Acronis

#CyberFit

Acronis
Cyber Protect Cloud

Modernize your cybersecurity and backup with integrated cyber protection

Dual headquarters
in Switzerland and Singapore

The threat landscape is becoming more complex

300%

spike in cybercrime during the COVID-19 pandemic

57%

of attacks are missed by traditional antivirus solutions

69%

spend more time managing tools than defending against the threats

Sources: Acronis Cyberthreats Report 2020, 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

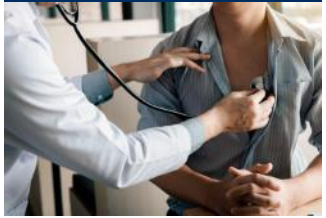
Deliver unmatched cyber protection

- 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

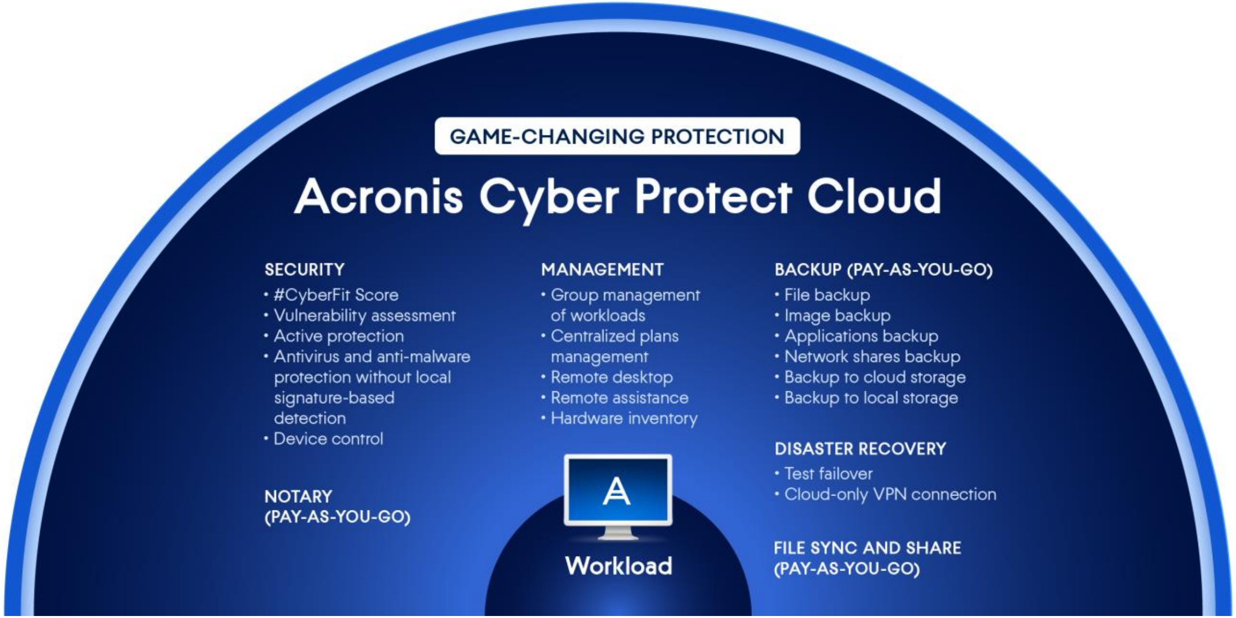
Recovery

Attack remediation without data loss and with integrated patching

Forensics

Fast and precise investigations with forensic-rich backups

Best-in-breed Backup with Integrated Security and Management



GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

SECURITY

- #CyberFit Score
- Vulnerability assessment
- Active protection
- Antivirus and anti-malware protection without local signature-based detection
- Device control

NOTARY (PAY-AS-YOU-GO)

MANAGEMENT

- Group management of workloads
- Centralized plans management
- Remote desktop
- Remote assistance
- Hardware inventory

BACKUP (PAY-AS-YOU-GO)

- File backup
- Image backup
- Applications backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY

- Test failover
- Cloud-only VPN connection

FILE SYNC AND SHARE (PAY-AS-YOU-GO)

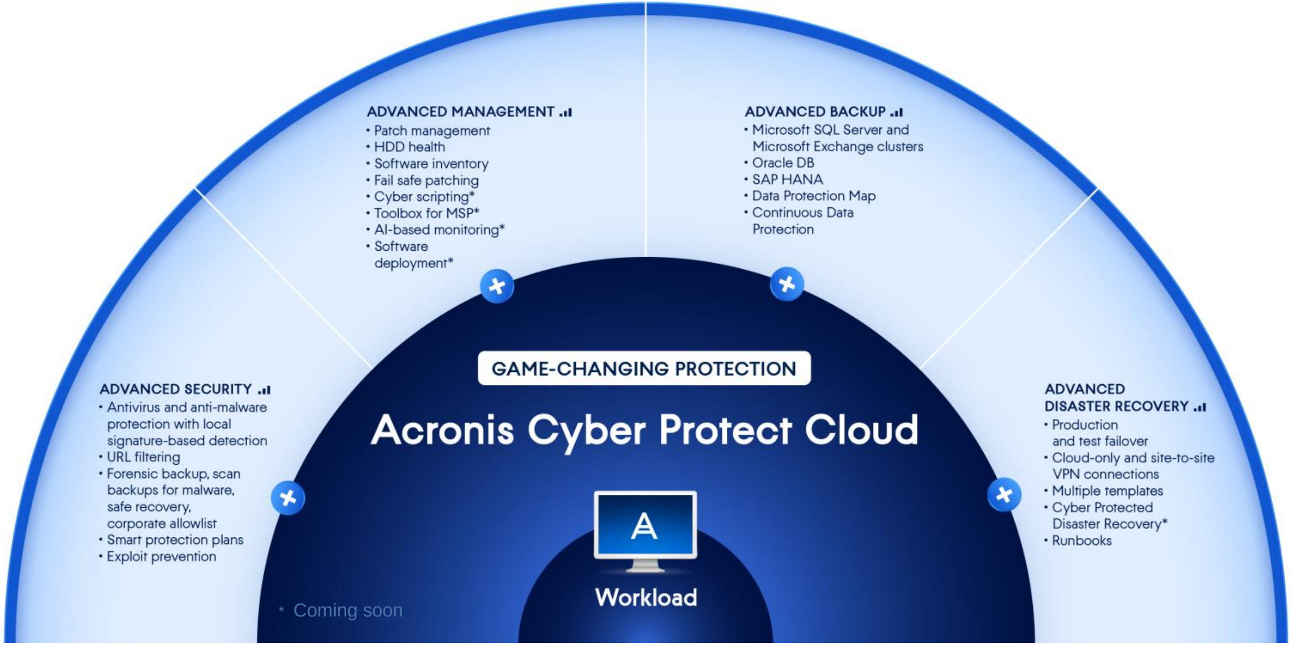
Protect every workload at no charge

Best-in-breed backup included

Strengthens your AV against zero-day threats

Accelerate security and manageability

Add Advanced Packs:
Security, Management, Backup, Disaster Recovery



ADVANCED MANAGEMENT

- Patch management
- HDD health
- Software inventory
- Fail safe patching
- Cyber scripting*
- Toolbox for MSP*
- AI-based monitoring*
- Software deployment*

ADVANCED BACKUP

- Microsoft SQL Server and Microsoft Exchange clusters
- Oracle DB
- SAP HANA
- Data Protection Map
- Continuous Data Protection

ADVANCED SECURITY

- Antivirus and anti-malware protection with local signature-based detection
- URL filtering
- Forensic backup, scan backups for malware, safe recovery, corporate allowlist
- Smart protection plans
- Exploit prevention

ADVANCED DISASTER RECOVERY

- Production and test failover
- Cloud-only and site-to-site VPN connections
- Multiple templates
- Cyber Protected Disaster Recovery*
- Runbooks

GAME-CHANGING PROTECTION

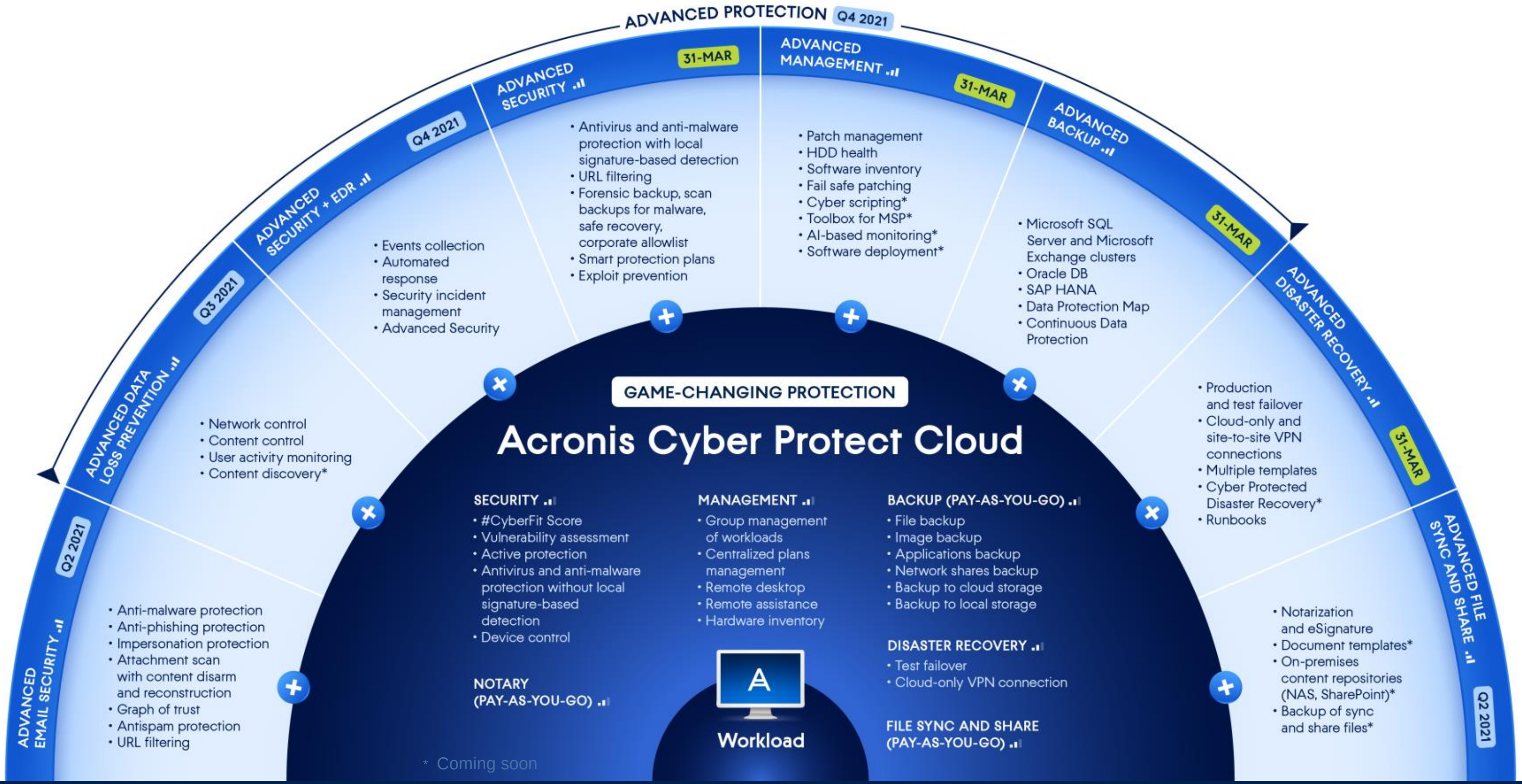
Acronis Cyber Protect Cloud

Workload

* Coming soon

Optimize for every workload **Easy to upsell** **Vendor consolidation**

2021 Roadmap for Service Providers



ADVANCED PROTECTION Q4 2021

ADVANCED EMAIL SECURITY Q2 2021

- Anti-malware protection
- Anti-phishing protection
- Impersonation protection
- Attachment scan with content disarm and reconstruction
- Graph of trust
- Antispam protection
- URL filtering

