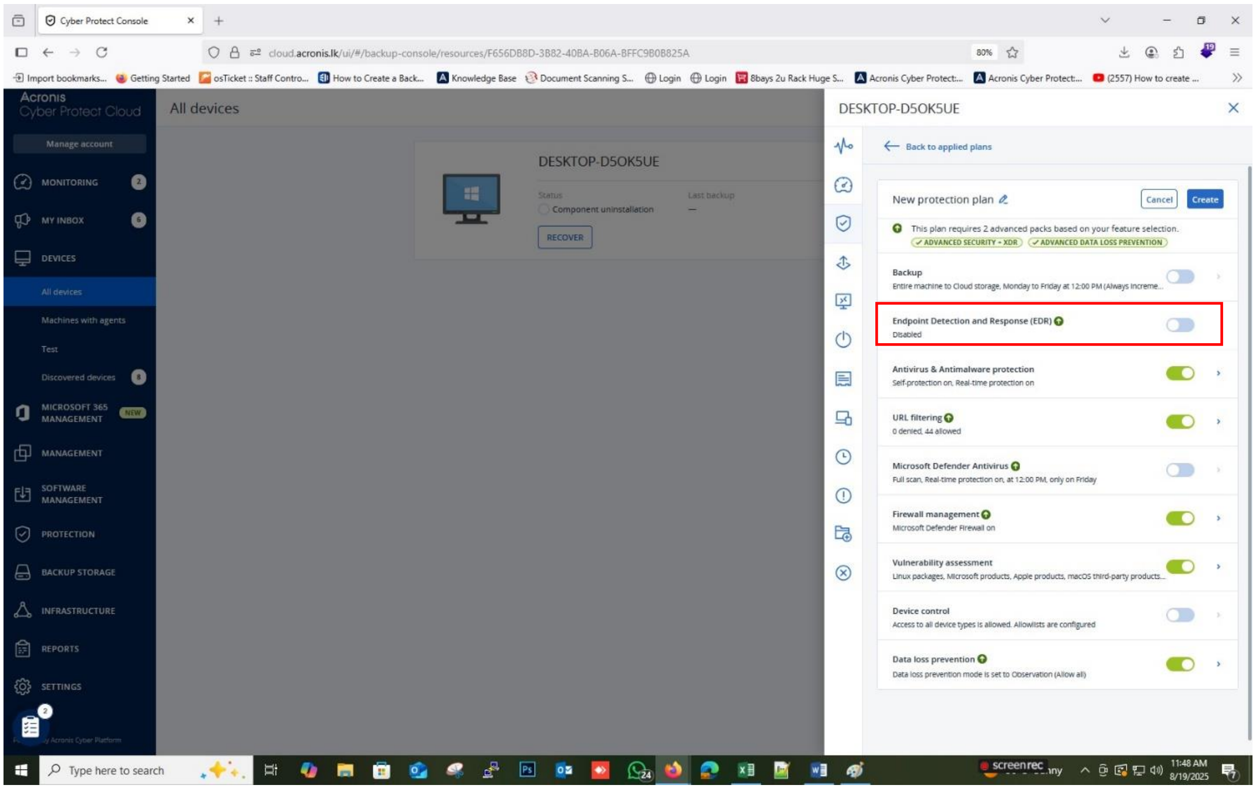
Antivirus & Antimalware protection
Self-protection on, Real-time protection on

URL filtering
0 denied, 44 allowed

Microsoft Defender Antivirus
Full scan, Real-time protection on, at 12:00 PM, only on Friday

Firewall management

4. **Enable EDR in the plan**
   Make sure **Endpoint Detection and Response (EDR)** is toggled on in the plan so telemetry and incident workflows are active for these devices (requires the Advanced Security + EDR entitlement on the tenant).



