



Acronis

**Acronis Partner Day
at MSP Global 2024**

Time to Go Native.

Acronis

Acronis Technology Roadmap

October 2024

#CyberFit



Oleg Shaikhatarov

Chief Product Officer, Acronis



Ronan McCurtin

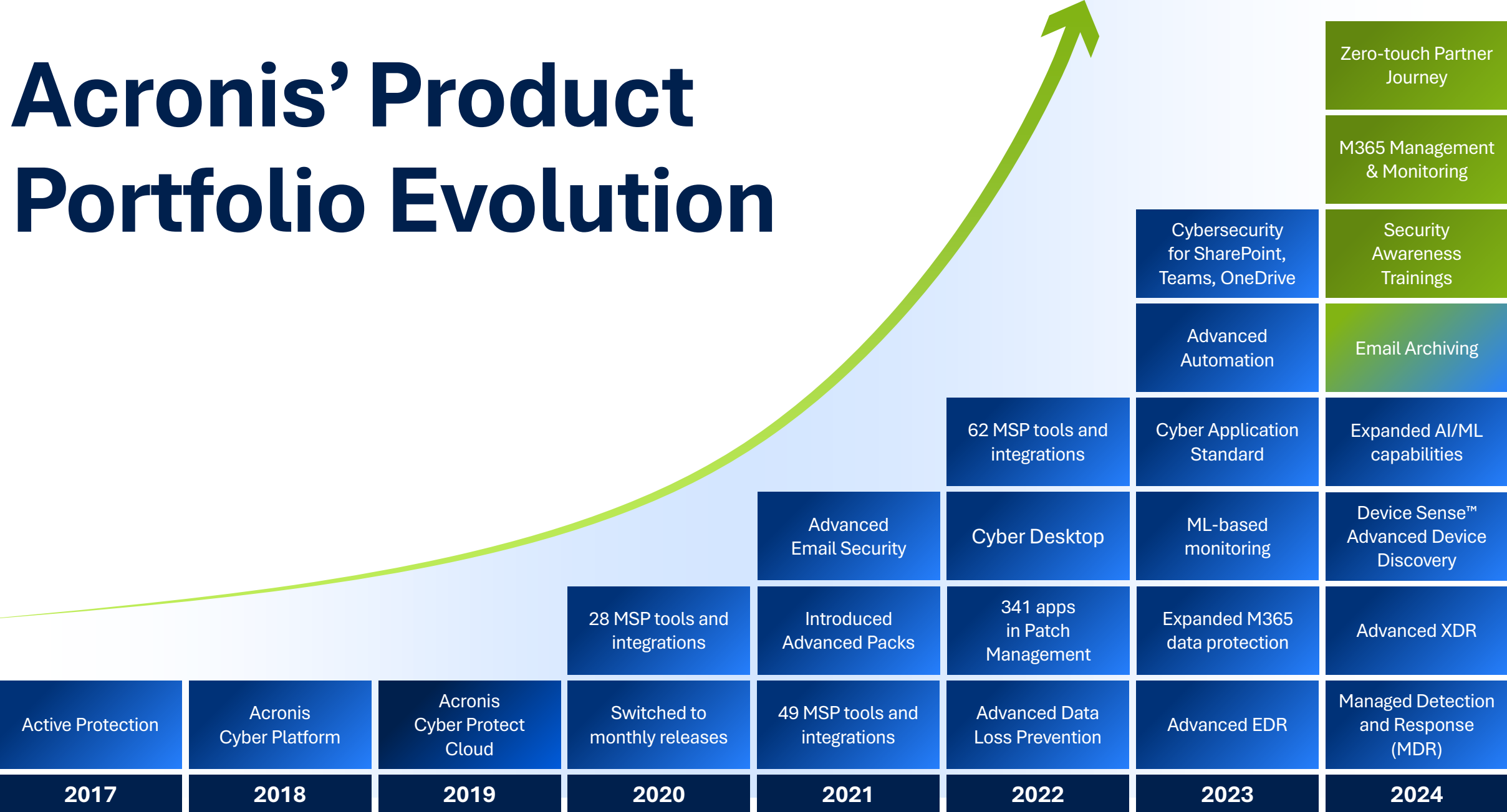
RVP EMEA, Acronis



Pat Hurley

RVP Americas, Acronis

Acronis' Product Portfolio Evolution



Acronis delivers the most complete cybersecurity and data protection in a single solution



**Natively
integrated**



**Highly
efficient**



**Built
for MSPs**

Modern and Complete Cyber protection

As service providers grow, so does Acronis Cyber Protect Cloud



This section features a light blue world map as a background. On the left side, there is an icon of a server rack. To the right of the icon, the text '40+ data destination countries' is displayed in a bold, dark blue font, highlighting the global reach of the service.