ADVANCED DATA LOSS PREVENTION Q3 2021

- Network control
- Content control
- User activity monitoring
- Content discovery*

ADVANCED SECURITY + EDR Q4 2021

- Events collection
- Automated response
- Security incident management
- Advanced Security

ADVANCED SECURITY 31-MAR

- Antivirus and anti-malware protection with local signature-based detection
- URL filtering
- Forensic backup, scan backups for malware, safe recovery, corporate allowlist
- Smart protection plans
- Exploit prevention

ADVANCED MANAGEMENT 31-MAR

- Patch management
- HDD health
- Software inventory
- Fail safe patching
- Cyber scripting*
- Toolbox for MSP*
- AI-based monitoring*
- Software deployment*

ADVANCED BACKUP 31-MAR

- Microsoft SQL Server and Microsoft Exchange clusters
- Oracle DB
- SAP HANA
- Data Protection Map
- Continuous Data Protection

ADVANCED DISASTER RECOVERY 31-MAR

- Production and test failover
- Cloud-only and site-to-site VPN connections
- Multiple templates
- Cyber Protected Disaster Recovery*
- Runbooks

ADVANCED FILE SYNC AND SHARE Q2 2021

- Notarization and eSignature
- Document templates*
- On-premises content repositories (NAS, SharePoint)*
- Backup of sync and share files*

GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

SECURITY

- #CyberFit Score
- Vulnerability assessment
- Active protection
- Antivirus and anti-malware protection without local signature-based detection
- Device control

NOTARY (PAY-AS-YOU-GO)

MANAGEMENT

- Group management of workloads
- Centralized plans management
- Remote desktop
- Remote assistance
- Hardware inventory

BACKUP (PAY-AS-YOU-GO)

- File backup
- Image backup
- Applications backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY

- Test failover
- Cloud-only VPN connection

FILE SYNC AND SHARE (PAY-AS-YOU-GO)

Workload

* Coming soon

Legacy Backup & AV solutions	Acronis Cyber Protect Cloud	
Complex Complicated licensing, deployment, and training, as well as agent conflicts	**All services managed from one place** Remove the complexity and risks associated with non-integrated solutions	**Easy**
Expensive Multiple tools, vendors, administration costs	**Smarter use of resources** Faster operations with integration and automation lets your team focus on your clients	**Efficient**
Unsecure Lack of integration creates gaps in defenses, management burden compromises security	**Total peace of mind for clients** Customize your services and deliver complete protection for every workload	**Secure**

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)

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

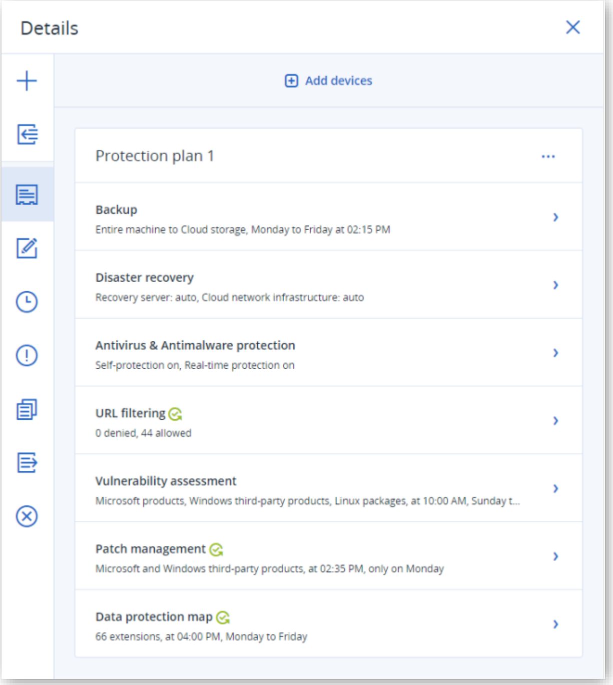
Deep integration enables new capabilities

Integration at all levels: management, products, technology – and your business

- ✓ **One** agent
- ✓ **One** policy
- ✓ **One** UX/UI
- ✓ **One** license
- ✓ **One** vendor

Harness the power of ONE:

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



Details

Add devices

Protection plan 1

Backup
Entire machine to Cloud storage, Monday to Friday at 02:15 PM

Disaster recovery
Recovery server: auto, Cloud network infrastructure: auto

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

URL filtering
0 denied, 44 allowed

Vulnerability assessment
Microsoft products, Windows third-party products, Linux packages, at 10:00 AM, Sunday t...

Patch management
Microsoft and Windows third-party products, at 02:35 PM, only on Monday

Data protection map
66 extensions, at 04:00 PM, Monday to Friday

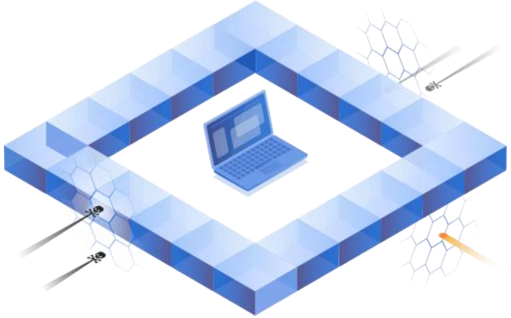
Innovative data protection scenarios

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

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

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

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



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

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

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

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

1. Continuous data protection

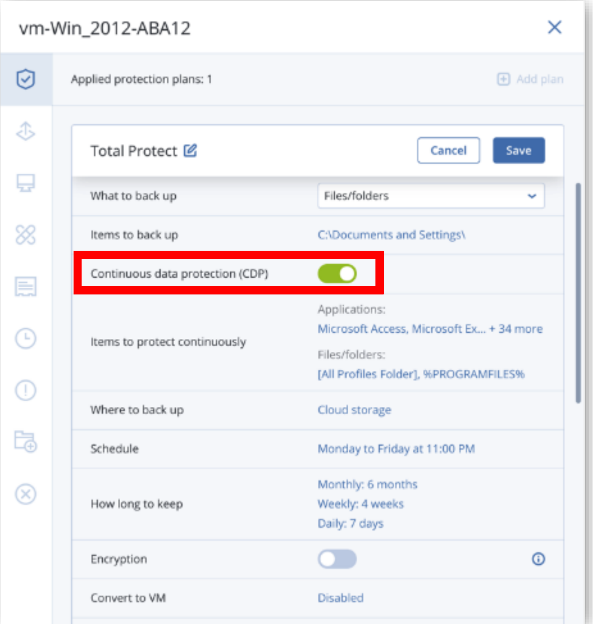
Advanced Backup

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.

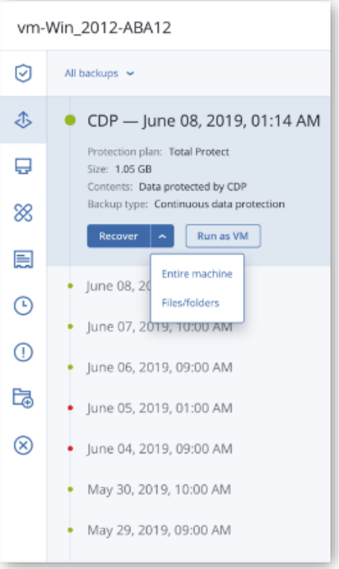


vm-Win_2012-ABA12

Applied protection plans: 1

Total Protect

What to back up	Files/folders
Items to back up	C:\Documents and Settings\
Continuous data protection (CDP)	●
Items to protect continuously	Applications: Microsoft Access, Microsoft Ex... + 34 more Files/folders: [All Profiles Folder], %PROGRAMFILES%
Where to back up	Cloud storage
Schedule	Monday to Friday at 11:00 PM
How long to keep	Monthly: 6 months Weekly: 4 weeks Daily: 7 days
Encryption	○
Convert to VM	Disabled



vm-Win_2012-ABA12

All backups

CDP — June 08, 2019, 01:14 AM

Protection plan: Total Protect
Size: 1.05 GB
Contents: Data protected by CDP
Backup type: Continuous data protection

- June 08, 20
- June 07, 2019, 10:00 AM
- June 06, 2019, 09:00 AM
- June 05, 2019, 01:00 AM
- June 04, 2019, 09:00 AM
- May 30, 2019, 10:00 AM
- May 29, 2019, 09:00 AM

Why? Protects client data – even between backups

2. Safe recovery

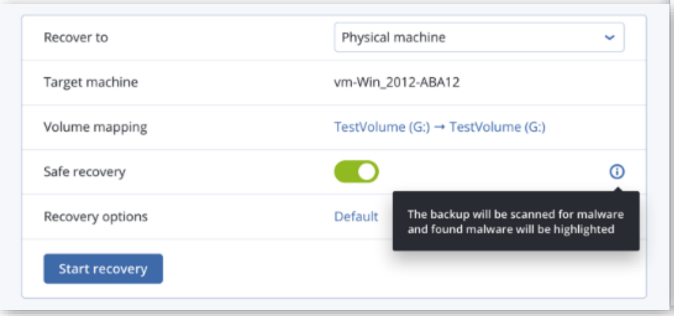
Advanced Security

Integrate AV updates and patch management into the recovery process

The OS image or applications in the backup can include vulnerabilities that could leave users at risk.

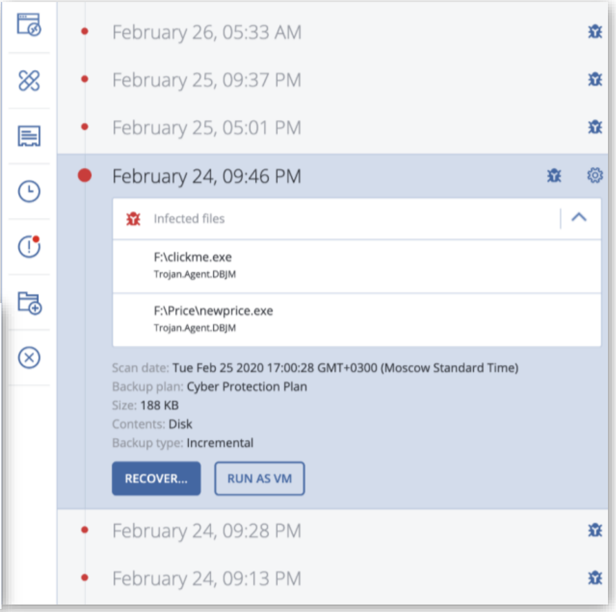
Patching the machine and applying the latest anti-malware definitions allows users to restore the OS image with the latest patches, reducing the chance of a reoccurring infection.