DESKTOP-D5OK5UE

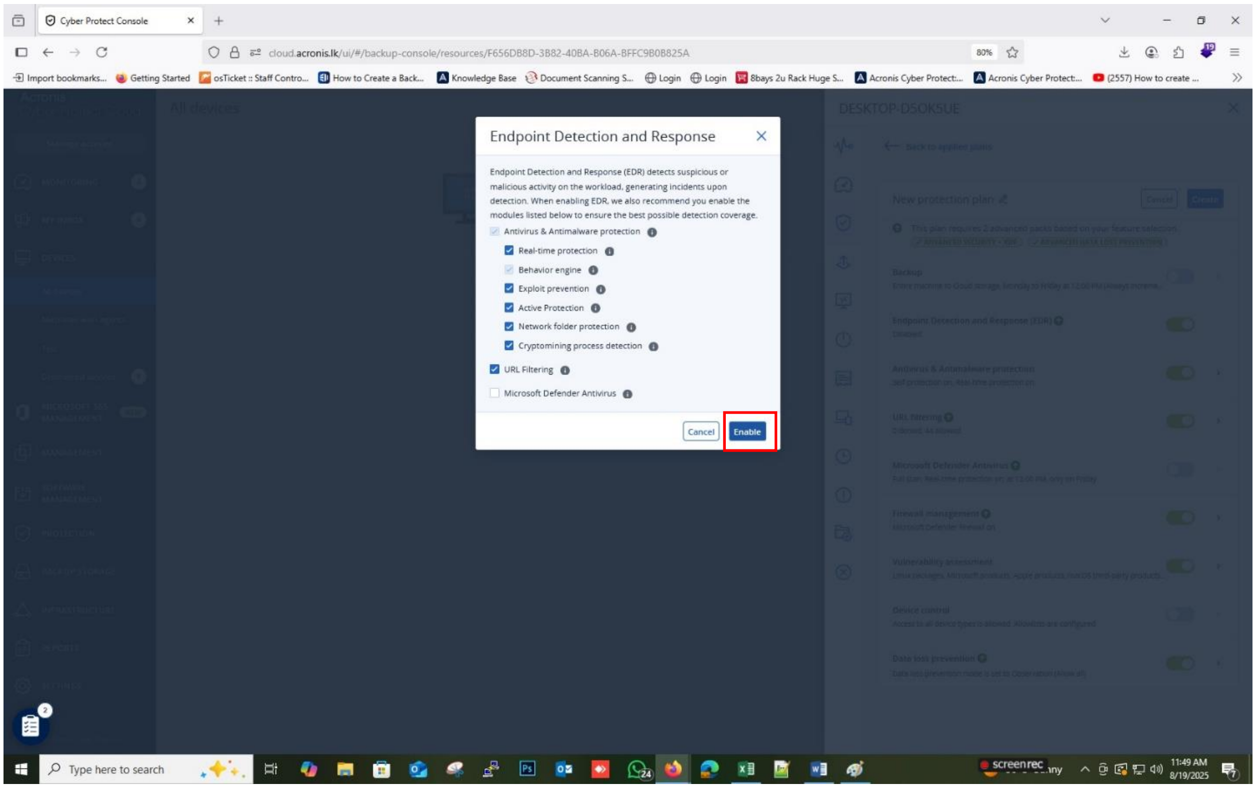
Back to applied plans

New protection plan

Cancel Create

This plan requires 2 advanced packs based on your feature selection.
✓ ADVANCED SECURITY + XDR ✓ ADVANCED DATA LOSS PREVENTION

Backup Entire machine to Cloud storage, Monday to Friday at 12:00 PM (Always increme...	○
Endpoint Detection and Response (EDR) Disabled	○
Antivirus & Antimalware protection Self-protection on, Real-time protection on	●
URL filtering 0 denied, 44 allowed	●
Microsoft Defender Antivirus Full scan, Real-time protection on, at 12:00 PM, only on Friday	○
Firewall management Microsoft Defender Firewall on	●
Vulnerability assessment Linux packages, Microsoft products, Apple products, macOS third-party products...	●
Device control Access to all device types is allowed. Allowlists are configured	○
Data loss prevention Data loss prevention mode is set to Observation (Allow all)	●