Modern and Complete Cyber protection

As service providers grow, so does Acronis Cyber Protect Cloud



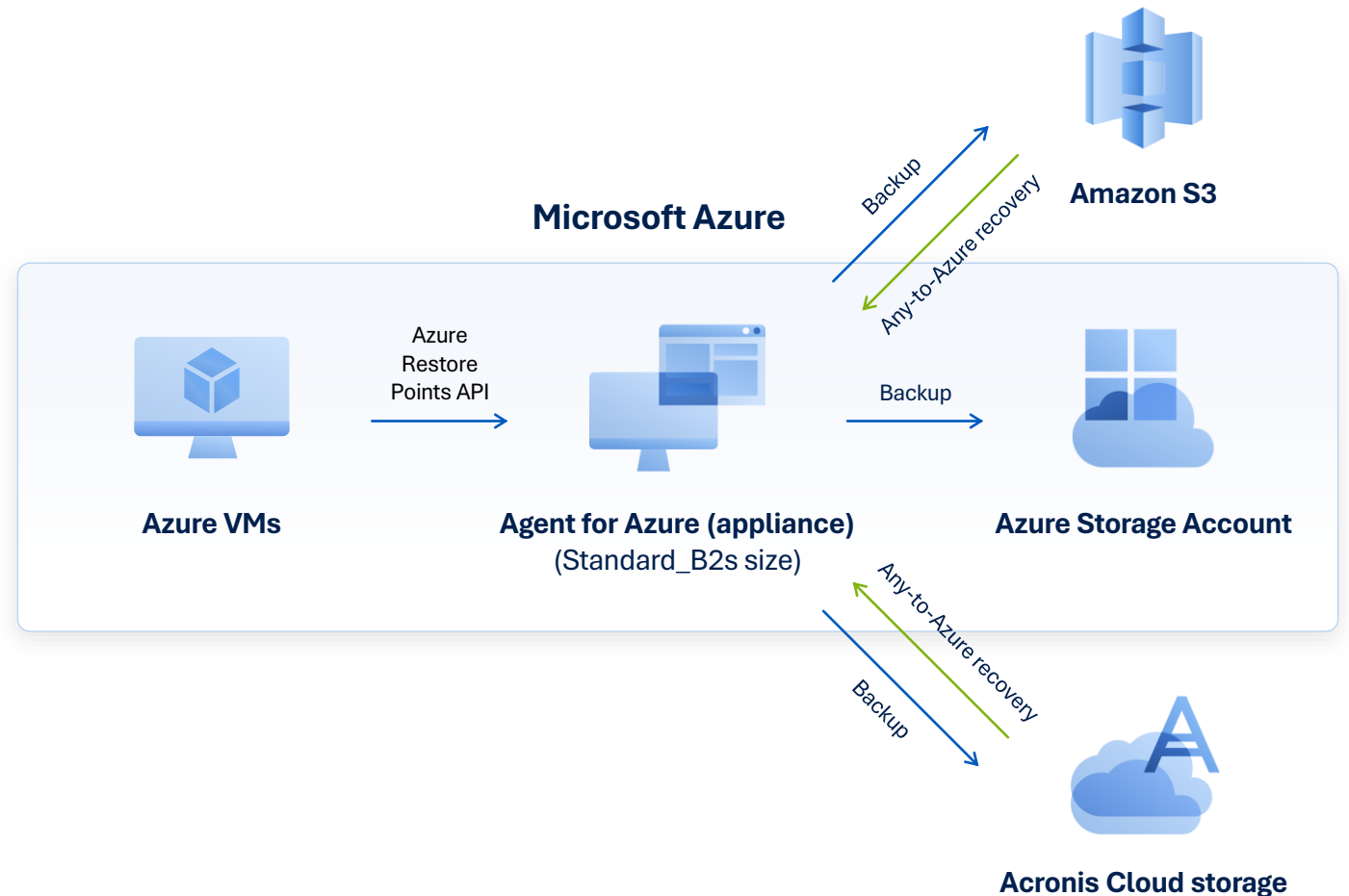
CyberApp integration technology

40+ data destination countries

New data centers

Agentless Backup for Azure Virtual Machines

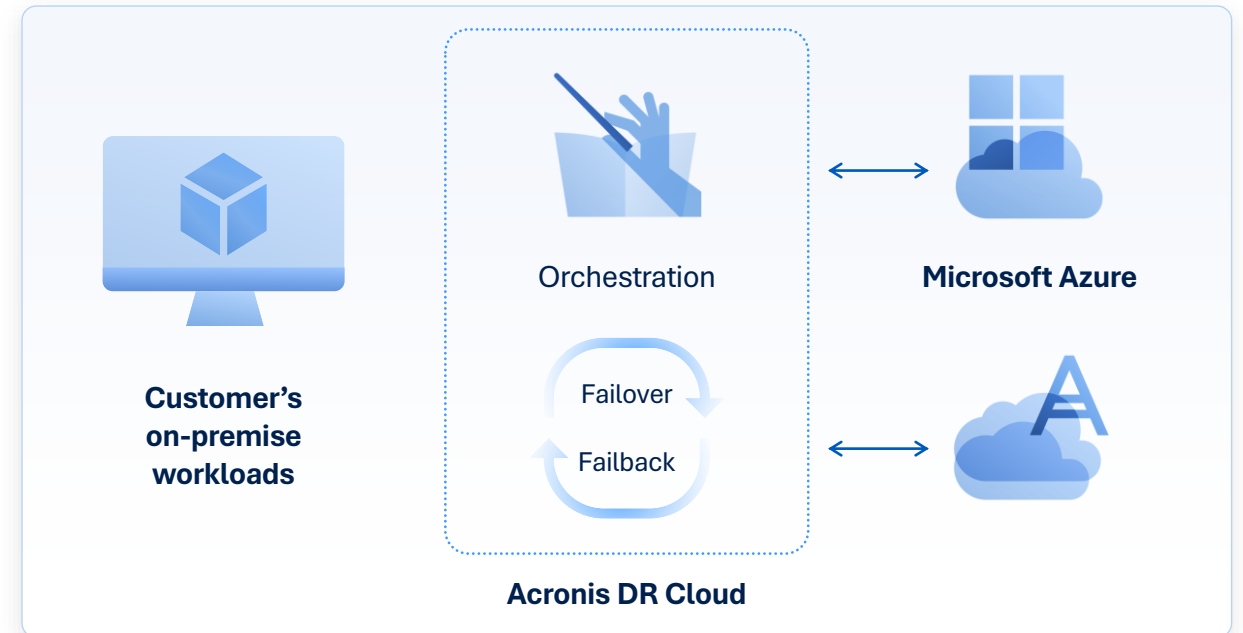
- **Efficient management:**
no need to install agent inside each VM
- **Automated deployment**
of the virtual appliance
- **Cross-platform recovery**
of physical machines backups
as Azure VMs



Disaster Recovery to Azure

Make your Azure site a disaster recovery platform

- **Increase adoption of Azure** by providing Disaster Recovery solution for on-prem workloads to Azure as a recovery site
- Enable an **alternative Disaster Recovery site** to run workloads during failover
- Leverage **advanced IaaS capabilities** of Azure such as different tiers of hot storage and custom network configurations
- **Orchestrate Disaster Recovery scenarios** using single Acronis Cyber Protect console



Acronis

Why does this matter?

