

Acronis

#CyberFit

Acronis Cyber Protect Cloud

Modernize your cybersecurity and backup with
integrated cyber protection

The threat landscape is becoming more complex



80%

**of companies reported to
have been attacked in
H2 2021**



57%

**of attacks are missed by
traditional antivirus
solutions**



69%

**of MSPs spend more time
managing tools than
defending against threats**

Sources: Acronis Cyberthreats Report 2022, Acronis Cyber Readiness Report, 2020, FBI

What if you could rely on just one integrated solution?



Boost your monthly recurring revenue

Easier upsells
using integrated solutions

Simplified renewals
with integrated reporting

Greater ROI via pre-built marketing campaigns



Cut cyber protection costs by up to 50%

One console, one license, one agent

Integration drives deeper automation

Consolidate vendor expenses



Deliver unmatched cyber protection

Reduce risk with 100% coverage of client workloads

Unique capabilities not available from your current security vendors

Leader in independent testing (VB100, AV-Test, AV-Comparatives)

AI-powered integration of data protection and cybersecurity



Prevention

Smart protection plans based on Acronis threat alerts



Detection

AI/ML-based threat detection and behavior analysis



Response

Attack response with complete AI-assisted visibility on the edge



Recovery

Attack remediation without data loss and with integrated patching



Forensics

Rapid and precise investigations with forensic-rich backups

Best-in-breed backup combined with integrated security and management



Protect every workload
at no charge

Best-in-breed backup
included

Strengthens your AV
against zero-day threats

Accelerate security
and manageability

Add advanced packs: Security, Management, Backup, Disaster Recovery, Email Security, Data Loss Prevention, File Sync and Share

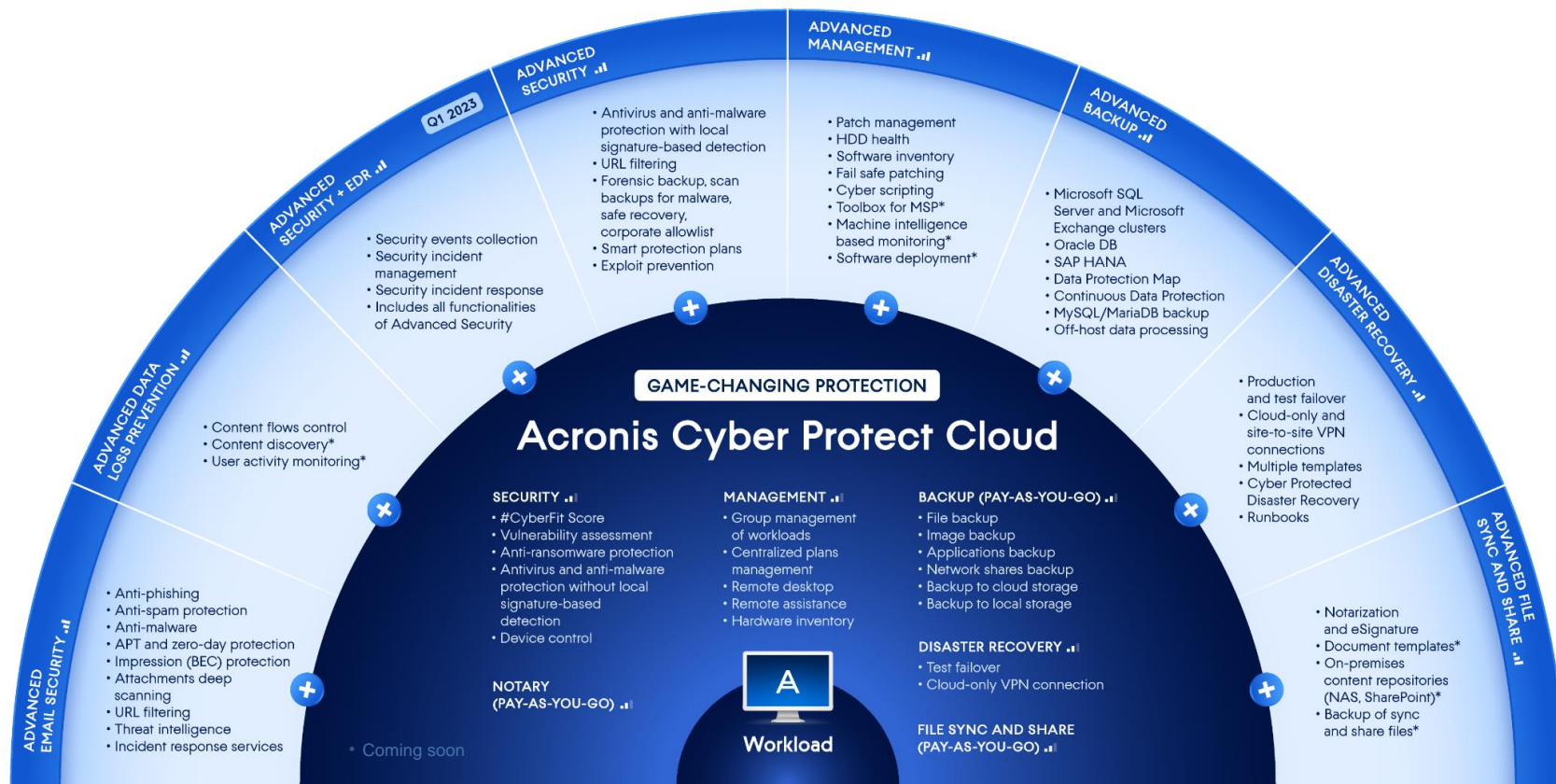


Optimize for every workload

Easy to upsell

Vendor consolidation

2022-2023 Roadmap for service providers



Legacy backup and AV solutions

Complex

Complicated licensing, deployment and training, as well as agent conflicts

Expensive

Multiple tools, vendors, administration costs

Unsecure

Lack of integration creates gaps in defenses, management burden compromises security

Acronis Cyber Protect Cloud

All services managed from one place

Easy

Remove the complexity and risks associated with non-integrated solutions

Smarter use of resources

Efficient

Faster operations with integration and automation lets your team focus on your clients

Total peace of mind for clients

Secure

Customize your services and deliver complete protection for every workload

Lower risk for your clients



Eliminate gaps in your defenses

Deliver comprehensive cyber protection with the unique integration of data protection and cybersecurity



Upgrade the protection of every workload

Ensure better protection for every workload with essential cyber protection



Recover instantly without losing data

Prevent downtime with near-zero RPOs and RTOs for all users and applications

Selling backup? Upsell to Acronis Cyber Protect

More than backup: The most secure, easy and reliable backup solution for MSPs

Proactive Protection

- Vulnerability assessment and patch management to avoid downtime and maintenance
- Malware removal from backups
- Prevention of reoccurring infections (patch on recovery)
- Prevention of backup deletion (immutable backups)

Active Protection

- Continuous data protection (CDP) to avoid any data loss
- Active protection against ransomware and other malware to avoid downtime
- Self-defense for the agent and backup storage

Reactive Protection

- Integrated disaster recovery capability
- Instant recovery: no data loss, near zero RTO & RPO
- Metadata storage for forensics and investigation of incidents

Productivity Improvements

- Maximum number of workloads protected per an MSP technician
- Integrated remote management for quick access to the protected workloads
- Pre-configured protection plans for remote workers

Selling security? Move to Acronis Cyber Protect

Unique capabilities deliver the most complete cyber protection solution for MSPs

Protection

- Protection for collaboration applications – Zoom, WebEx, Microsoft Teams
- AI-based hard-drive failure prediction
- Integrated, secure file sync and share solution for collaboration

Security

- AI-based injection detection
- Entropy analysis against advanced ransomware
- Rootkit detection by scanning cold backup data
- Aggressive heuristics enabled by allowlists created from backups

Performance

- Antivirus scans in backups, decreasing the load on protected devices
- Reduced downtime with fail-safe patch management
- Allowlisting applications by scanning backups

Productivity benefits

- Quick assessment of a device's protection status with built-in #CyberFit score
- Data protection map to discover and protect important data
- Remote desktop connection to office networks for end customers

Acronis

#CyberFit

Integration enables new cyber protection capabilities

Deep integration enables new capabilities

Integration at all levels: management, products, technology

Harness the power of ONE:

- Eliminate complexity
- Deliver new security capabilities
- Keep costs down
- Manage all clients from one console
- Efficient support escalation with one vendor

One

Agent



Policy



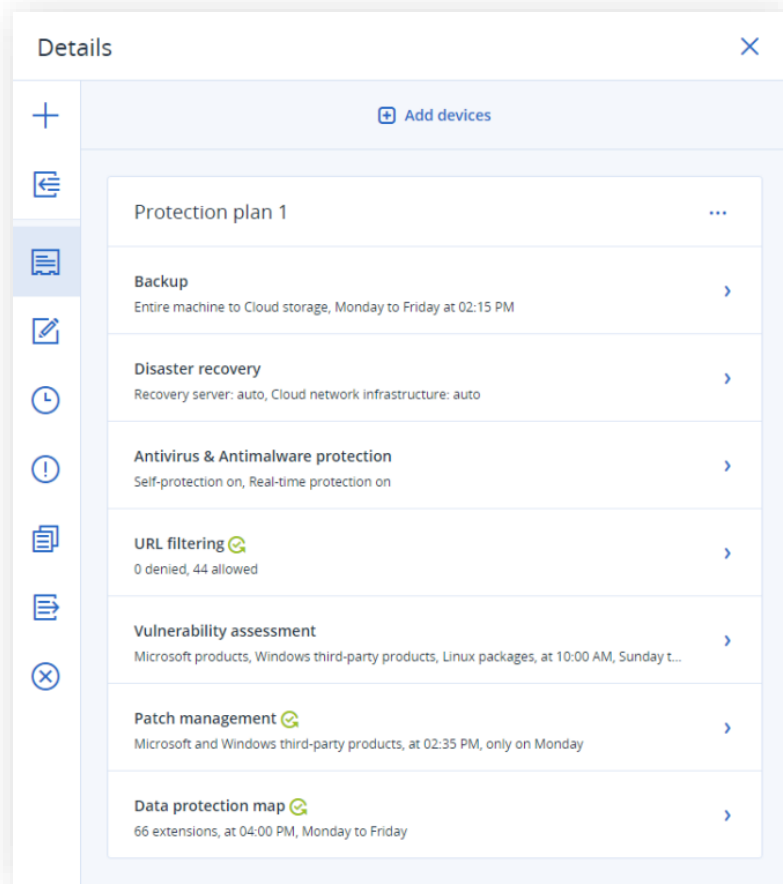
UX/UI



License



Vendor



Innovative cyber protection scenarios



Next-gen continuous data protection: Avoid even the smallest data loss in key applications



Smart protection plan: Auto-adjust patching, scanning, and backing up based on threat alarms from Acronis Cyber Protection Operations Centers



Better protection with less resources: Enable more aggressive scans and vulnerability assessments by offloading data to central storage, including the cloud



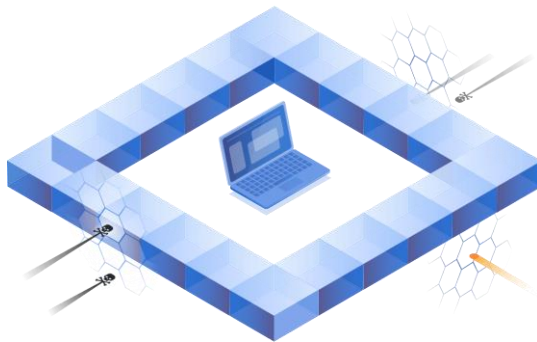
Safe endpoint recovery: Integrate anti-malware updates and patches into the recovery process



Fail-safe patching: Automatically back up endpoints before installing any patches, enabling immediate rollback



Streamlined data loss prevention: Automate service provisioning, initial client-specific policy creation and follow-up adjustments, and minimize the impact of human errors.



Data protection map: Monitor the protection status of files with classification, reporting, and unstructured data analytics



Forensic backup: Image-based backups that capture additional data needed for forensic investigations



Global and local allowlists: Created from backups to support more aggressive heuristics, preventing false detections



Block email threats: Protect mailboxes from spam, phishing, business email compromise (BEC), account takeover (ATO), malware, zero-day and advanced persistent threats (APTs)



Out-of-the-box scripting: Automate repetitive/day-to-day workload monitoring and management tasks through scripting

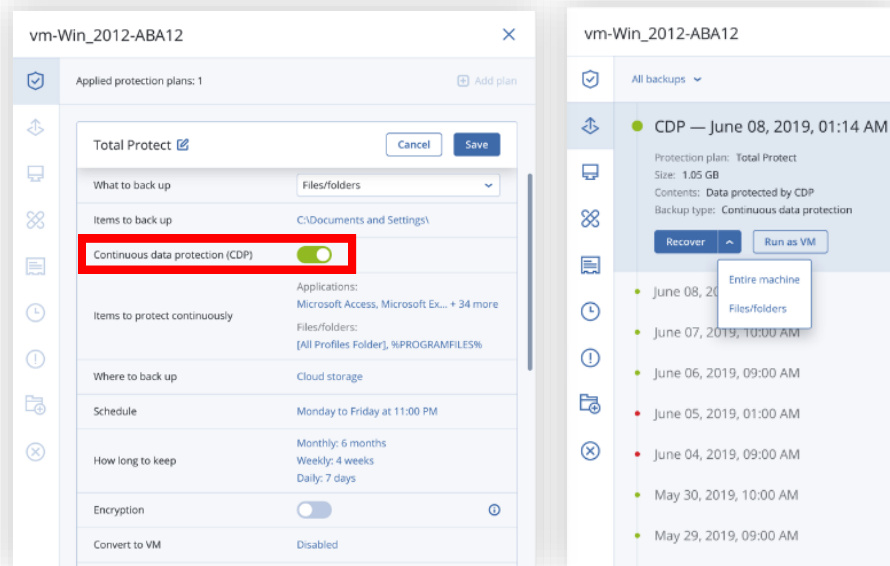
1. Continuous data protection

Gain safe and instant remediation without data loss and near-zero RPOs

Define the list of critical apps for every device that users are working with most often. Acronis' agent monitors every change made in the listed applications.

In case of a malware infection, you can restore the data from the last backup and apply the latest collected changes so no data is lost.

- Ensures users won't lose their work in-progress
- IT controls what is continuously backed up — Office documents, financial forms, logs, graphic files, etc.