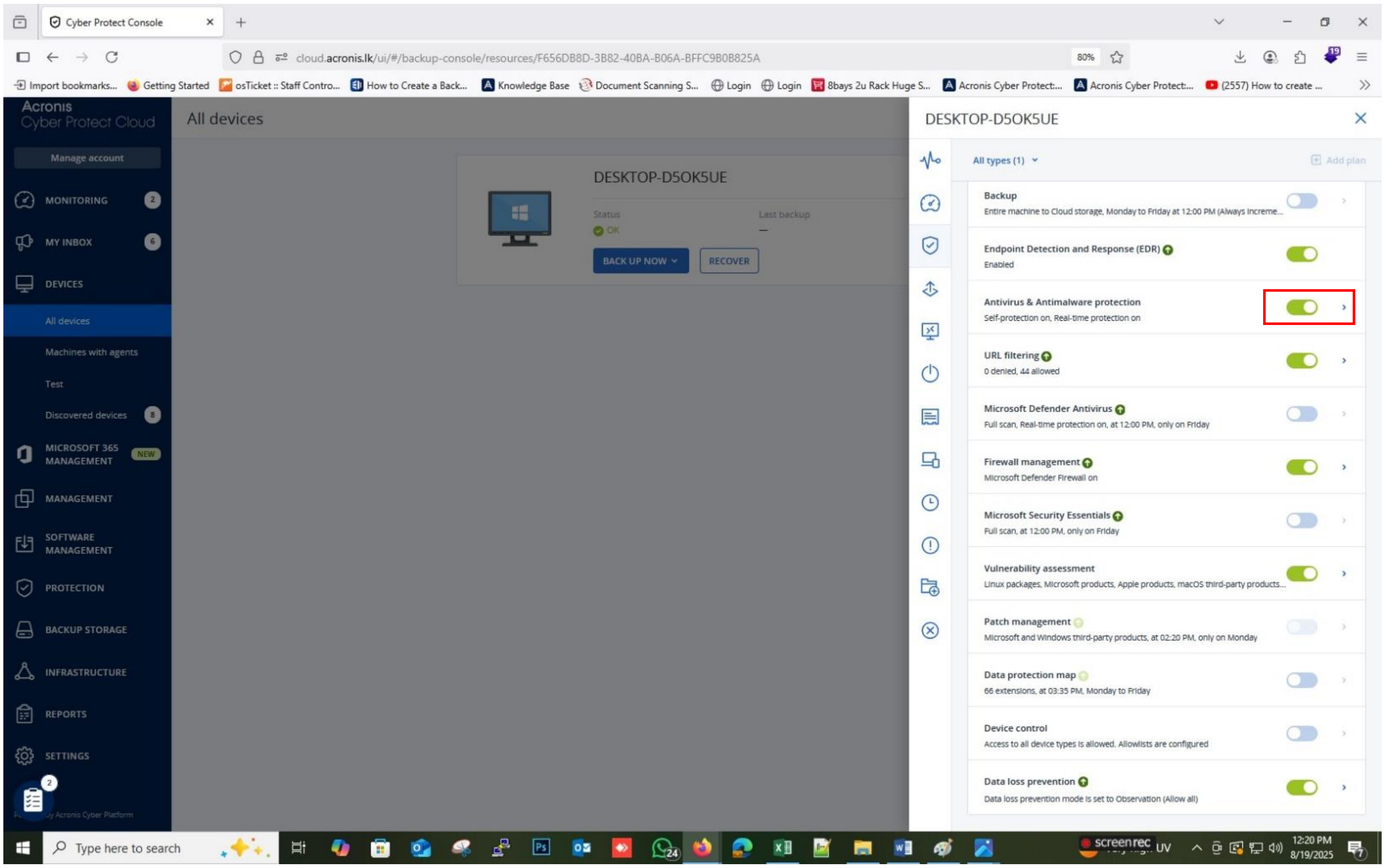
Endpoint Detection and Response

Endpoint Detection and Response (EDR) detects suspicious or malicious activity on the workload, generating incidents upon detection. When enabling EDR, we also recommend you enable the modules listed below to ensure the best possible detection coverage.