Growing Protection of Cloud and SaaS Applications

Protected	
Exchange Online	Teams
SharePoint Online	OneDrive
OneNote	Google Workspace
Azure VM	Amazon EC2

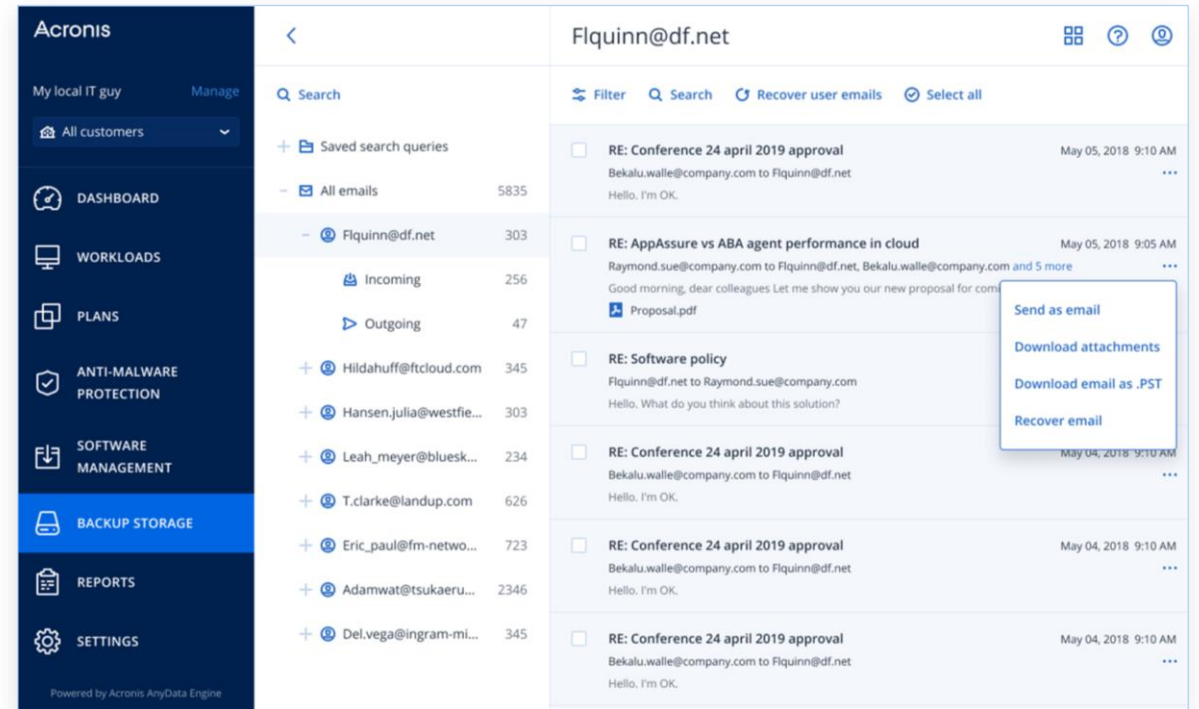
Pipeline	
Entra ID	Dynamics 365
Power Apps	Planner
Zoho	HubSpot
QuickBooks	Zendesk



Email Archiving for Microsoft 365

Expanding protection for Microsoft 365

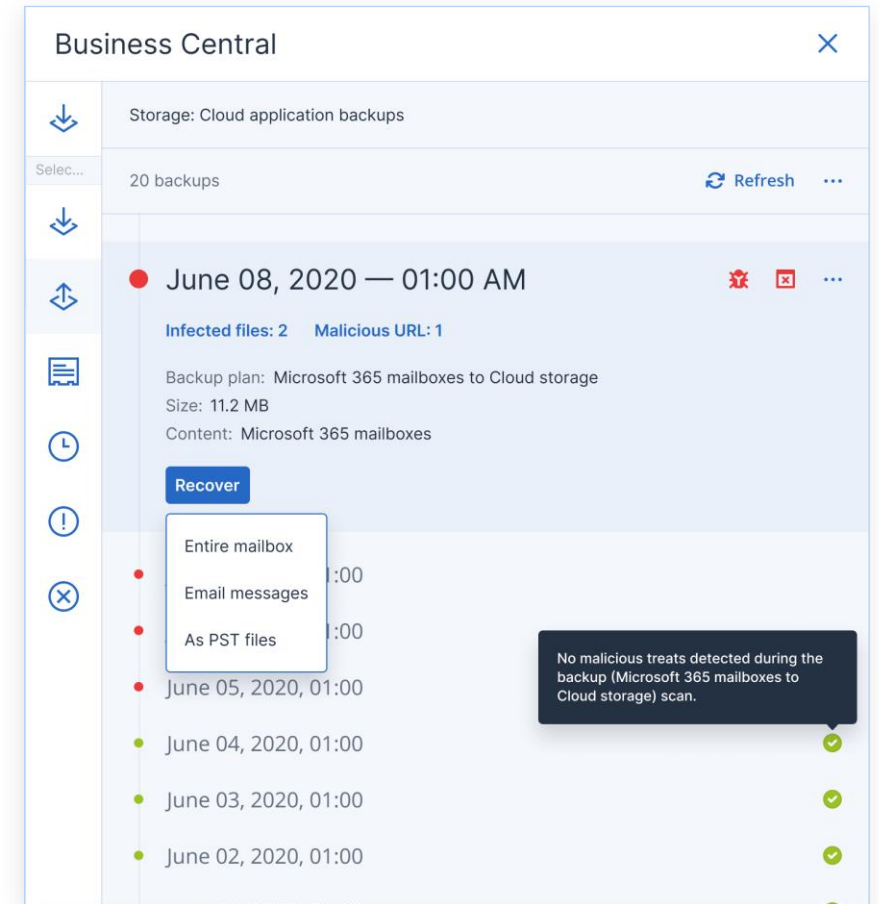
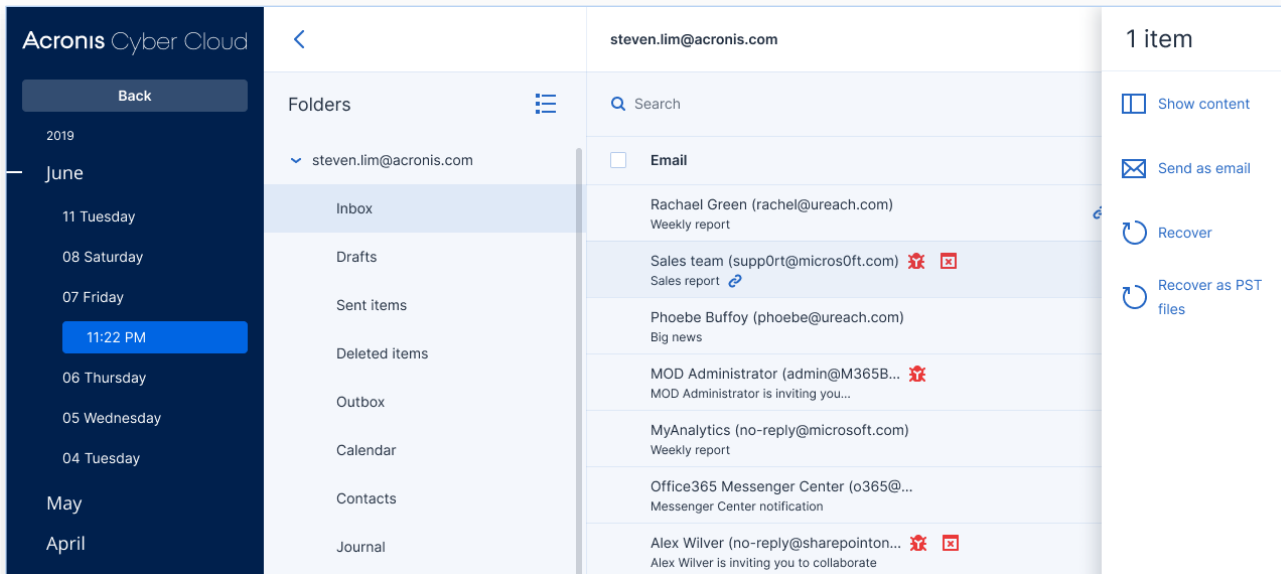
- **Compliance:** ensures the preservation of all communications, which is key for meeting legal, regulatory, and industry compliance requirements
- **Robust Search Capability:** helps users quickly locate specific emails, making it more efficient to retrieve necessary data for decision-making or audit purposes.
- **Optimized Performance:** By offloading storage of old emails from the primary system to archive