Why? Protects client data – even between backups

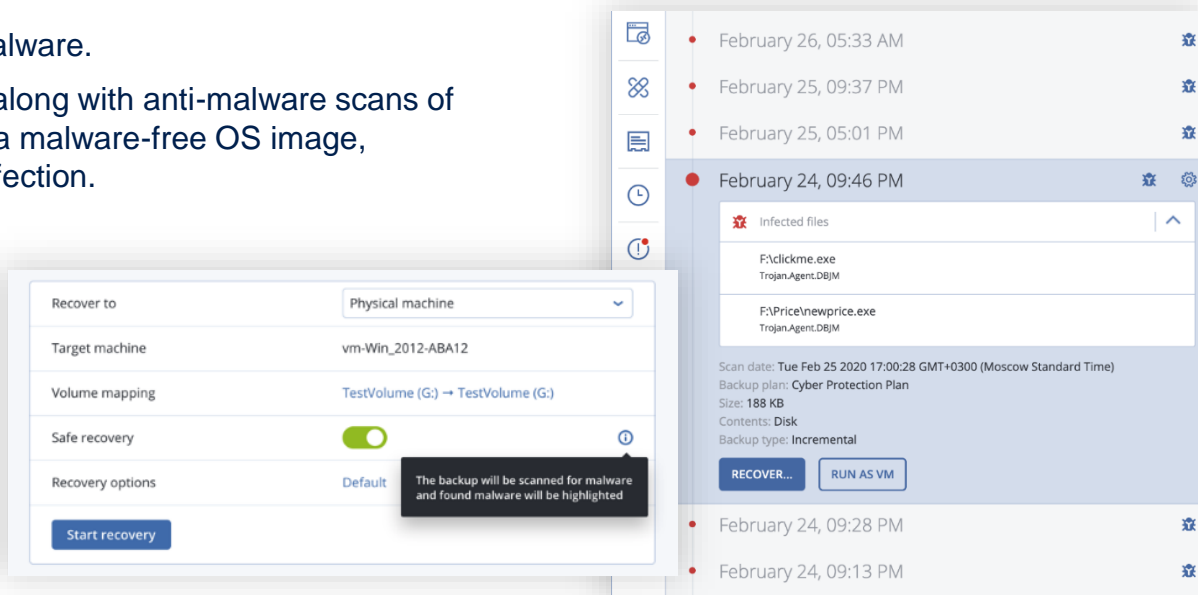
2. Safe recovery

Integrate anti-malware scans and AV updates into the recovery process

Backed up data can be infected with malware.

Applying the latest antivirus definitions along with anti-malware scans of backup images allows users to restore a malware-free OS image, reducing the chance of a reoccurring infection.

- Updates the antivirus database
- Scans backup images for malware



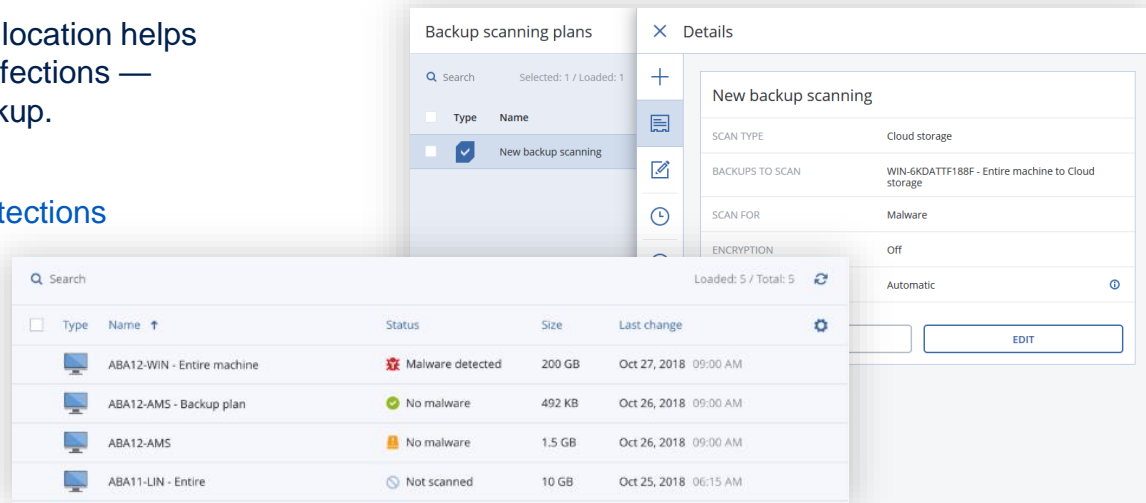
Why? Saves time, effort and data: recover infected images quickly with no efforts

3. Virus and malware scans in the Acronis Cloud

Prevent restoring infected files from backups

Scanning full disk backups at a centralized location helps find potential vulnerabilities and malware infections — ensuring users restore a malware-free backup.

- Increases potential rootkit and bootkit detections
- Restores only clean data
- Reduces loads of client endpoints



Why? Better protection with less effort and fewer resources. Offload endpoints for aggressive scans

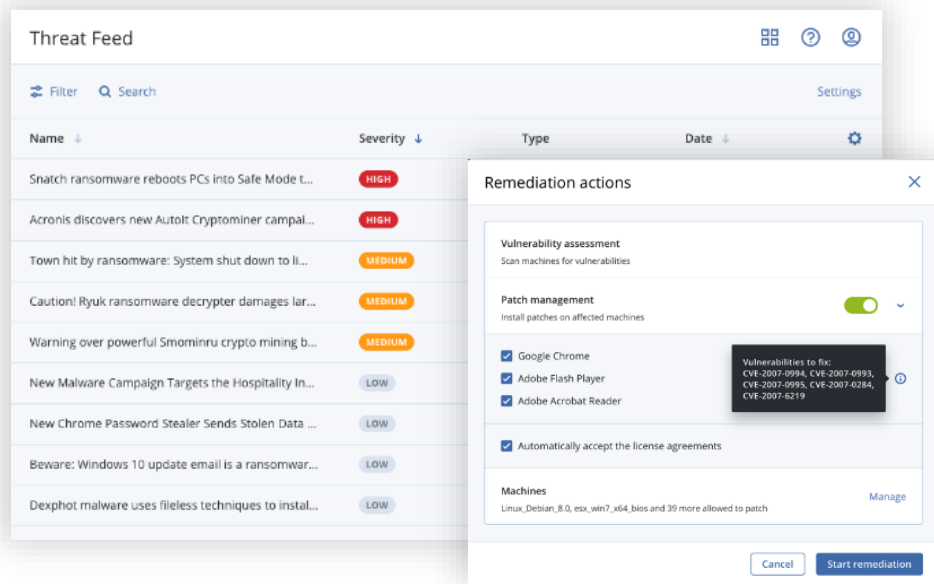
4. Smart protection plans

Use alerts from Acronis CPOCs to mitigate risks from even the latest threats

Acronis CPOCs monitor the cybersecurity landscape and release threat alerts. Acronis products automatically adjust protection plans based on these security alerts. This approach can result in more frequent backups, deeper AV scans, specific patch installs, etc. — and greater protection.

Protection plans will be restored when the situation returns to normal.

- Minimize business downtime from a malware epidemic, natural disaster, etc.
- Reduce reaction times
- Avoid data loss



Why? Faster reaction times, as well as prevention of downtime and data loss

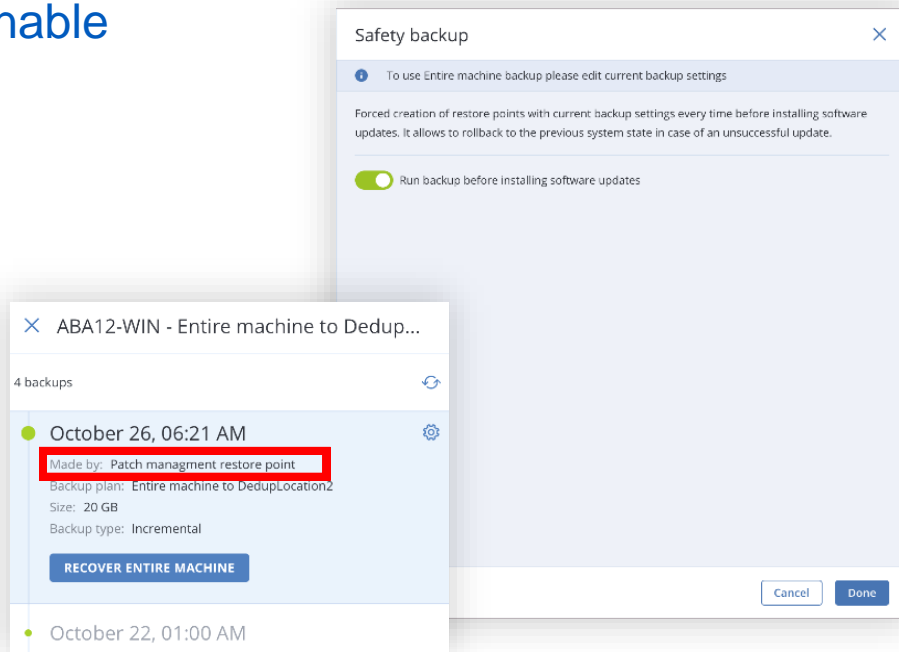
5. Fail-safe patching

Back up workloads before patching to enable quick rollback to a working state

A bad system patch can render a system unusable, but patch management rollbacks have limitations and can be slow.

Fail-safe patching creates an image backup of selected machines before installing a system or application patch for rapid rollbacks.

- Full image backups are the fastest and easiest way to revert to a usable state



Why? Saves resources, while supporting faster and more reliable operations

6. Data loss prevention

Prevent leakage of sensitive data and help enforce compliance with the ease you need



Content-aware DLP for peripheral devices and network channels (70+ controlled channels)

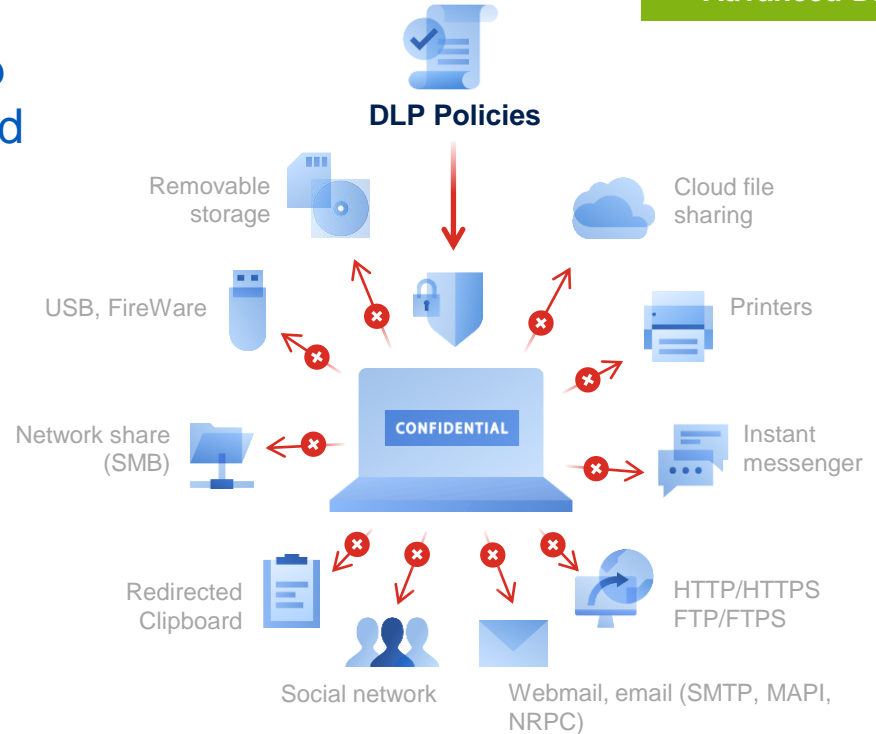


Behavior-based policy creation and extension to continuously maintain business-specific policies



Better reactivity to DLP events, auditing and investigating with policy-based alerting and logging in a central audit log

Advanced DLP



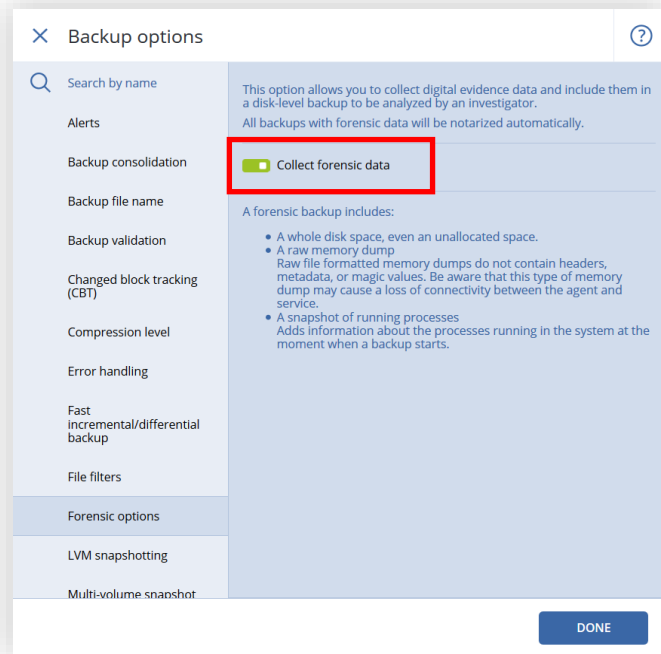
Why? Protect clients' sensitive data with the ease and speed you need.

7. Forensic information backup

Back up vital data as well as information needed for future analysis and investigation

By activating a special “Forensic Mode” in the product, memory dumps and full HDD images on a sector level can be collected.

- Keeps key evidence secure in the backup
- Makes future investigations easier and less costly

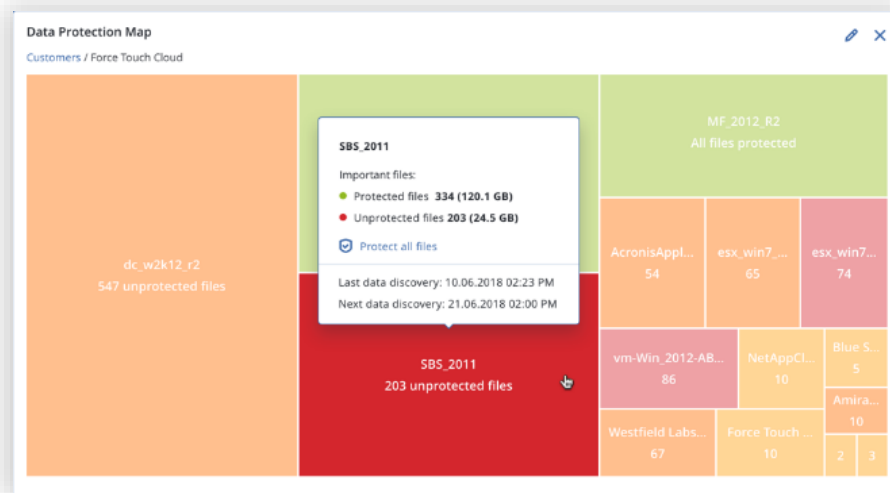


Why? Enables investigation and better compliance.