- Updates the anti-malware database
- Installs the latest security patches



Recover to	Physical machine
Target machine	vm-Win_2012-ABA12
Volume mapping	TestVolume (G:) → TestVolume (G:)
Safe recovery	●
Recovery options	Default

The backup will be scanned for malware and found malware will be highlighted



- February 26, 05:33 AM
- February 25, 09:37 PM
- February 25, 05:01 PM
- February 24, 09:46 PM

Infected files

F:\clickme.exe
Trojan.Agent.DBJM

F:\Price\newprice.exe
Trojan.Agent.DBJM

Scan date: Tue Feb 25 2020 17:00:28 GMT+0300 (Moscow Standard Time)
Backup plan: Cyber Protection Plan
Size: 188 KB
Contents: Disk
Backup type: Incremental

- February 24, 09:28 PM
- February 24, 09:13 PM

Why? Saves time, effort and data. Quickly recover using infected/vulnerable images, no extra steps

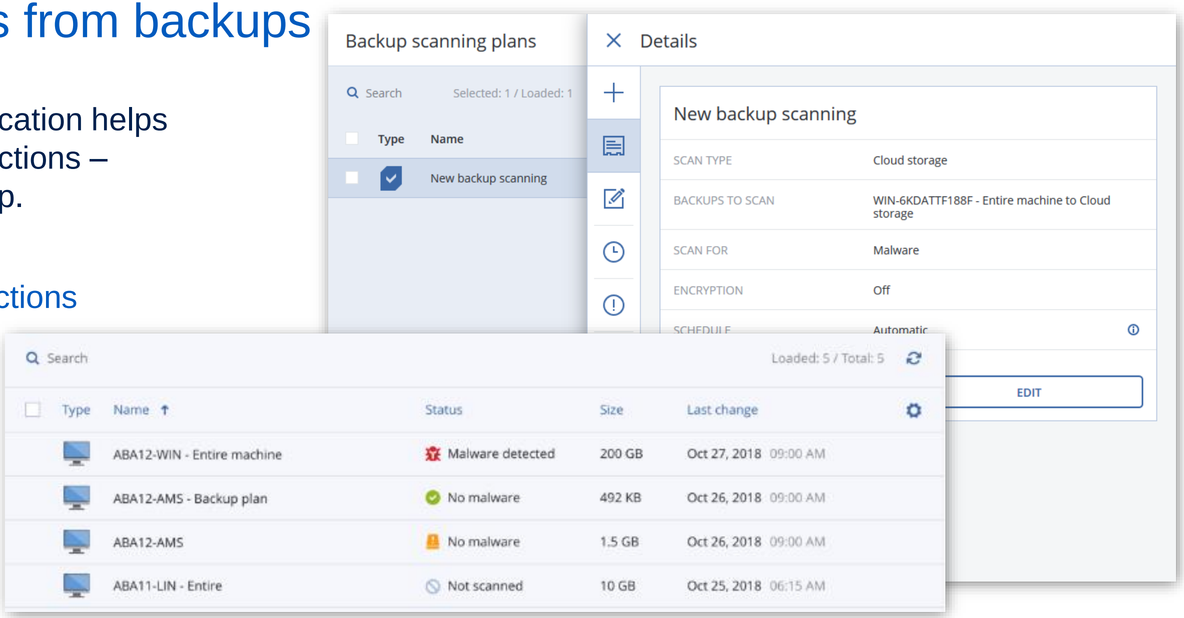
3. Virus and malware scans in the Acronis Cloud

Advanced Security

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



Backup scanning plans

Search Selected: 1 / Loaded: 1

Type	Name
✓	New backup scanning

Details

New backup scanning

SCAN TYPE Cloud storage

BACKUPS TO SCAN WIN-6KDATTF188F - Entire machine to Cloud storage

SCAN FOR Malware

ENCRYPTION Off

SCHEDULE Automatic

EDIT

Search Loaded: 5 / Total: 5

Type	Name ↑	Status	Size	Last change
	ABA12-WIN - Entire machine	Malware detected	200 GB	Oct 27, 2018 09:00 AM
	ABA12-AMS - Backup plan	No malware	492 KB	Oct 26, 2018 09:00 AM
	ABA12-AMS	No malware	1.5 GB	Oct 26, 2018 09:00 AM
	ABA11-LIN - Entire	Not scanned	10 GB	Oct 25, 2018 06:15 AM

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

4. Smart protection plans

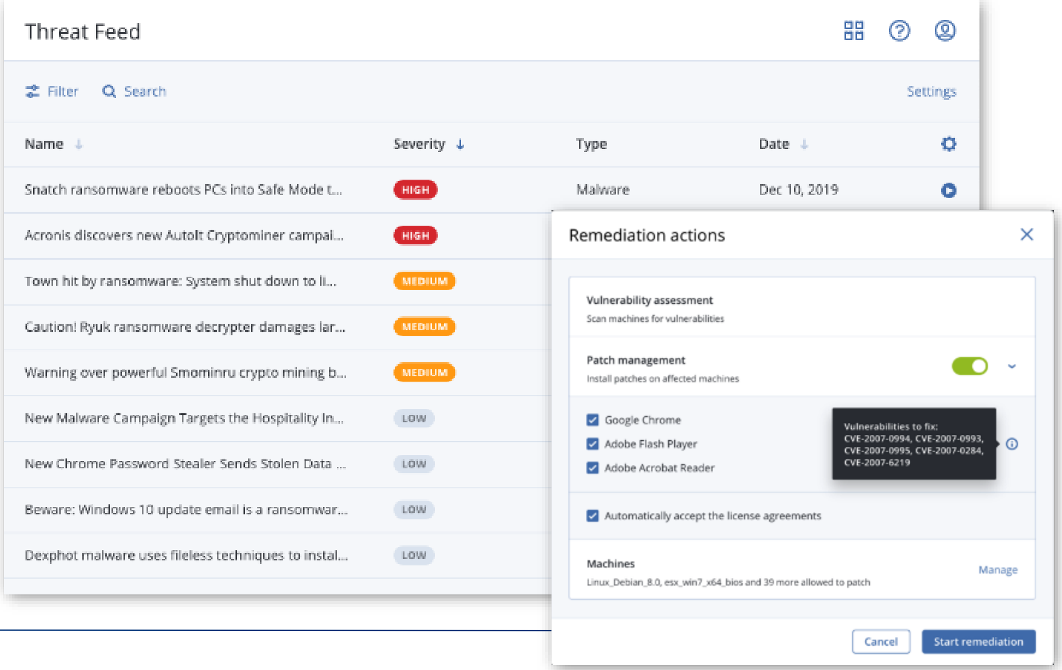
Advanced Security

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 is back to normal.

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



Threat Feed

Filter Search Settings

Name	Severity	Type	Date
Snatch ransomware reboots PCs into Safe Mode t...	HIGH	Malware	Dec 10, 2019
Acronis discovers new AutoIt Cryptominer campai...	HIGH		
Town hit by ransomware: System shut down to li...	MEDIUM		
Caution! Ryuk ransomware decrypter damages lar...	MEDIUM		
Warning over powerful Smominru crypto mining b...	MEDIUM		
New Malware Campaign Targets the Hospitality In...	LOW		
New Chrome Password Stealer Sends Stolen Data ...	LOW		
Beware: Windows 10 update email is a ransomwar...	LOW		
Dexphot malware uses fileless techniques to instal...	LOW		

Remediation actions

Vulnerability assessment
Scan machines for vulnerabilities

Patch management
Install patches on affected machines

☑ Google Chrome
☑ Adobe Flash Player
☑ Adobe Acrobat Reader

Vulnerabilities to fix:
CVE-2007-0994, CVE-2007-0993, CVE-2007-0995, CVE-2007-0284, CVE-2007-6219

☑ Automatically accept the license agreements

Machines
Linux_Debian_8.0, esx_win7_x64_bios and 39 more allowed to patch

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

5. Fail-safe patching

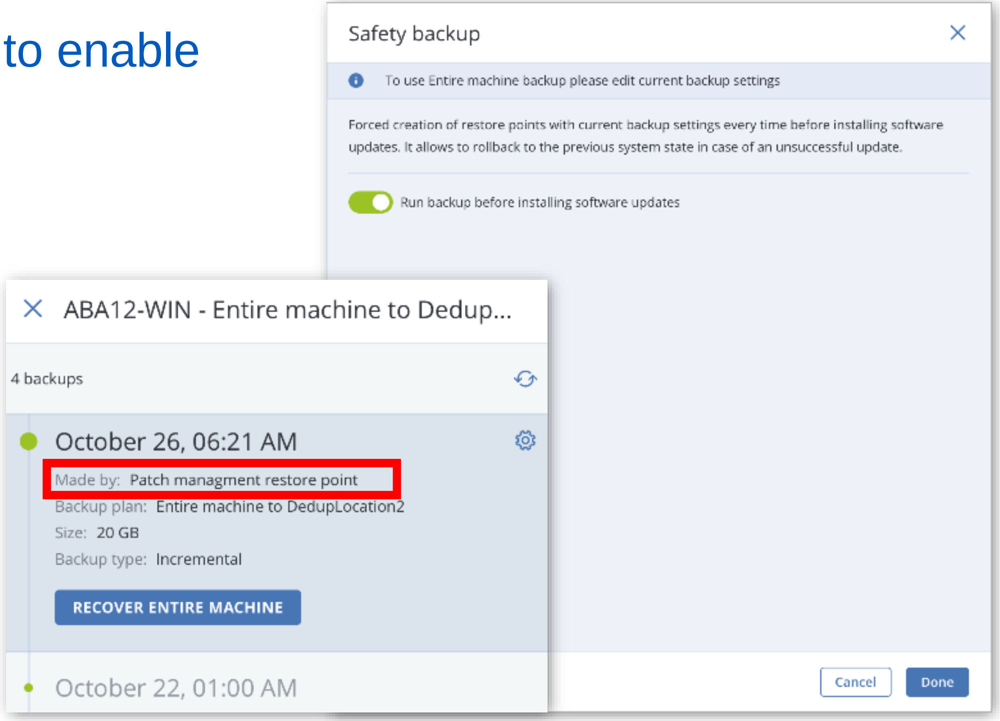
Advanced Management

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 quick rollbacks.

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



Safety backup

To use Entire machine backup please edit current backup settings

Forced creation of restore points with current backup settings every time before installing software updates. It allows to rollback to the previous system state in case of an unsuccessful update.

Run backup before installing software updates

ABA12-WIN - Entire machine to Dedup...

4 backups

October 26, 06:21 AM

Made by: Patch managment restore point

Backup plan: Entire machine to DedupLocation2

Size: 20 GB

Backup type: Incremental

October 22, 01:00 AM

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

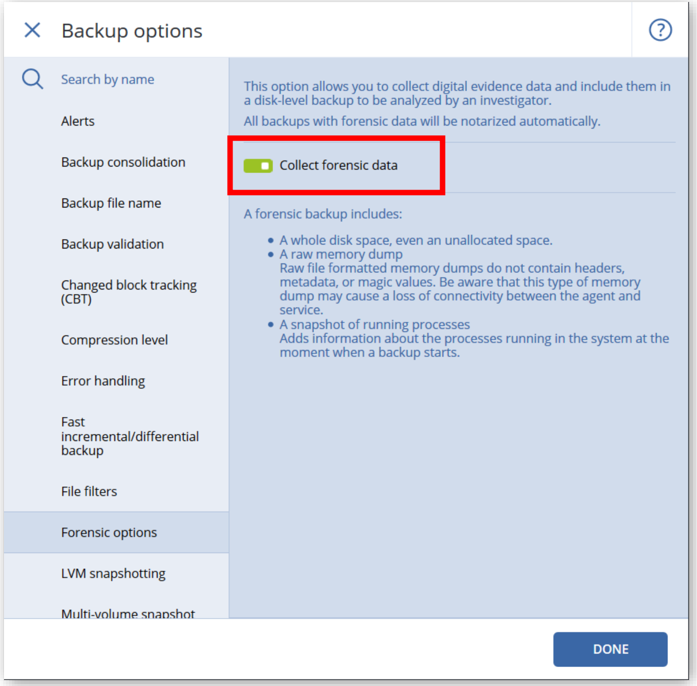
6. Forensic information backup

Advanced Security

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



This option allows you to collect digital evidence data and include them in a disk-level backup to be analyzed by an investigator.

All backups with forensic data will be notarized automatically.

● Collect forensic data

A forensic backup includes:

- A whole disk space, even an unallocated space.
- A raw memory dump
  Raw file formatted memory dumps do not contain headers, metadata, or magic values. Be aware that this type of memory dump may cause a loss of connectivity between the agent and service.
- A snapshot of running processes
  Adds information about the processes running in the system at the moment when a backup starts.