Antimalware Scan of Microsoft 365 Backups

Ensure malware free email recovery from Microsoft 365 mailbox backups

- Offer a **second layer of defense** when the email security solution fails to detect malicious content
- **Detect malicious content** within Microsoft 365 mailbox backups



M365 Security Posture Monitoring and Management

- **Single pane of glass** for security posture of all M365 tenants that you manage
- Ensure compliance with **best practices security baselines**
- Effectively **track M365 security events**, identify suspicious activities
- **Monitor M365 user activities**, access levels, and permissions

Acronis Cyber Protect Cloud

My local IT guy Manage

All customers

MONITORING

WORKLOADS

MICROSOFT 365 MANAGEMENT **NEW**

Security posture

Baselines

Users

Baseline templates

Powered by Acronis AnyData Engine

Security posture

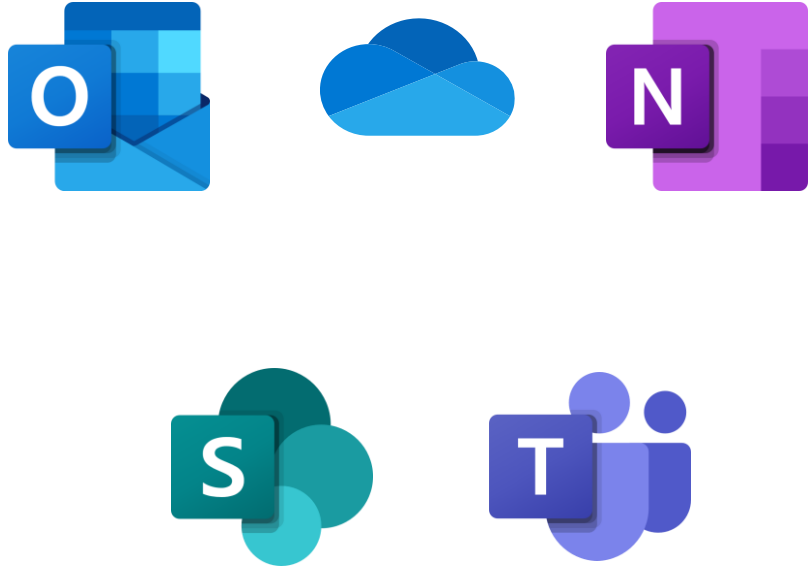
3 tenants 2 tenant baseline deviations

Search

Name	Tenant baselines	Group baselines
<input checked="" type="checkbox"/> CloudPro-Asia	13 deviations	1 deviation
<input type="checkbox"/> CloudPro-EU	5 deviations	4 deviations
<input type="checkbox"/> VCloudWare Europe	No deviations	No deviations

Complete & Unified Protection of Microsoft 365

Multiple layers of protection:

Data protection	Backup	Ultimate Protection	✓	
	Email Archiving		✓	
Security	Email Security		✓	
	SharePoint, Team, OneDrive security		✓	
	Scan of backups for malicious content		✓	
Management	Security posture monitoring & management		✓	

Acronis

So what?

Security Awareness Training

Boost security awareness of customers and employees to reduce incidents.



Human firewall

- Strengthen the employee's awareness with **simple trainings**.
- Thwart social engineering attacks.

Compliance

- Stay compliant with regulations with **easy tracking** of progress.
- Fulfill cyber insurance requirements with **policy management**.

Cost savings

- Conduct **security assessment** to prevent security incidents from materializing.
- **Simulate phishing attacks** to reduce risk during a real attack.