8. Data compliance reporting and Data Protection Map

Use automatic data classifications to track the protection status of important files. IT will be alerted as to whether the files were backed up or not.

- Data distribution across endpoints is clearly visible
- Protection of specific files and inclusion in backup plans is easily confirmed
- Risk mitigation steps are easy to execute
- Collected data is used as the basis for compliance reports



Why? Complete protection that's easy, with no important data missed

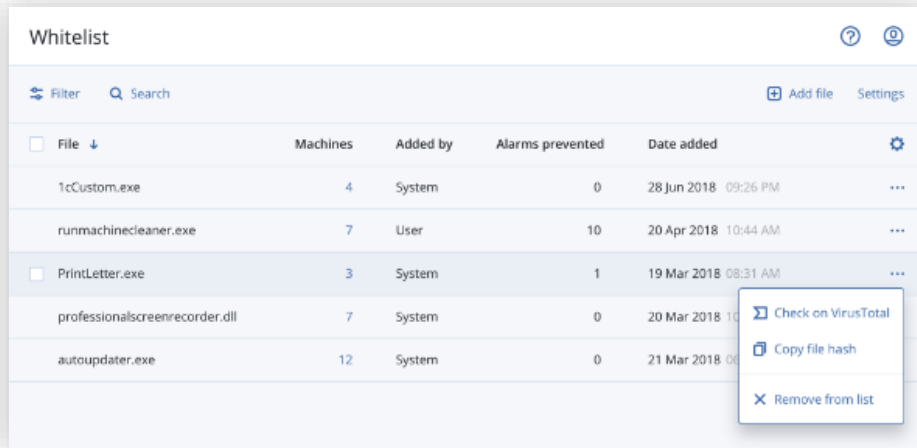
9. Automatic allowlisting from backups

Build global and local allowlists to prevent false detections while making more aggressive, accurate heuristics

Improved detection rates may lead to more false positive alerts. Traditional, global allowlisting does not support custom applications.

Acronis Cyber Protect scans backups with anti-malware technologies (AI, behavioral heuristics, etc.) to allowlist organizationally unique apps and avoid future false positives.

- Eliminates the time-consuming process of manually allowlisting unique apps
- Improves detection rates via improved heuristics
- Supports manual allowlisting

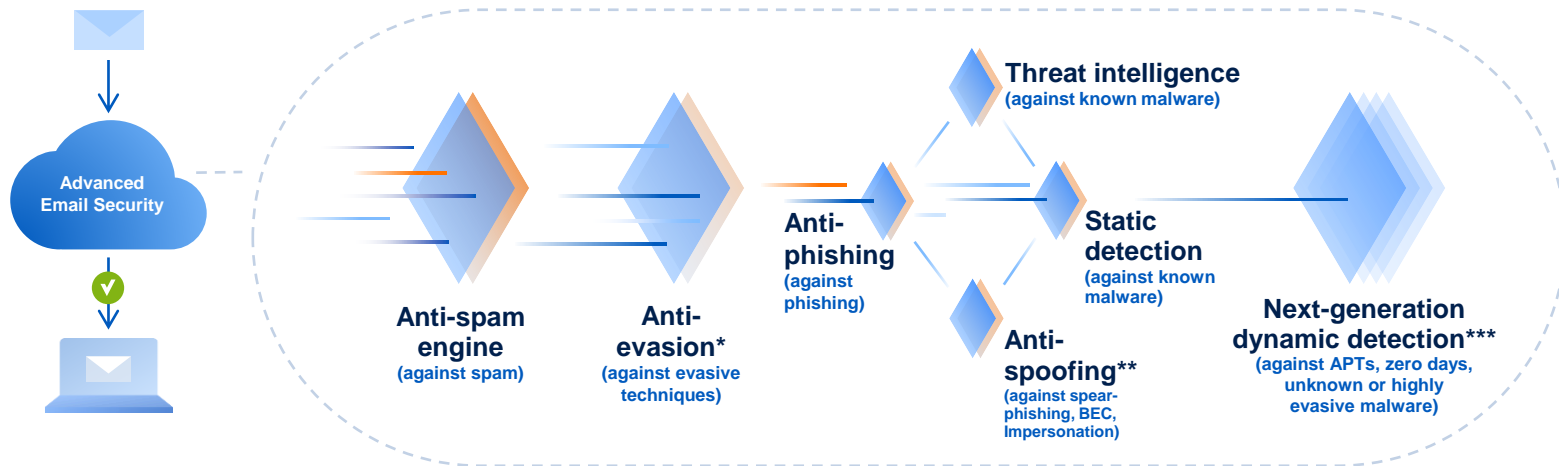


File	Machines	Added by	Alarms prevented	Date added	
1cCustom.exe	4	System	0	28 Jun 2018 09:26 PM	...
runmachinecleaner.exe	7	User	10	20 Apr 2018 10:44 AM	...
PrintLetter.exe	3	System	1	19 Mar 2018 08:31 AM	...
professionalscreenrecorder.dll	7	System	0	20 Mar 2018 10:44 AM	...
autoupdater.exe	12	System	0	21 Mar 2018 08:31 AM	...

Why? False positives can prevent access to data/apps. Automation saves time and improves protection

10. Multilayered protection

Seven layers of protection against modern email-borne threat



*Anti-evasion: Recursively unpacks embedded files and URLs into their individual components to identify hidden malicious content

**Anti-spoofing: Catch any impersonation attempt or BEC with a machine learning-based technology that inspects all relevant data and metadata (IP reputation, SPF, DKIM, and DMARC record checks; text and metadata analysis; scoring of senders; other algorithms) to detect spoofing attempts well before they reach the end-user

***Next-generation dynamic detection: Unique CPU-level technology that acts earlier in the attack chain (at the exploit stage, prior to malware release) by analyzing the execution flow during runtime by reading the assembly code to catch and stop advanced threats such as APTs and zero-days.

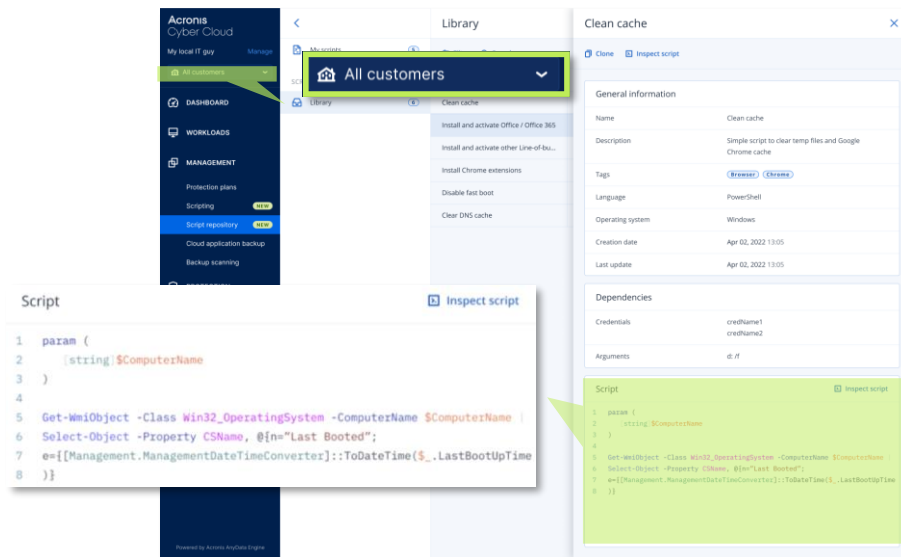
Why? Block modern email-borne threat before it reaches end users

11. Automation via scripting

Manage more workloads with less effort

Manage and execute custom pre-approved PowerShell / Bash scripts on remote Windows and Mac machines.

- Increase the efficiency of your MSP technicians by automating repetitive/day-to-day tasks through scripting
- Minimize the risk of human error with Acronis-verified set of scripts or scripts created by your IT administrators
- Centrally manage and monitor the scripts on partner and customer levels
- Run scripts on demand, on schedule, or when start conditions are met



Why? Automate manual and mundane workload monitoring and management tasks.

Top use cases for Acronis Cyber Protect Cloud

- **Simplified onboarding.** Discover all devices that require protection and remotely install a single agent (instead of many) for anti-malware, backup, remote desktop, patch, data loss prevention, etc.
- **Zero-day malware and ransomware protection.** Get our industry-leading, AI-based Acronis Active Protection, which now includes a static analyzer and behavioral analysis.
- **Compliance and forensic investigations.** Offer services to industries with high compliance requirements — Acronis equips you with image-based backup and forensic data like free space and memory dumps.
- **Better SLAs.** Keep and improve availability KPIs for clients with proactive, active and reactive cyber protection.
- **Post malware-attack recovery.** Lower risk of reinfection and ensure fewer operations with anti-malware scans of backups in centralized locations and safe and quick recovery — patch updates ensure backups are covered too.
- **Protection for all key files.** See what data is covered at a glance via Acronis' comprehensive Data Protection Map.
- **Centralized patching.** Protect all client software (not just Microsoft) and cover all clients using one multitenant tool.
- **Demonstrate your service value to clients.** Use flexible, detailed reporting to simplify contracts renewals and enable easier sales with vulnerability assessments in backup service.
- **Real-time protection of important documents.** Count on continuous data protection to immediately save all changes to critical files, even between backups.
- **Auto-response to emerging threats.** Adjust the scope and the schedule of backups or anti-malware scans, based on real-time alerts from Acronis Cyber Protection Operation Centers (CPOCs).
- **Intercept modern email-borne attacks within seconds.** Block email threats, including spam, phishing, business email compromise (BEC), account takeover (ATO), malware, advanced persistent threats (APTs), and zero-days before they reach end-users' mailboxes.
- **Minimal planned and unplanned downtime, plus automation.** Benefit from automated and simplified maintenance routines and proactive protection, including: out-of-the-box scripting, hard drive health checks, on-time patches, and regular vulnerability assessments.
- **Protection against unauthorized exfiltration.** Prevent data leaks from endpoints — without requiring months to deploy, teams to maintain, or a Ph.D. in privacy law to understand.

Key features overview

Built on the best-in-breed backup for MSPs

Hybrid cloud
architecture

1

20+ workload
types protected

2

File and
image backup

3

Instant recovery

4

Flexible storage

5

Built for MSPs

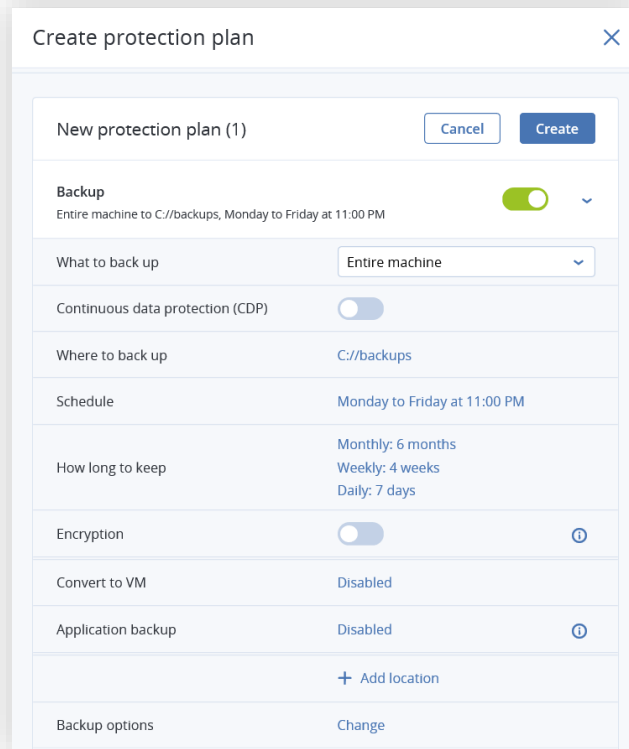
6

Why? Faster recovery and better RTOs

Full-image and file-level backups

Back up individual files or safeguard an entire business with a few clicks

- **File-level backup:** Use this option to protect specific data, reduce the backup size, and save storage space
- **Full-image backup:** Easily back up the entire system as a single file, ensuring bare metal restores
- In the event of data disaster, you can easily restore all information to new hardware



The screenshot shows the 'Create protection plan' window with a close button (X) in the top right. The main title is 'New protection plan (1)' with 'Cancel' and 'Create' buttons. The 'Backup' section is active, showing 'Entire machine to C://backups, Monday to Friday at 11:00 PM' with a green toggle switch and a dropdown arrow. Below this is a table of settings:

What to back up	Entire machine	▼
Continuous data protection (CDP)	<input type="checkbox"/>	
Where to back up	C://backups	
Schedule	Monday to Friday at 11:00 PM	
How long to keep	Monthly: 6 months Weekly: 4 weeks Daily: 7 days	
Encryption	<input type="checkbox"/>	ⓘ
Convert to VM	Disabled	
Application backup	Disabled	ⓘ
+ Add location		
Backup options	Change	

Why? Ensure business continuity with flexible backup options and avoid downtime and data loss

Flexible storage options

Meet data sovereignty or cost requirements

Cloud storage



Three turnkey cloud storage options



Other public clouds
(via Acronis Backup Gateway)



Your own or third-party cloud storage

On-premises storage



Local disks



SMB/CIFS/DFS and
NFS shares



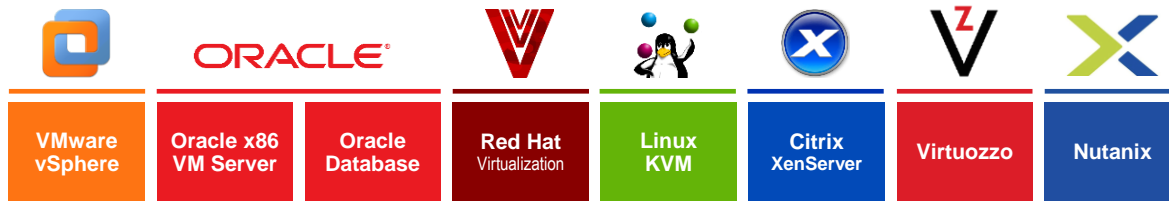
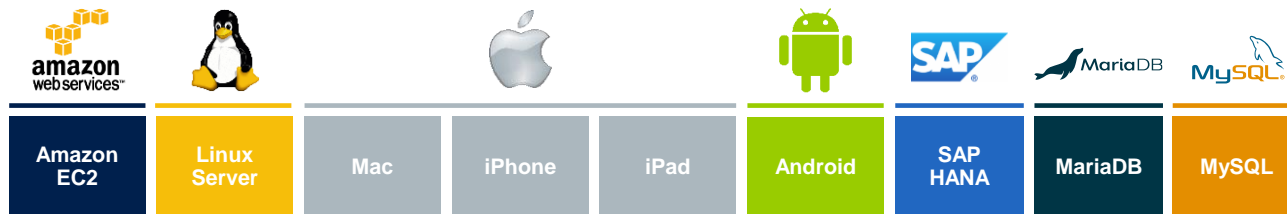
On-premises
Acronis Storage

”

Other solutions shoehorned us into a situation where we had to tell our customers they couldn't do certain things. **With Acronis we have complete flexibility**, and this allows us to offer the best user experience.