- ☑ Antivirus & Antimalware protection
  - ☑ Real-time protection
  - ☑ Behavior engine
  - ☑ Exploit prevention
  - ☑ Active Protection
  - ☑ Network folder protection
  - ☑ Cryptomining process detection
- ☑ URL Filtering
- □ Microsoft Defender Antivirus

Cancel Enable

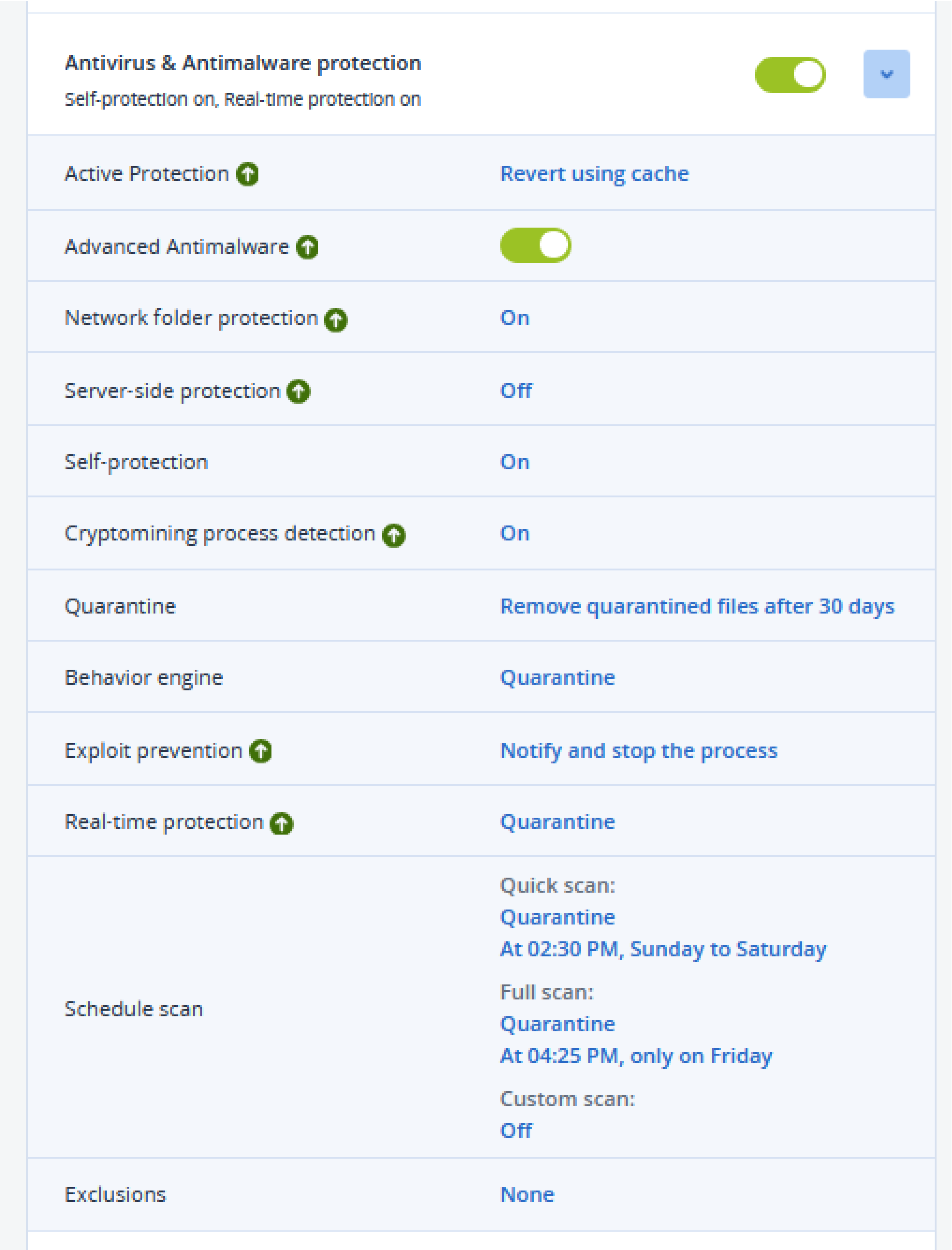
5. **Enable core security modules**
   In the same plan editor, expand and configure only the security features you want:
   - **Antimalware protection** → turn on **Real-time protection**, set desired action (e.g., Quarantine), add exclusions, and schedule scans.
   - **Exploit prevention**, **URL filtering**, **Device control**, **Vulnerability assessment / Patch management** as needed. The Acronis product demo covers where these live in the protection plan.