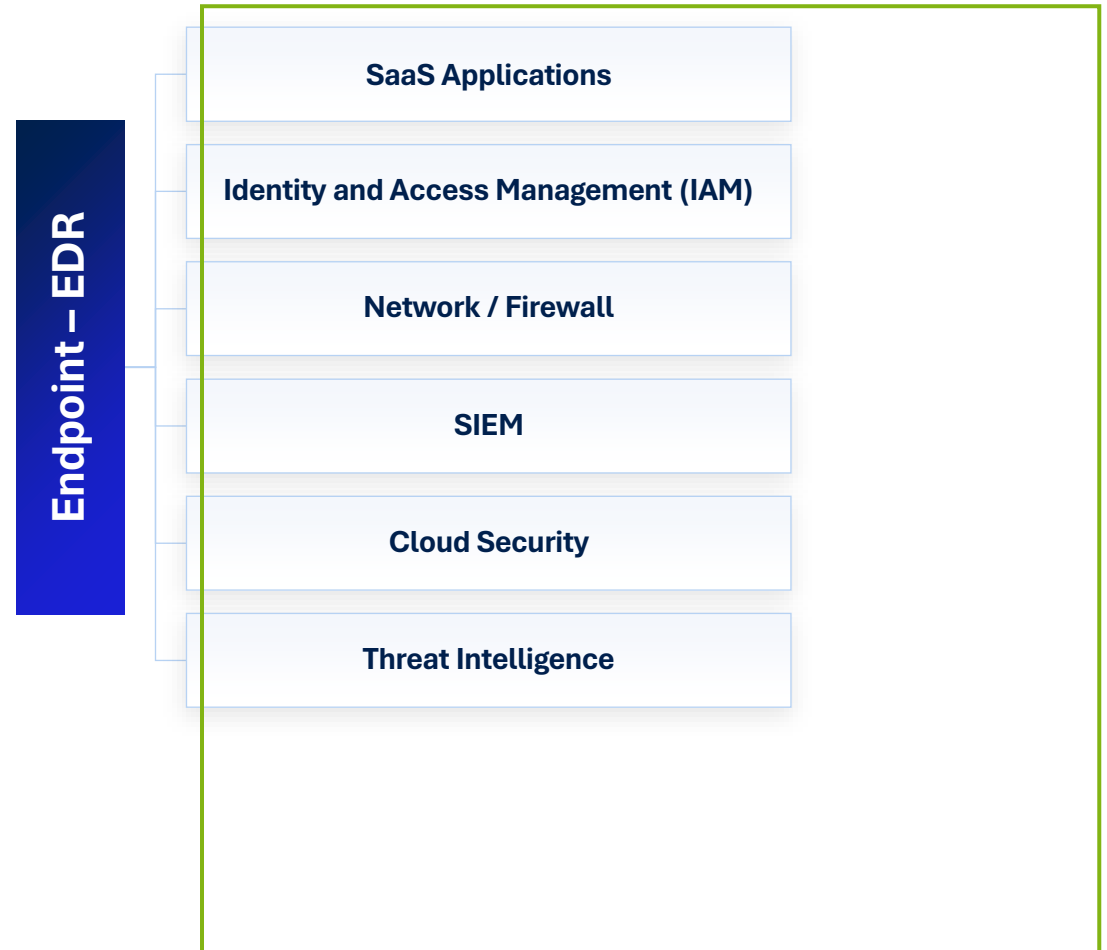
Extended Detection & Response (XDR)

XDR is needed to:

- Extend visibility and protection beyond endpoints
- Integrate with ID provider, network security, email, etc.
- Automate response actions across the entire infrastructure
- Enable threat intelligence across infrastructure