Jason Amato,
Marketing Manager at
Centorrino Technologies

Provide protection for 20+ workload types from infrastructure to SaaS apps



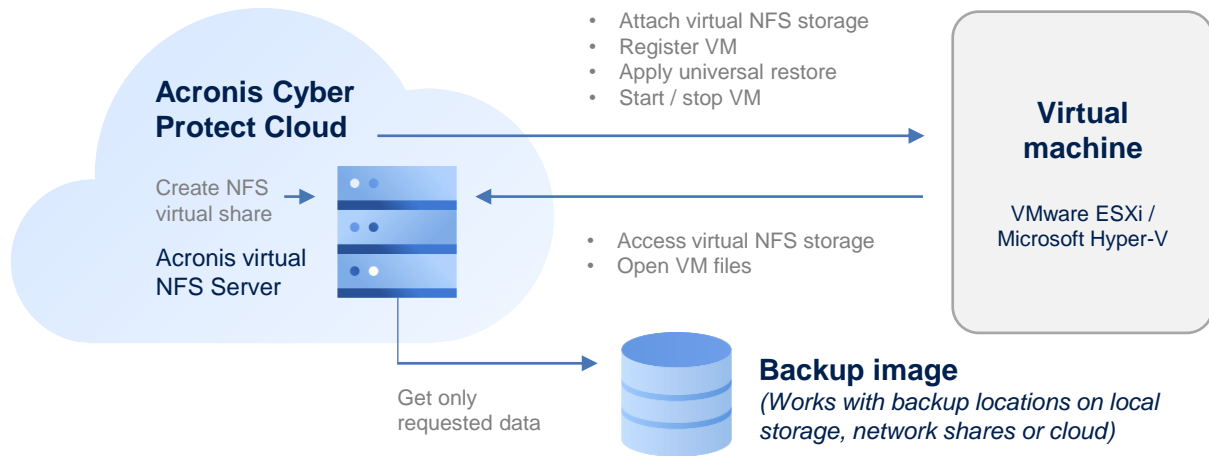
Streamline delivery of cyber protection using just one solution



Best-in-industry RTOs with Acronis Instant Restore

Acronis Instant Restore is patented technology that allows you to recover systems in seconds by starting any Windows or Linux system (physical or virtual) directly from the backup storage on your existing Microsoft Hyper-V or VMware vSphere ESXi host — without moving data.

How it works



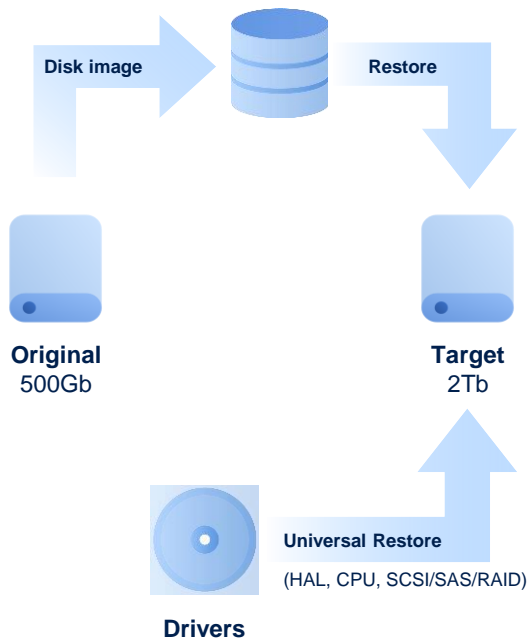
Benefits

- RTO in seconds
- Recover any virtual, physical or cloud server, Windows or Linux
- Reduced network consumption

Acronis Universal Restore

Restore Windows and Linux systems to dissimilar hardware

- Quick and easy system recovery to dissimilar hardware, including bare-metal physical, virtual or cloud environments
- After recovering a disk image as is, Acronis Universal Restore analyzes the new hardware platform and tunes the Windows or Linux settings to match the new requirements



Why? Reduce RTOs and ensure quick, easy system migration with a few clicks

Error-proof immutable backups

Prevent accidental and malicious data loss

Ensure backups cannot be encrypted or deleted by a ransomware attack on the endpoint through immutable storage, enabling you to recover quickly to the most recent clean state.

The immutable storage is currently available in a governance mode, enabling admins to modify the retention settings and delete the backups.

The governance mode can be used for testing immutability or in case you want to protect backups from “regular” users (not admins).



Why? Prevent backups from being deleted by malware or malicious users.

Acronis

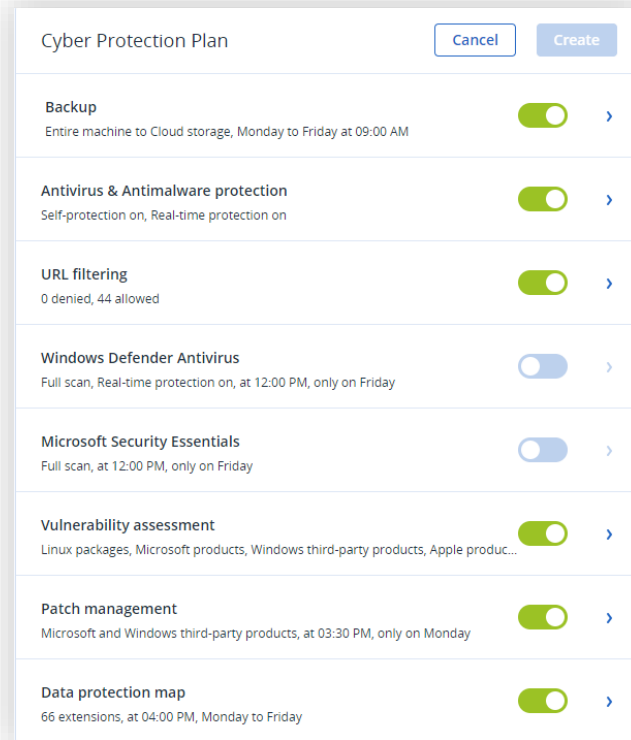
#CyberFit

**Backup is dead —
Acronis Cyber Protect is better
~~backup~~ protection**

One protection plan

Efficiently enable, disable and configure services and policies on a per-client or group level:

- Backup
- Anti-malware protection
- Disaster Recovery
- URL filtering
- Vulnerability assessments
- Patch management
- Data discovery (via data protection map)
- Microsoft Defender Antivirus and Microsoft Security Essentials management



Why? Better protection with less effort, automated

Significantly extended anti-malware capabilities

Acronis Cyber Protect Cloud



Acronis Active Protection

Anti-ransomware,
anti-cryptojacking, AI- and
ML-enabled



Acronis static AI analyzer

On-access
and on-demand
detection



Acronis antimalware engine

Any malware
(cloud and local
detection)



Acronis behavioral engine

On-access
detection

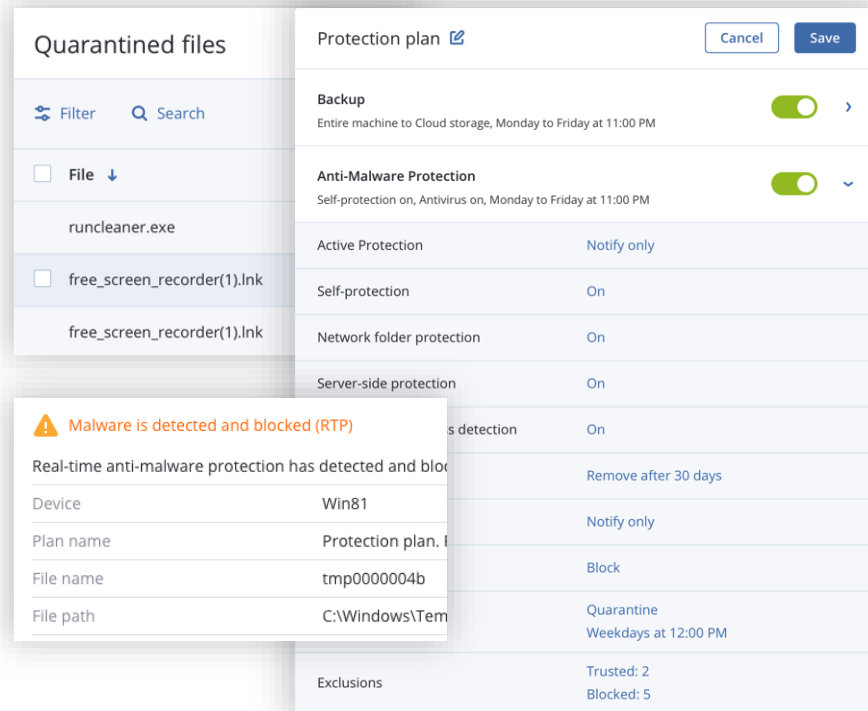
Native integration with Windows Security Center

Why? Active prevention of downtime and data loss, not just recovery after an attack

AI-based protection against zero-day malware

Anti-malware protection for Windows, Linux and macOS

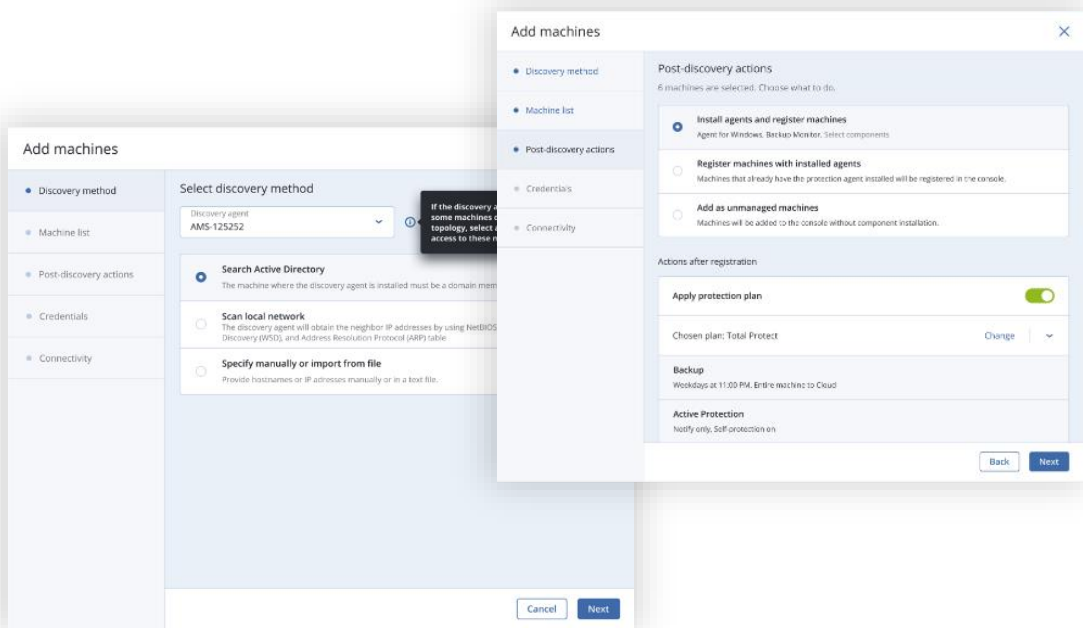
- Ransomware detection and data recovery
- Cryptomining process detection
- Real-time protection and on-demand scanning
- Self-protection: Protect Acronis components (e.g., registry, service stopping, Acronis file protecting)
- Network folder protection: Protect the data in shared folders on your machine against ransomware
- Server-side protection: Protect the data in shared folders within your network against ransomware
- Files quarantine
- Exclusions management: Specify processes that will not be considered malware; exclude folders where file changes will not be monitored; select files and folders where scheduled scanning will not be executed



Devices auto discovery and remote agent installation

Simplify the process of installing multiple agents at once – both in the cloud and on-premises

- Network-based discovery
- Active Directory-based discovery
- Import a list of computers from the file
- Auto-apply a protection plan
- Batch remote agent installations with a discovery wizard

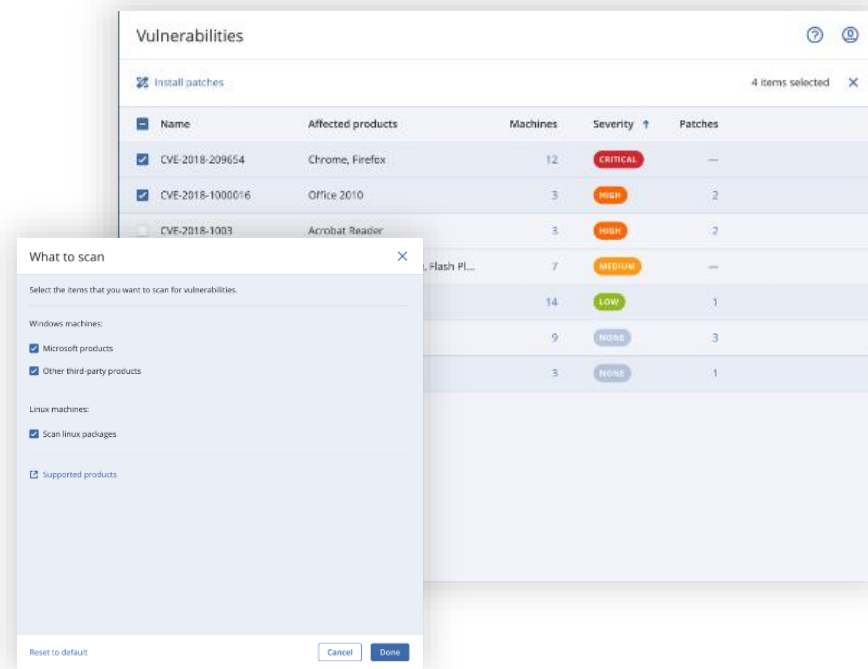


Why? Easier and faster onboarding. Fewer resources required. Completeness of protection.