DESKTOP-D5OK5UE

All types (1)   Add plan

- Backup — Entire machine to Cloud storage, Monday to Friday at 12:00 PM (Always increme...
- Endpoint Detection and Response (EDR) — Enabled
- Antivirus & Antimalware protection — Self-protection on, Real-time protection on
- URL filtering — 0 denied, 44 allowed
- Microsoft Defender Antivirus — Full scan, Real-time protection on, at 12:00 PM, only on Friday
- Firewall management — Microsoft Defender Firewall on
- Microsoft Security Essentials — Full scan, at 12:00 PM, only on Friday
- Vulnerability assessment — Linux packages, Microsoft products, Apple products, macOS third-party products...
- Patch management — Microsoft and Windows third-party products, at 02:20 PM, only on Monday
- Data protection map — 66 extensions, at 03:35 PM, Monday to Friday
- Device control — Access to all device types is allowed. Allowlists are configured
- Data loss prevention — Data loss prevention mode is set to Observation (Allow all)



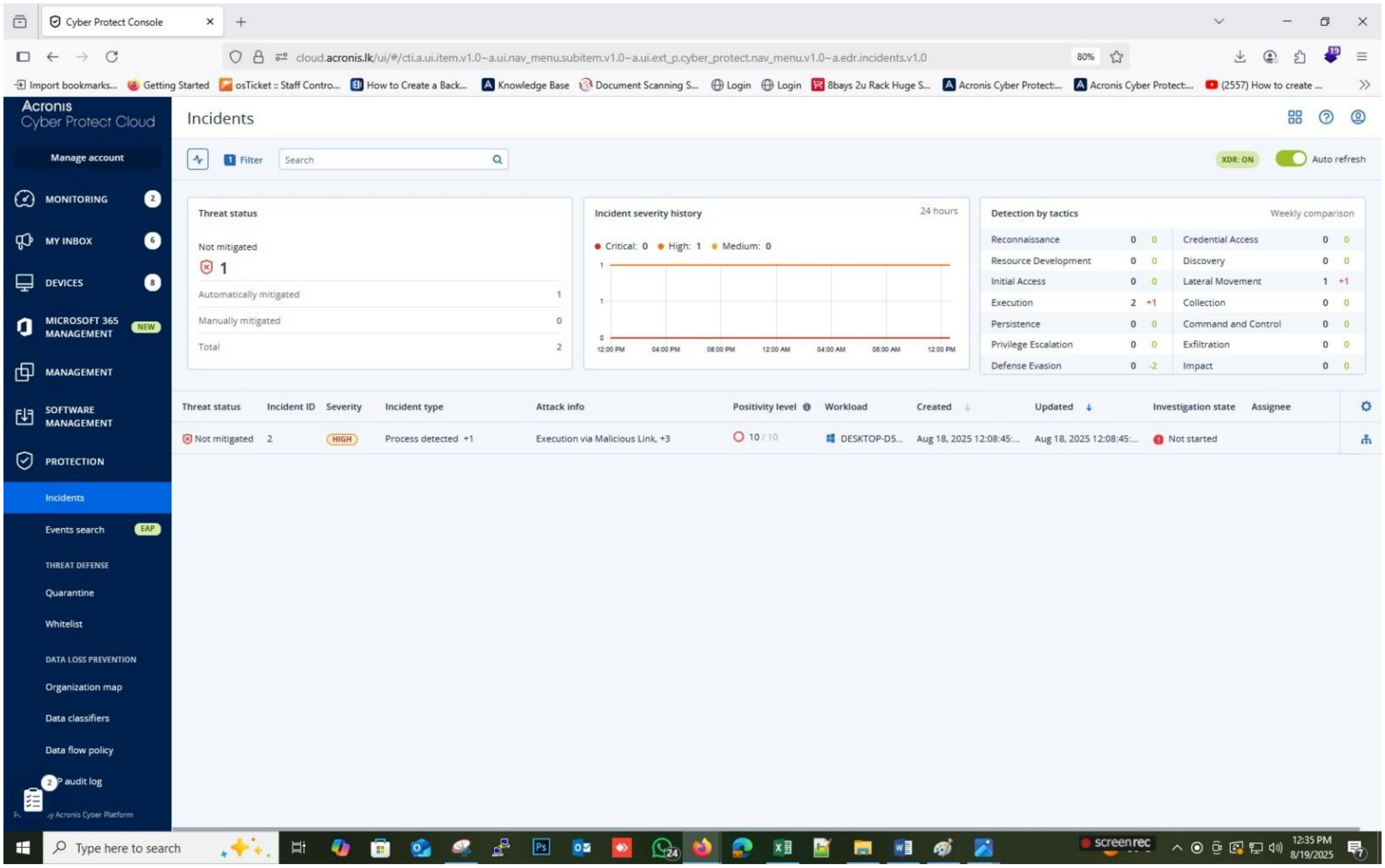
Antivirus & Antimalware protection
Self-protection on, Real-time protection on