Integrations – XDR



Acronis XDR 2.0

Use case driven intelligent correlation across native & third-party sources



Detections based on 3rd party sources



Trigger **incident** based on 3rd party sources



Auto **correlation** of events from multiple sources



Incident creation based on **custom IoCs**

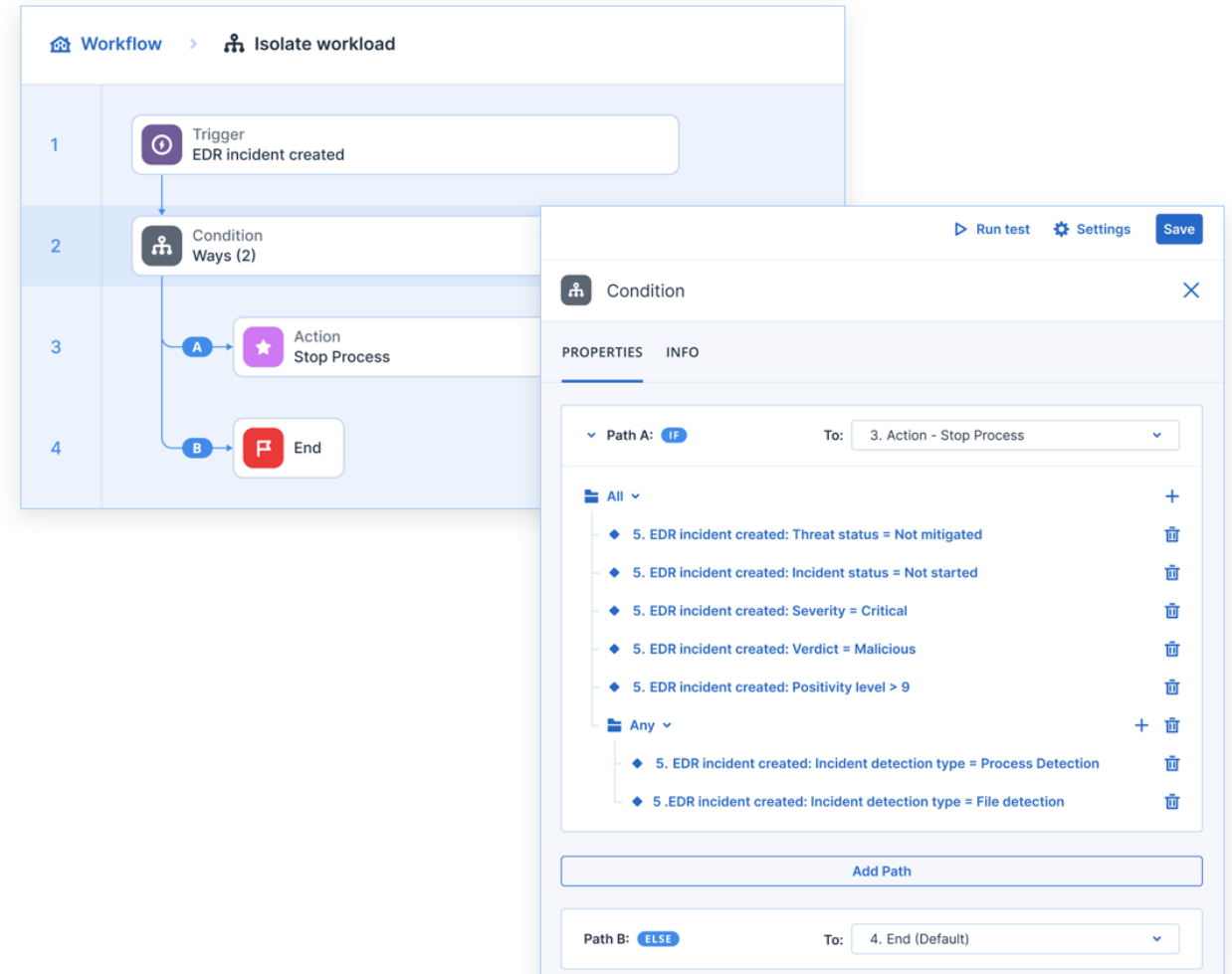


Enhanced multi-host **graph visualization**

Automated Response Playbook

Automate remediation of EDR incidents

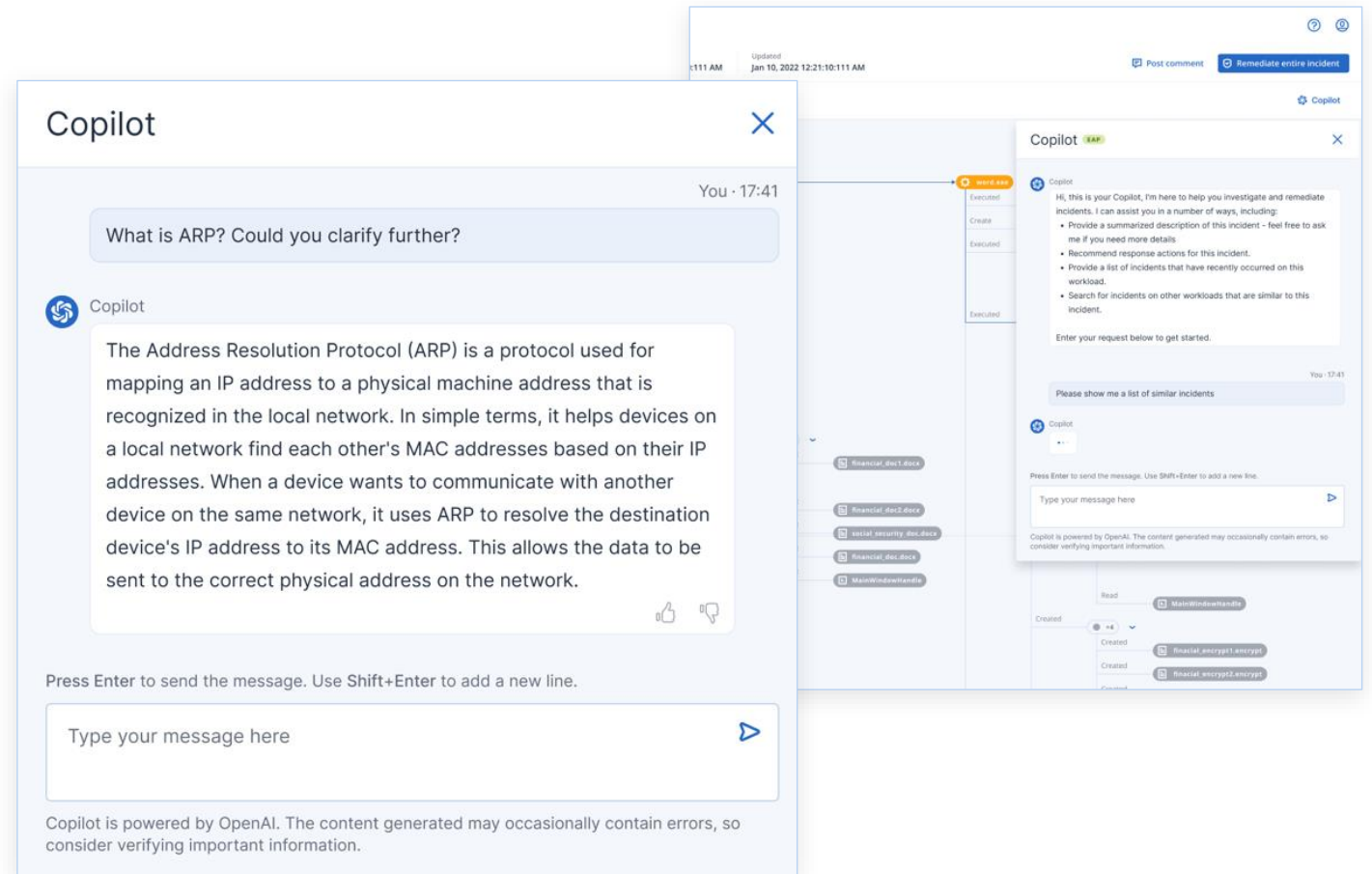
- **Automate responses** to XDR/EDR incidents
- Reduce operational burden and **improve time to respond**
- Create **predefined workflows** to trigger a series of response actions e.g. isolate workload, quarantine process, send alert message
- Trigger workflows based on specific incident conditions e.g., severity or incident type



Copilot for Advanced Security + XDR (Early Access)

An AI-assisted chat tool that helps in the investigation and remediation of security incidents

- **Designed for MSP technicians** with limited security skills
- Enables MSP to strengthen their security posture by quickly identifying and mitigating threats



Managed Detection & Response (MDR)

Let the experts monitor and react 24/7 to incidents in Acronis EDR for you.

Faster response



Outsource some or all response actions in real time and stop attacks fast.

Don't get flooded



Triage incidents, escalate when needed.

Save time and teams



MDR handles alerts in the middle of the night or around the clock.

Experienced



Get expert help with new incidents.