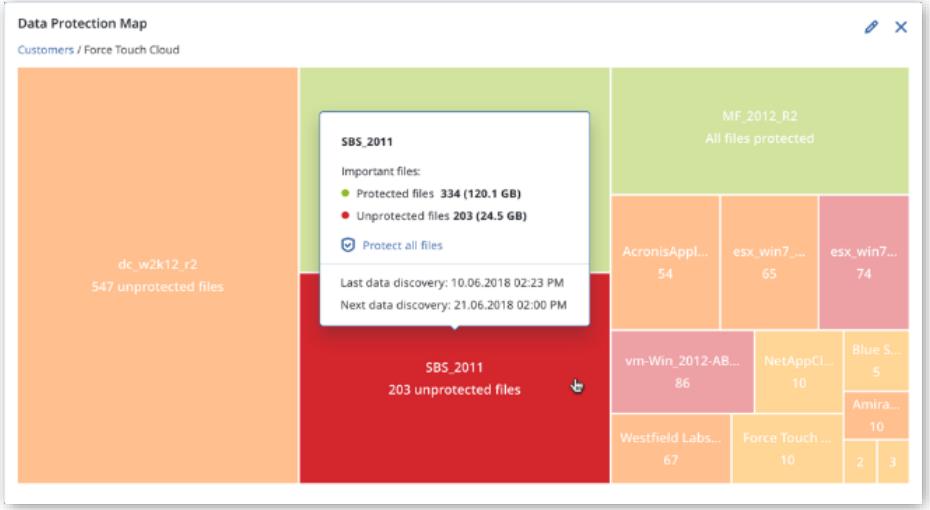
Why? Enables investigation and better compliance

7. Data compliance reporting and Data Protection Map

Advanced Backup

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



Data Protection Map

Customers / Force Touch Cloud

SBS_2011

Important files:

- ● Protected files **334 (120.1 GB)**
- ● Unprotected files **203 (24.5 GB)**

Protect all files

Last data discovery: 10.06.2018 02:23 PM

Next data discovery: 21.06.2018 02:00 PM

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

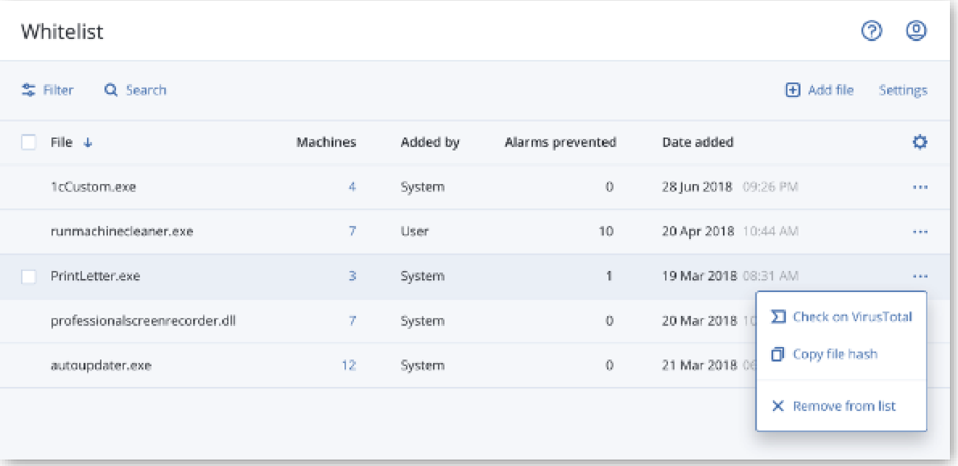
8. Automatic allowlisting from backups

Advanced Security

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.



Whitelist

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 1
autoupdater.exe	12	System	0	21 Mar 2018 0

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

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

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, 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 multi-tenant 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).
- **Minimal planned and unplanned downtime.** Benefit from simplified maintenance routines and proactive protection, including: hard drive health checks, on-time patches, and regular vulnerability assessments – as well as improved real-time Acronis Active Protection.

Acronis

#CyberFit

Key features overview

Built on the Best-in-Breed Backup for MSP

1 Hybrid cloud architecture

2 20+ workload types protected

3 File & Image Backup

4 Instant recovery

5 Flexible Storage

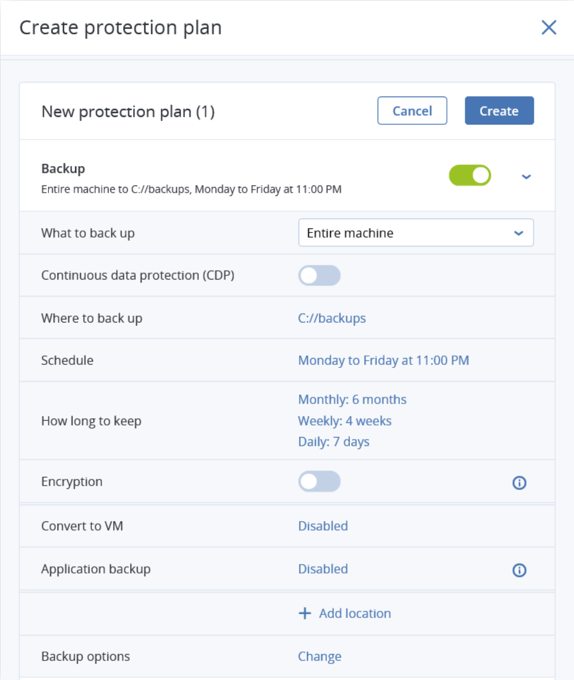
6 Built for MSP

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



Create protection plan

New protection plan (1)

Backup
Entire machine to C://backups, Monday to Friday at 11:00 PM

What to back up	Entire machine
Continuous data protection (CDP)	○
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	○
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

Google Cloud Platform

Acronis Cyber Cloud Storage

Azure

Three turnkey cloud storage options

aws

IBM Cloud

IIJ

Alibaba Cloud

wasabi

Other public clouds
(via gateway)

Your own or third-party cloud storage

On-premises storage

Local disks

SMB/CIFS/DFS and NFS shares

Acronis Cyber Infrastructure

> 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

Microsoft

- Azure
- Windows Server
- Windows PC
- Exchange
- SQL Server
- Share Point
- Active Directory
- Hyper-V
- Microsoft 365

- Google Workspace

amazon web services

- Amazon EC2

- Linux Server

- Mac
- iPhone
- iPad

- Android

SAP

- SAP HANA

- VMware vSphere

ORACLE

- Oracle x86 VM Server
- Oracle Database

- Red Hat Virtualization

- Linux KVM

- Citrix XenServer

- Virtuozzo

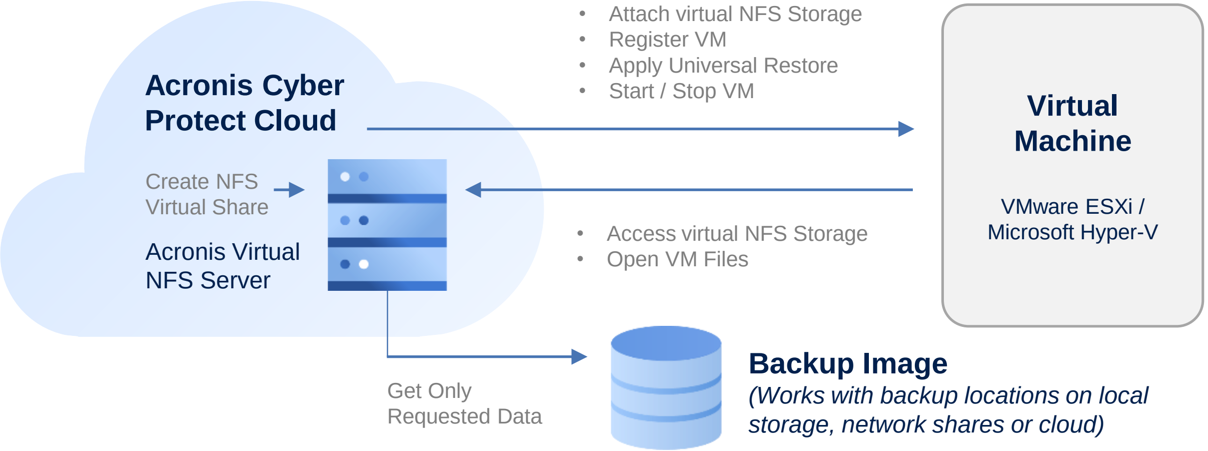
- Nutanix

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


Acronis Cyber Protect Cloud
Create NFS Virtual Share
Acronis Virtual NFS Server
Attach virtual NFS Storage
Register VM
Apply Universal Restore
Start / Stop VM
Virtual Machine
VMware ESXi / Microsoft Hyper-V
Access virtual NFS Storage
Open VM Files
Get Only Requested Data
Backup Image
(Works with backup locations on local storage, network shares or cloud)

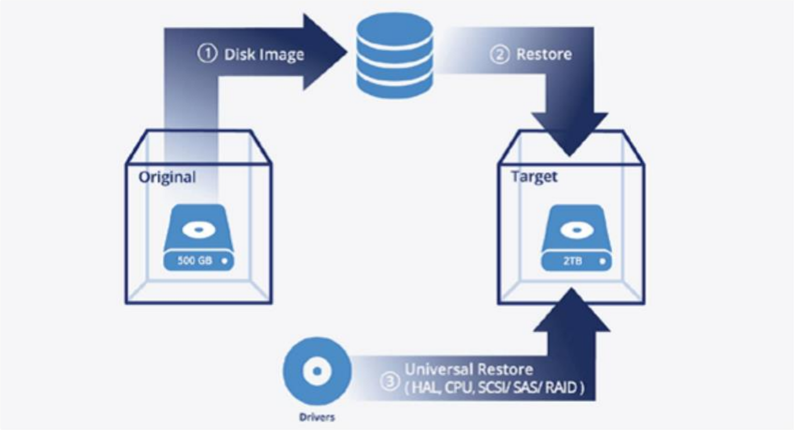
Benefits

- 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?

- Ensure quick, easy system migration with a few clicks
- Reduce RTOs
- Minimize expensive downtime

Acronis

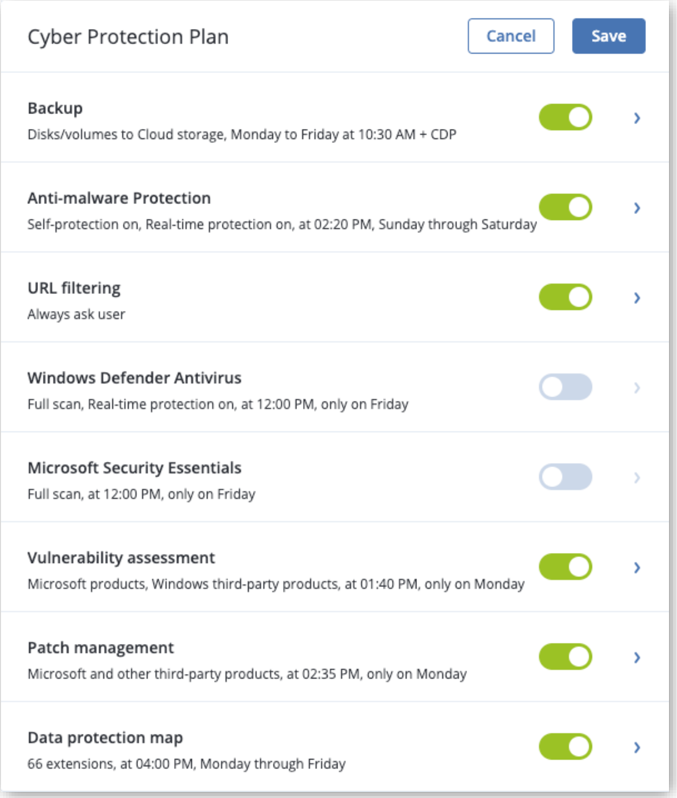
#CyberFit

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



Backup
Disks/volumes to Cloud storage, Monday to Friday at 10:30 AM + CDP

Anti-malware Protection
Self-protection on, Real-time protection on, at 02:20 PM, Sunday through Saturday

URL filtering
Always ask user

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

Microsoft Security Essentials
Full scan, at 12:00 PM, only on Friday

Vulnerability assessment
Microsoft products, Windows third-party products, at 01:40 PM, only on Monday

Patch management
Microsoft and other third-party products, at 02:35 PM, only on Monday

Data protection map
66 extensions, at 04:00 PM, Monday through Friday

Why? Better protection with less effort, automated

Significantly extended anti-malware capabilities

Acronis Cyber Protect

Acronis Cyber Backup

Acronis Active Protection

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

+

Acronis static AI analyzer

On-access and on-demand detection

Acronis anti-malware engine

Any malware (cloud and local detection)

Acronis behavioral engine

On-access detection

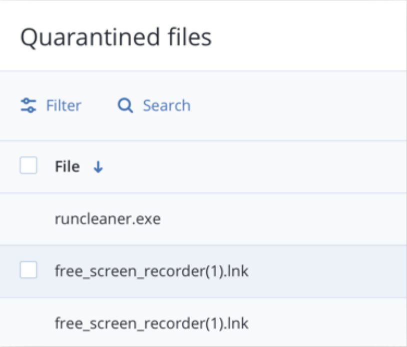
Native integration with Windows Security Center