Vulnerability assessments

Discover an issue before it's a problem

- Continuous, daily updates of Acronis' vulnerability and patch management database
- Comprehensive dashboard for vulnerability detection, their severity and patch availability
- **Constantly expanding support for:**
 - Microsoft stack:
 - a) Workstations – Windows 7 and later
 - b) Server – Windows Server 2008R2 and later
 - c) Microsoft Office (2010 and more) and related components
 - d) .NET Framework and server applications
 - MacOS workloads
 - Adobe, Oracle Java
 - Collaboration software: Zoom, Teams, VPNs
 - Browsers and other software

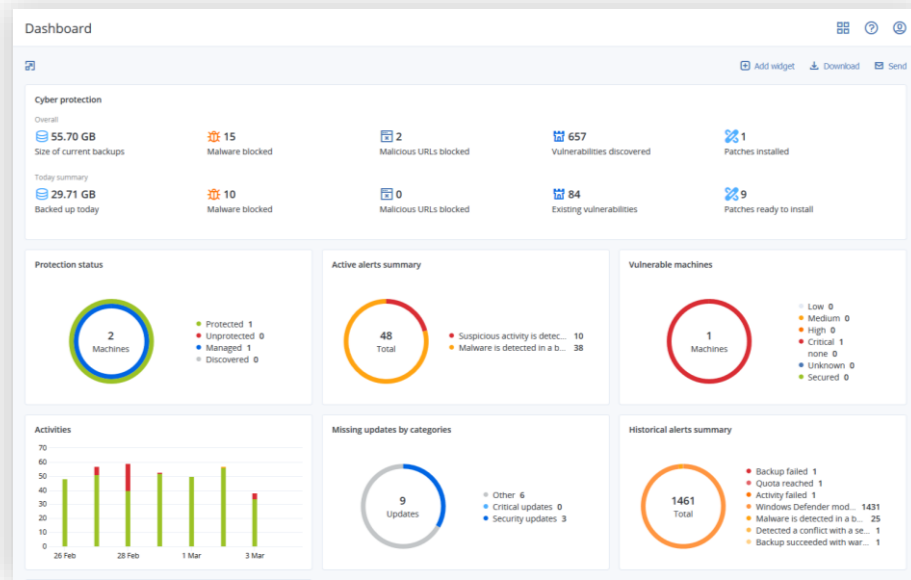


Why? Mitigates potential threats and prevents attacks

Flexible reporting and report scheduling

Powerful reporting through a single pane of glass:

- Active alert control
- Identify missing updates
- Customizable dashboard widgets
- Quickly identify problems
- Fast access to management actions
- Customizable client executive summary reports to drive a strategic conversation with your clients
- Report scheduling
 - a) Share internally or with clients
 - b) Use your format of choice: XLS, PDF or CSV



Why? Demonstrate MSP value, enable faster operations and simplify renewals

Hardware inventory collection

- Discover all hardware assets on all protected endpoints of the organization (e.g., CPU, GPU, motherboard, RAM, network adapters, etc.)
- Get up-to-date information about hardware assets:
 - Regular scans can be scheduled to run automatically
 - On-demand scans can be manually triggered by engineers
- Get detailed hardware information about hardware assets such as model, manufacturer, serial number, etc.
- Browse all hardware assets, or search and filter by multiple criteria: processor model, processor cores, disk total size, memory capacity
- Generate hardware inventory reports

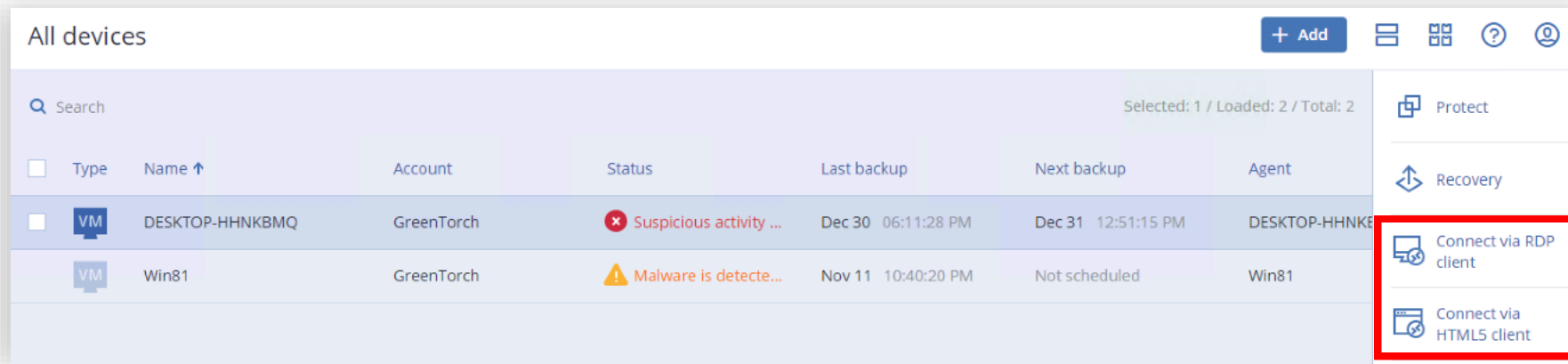
The screenshot displays the Acronis Cyber Protect console interface. On the left, a table lists 'All devices' with columns for 'Type' and 'Name'. The device 'DESKTOP-GLN477D' is selected. On the right, a detailed view for 'DESKTOP-GLN477D' is shown, including tabs for 'OVERVIEW', 'PLANS', 'DETAILS', 'SOFTWARE', 'HARDWARE', and 'ACTIVITIES'. The 'HARDWARE' tab is active, showing the 'Last hardware scan' as 'Mar 31, 13:00'. Below this, two sections provide detailed hardware information:

Motherboard	
Name	Z170X
Manufacturer	Gigabyte Technology Co. Ltd.
Model	Z170X Gaming
Serial number	132-LF-E657

Processors	
Intel(R) Core(TM) i5-9600K CPU	
Manufacturer	Intel Corporation
Model	9600K
Max clock speed	3.7 GHz
Number of cores	4 Cores, 8 Logical Processors

Why? Save time and effort with up-to-date hardware inventory information

Remote Desktop and Remote Assistance



The screenshot displays the Acronis Cyber Protect console interface. At the top, it says "All devices" with a "+ Add" button and icons for list, grid, help, and user. Below is a search bar and a status indicator "Selected: 1 / Loaded: 2 / Total: 2". The main table lists devices with columns for checkboxes, Type, Name, Account, Status, Last backup, Next backup, and Agent. Two devices are listed: "DESKTOP-HHNKBMQ" (VM) with status "Suspicious activity ..." and "Win81" (VM) with status "Malware is detecte...". On the right sidebar, there are buttons for "Protect", "Recovery", "Connect via RDP client", and "Connect via HTML5 client". The "Connect via RDP client" and "Connect via HTML5 client" buttons are highlighted with a red rectangle.

<input type="checkbox"/>	Type	Name ↑	Account	Status	Last backup	Next backup	Agent
<input type="checkbox"/>	VM	DESKTOP-HHNKBMQ	GreenTorch	✖ Suspicious activity ...	Dec 30 06:11:28 PM	Dec 31 12:51:15 PM	DESKTOP-HHNKBMQ
<input type="checkbox"/>	VM	Win81	GreenTorch	⚠ Malware is detecte...	Nov 11 10:40:20 PM	Not scheduled	Win81

Remotely operate any endpoint as if you are near the device

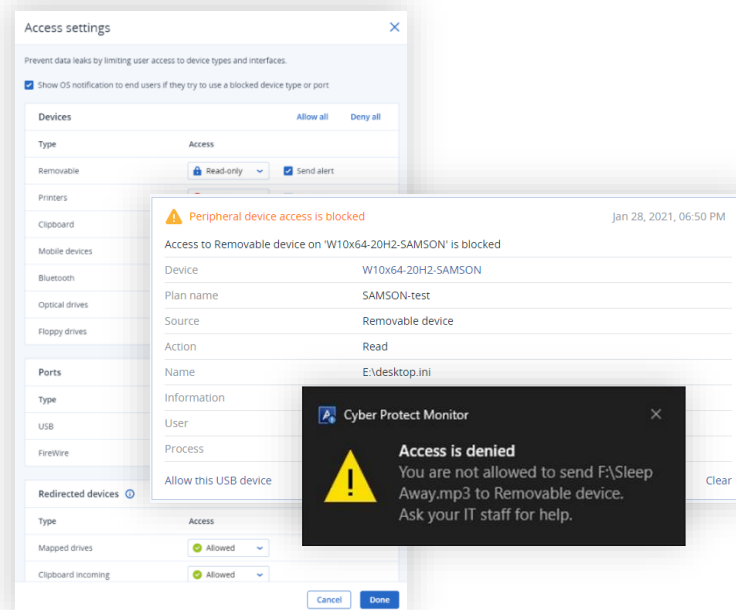
- Securely connect to remote machines even behind a firewall on a private network without changing firewall settings or establishing additional VPN tunnels
- Allow your engineers to view a user's screen, to provide support with specific tasks or fix issues

Why? Fewer tools, plus less effort to connect, and faster reaction times, reduced costs

Device control

Strengthen your security services and minimize the risk of data leaks for clients with essential data loss prevention (DLP)

- Controlled channels (local workloads) - Endpoints (Windows PC, workstation, server), ports, peripheral and redirected devices, clipboard, virtualized sessions
- Capabilities:
 - Selective access control per device/port type (deny, allow, read only)
 - Real-time alerts and notifications
 - a) On workloads – on/off for all devices and ports
 - b) In console – on/off per device/port type
 - Control clipboard copy/paste operations
 - Control screenshot captures (PrintScreen and any third party app)
 - Support of encrypted removable media
 - Allowlisting
 - a) Device type
 - b) USB – granular, down to serial number
 - c) Clipboard operations – within applications

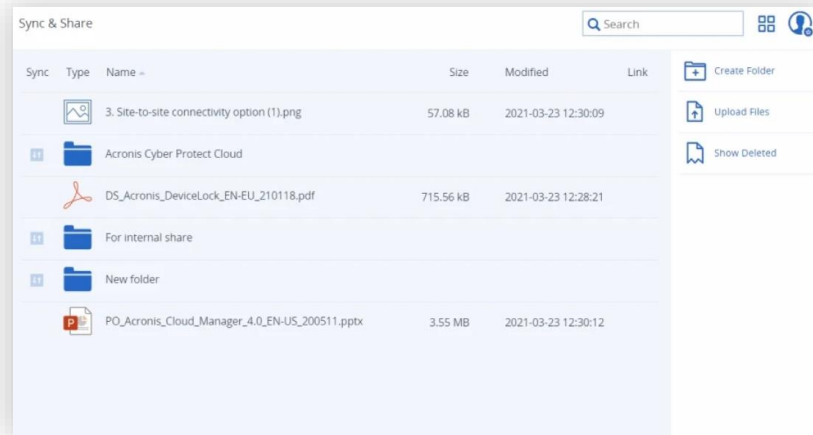


Why? Proactively prevent data leaks and control data flows between devices and peripherals

Secure file sync and share

Boost revenue growth with an integrated file sync and share service

- Reduce deployment time, improve efficiency and remove silos with a single, unified Acronis Cyber Files Cloud and Acronis Cyber Protect Cloud agent.
- Empower clients to securely create, edit and share content using their own smartphones (iOS and Android), tablets, PCs, Macs and web-enabled devices.
- Boost the productivity of mobile users with complete support of Microsoft 365 mobile applications and a convenient PDF editing and annotation tool.
- Provide complete end-to-end encryption, enterprise-class audit trails, control over files and folders, plus sophisticated policy controls for users, applications and data.

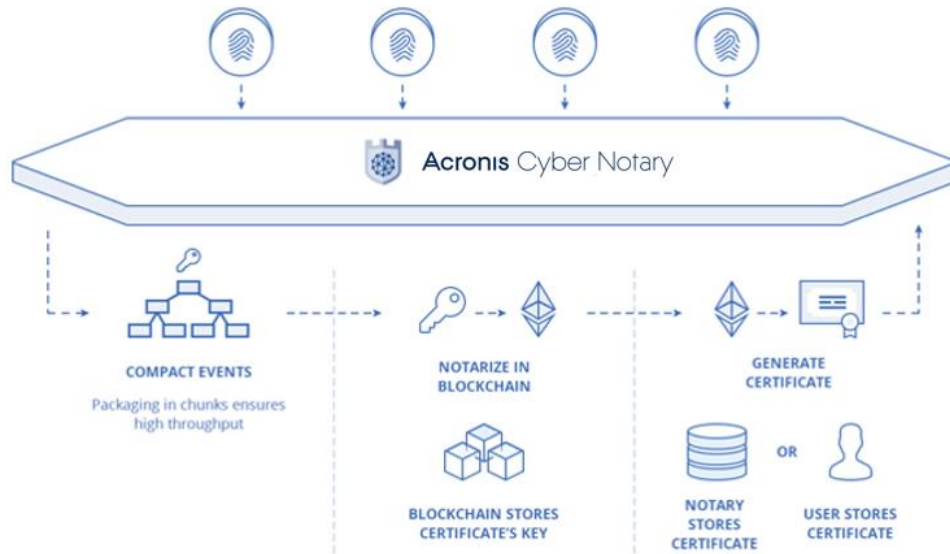


Why? Take full control over data location, management and privacy with an integrated file sync and share service

Blockchain-based notarization

Ensure data integrity with innovative blockchain-based Acronis Cyber Notary

- Highly scalable micro-service architecture
- API interface (REST), queue interface (AMQP) for integration
- High throughput (xx10,000 objects per blockchain transaction)
- Notarization certificates with built-in verification
- Embeddable e-signatures and document templates



Why?

- Ensure the integrity of business critical data
- Achieve greater regulatory transparency
- Reduce security risks

Client Executive Summary Report

Drive a strategic conversation with your clients monthly

Easily demonstrate the value of the services you deliver to your clients with the customizable Client Executive Summary Report.