Focus on core business

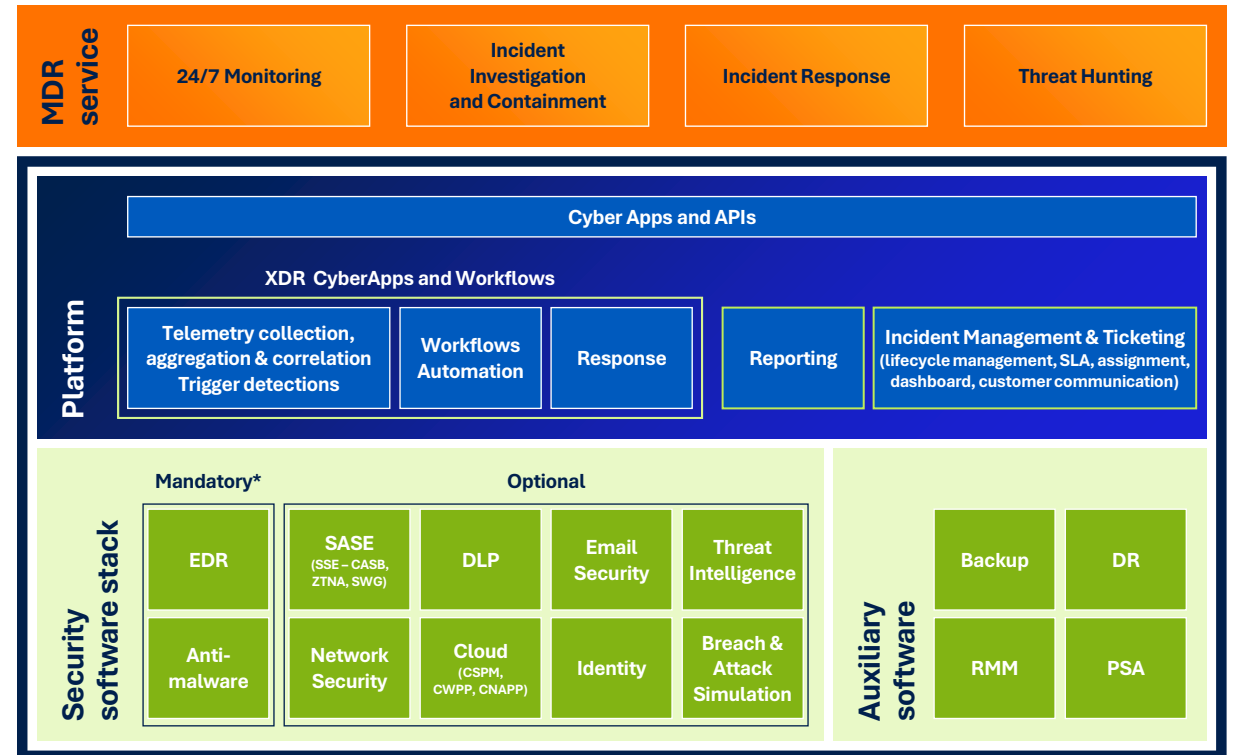


You focus on customers and building your business.

Dedicated MSSP Program

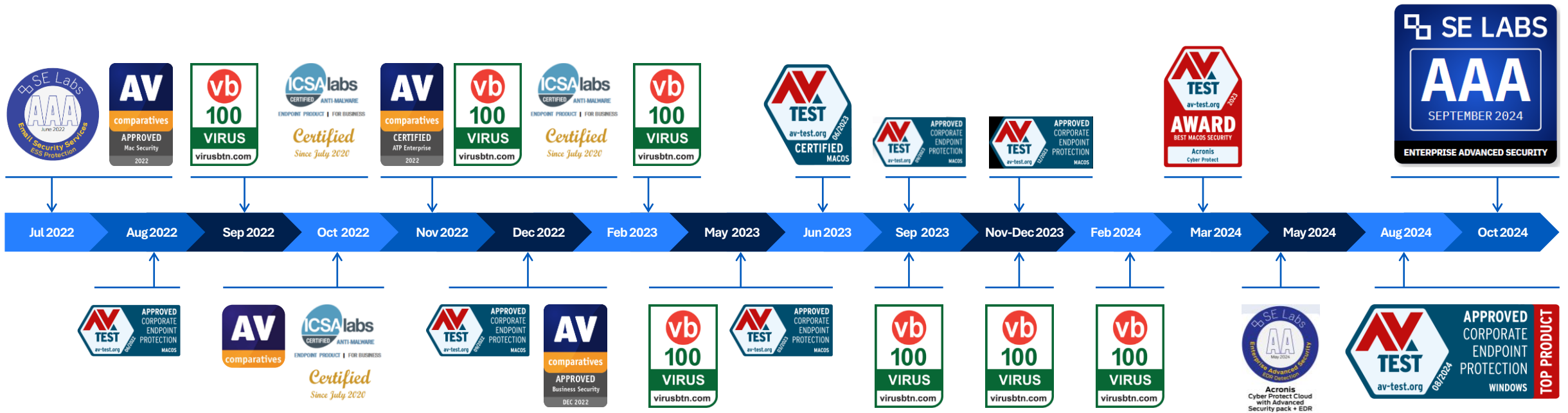
Platform for MSSPs to provide Managed Detection and Response (MDR) service to Acronis MSP/SP

- Empower MSSPs to offer MDR services through the Acronis platform and software, including EDR, XDR, automated workflows, and Advanced Automation.
- A dedicated partner program to recruit MSSPs for delivering MDR services to Acronis MSPs
- Support growth by leveraging the trusted role of regional MSSP among SPs/MSPs.
- Enhance security service capabilities through comprehensive product training and guidance to effectively provide MDR.



* That is Acronis Advanced Security + XDR pack

Acronis security proven by independent evaluations



Acronis
Threat Research Unit

Acronis

What is it about?

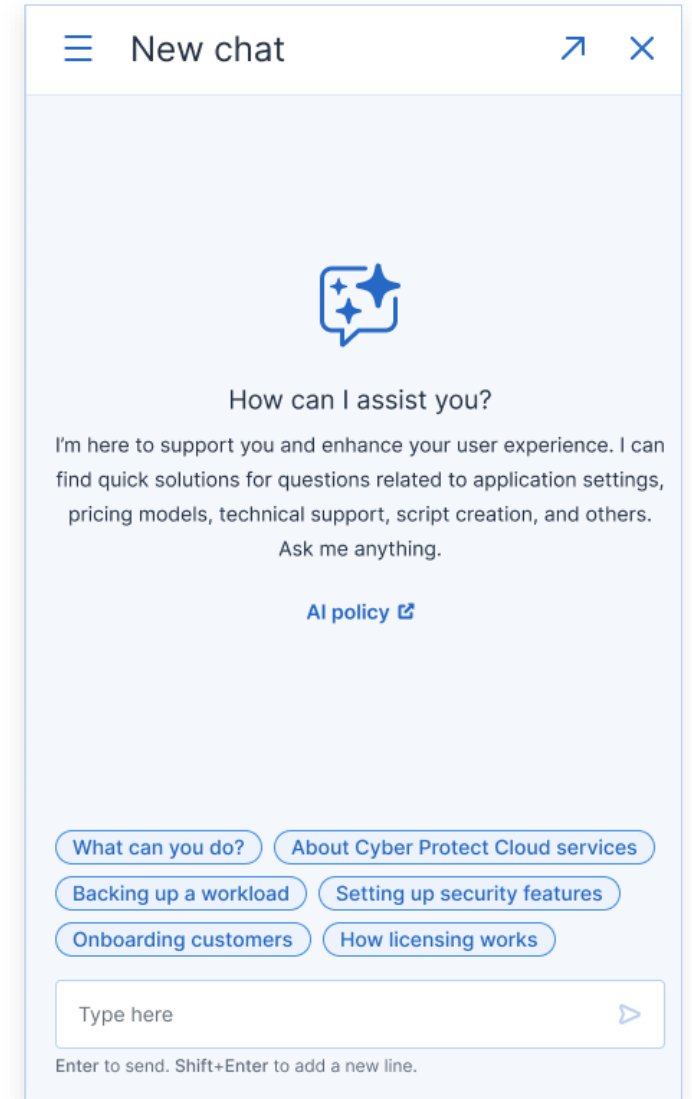
Communication Center (in-product inbox)

- **Critical product updates**
- Messages from Acronis Sales and Academy
- Invitations to **trainings and webinars**
- **Meeting requests** with Partner Success Managers
- **Interview invitations** from Product managers
- **Always available** – right next to the Dashboard!