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

AI-based protection against zero-day malware

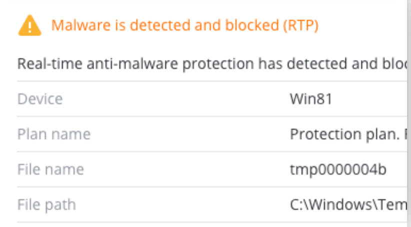
Anti-malware protection for Windows, Linux and macOS

- 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



Quarantined files

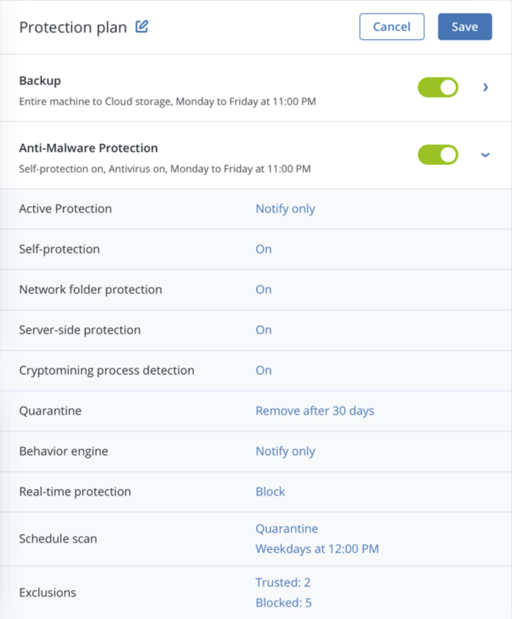
□ File ↓
runcleaner.exe
□ free_screen_recorder(1).lnk
free_screen_recorder(1).lnk



⚠ Malware is detected and blocked (RTP)

Real-time anti-malware protection has detected and bloc

Device	Win81
Plan name	Protection plan. I
File name	tmp0000004b
File path	C:\Windows\Tem



Protection plan

Backup
Entire machine to Cloud storage, Monday to Friday at 11:00 PM

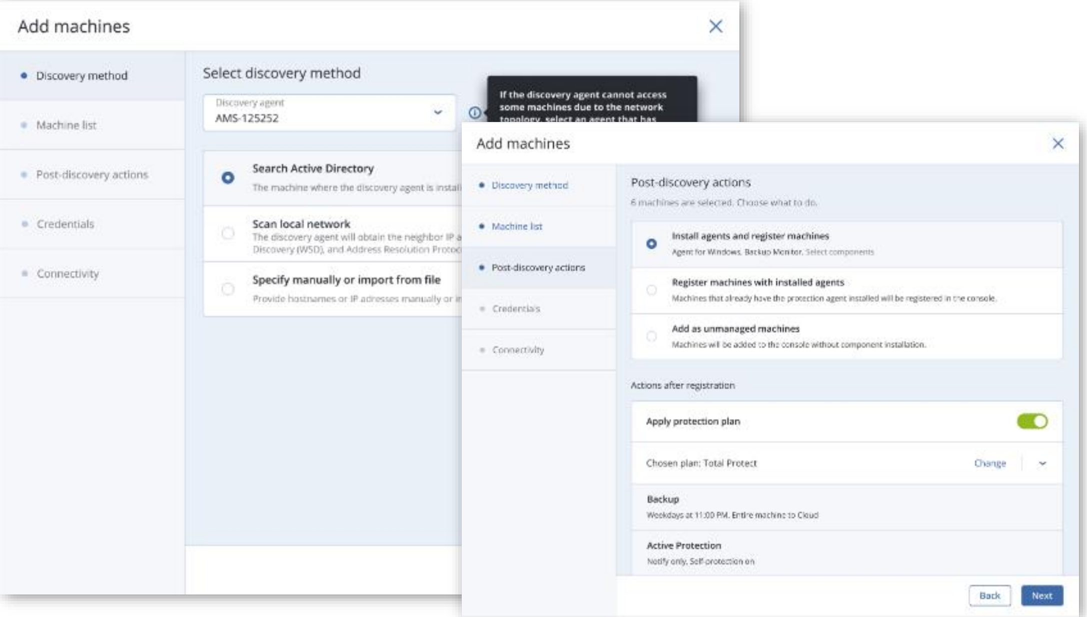
Anti-Malware Protection
Self-protection on, Antivirus on, Monday to Friday at 11:00 PM

Active Protection	Notify only
Self-protection	On
Network folder protection	On
Server-side protection	On
Cryptomining process detection	On
Quarantine	Remove after 30 days
Behavior engine	Notify only
Real-time protection	Block
Schedule scan	Quarantine Weekdays at 12:00 PM
Exclusions	Trusted: 2 Blocked: 5

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



Add machines

- Discovery method
- Machine list
- Post-discovery actions
- Credentials
- Connectivity

Select discovery method

Discovery agent: AMS-125252

If the discovery agent cannot access some machines due to the network topology, select an agent that has

● Search Active Directory
The machine where the discovery agent is install

○ Scan local network
The discovery agent will obtain the neighbor IP a
Discovery (WSD), and Address Resolution Protoc

○ Specify manually or import from file
Provide hostnames or IP adresses manually or in

Add machines

- Discovery method
- Machine list
- Post-discovery actions
- Credentials
- Connectivity

Post-discovery actions

6 machines are selected. Choose what to do.

● Install agents and register machines
Agent for Windows, Backup Monitor. Select components

○ Register machines with installed agents
Machines that already have the protection agent installed will be registered in the console.

○ Add as unmanaged machines
Machines will be added to the console without component installation.

Actions after registration

Apply protection plan

Chosen plan: Total Protect — Change

Backup
Weekdays at 11:00 PM. Entire machine to Cloud

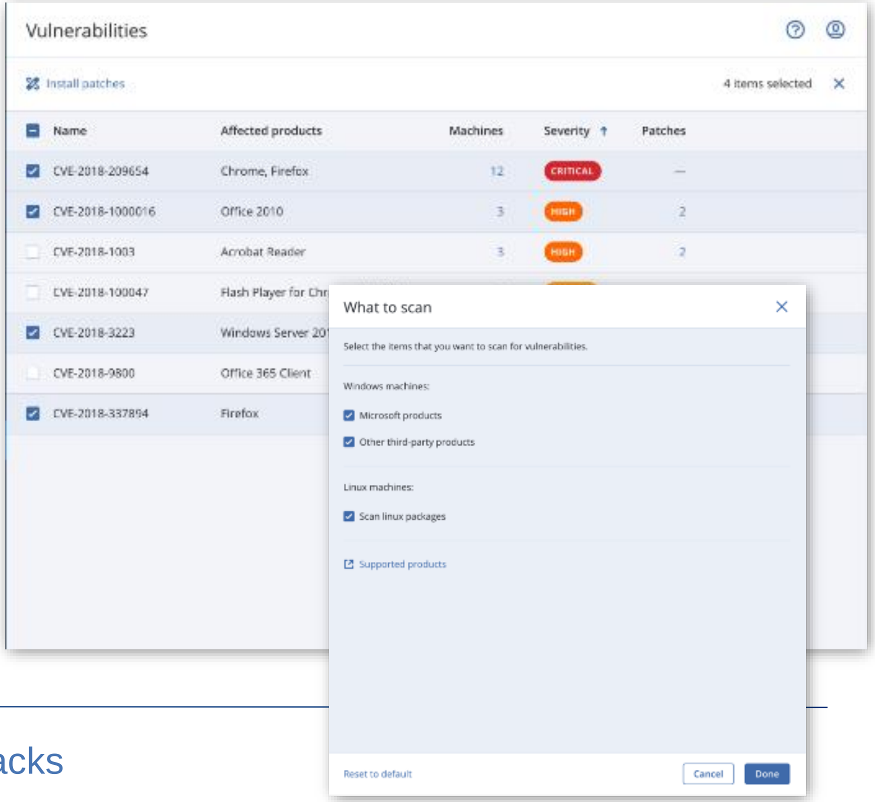
Active Protection
Notify only. Self-protection on

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
  - Adobe, Oracle Java
  - Collaboration software: Zoom, Teams, VPNs
  - Browsers and other software



Vulnerabilities

Install patches

4 items selected

☐	Name	Affected products	Machines	Severity ↑	Patches
☑	CVE-2018-209654	Chrome, Firefox	12	CRITICAL	–
☑	CVE-2018-1000016	Office 2010	3	HIGH	2
☐	CVE-2018-1003	Acrobat Reader	3	HIGH	2
☐	CVE-2018-100047	Flash Player for Chr			
☑	CVE-2018-3223	Windows Server 20			
☐	CVE-2018-9800	Office 365 Client			
☑	CVE-2018-337894	Firefox			

What to scan

Select the items that you want to scan for vulnerabilities.

Windows machines:

☑ Microsoft products

☑ Other third-party products

Linux machines:

☑ Scan linux packages

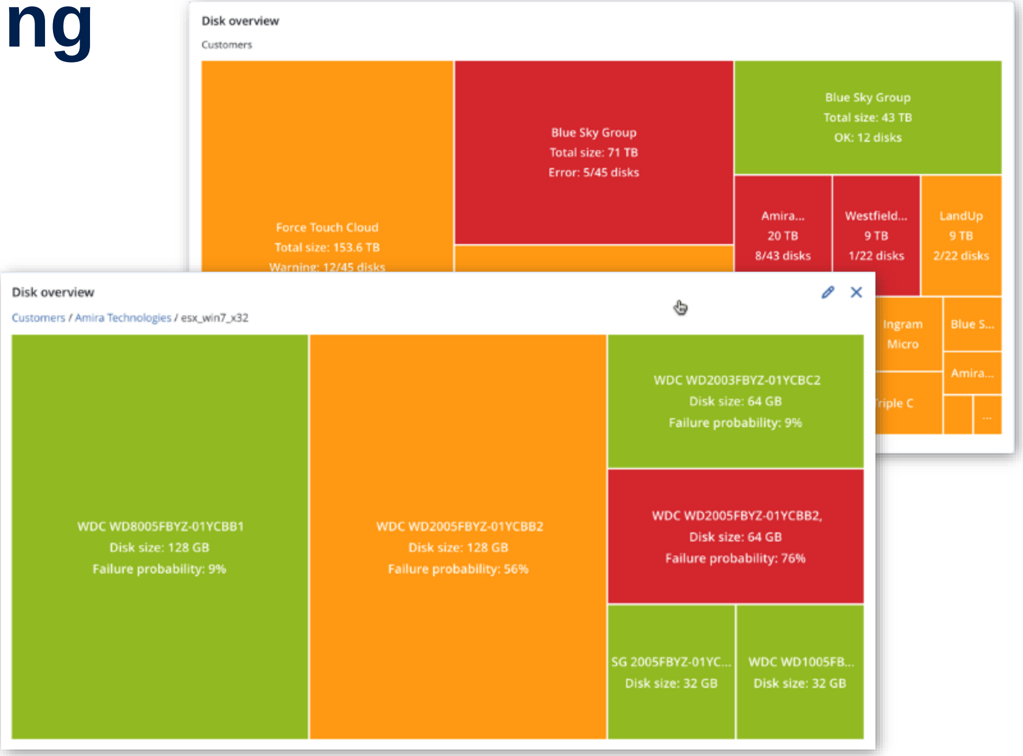
Supported products

Why? Mitigates potential threats and prevents attacks

Drive health monitoring

Know about a disk issue before an issue happens

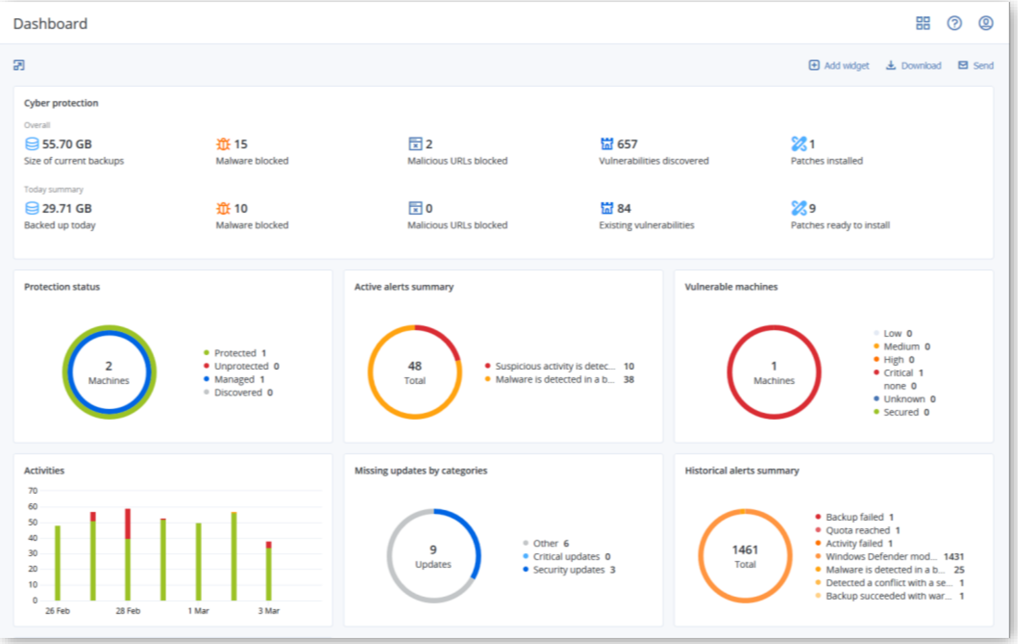
- Uses a combination of machine learning, S.M.A.R.T. reports, drive size, drive vendor, etc. to predict HDD/SSD failures
- The machine-learning model currently delivers 98.5% accuracy in its predictions – and we keep improving it
- Once a drive alert is raised, you can take action (backing up critical files from the failing drive, for example)



Why? Avoid unpredictable customer data loss, proactively improve uptime, differentiate yourself

Flexible monitoring and reporting

- Hardware health monitoring (HDD, SSD)
- Security update statuses visibility
- Quickly identify problems
- Fast access to management actions
- Customizable dashboard widgets



Cyber protection

Overall

55.70 GB Size of current backups | 15 Malware blocked | 2 Malicious URLs blocked | 657 Vulnerabilities discovered | 1 Patches installed

Today summary

29.71 GB Backed up today | 10 Malware blocked | 0 Malicious URLs blocked | 84 Existing vulnerabilities | 9 Patches ready to install

Protection status

2 Machines

- Protected 1
- Unprotected 0
- Managed 1
- Discovered 0

Active alerts summary

48 Total

- Suspicious activity is detec... 10
- Malware is detected in a b... 38

Vulnerable machines

1 Machines

- Low 0
- Medium 0
- High 0
- Critical 1
- none 0
- Unknown 0
- Secured 0

Activities

Missing updates by categories

9 Updates

- Other 6
- Critical updates 0
- Security updates 3

Historical alerts summary

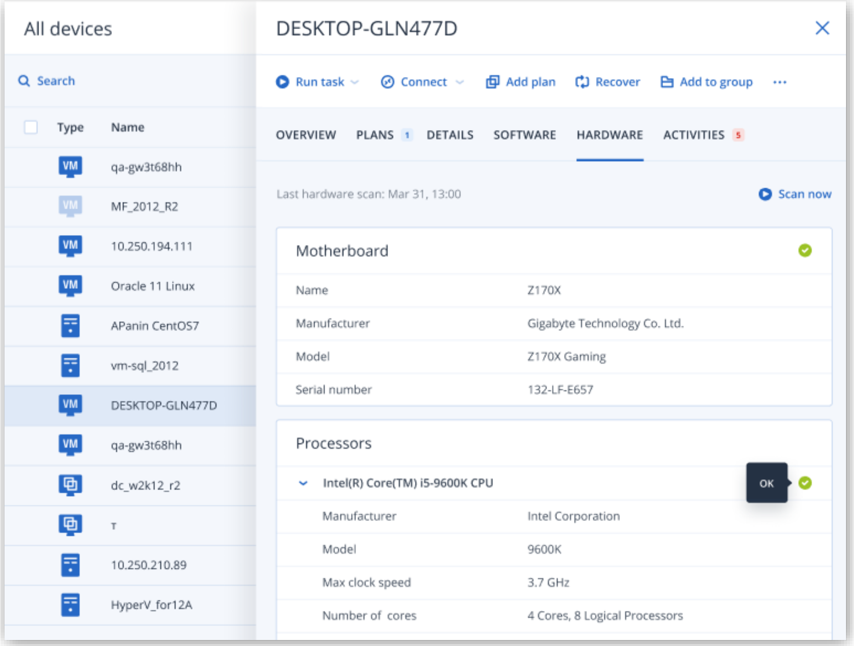
1461 Total

- Backup failed 1
- Quota reached 1
- Activity failed 1
- Windows Defender mod... 1431
- Malware is detected in a b... 25
- Detected a conflict with a se... 1
- Backup succeeded with war... 1

Why? Single pane of glass, faster operations, helps demonstrate MSP value 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



All devices

Search

Type	Name
VM	qa-gw3t68hh
VM	MF_2012_R2
VM	10.250.194.111
VM	Oracle 11 Linux
	APanin CentOS7
	vm-sql_2012
VM	DESKTOP-GLN477D
VM	qa-gw3t68hh
	dc_w2k12_r2
	T
	10.250.210.89
	HyperV_for12A

DESKTOP-GLN477D

Last hardware scan: Mar 31, 13:00

Motherboard

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

Processors

Intel(R) Core(TM) i5-9600K CPU — OK

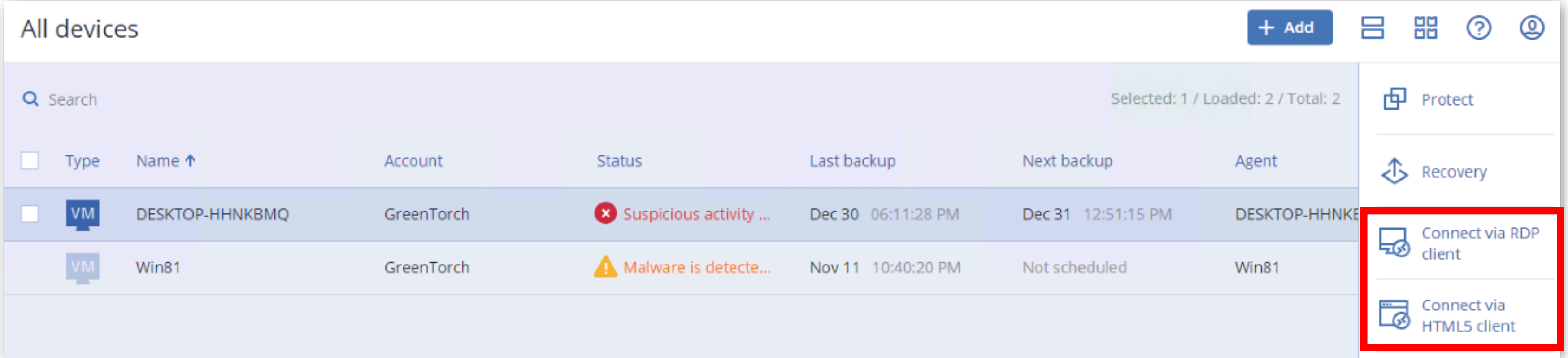
Manufacturer	Intel Corporation
Model	9600K
Max clock speed	3.7 GHz
Number of cores	4 Cores, 8 Logical Processors

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

Remote Desktop & Remote Assistance

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



Selected: 1 / Loaded: 2 / Total: 2

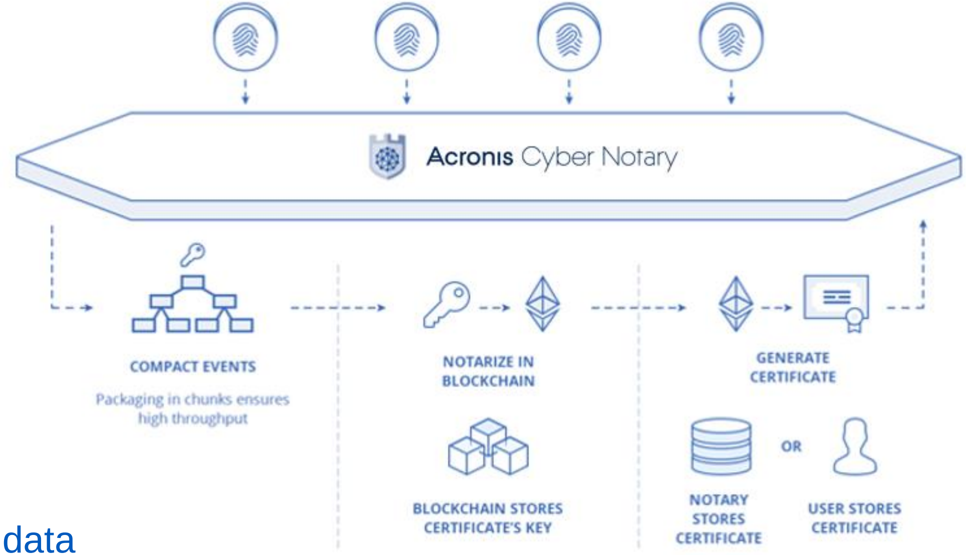
□	Type	Name ↑	Account	Status	Last backup	Next backup	Agent
□	VM	DESKTOP-HHNKBMQ	GreenTorch	Suspicious activity ...	Dec 30 06:11:28 PM	Dec 31 12:51:15 PM	DESKTOP-HHNKE
	VM	Win81	GreenTorch	Malware is detecte...	Nov 11 10:40:20 PM	Not scheduled	Win81

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

Blockchain notarization

Ensure data integrity with innovative blockchain-based Acronis Cyber Notary

- Highly scalable micro-service architecture
- API interface (REST), queue interface (AMPQ) for integration
- High throughput (xx10,000 objects per blockchain transaction)
- Notarization certificates with built-in verification


Acronis Cyber Notary
COMPACT EVENTS
Packaging in chunks ensures high throughput
NOTARIZE IN BLOCKCHAIN
BLOCKCHAIN STORES CERTIFICATE'S KEY
GENERATE CERTIFICATE
NOTARY STORES CERTIFICATE
OR
USER STORES CERTIFICATE

Why?