Show key performance metrics for your delivery of:

- Backup
- Disaster recovery
- Antimalware protection
- Vulnerability assessment and patch management
- Data loss prevention
- Cyber Files
- Cyber Notary



**Demonstrate
Value**



**Set
Expectations**



**Ensure
Success**



- Download via PDF or Excel format
- Customizable
- Set up automatic delivery

Acronis

#CyberFit

**Easy, efficient, secure cyber
protection with advanced packs**

Add advanced packs: Security, Management, Backup, Disaster Recovery, Email Security, Data Loss Prevention, File Sync and Share



Optimize for every workload

Easy to upsell

Vendor consolidation

Acronis Cyber Protect Cloud with Advanced Backup

Protect your clients' data confidently with best-in-breed backup
enhanced with cyber protection



Increase automation and productivity

Scheduled backup reports, paired with cloud backup enhancements – like continuous data protection – helps you save time while saving your clients from data loss



Deliver the most secure backup

Acronis delivers a unique approach by combining cloud backup with cyber protection features, such as antimalware and antivirus – helping you keep clients' data secure



Protect more workloads on more platforms

From a single console, protect more than 20 workload types, including Microsoft Exchange, Microsoft SQL Server, Oracle DBMS Real Application clusters, and SAP HANA

Acronis Cyber Protect Cloud with Advanced Disaster Recovery

Improve security by detecting more threats, save on simplified security management, and deliver better remediation with integrated cyber protection



Less downtime

Get clients running in mere minutes by spinning up IT systems in the Acronis cloud with full site-to-site connectivity and the ability to recover them to similar or dissimilar hardware



Minimize complexity

No need to add, learn, or manage another platform. It's one solution for any workload managed from a single interface that enables you to build a complete cyber protection service



Grow recurring revenue

Deliver more value, deepen client relationships, and increase retention by offering clients the disaster recovery services they are looking for – while increasing your monthly recurring revenue

Acronis Cyber Protect Cloud with Advanced Security

Improve security by detecting more threats, save on simplified security management, and deliver better remediation with integrated cyber protection



Full-stack anti-malware

Acronis Active Protection, enhanced with exploit prevention, URL filtering, antimalware detection for backed-up data, and improved detection rate to catch more threats faster



Security automation

Smart protection plans, auto-allowlist custom apps, automatic malware scans and AV definitions updates as part of recovery process to deliver services more effortlessly



Efficient forensics

Collect digital evidence and save it in a secure central repository to enable thorough post-incident investigations and proper remediation, while keeping costs down.

Acronis Cyber Protect Cloud with Advanced Email Security

powered by  **PERCEPTION
POINT**

Improve clients' security by detecting modern email-borne attacks before it reaches end-users



Stop phishing, spoofing and account takeover

Minimize email risk for clients with powerful threat intelligence, signature-based detection, URL reputation checks, unique image-recognition algorithms, and machine learning with DMARC, DKIM, and SPF record checks. Detect and mitigate account takeover (ATO) attack



Catch advanced evasion techniques

Detect hidden malicious content by recursively unpacking embedded files and URLs and separately analyzing them with dynamic and static detection engines.



Prevent APTs and zero-day attacks

Prevent advanced email threats that evade conventional defenses with Perception Point's unique CPU-level technology able to act earlier in the attack chain to block exploits before malware is released, delivering a clear verdict within seconds.

Acronis Cyber Protect Cloud with Advanced Data Loss Prevention (DLP)

Protect sensitive data from getting in the hands of unauthorized parties and stay compliant



Protection for sensitive data across 70+ channels

Protect clients' sensitive data — prevent data leakage from workloads via peripheral devices and network communications by analyzing the content and context of data transfers and enforcing policy-based preventive controls.



Automatic, behavior-based DLP policy creation

Automatically baseline and profile sensitive data flows to create and continuously adjust DLP policies to ever-changing business specifics, ensuring protection against the most common causes of data leaks.



Prompt reactivity to DLP events

Enable rapid response and forensic investigations and simplify DLP policy maintenance via centralized audit logs and alerts on security events. Ease reporting with information-rich widgets.

Acronis Cyber Protect Cloud with Advanced Management

Improve clients' protection by keeping systems up to date while automating routine work, and decreasing management burdens and TCO



Out-of-the-box scripting

Automate routine tasks like provisioning, configuration and maintenance with ready-to-use, Acronis-verified scripts you can easily customize — or create your own.



Automated patch management

Keep client systems up to date and close security gaps with integrated vulnerability assessments and automated patch management for 270+ applications.



Comprehensive management tools

Streamline your planning with hardware and software inventory collection, remote desktop assistance and drive health monitoring.

Acronis Cyber Protect Cloud with Advanced File Sync and Share

Take full control over data location, management, and privacy with a superior file sync and share service extended with fully remote notarization, verification, and online signing



Maximize productivity and collaboration

Support your clients' digital transformation with simple file and link sharing, controlled access with custom permissions, eSigning, and file notarization



Mitigate security risks

Leverage a HIPAA-compliant file sync and share service with encryption at rest and in transit, full control over data location, and data authenticity powered by Ethereum blockchain to record and verify notarizations



Boost revenue growth

Increase client retention and generate new revenue streams by expanding your offering with an advanced file sync and share service that supports all platforms

Acronis

#CyberFit

Why Acronis Cyber Protect Cloud?

Benefits of Acronis cyber protection

Fastest return to productivity: autonomous, integrated and modular cyber protection



Ease of Use

Fewer human errors, faster deployment, more workloads supported by an IT professional, more customers protected



Low TCO

Protection accessible for customer of any size, and low cost means higher margins for partners



Security

Protection solutions natively designed for security decrease partner risk of liability



Control

Control over data location, protection configuration and rights delegation reduced partner risks



Reliability

Scalable and highly available cyber protection allows partners to offer higher SLAs to their customers

Innovative cyber protection

1

All-in-one security solution

An integrated combination of the most useful protections: anti-malware, vulnerability assessment, backup, patch management

2

Multilayered approach

Total control of data lifecycle on protected systems: proactively avoid incidents, active protection and reactive stage

3

Excellent performance

A single agent sharing low-level interceptions for both backup and anti-malware protection

4

Best tech in the industry

Proven expertise in anti-malware protection, backup, and AI/ML

5

Simple tool against sophisticated threats

Single pane of glass, unified reporting, touch-friendly UI, one protection plan

Benefits for service providers

Protect a client's infrastructure and data beyond backup



Increase ARPU

- Sell more cyber protection services
- Get more margin on in-demand services
- Improve attach rate and sell more



Improve SLAs

- Proactively avoid downtime
- Faster remediation with improved workload protection
- Win more clients with better SLAs



Control costs

- Reduce expenses by using one tool for all daily tasks:
 - Onboarding
 - Monitoring
 - Management
 - Assistance
- No new hardware/staff required
- Improved granular licensing



Decrease churn

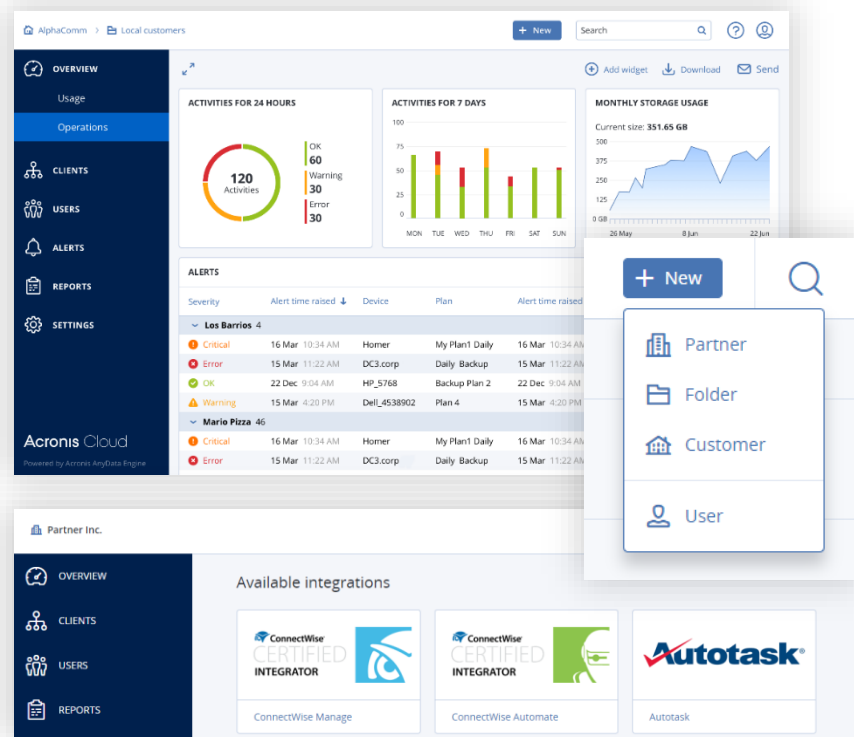
- Improve customer satisfaction and keep them coming back for more
- Demonstrate value and simplify renewals
- More services – mean stickier clients



Offer managed security

- Easy additional revenue:
 - No investment
 - No risk
 - No hunting for expensive security specialists
- Better protection for clients

Built for service providers



Easy, scalable management of customers' accounts via an easy-to-use web console



Integration with 60+ commonly used service provider systems and tools



Integration with custom provisioning systems via RESTful management API



Comprehensive white-labelling

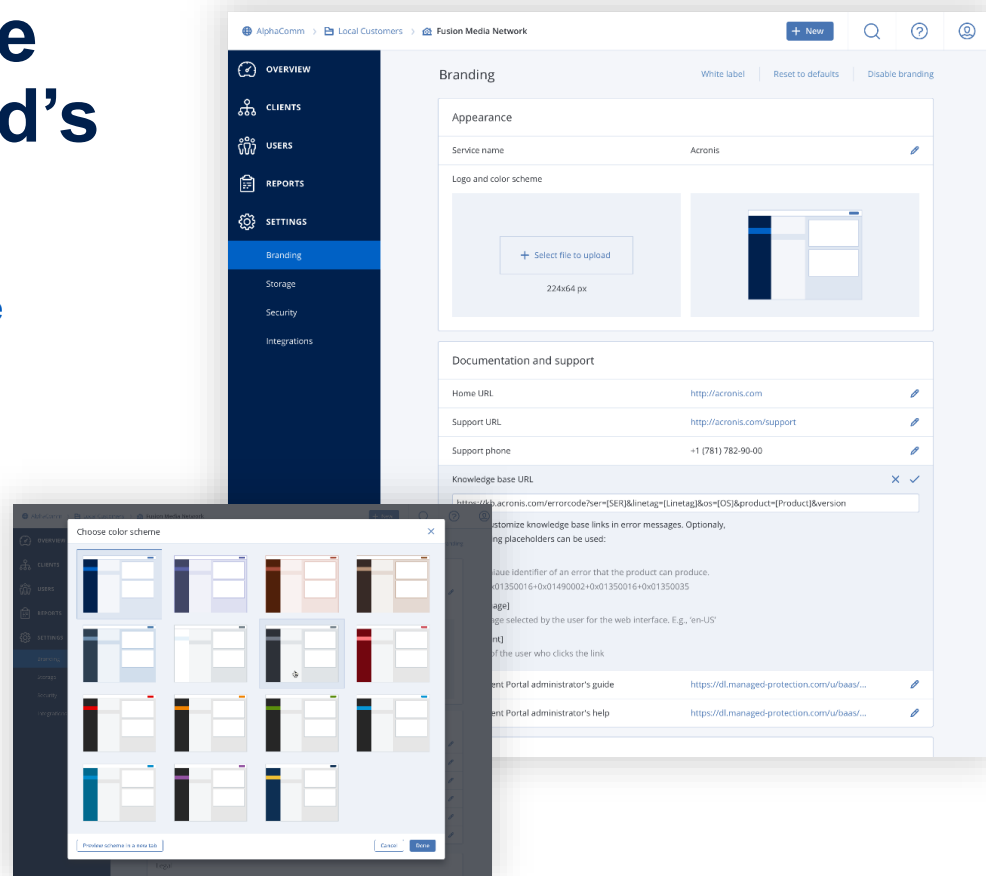


Straightforward pay-as-you-go pricing

White label the service to maintain your brand's unique look and feel

Design the management portal's user interface and your backup and disaster recovery services as desired. You can remove any association with Acronis or higher-level partners. Nearly 20 branding items offer key flexibility, such as:

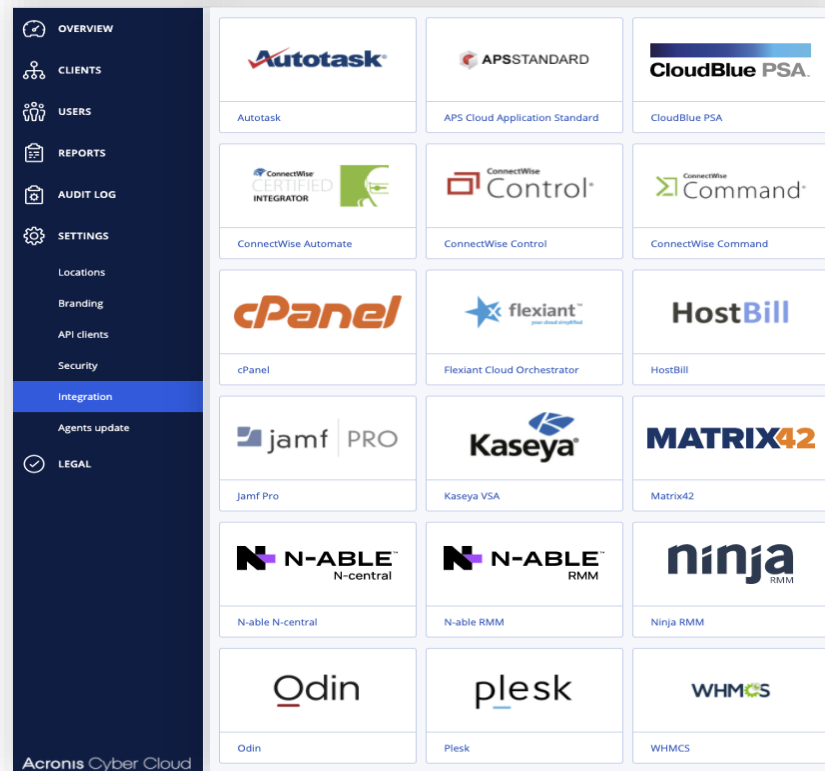
- Web-console color scheme
- Logos
- Company and service names
- Customizable email settings



Integration with service provider tools

Need a solution that seamlessly integrates with your business automation systems?