The screenshot displays the Acronis Cyber Cloud Communication Center interface. On the left is a dark blue sidebar with navigation options: My local IT guy (Manage), All customers, DASHBOARD (7), MY INBOX (1), WORKLOADS (All workloads, Machines with agents, Unmanaged machines, Data protection map), PLANS, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, BACKUP STORAGE, and REPORTS. The main content area is titled 'My inbox' and features a search bar, filters for Category (All), Importance (All), and Response actions (All), and a 'Show only unread' toggle. The inbox list shows messages from 'Today', 'Yesterday', and 'Last week'. The selected message is from '07 Jun 2024 14:21' with the subject 'Register now for XDR solution webinar'. The message body includes a greeting, an invitation to a webinar, and details: Date: 7th of July, 2024; Time: 13:00, UTC (+3); Duration: 2 hours. A yellow warning box states 'This action should be completed before 21 Jun 2024, 15:00.' and a blue 'Register now' button is at the bottom.

AI-based Chat

- Finds an answer for **any question**, from licensing clarification to detailed how-to guide
- Provides links to **source documents**
- Transfers to a live agent, if required
- Speaks **your language**
- Allows to have **multiple chats**



AI-based Workflow builder and playbooks

- Automate standard operating procedures
- Do If-This-Then-That processes tasks
- Connect with third-party services, such as Slack, Outlook in a few clicks
- Simple, intuitive, UI-driven
- Samples catalog

The screenshot displays a workflow builder interface for a workflow named "Isolate workload". The interface is divided into several sections:

- Workflow Editor:** A central canvas showing a sequence of steps in a flowchart. The steps are:
 1. Trigger: EDR incident created
 2. Condition: Ways (2)
 3. Action: Stop Process
 4. Condition: Ways (3)
 5. Action: Quarantine Process
 6. Condition: Ways (3)
 7. Action: Isolate device (highlighted with a red border and a red error icon)
 8. Action: Add comment
 9. Action: Send email
 10. End
 11. Go to: 8 - Add comment
 12. Go to: 8 - Add comment
 13. Go to: 7 - Isolate device
 14. End
- Execution History:** A table on the left showing the execution status of the workflow. It includes columns for date and time, and a status column with icons (green checkmark for success, red X for error, yellow warning triangle for warning).

Date	Status
Today	Success
Jul 10, 2024 19:21:10 (7 m 24 sec)	Success
Jul 10, 2024 19:21:10 (7 m 24 sec)	Error
Jul 9, 2024	Success
Jul 9, 2024 19:21:10 (7 m 24 sec)	Warning
Jul 9, 2024 19:21:10 (7 m 24 sec)	Success
Jul 9, 2024 19:21:10 (7 m 24 sec)	Error
Jul 9, 2024 19:21:10 (7 m 24 sec)	Error
Jul 9, 2024 19:21:10 (7 m 24 sec)	Warning
Jul 2, 2024	Success
Jul 2, 2024 19:21:10 (7 m 24 sec)	Success
Jul 2, 2024 19:21:10 (7 m 24 sec)	Success
- Condition Details Panel:** A panel on the right showing details for the selected "Condition" step (Step 2).

Field	Value
Object	Condition
Description	-
Step number	2
Status	Succeeded
Status details	-
Started at	Jul 10, 2024 19:21:10
Finished at	Jul 10, 2024 19:21:34
Duration	24 sec
- Path Details:** A section at the bottom right showing the execution path. Path A (Accepted) includes Step 3 - Action - Stop Process. Path B (Declined) includes Step 4 - End (Default).

Power of CyberApp and Native integrations

Native integration between Acronis services

- Safe recovery
- Fail-safe patching
- Backup scanning for malware
- ... and many more

Native integration between Acronis and ISVs

- Seamless integration of third-party service into Acronis Cyber Protect Cloud console

Remediate entire incident ✕

Analyst verdict

True positive False 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 registry, scheduled tasks and/or files existing on the workload prior to the attack.
To optimize speed, rollback tries to recover items from the local cache. Items that fail to be recovered will be recovered by the system from backup images.

Allow this response action to access encrypted backups using your stored credentials

Affected items: [Show \(40\)](#)

Recover workload
If any of the above selected remediation steps fail completely or partially.

Recovery point: [20 Jan, 2021, 6:45:23 AM](#) [✎](#)

Items to be recovered: **Entire workload**

Prevention actions

Add to blocklist
Adds all threats from the incident to the blocklist in the selected protection plans. This action will prevent these threats from future executions.

Patch workload
Prevents further attacks by patching software that contains vulnerabilities used by attackers in order to get a foothold on the workload.

Ecosystem growth – 270+ integrations!

Integrations catalog

<https://solutions.acronis.com>



40+ New integrations



Sponsors



Acronis

The Platform journey continues!

Talk to us at the booth



Yury Averkiev

SVP, Product Management



Nidhi Singh

Director, Product Management,
Cybersecurity



Ramil Yusupov

Lead Product Manager,
Backup



Dragos Florin Botin

Lead Product Manager,
Management



Marina Smolyanaya

Senior Director of Product Management,
Platform & Ecosystem



Rene Beekman

Lead Product Manager,
Ecosystem



Ignacio Digon

Senior Product Manager, ISV
integrations

Email us at: pm@acronis.com

Acronis Education

Grow your business with MSP Academy



Short modules.
Big impact.
Enroll today!





Acronis

**Acronis Partner Day
at MSP Global 2024**

Time to Go Native.

Thank you, Ecosystem partners!





in association with

Acronis

Join us in 2025!

Acronis Partner Day at MSP Global
October 20-21 | PortAventura, Spain



Register today:

go.acronis.com/MSPGlobal2025