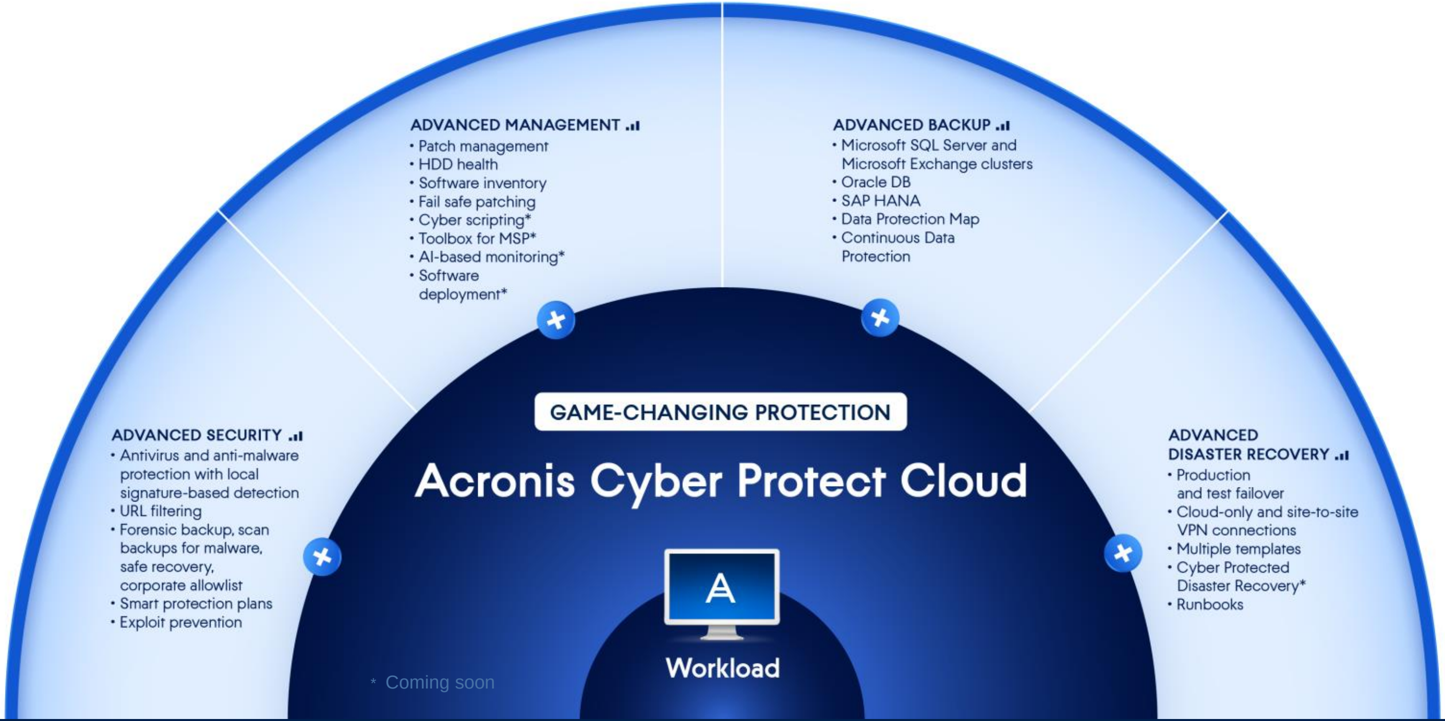
- Ensure the integrity of business critical data
- Achieve greater regulatory transparency
- Reduce security risks

Acronis

#CyberFit

Easy, Efficient, Secure cyber protection with Advanced Packs

Advanced Packs: Security, Management, Backup, Disaster Recovery



ADVANCED MANAGEMENT

- Patch management
- HDD health
- Software inventory
- Fail safe patching
- Cyber scripting*
- Toolbox for MSP*
- AI-based monitoring*
- Software deployment*

ADVANCED BACKUP

- Microsoft SQL Server and Microsoft Exchange clusters
- Oracle DB
- SAP HANA
- Data Protection Map
- Continuous Data Protection

ADVANCED SECURITY

- Antivirus and anti-malware protection with local signature-based detection
- URL filtering
- Forensic backup, scan backups for malware, safe recovery, corporate allowlist
- Smart protection plans
- Exploit prevention

ADVANCED DISASTER RECOVERY

- Production and test failover
- Cloud-only and site-to-site VPN connections
- Multiple templates
- Cyber Protected Disaster Recovery*
- Runbooks

GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

Workload

* Coming soon

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 antimalware

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 safe 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 Management

Improve clients’ protection by keeping systems up-to-date while decreasing the management burden and TCO

Advanced patch management

Keep systems up-to-date and proactively mitigate vulnerabilities.

Patch management automation

Save time and effort with patch management automation and fail-safe patching technology

Comprehensive management tools

Streamline your planning with software inventory collection, report scheduling, and drive health monitoring.

Acronis Cyber Protect Cloud

Features by Advanced Packs

Advanced Backup:

- ✓ Continuous data protection
- ✓ Backup support for Microsoft SQL Server Clusters, Microsoft Exchange Clusters, Oracle DB, SAP HANA
- ✓ Data protection map and compliance reporting
- ✓ Scheduled backup reports

Advanced Disaster Recovery:

- ✓ Production and test failover to Acronis Cloud
- ✓ Runbooks: disaster recovery orchestration
- ✓ VPN-less deployment option
- ✓ IPsec Multisite VPN support, L2 site-to-site open VPN
- ✓ Multiple templates
- ✓ Custom DNS configuration

Advanced Security:

- ✓ URL filtering
- ✓ Exploit prevention
- ✓ Enhanced signature-based detection
- ✓ Anti-malware scans of data in the Acronis Cloud
- ✓ Forensics data in backups
- ✓ Smart protect plans
- ✓ Automatic allowlisting
- ✓ Safe recovery
- ✓ Remote device wipe
- ✓ Windows anti-malware management

Advanced Management:

- ✓ Automated patch management
- ✓ Software inventory collection
- ✓ Drive health monitor
- ✓ Fail-safe patching
- ✓ Report scheduling

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

Data privacy map

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 HW/staff required
- Improved granular licensing

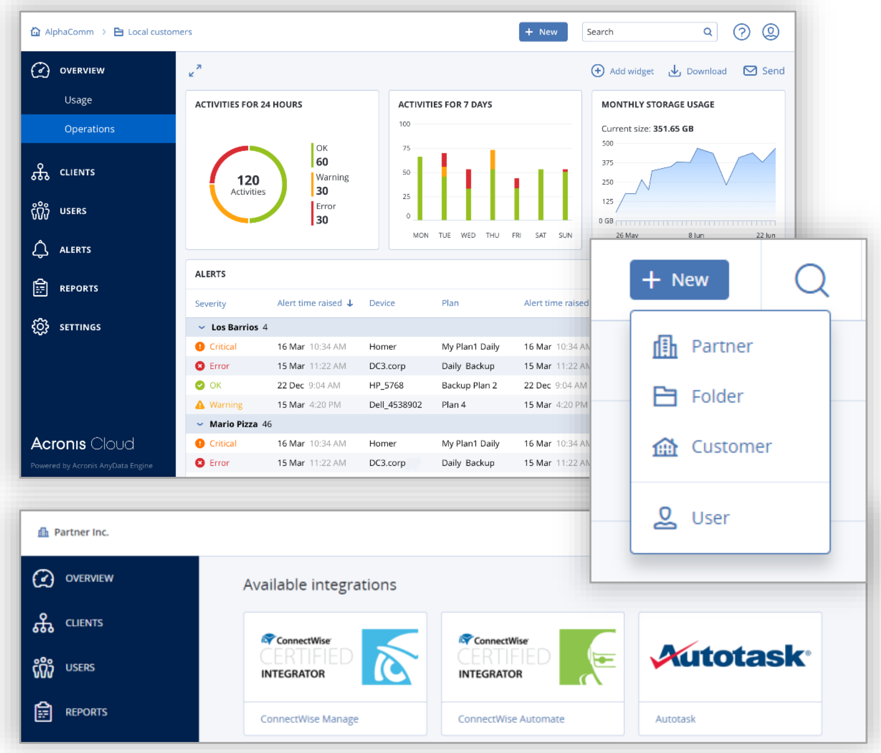
Decrease Churn

- 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



ALERTS

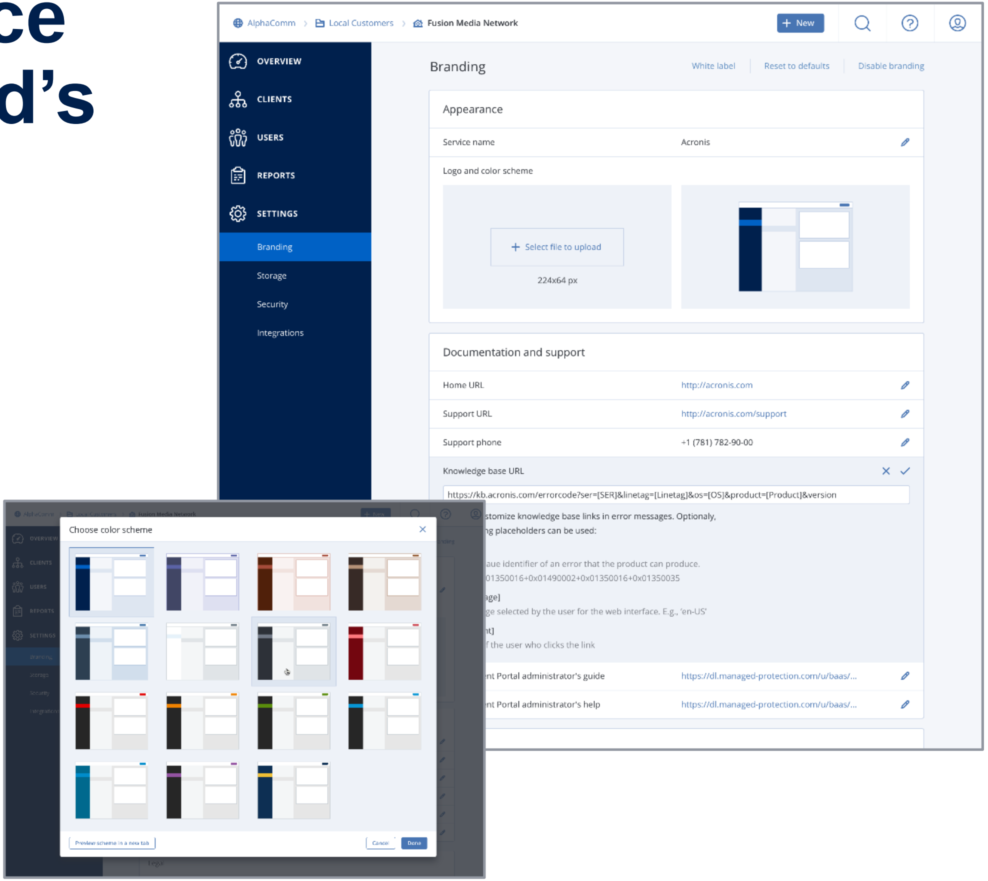
Severity	Alert time raised ↓	Device	Plan	Alert time raised
Los Barrios 4				
Critical	16 Mar 10:34 AM	Homer	My Plan1 Daily	16 Mar 10:34 A
Error	15 Mar 11:22 AM	DC3.corp	Daily Backup	15 Mar 11:22 A
OK	22 Dec 9:04 AM	HP_5768	Backup Plan 2	22 Dec 9:04 AM
Warning	15 Mar 4:20 PM	Dell_4538902	Plan 4	15 Mar 4:20 PM
Mario Pizza 46				
Critical	16 Mar 10:34 AM	Homer	My Plan1 Daily	16 Mar 10:34 A
Error	15 Mar 11:22 AM	DC3.corp	Daily Backup	15 Mar 11:22 A

- ✓ Easy, scalable management of customers' accounts via an easy-to-use web console
- ✓ Integration with Autotask, ConnectWise Automate, and ConnectWise Manage
- ✓ 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



Branding

Appearance

Service name	Acronis
Logo and color scheme	

Documentation and support

Home URL	http://acronis.com
Support URL	http://acronis.com/support
Support phone	+1 (781) 782-90-00
Knowledge base URL	

https://kb.acronis.com/errorcode?ser=[SER]&linetag=[Linetag]&os=[OS]&product=[Product]&version

stomize knowledge base links in error messages. Optionaly,
ng placeholders can be used:

aue identifier of an error that the product can produce.
01350016+0x01490002+0x01350016+0x01350035

age]
ge selected by the user for the web interface. E.g., 'en-US'

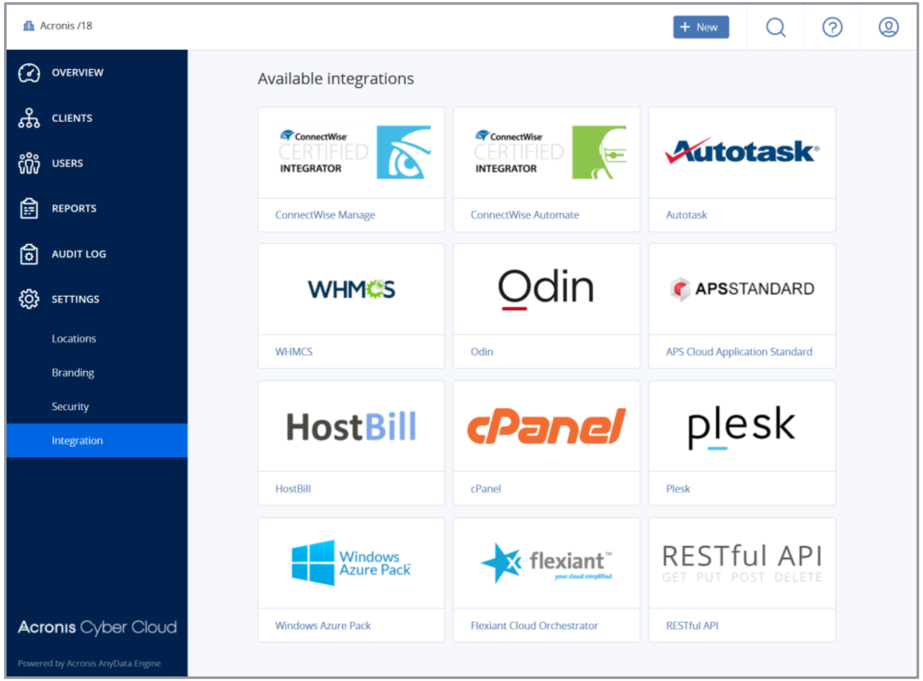
nt]
f the user who clicks the link

nt Portal administrator's guide	https://dl.managed-protection.com/u/baas/...
nt Portal administrator's help	https://dl.managed-protection.com/u/baas/...