- **Configure integrations** with a variety of third-party systems, including:
 - **RMM and PSA tools:** ConnectWise (Automate, Manage, Control), Kaseya (VSA and BMS), Datto (Autotask and RMM), N-able (RMM and N-central), Jamf Pro, Addigy, Ninja, Tigerpaw and more
 - **Hosting control panels and billing systems:** cPanel, Plesk, WHMCS, DirectAdmin, HostBill
 - **Marketplace providers:** CloudBlue, AppDirect, interworks.cloud, Cloudmore, ALSO and more
- Utilize a powerful **RESTful management API** for custom integrations



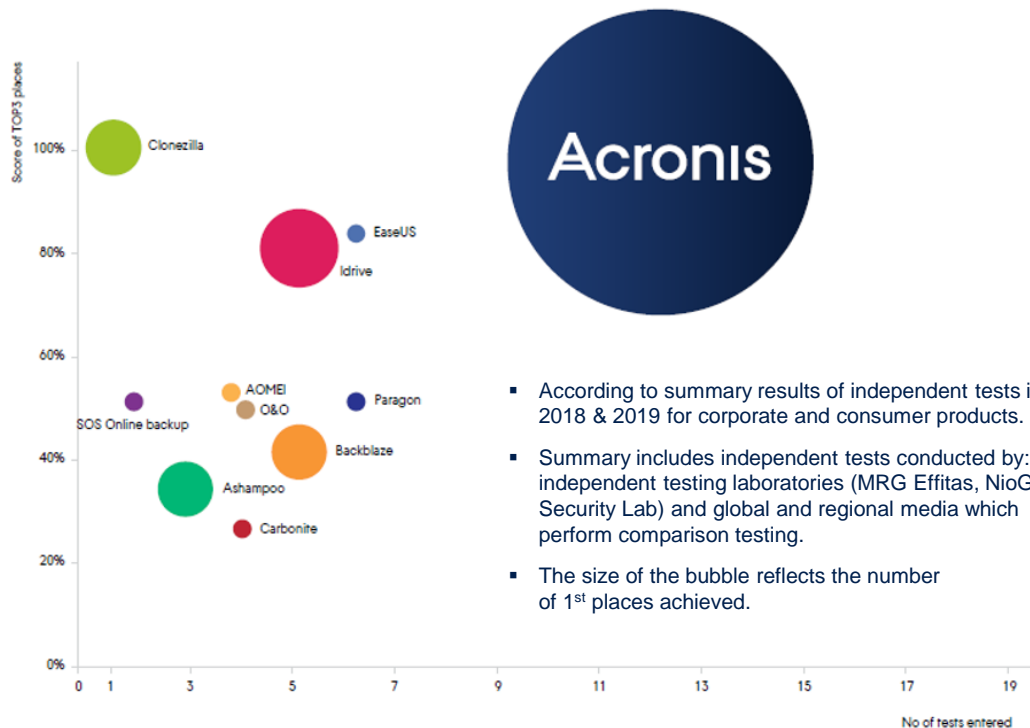
Ensure compliance and a local presence

Choose from 51 data centers worldwide to store data – Acronis Hosted, Google Cloud and Microsoft Azure

44+7
DATA CENTERS



Leader in independent tests results



Acronis security industry recognition



MVI member



VIRUSTOTAL member



Cloud Security Alliance member



Anti-Malware Testing Standard Organization member



Anti-Phishing Working Group member



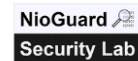
MRG-Effitas participant and test winner



Anti-Malware Test Lab participant and test winner



ICSA Labs certified



NioGuard Security Lab participant and test winner



AV-Comparatives approved business security product



VB100 certified



AV-Test participant and test winner

Acronis security related certifications

FIPS 140-2

Acronis AnyData Cryptographic Library has been [successfully verified by NIST](#)



ISO 27001

Acronis has Information Security Management System in accordance with standard ISO 27001:2013.



GDPR

Acronis is GDPR compliant through self-assessment as of May 25, 2018.



ISO 9001

Compliant with ISO 9001:2015

GLBA (Gramm-Leach-Bliley Act)

GLBA is applicable to financial institutions, compliant to Title V, Subtitle A, Section 501.(b)



TAA

Acronis products are "TAA compliant" as manufactured or "substantially transformed" in Switzerland

HIPAA

An independent third party gap analysis, showing that Acronis is compliant with HIPAA rules



Privacy Shield

Acronis is EU-US and Swiss-US Privacy Shield certified

Acronis Cyber Protect Cloud partners



Union Technology Cooperative (UTC) is a worker-owned managed service provider based in Middleton, Wisconsin that provides technology solutions to organizations.



TechnoPeak is a fast-growing systems integrator providing business automation, technology services, and digital transformation solutions. The company operates in Europe, CIS, and the Middle East, and it has over 500 IT professionals supporting over 3,000 customers.



Zebra Systems is a cloud distributor in the Czech Republic focused on backup, disaster recovery, and security products.



DataTegra delivers managed security services to commercial and public sector clients in South Africa and across Africa. The company has been operating for over a decade and provides a wide range of security services.



VMotion IT Solutions is focused on providing web hosting and cloud solutions through data center facilities located in Ireland.



i3-Software & Services LLC (S&S) is a managed service provider based in Louisiana that specializes in supporting local government. The company develops and sells IT solutions into municipal, parish/county, and state agencies.

MSPs on Acronis Cyber Protect Cloud

“ There is just **a lot of really smart stuff in the product**. It is really smart to come at it from the data protection angle because you are thinking of things that other vendors wouldn't consider. There is just a ton of opportunity with the product, and we are really excited about all of it.

Our goal (with Acronis Cyber Protect) is to drive as much penetration into our existing customers and then start to prospect for new customers.

One of the biggest values in Acronis Cyber Protect is the integration and getting customers to actually back up their data.

In addition to Symantec, we are also using Cisco Umbrella for DNS filtering and Panorama 9 for remote monitoring and patch management. Of course we use Acronis for backup. It would be great if we could **combine separate security solutions into just one** thing which is the direction you guys are going. It's a great vision in terms of where things are going and leveraging one tool to do a lot of things.

There is just a huge opportunity to say this **product works great**, it is really easy to use. We will come out to your site, train you – we know you are going to love it because we do.



Acronis

#CyberFit

Licensing and pricing

Acronis Cyber Protect Cloud:

Cyber protection for every workload at no cost

Protect your clients' workloads with essential cyber protection functionalities and pay nothing

Features		Acronis Cyber Protect Cloud
Security	#CyberFit Score	Included
	Vulnerability assessment	Included
	Anti-ransomware protection	Included
	Antivirus and Anti-malware protection: Cloud signature-based file detection only (no local signature-based detection)	Included
	Antivirus and Anti-malware protection: Pre-execution AI based file analyzer, behavior based cyber engine	Included
Cyber protection management	Group management of devices	Included
	Centralized plans management	Included
	Dashboards and reports	Included
	Remote desktop and remote assistance	Included
	Hardware inventory	Included
Data Loss Prevention	Device control	Included

Acronis Cyber Protect Cloud: Pay-as-you-go features

Ensure further protection of your clients' workloads with Acronis Cyber Protect Cloud pay-as-you-go features. Choose a licensing model and apply it on a client level. Both per-GB and per-workload are available.

Features		Acronis Cyber Protect Cloud
Backup	Workstations, Servers (Windows, Linux, Mac) backup	PAYG
	Virtual machine backup	PAYG
	File backup	PAYG
	Image backup	PAYG
	Immutable backups	PAYG
	Standard applications backup (Microsoft 365, Google Workspace, Microsoft Exchange, Microsoft SQL)	PAYG
	Network shares backup	PAYG
	Backup to local storage	PAYG
	Backup to cloud storage	PAYG
Disaster Recovery	Test failover in isolated network environment	32 compute points / month*
	Cloud-only VPN Connection	PAYG
	Firewall policies management	PAYG
File Sync and Share	File Sync and Share functionality	PAYG
Notary	Notarization, e-signature, document templates	PAYG

* Partners get 32 compute points for test failover that can be used to run several virtual machines of the same or different type. Fewer VMs or less powerful VM types will run for longer.

Two licensing models



Per-GB model

The per-GB model is simple – you only pay for the storage used, including native cloud storage (Acronis Cloud, Google Cloud Platform, Microsoft Azure), service provider cloud storage, third-party cloud storage and local storage. There is no limit on the number of protected devices.



Per-workload model

The per-workload model requires you to pay for each protected device (there are different prices for different types of devices) as well as for native cloud storage (Acronis Cloud, Google Cloud Platform, Microsoft Azure). However, you won't be charged additionally if using local storage or service provider cloud storage.

Advanced packs: Feature split

Advanced Packs	Features	
Advanced Security	Antivirus and Anti-malware protection: Local signature-based file detection	Included
	URL filtering	Included
	Forensic backup, scan backups for malware, safe recovery, corporate whitelist	Included
	Smart protection plans (integration with CPOC alerts)	Included
Advanced Backup	Microsoft SQL Server and Microsoft Exchange clusters	Included
	Oracle DB	Included
	SAP HANA	Included
	MySQL / MariaDB	
	Continuous data protection	Included
	Off-host data processing	
	Data protection map	Included
Advanced Management	Patch management	Included
	HDD health	Included
	Software inventory	Included
	Fail-safe patching	Included
	Cyber Scripting	Included
	Toolbox for MSP: processes/services, remote task manager*	Included
	AI-based monitoring*	Included
	Software deployment*	Included

Advanced Packs	Features	
Advanced Disaster Recovery	Runbooks	Included
	Production and test failover	Included
	Cloud only and site-to-site VPN Connection	Included
	Multiple templates	Included
	Cyber Protected Disaster Recovery (DR site automatic launch in the event of a cyberattack)*	Included
Advanced Email Security <small>Powered by Perception Point</small>	Anti-phishing, anti-spam protection, anti-malware, APT and zero-day protection, impression (BEC) protection, account takeover (ATO) detection, attachments deep scanning, URL filtering, threat intelligence, incident response services	Included
Advanced File Sync and Share	Notarization and e-signature	Included
	Document templates*	Included
	On-premises content repositories (NAS, SharePoint)*	Included
	Backup of sync and share files*	Included
Advanced Data Loss Prevention	Content flows control	Included
	Content discovery*	Included (Q4, 2022)
	User activity monitor*	Included (Q4, 2023)
Advanced Security + EDR (Q1, 2023)	All Advanced Security features + Endpoint Detection and Response (events collection, automated response, security incident management)	Included (Q1, 2023)

Note: All features marked with asterisk (*) will be available at a later date

Advanced packs: Administration



Partners can leverage **all advanced packs** within the Acronis Cyber Protect Cloud management console



Clients' workloads can be protected by **one, multiple, or all advanced packs** in both per-GB and per-workload licensing models



You can easily **enable or disable an advanced pack** via the Acronis Cyber Protect Cloud management console

Acronis

#CyberFit

About Acronis

Acronis is a Leader in Cyber Protection

AI-powered Cyber Protection, Cyber Cloud, Cyber Platform

Swiss

Since 2008 Corporate
HQ in Schaffhausen,
Switzerland

Singaporean

Founded in 2003 in
Singapore, currently
the International HQ

Dual Headquarters for Dual Protection



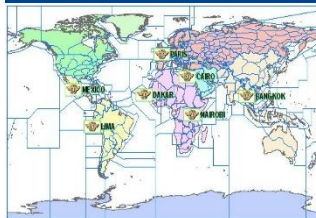
Scale, Growth and Reach

\$300M+ billings
50% business growth
100%+ cloud growth
100% of Fortune 1000
1,000,000+ businesses
50,000+ partners



Global Local Presence

1,500+ employees
33+ locations
150+ countries
33+ languages
DCs in 100+ countries
in the next 24 months



304 Flight Information Regions (FIR)

Acronis Cyber Protect

1,000,000+ workloads
protected
1,000,000+ attacks
prevented
9,000+ Cloud
partners



Solution: Integrated and Autonomous Cyber Protection

Acronis mission is to protect all data, applications and systems (workloads)

S

Safety

Nothing is lost:
there is always a
copy for recovery



A

Accessibility

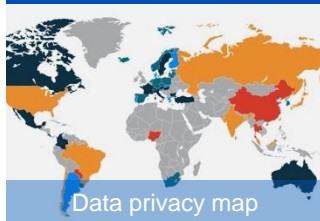
Access from
anywhere
at any time



P

Privacy

Control over
visibility
and access



Data privacy map

A

Authenticity

Proof that a copy
is an exact replica
of the original



S

Security

Protection against
bad actors



Acronis Cyber Singularity

Autonomous, integrated and modular cyber protection for everybody

Acronis Cyber Protect

Making cyber protection available as a Cloud service and on-premises "Classic" solution



Acronis Cyber Cloud

Control panel for Classic & Cloud: 15k+ resellers and 30k+ service providers by 2022



da Vinci Surgical System

Acronis Cyber Platform

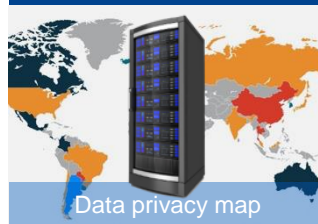
More services for partners, higher margin on more services offered 10k+ certified developers in 2022



Rich ecosystem

Acronis Cyber Infrastructure

Cloud, hardware and software appliances 100+ Acronis DCs, 1,000+ Partner DCs for compute and storage after 2022



Data privacy map

Acronis Cyber Services

Premium support, Acronis #CyberFit Academy, marketing, sales, and development services



Acronis Cyber Foundation

Program

Transforming lives through education

Let's work together to create new knowledge,
putting our diverse experiences and strengths
towards a brighter future!



Join us!



Acronis

#CyberFit

What's new

Acronis Cyber Protect Cloud – March 2023



Advanced Backup: Remote boot media control

Manage bootable media remotely via a web interface in Acronis Cyber Protect Cloud when there is no screen to access the workload.



Advanced Management: Automatic authentication of remote connections using saved credentials

Reduce overload and manual work for technicians via the automatic authentication of web connections by using saved credentials, enabling instant connections to remote workloads for streamlined troubleshooting.



“What’s new” link in Cyber Protect Console

Quickly and easily check all new capabilities included in the latest software release at any time.



Support for range offering items in PSA integrations

Streamline your billing process with added support for range offering items in our integrations with ConnectWise Manage, Autotask PSA, Kaseya BMS and HaloPSA. Report the total usage of Acronis products based on your preferred billing cycle - current or previous calendar month, or a custom billing month with a configurable start date.



NinjaOne version 2.0

Solve your clients' cyber protection challenges faster and streamline the provisioning, ticketing, monitoring and management of customer devices — all through NinjaOne RMM.



Support for Class 1 / Class 2 usage reporting in PSA integrations

You can now separate billing and usage reporting for free and paid storage, and provide greater detail to your customers for Microsoft 365 seats or any additional paid storage. Now available with our integrations for Kaseya BMS and HaloPSA.



Partner tenant billing in Autotask PSA

Our new partner tenant billing saves your time and efforts if you need to do aggregate billing for partner tenants under your Acronis account.