Active Protection	Revert using cache
Advanced Antimalware	On
Network folder protection	On
Server-side protection	Off
Self-protection	On
Cryptomining process detection	On
Quarantine	Remove quarantined files after 30 days
Behavior engine	Quarantine
Exploit prevention	Notify and stop the process
Real-time protection	Quarantine
Schedule scan	Quick scan: Quarantine At 02:30 PM, Sunday to Saturday Full scan: Quarantine At 04:25 PM, only on Friday Custom scan: Off
Exclusions	None

6. **(Optional) Coordinate with Microsoft Defender**
   If you use Defender alongside Acronis, recent updates let you manage Defender settings and support automatic AV handoff from within protection plans. Configure this here if applicable.

7. **Save and apply**
   Click **Create** / **Save**, choose **Apply to selected devices**, and (optionally) kick off an initial on-demand scan.

8. **Verify deployment**
   - **Devices** page: confirm the new plan is listed under each endpoint.
   - **Security → Incidents**: verify EDR telemetry/alerts start appearing. (Roles such as *Security Analyst* have access to manage EDR incidents.)



Incidents

Threat status

Not mitigated 1

Automatically mitigated	1
Manually mitigated	0
Total	2

Detection by tactics — Weekly comparison

Reconnaissance	0	0	Credential Access	0	0
Resource Development	0	0	Discovery	0	0
Initial Access	0	0	Lateral Movement	1	+1
Execution	2	+1	Collection	0	0
Persistence	0	0	Command and Control	0	0
Privilege Escalation	0	0	Exfiltration	0	0
Defense Evasion	0	-2	Impact	0	0

Threat status	Incident ID	Severity	Incident type	Attack info	Positivity level	Workload	Created	Updated	Investigation state	Assignee
Not mitigated	2	HIGH	Process detected +1	Execution via Malicious Link, +3	10 / 10	DESKTOP-D5...	Aug 18, 2025 12:08:45:...	Aug 18, 2025 12:08:45:...	Not started	

Notes & troubleshooting

- If you see **"Protection plan not applied"** in Monitoring after assigning a **protection-only** plan, this is a known behavior for plans without backup — the plan is still active.
- If applying/saving the plan errors out about licensing (e.g., "plan cannot be applied… license does not allow requested functionality"), the device/tenant likely lacks the required security/EDR quota. Fix the subscription and re-apply.
- As of Jan 2024, **Advanced Security + EDR** was merged into **Advanced Security**; in the UI you might simply see **Advanced Security** while still having EDR features.