Acronis Files Cloud: Share Groups for easier sharing of files

Simplify the sharing of cloud files with multiple team members via Acronis Files Cloud. Create Share Groups and use them to easily share files with all group members via an email link.

Acronis Cyber Protect Cloud – January 2023



Advanced Backup: Save time and effort with group management for Microsoft 365 and Google Workspace

Simplify protection management for multiple Microsoft 365 and Google Workspace seats by eliminating the need to configure custom protection settings for each individual MS365 or Google Workspace workload.



Reduce onboarding costs with Datto RMM integration

The updated integration enables you to quickly and easily onboard customers by provisioning Acronis customer tenants based on Datto RMM sites. You can provision all or selected sites from Datto RMM as new tenants, map sites to existing tenants, or configure automatic tenant provisioning based on Datto RMM sites.

Acronis Cyber Protect Cloud – December 2022



New Advanced pack: Advanced Security + EDR

[Advanced Security + EDR](#) is finally available for Early Access program participants! Protect clients against advanced threats like zero days or hacking with an MSP-class EDR.



Advanced Disaster Recovery: Automated test failover

Save time and effort with a simplified, automated test failover. Now you can perform scheduled test failover for any server on a monthly or weekly basis, giving you the confidence that you can recover quickly and successfully.



Advanced Management: New remote desktop and assistance

Increase the efficiency of IT technicians and save time and resources from having to travel on-site with an easy to use, single application for seamless access and support for Windows, macOS, and Linux workloads.



Compliance mode for immutable storage

Ensure client backups do not get lost and can easily be recovered in the case of a malware attack, accidental deletion, or malicious deletion by a rogue administrator.



New agent for Synology NAS backup

Reduce operational costs by removing the need for a dedicated server that will enable NAS backup. The new agent enables you to get improved performance by accessing the data from NAS shares locally, instead of reading it over the network via SMB.



Provision N-able N-sight RMM 2.0 customer tenants in Acronis Cyber Protect Cloud

Emerging service providers using N-able N-sight RMM to monitor and manage customer workloads will be able to reduce the cost and fasten the speed of onboarding customers by easily provisioning tenants as new customer tenants in Acronis or mapping to existing Acronis customer tenants.



Secure sharing of confidential files and folders with external users

Get more flexibility and improved security with the ability to share files and folders with external users and enable them to access and preview the shared content, but also disabling the option to download the content.



Advanced DLP: Customize sensitive data detection in DLP rules by file types

Gain more granular control of DLP rules and reduce the risk of sensitive data leakage on client endpoints by customizing the DLP policy with rules that prevent unauthorized transfers of specific sensitive file types.



Advanced Email Security: Increased visibility of the scope of protected email users

In December, we're updating Advanced Email Security's dashboard to show a detailed view of all protected email users per client to enable you to easily verify newly protected mailboxes and report on the protection scope on a per-client basis with the goal to also reduce billing-related support tickets.



Recovery of deleted accounts

Reduce the risk of revenue loss, client churn, reputational damage, legal expenses and fines in the case of an unwanted data deletion caused by accidental data deletion, accidental service de-provisioning, a glitch in partner's integration, malicious impact, and more.



In-product maintenance notifications

Stay informed about potential service issues, maintenance in progress and upcoming maintenance events.



Advanced Email Security: Improved technical documentation

We have updated the technical documentation for onboarding technical staff and for configuring Advanced Email Security to introduce a centralized documentation space that is accessible in-product, improving its facility and accessibility.

Acronis Cyber Protect Cloud – November 2022



MI-assisted backup validation via boot screenshot analysis

Ensure consistency and recoverability of backups with MI-assisted validation via boot screenshot analysis. The screenshots are auto-analyzed by an AI / ML engine, eliminating the need for any user interaction.



New integration with HaloPSA

The new HaloPSA integration enables you to save time and reduce efforts by automating various customer management tasks, including tenant and product provisioning, ticket resolution, and usage reporting and billing.



Simplified workload registration

Now you can register workloads directly from the partner account — eliminating the need to log in with customer administrator credentials to register workloads in Acronis Cyber Protect Cloud.

Acronis Cyber Protect Cloud – October 2022



Expanded protection for Microsoft 365 OneNote

Recover Microsoft 365 OneNote notebooks quickly and easily directly into the Microsoft 365 account.



Integration with ConnectWise Asio platform

Acronis Cyber Protect Cloud is now fully integrated with ConnectWise Asio – the new unified IT management platform for MSPs, evolving from the existing ConnectWise Command platform.



macOS 13 Ventura support

Now you can protect macOS 13 Ventura workloads with Acronis Cyber Protect Cloud.



Acronis Cyber Files Cloud: public links to a folder

Enable users to create a direct link to a folder and share files with external users.

The flexible configuration allows setting up different parameters for the public link, such as expiration date and different access permissions (view only or view and download).

Acronis Cyber Protect Cloud – September 2022



Advanced Data Loss Prevention (DLP) General Availability: Effortlessly protect clients' sensitive data against leakage

Protect clients' sensitive data against leakage and strengthen compliance. Minimize effort and cost to value, aided by behavior-based DLP policy creation and extension, thereby unlocking unique simplification and scalability to boost profits.



Advanced Security: Firewall management for Microsoft Defender

Reduce the attack surface of a client workload by enabling Microsoft Defender Firewall in the protection plan. Receive prompt alerts in case unintended tampering of the firewall settings occurs.



Advanced Email Security: Improved license usage measuring

Maximize billing accuracy and predictability with standardized license usage measuring methods for the Advanced Email Security pack. Manually adjust and manage licenses in cases where the auto-measuring method is not applicable



Acronis Cyber Files Cloud: Rapid and efficient local synchronization

Downloading the entirety of your data from the cloud is no longer required when moving or copying local files and folders. Changes in clients' files and folders are directly synchronized on the local machine, thus increasing bandwidth, and saving time and system resources.



Acronis Cyber Files Cloud available in Turkish

Provide a higher quality experience for your clients, increase usability, and gain more convenience while working with Acronis Cyber Files Cloud. The user interface is now available in Turkish.



Unified integrations catalog in Acronis' console and website

The ISV integrations list has been redesigned to improve consistency and provide the same user experience whether you're accessing the Acronis website or the Management portal.

Acronis Cyber Protect Cloud – August 2022



Advanced Email Security: ATO protection for M365

Protect your clients against email account compromise by preventing attackers from phishing user credentials, constant monitoring of email accounts suggesting a compromise, and ensuring fast remediation and account containment in case of ATO.



Advanced Email Security: Comprehensive audit log

Enabling the auditing and investigation of any incident with full visibility into all actions performed by admin users and the Incident Response team.



Advanced Email Security: Localized user interface

The management console UI is now available in your preferred language — English, or newly added Spanish, German, French, Italian, and Portuguese.



Advanced Email Security: 24/7 chat support

Partners are now able to chat with the Incident Response team directly from the management console.



Advanced Email Security: Quickly downloadable reports

Establish transparency and accountability, build customer trust, demonstrate your service value to clients, and simplify upsells and renewals with reports downloadable as PDFs.



Advanced DR: Extend protection for Windows 2022 & Ubuntu

Empower partners to extend their protection of clients' critical infrastructure to Windows Server 2022 and Ubuntu Server 20.x/21.x with quick automated failover.



Extend anti-malware protection for Macs

Expand anti-malware protection of macOS workloads with Apple M1/M2 CPUs (on top of already-supported Intel CPUs) against new and unknown threats.



Improvements for blocked seats for M365 licensing

From August 2022 onward, Acronis will not charge for blocked seats (inability to log into Microsoft 365) with access to the protected SharePoint Online site and/or Teams, in case their OneDrive and/or mailbox are not protected.



Scale business opportunities with PAYG with AppDirect integration

If partners are leveraging the integration with AppDirect, they can implement new pricing models to sell the Acronis Cyber Protect Cloud and Advanced packs with flexible usage-based billing.



Effortlessly report on storage usage with ConnectWise integration

Partners are now able to separately report and bill their clients on storage that is either billable or non-billable (e.g., included storage in Microsoft 365 protection) from Acronis.



Acronis Cyber File: Easily access synchronized bookmarked folders

Users of the Acronis Cyber Files mobile application are now able to bookmark frequently-used folders. Easily navigate to the bookmarked folders faster and all the bookmarks are synchronized across all iOS devices.

Acronis Cyber Protect Cloud – July 2022



Advanced Disaster Recovery: Support for VMware ESXi 7.0 workloads

Extend your disaster recovery protection to VMware ESXi 7.0 workloads that are backed up agentless.



Advanced Email Security: Localized user interface

Get more value and convenience by using the user interface in your preferred language. Spanish is already available, and more to follow!



Acronis Cyber Files Cloud: File upload request

The files upload request gives end users a fast and secure way to request and obtain files from anyone, with all files being automatically organized into a user folder. Using an easy, drag-and-drop graphic interface, the file upload request enables end users to securely upload files without being added as a guest user or having access to the particular user account.

Acronis Cyber Protect Cloud – June 2022



Advanced Management: Out-of-the-box Cyber Scripting

Automate repetitive / day-to-day workload monitoring and management tasks through scripting. Start fast with Acronis-verified scripts that provide out-of-the-box automation for the most common partners' tasks.



Management of multiple clients on the partner level

Centrally manage all of your direct clients in the Acronis Cyber Protect Cloud console to streamline operations, including scripting management, and alerts and activities monitoring.



Advanced Backup: One-click recovery

Empower end-users to rapidly recover their workloads by enabling them to start an automated recovery with a single click.



Advanced DLP: Encrypted removable storage support

Detect encrypted removable storage devices and allow data transfers only to them. Neutralize the risks of sensitive data leaving clients' workloads.



Download and backup of Microsoft OneNote files

Protect Microsoft OneNote files from being lost by backing them up as part of the Microsoft OneDrive and Microsoft SharePoint Online backup process.



Local recovery of Microsoft 365 mailbox data to PST

Minimize the chance of clients not having their in-mail data available by enabling local recovery of emails as PST files even when Microsoft 365 is unavailable.



Application-consistent backup and recovery of web-hosted servers managed via DirectAdmin

Recover the entire server in case of a disaster, or granularly restore individual web-hosting accounts, files, databases, websites and local mailboxes — consistent with the cPanel and Plesk integrations.



URL customization with Let's Encrypt

Emphasize your brand identity by customizing the Acronis Cyber Protect Cloud access URL, and minimize maintenance efforts and costs with free-of-charge, automatically-renewed SSL certificates.



Automatic maintenance notifications via email

Provide your partners and clients with greater visibility into maintenance work in Acronis data centers by setting up automatic notifications via email per tenant.



Data center status and services availability portal

The new data center status page, available in Acronis Cyber Protect Cloud and the Partner Portal, provides a self-service where partners can check services status and upcoming maintenance schedule.



Partner tenant billing in ConnectWise Manage

Manage services and bill usage on a partner tenant level with ease in ConnectWise Manage integration.



Enable or disable ticket synchronization in Kaseya VSA

Effortlessly switch off ticket synchronization — either during tenant provisioning or in the organization settings.

Acronis Cyber Protect Cloud – May 2022



Chat with an Acronis account manager in the management portal

Consult with an Acronis account manager about planning, launching, and scaling your services with us, directly in the Cyber Protect console. The functionality will be available in all Acronis data centers for partners that do not use complete white-labeling.



Automated email security service provisioning for Microsoft 365

Simplify the initial configuration process with a ready-to-use script that automatically sets up routing between Microsoft and Advanced Email Security.



Auto-generation of product names in mapping wizard for Kaseya BMS and Tigerpaw PSA integrations

Acronis Cyber Protect Cloud automatically generates suggested names for new PSA products, using a predictable and understandable naming pattern, simplifying the process of mapping products to Kaseya BMS and Tigerpaw PSA integrations.



Malicious email detection alerts in the Cyber Protect console

Prevent potential damage by promptly reacting to malicious email detection alerts in the Cyber Protect console. Demonstrate your email security service value to end-customers with consolidated statistics on detected malicious emails in the Overview dashboard..



Configuration improvements in the ConnectWise Manage integration

Partners can manually trigger the synchronization of usage and quotas for one or more customer tenants between Acronis and ConnectWise Manage. Usage is now reported more accurately to ConnectWise Manage, using float point quantities where applicable.

Acronis Cyber Protect Cloud – April 2022



Advanced Data Loss Prevention (DLP): Early Access Program

Start planning your service upgrade. Experience a data loss prevention (DLP) solution designed for MSPs — at no cost during the early access period — that will enable you to prevent leakage of clients' sensitive data without extra cybersecurity headcount.



Sharing of files and folders with external users via Acronis Files Cloud

Empower users to share files and folders with “guest users” identified by their email addresses..



Management of macOS and Linux workloads via Kaseya VSA integration

Enable mass deployment, management of protection plans, and monitoring of protection status for macOS and Linux workloads — together with existing support for Windows from within the Kaseya VSA.



New “Partner profile” option

Enhance your team's focus with visibility into role-specific billing, business and / or technical updates from Acronis. .



Reduced service delivery complexity when using both Acronis Cyber Protect Cloud and Splashtop

Eliminate the need to manually switch between the Acronis Cyber Protect Cloud and Splashtop consoles via a native integration.



Advanced Email Security: Improved visual experience

Enable clients to see all the emails that are included in an e-signing invitation along with key information for sender and recipient.

Acronis Cyber Protect Cloud – March 2022



Failover of Azure VMs to Acronis Cyber Protect Cloud

Enable enhanced protection against Azure cloud outages while utilizing the public cloud. Benefit from the predictable and simple monthly billing that Acronis provides, unlike the billing of native Azure disaster recovery tools — Acronis MSP partners are billed only for storage and not for outbound network traffic consumption and / or hot disk usage.



Effortless recovery of workloads protected by BitLocker

Leverage a streamlined, intuitive process for the recovery of BitLocker-protected workloads. Recover disks, volumes and files encrypted by BitLocker with the ease you recover unencrypted ones — without the need to reboot or take any additional steps.



Provide anti-malware services for Apple M1 ARM-based workloads

Protect and manage all Mac-based devices for clients, regardless of the hardware inside. With Acronis, you can now extend your anti-malware services to the ever-growing market of Mac devices based on M1 ARM-based chips.



Usage reporting for trial tenants in Autotask PSA and ConnectWise Manage

Enable reporting on usage for trial tenants by empowering service technicians to set up a pay-as-you-go (PAYG) or prepaid option with overage billing models. This enhances the capability to provision clients as trial tenants, which was introduced in this past February's update.