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:** Autotask, ConnectWise (Automate, Manage, Control), Kaseya
  - **Hosting control panels and billing systems:** cPanel, Plesk, WHMCS, HostBill
  - **Marketplace providers:** CloudBlue, AppDirect
- Utilize a powerful **RESTful management API** for custom integrations



Available integrations

ConnectWise Manage

ConnectWise Automate

Autotask

WHMCS

Odin

APS Cloud Application Standard

HostBill

cPanel

Plesk

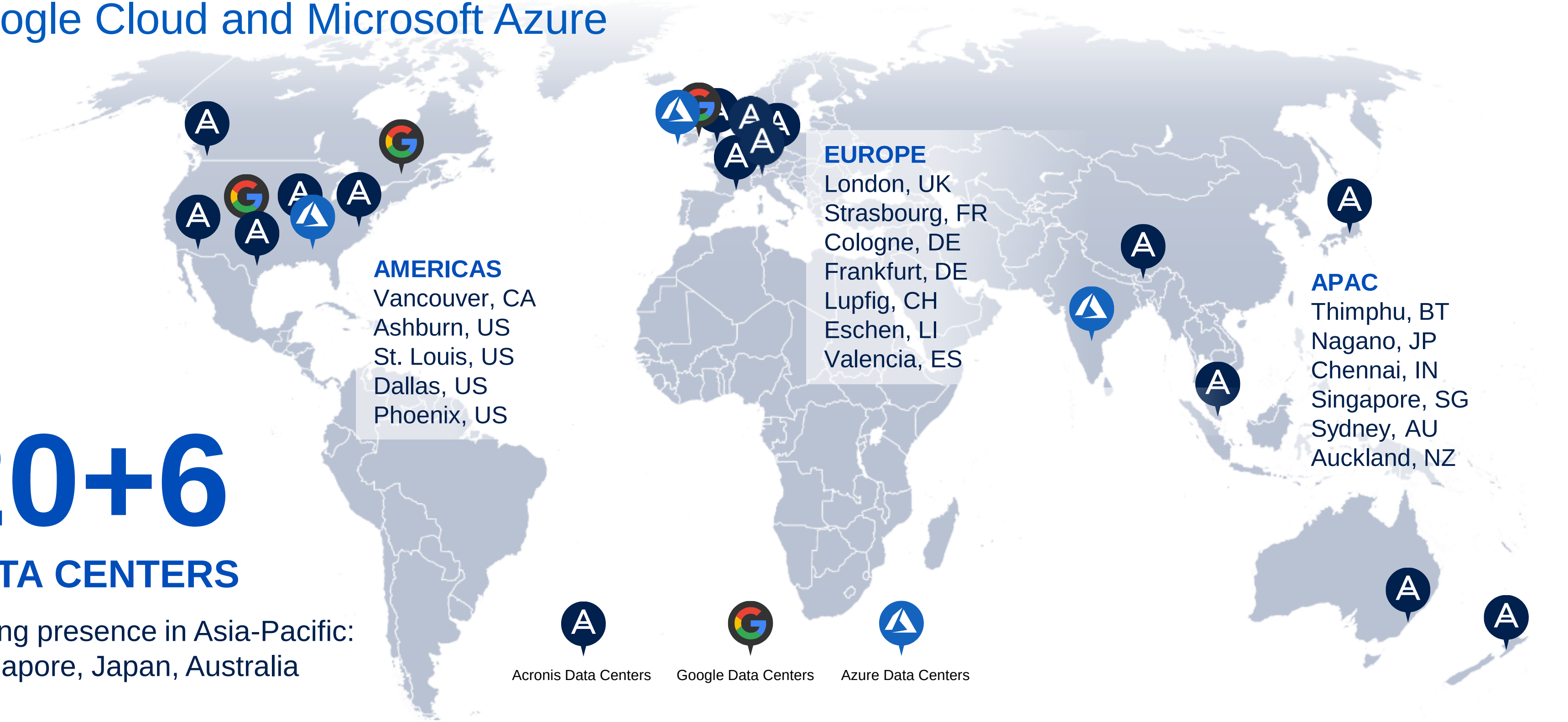
Windows Azure Pack

Flexiant Cloud Orchestrator

RESTful API

Ensure Compliance and a Local Presence

Choose from 26 data centers worldwide to store data – Acronis-hosted, Google Cloud and Microsoft Azure



AMERICAS
Vancouver, CA
Ashburn, US
St. Louis, US
Dallas, US
Phoenix, US

EUROPE
London, UK
Strasbourg, FR
Cologne, DE
Frankfurt, DE
Lupfig, CH
Eschen, LI
Valencia, ES

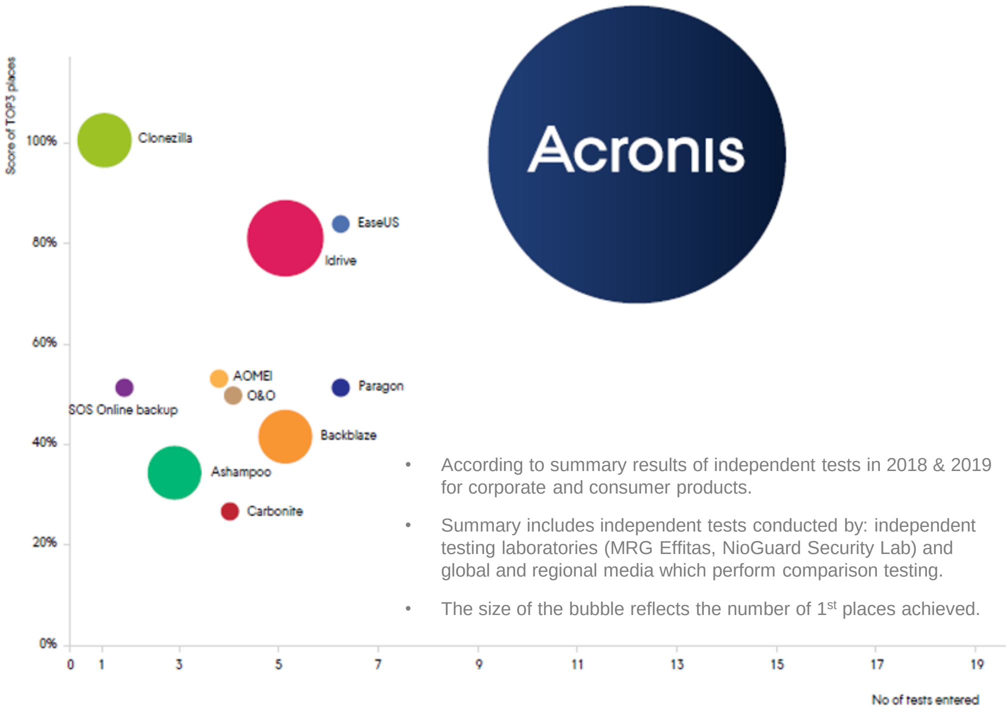
APAC
Thimphu, BT
Nagano, JP
Chennai, IN
Singapore, SG
Sydney, AU
Auckland, NZ

20+6

DATA CENTERS

Strong presence in Asia-Pacific:
Singapore, Japan, Australia

Leader in independent tests results



- According to summary results of independent tests in 2018 & 2019 for corporate and consumer products.
- Summary includes independent tests conducted by: independent testing laboratories (MRG Effitas, NioGuard Security Lab) and global and regional media which perform comparison testing.
- The size of the bubble reflects the number of 1st places achieved.

SME 2020-21 DCIG TOP 5 ANTI-RANSOMWARE BACKUP

Gold Self-Protection Award Anti-Malware Test Lab

vb 100 VIRUS virusbtn.com

AV TEST av-test.org 04/2017 APPROVED BACKUP & DATA SECURITY SOFTWARE

AV TEST av-test.org 02/2019 APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT

MRG Effitas CERTIFIED

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

GDPR

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

GLBA (Gramm-Leach-Bliley Act)

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

HIPAA

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

ISO 27001

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

ISO 9001

Compliant with ISO 9001:2015

TAA

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

Privacy Shield

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

Acronis Cyber Protect Cloud Partners

Union Tech Coop

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

Zebra Systems

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

Vmotion IT

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

Acronis Cyber Protect Cloud Partners

Technopeak

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.

DataTegra

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.

i3-Software & Services

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

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

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

*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.*

*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

Overview of Licensing Changes for Existing Partners

1. **Acronis Cyber Protect Cloud** includes all features of **Acronis Cyber Backup Cloud Standard** extended with essential cyber protection functionality
2. **PAYG Acronis Cyber Protect Cloud functionality:**
   - Backup, Disaster Recovery (test failover), File Sync & Share, Notarization
3. **Free Acronis Cyber Protect Cloud functionality:**
   - Security
   - Management
4. **Acronis Cyber Backup Cloud** discontinued (completely incorporated into Acronis Cyber Protect Cloud or Advanced Backup pack), **Acronis Cyber Disaster Recovery** discontinued, functionality split between Acronis Cyber Protect Cloud and Advanced Disaster Recovery Pack
5. **Advanced packs instead of editions:**
   - Different advanced packs can be added to different workloads on a customer level
   - All advanced packs will be applicable to both per-GB and per-workload licensing models
6. **Pricing changes**
   - Cyber protection functionality will be available in per-GB licensing model

A simplified approach

	Acronis Cyber Cloud C20.08	Acronis Cyber Cloud C21.03
Licensing model (per GB/per workload)	Customer level	Customer level
Product/editions	**Two editions:** • **Acronis Cyber Backup** (per-GB) – backup only • **Acronis Cyber Protect** (per-workload) – four editions	**Single product – Acronis Cyber Protect Cloud** • No editions
Additional functionality	Higher edition (per-workload model only)	Advanced packs
Number of SKUs	43	38
FREE cyber protection functionality	No	Yes
Free cloud storage	Yes (Acronis Cyber Protect Cloud only)	Yes (MS365 and Google workspace)

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
	Weak passwords check	Included
	Vulnerability assessment	Included
	Anti-Ransomware protection: Acronis Active Protection	Included
	Antivirus and Antimalware protection: Exploit prevention	Included
	Antivirus and Antimalware protection: Cloud signature-based file detection (no local signature-based detection)	Included
	Antivirus and Antimalware 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
	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	4h / month
	Cloud-only VPN Connection	PAYG
File Sync & Share	File Sync & Share functionality	PAYG (Q2)
Notary	Notarization and e-signature	PAYG

Two Licensing Models

Per-GB model

The per-GB model is simple – you only pay for the backup storage used.

Per-workload model

The per-workload model requires you to pay for each protected workload (there are different prices for different types of workloads) as well as for cloud storage.

Advanced Packs: Feature split

Advanced Packs	Features	
Advanced Security	Anti-virus 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
	Continuous Data Protection backup	Included
	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 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 File Sync and Share (Q2)	Notarization and e-signature	Included
	Document templates*	Included
	On-premises content repositories (NAS, SharePoint)*	Included
	Backup of sync and share files*	Included
Advanced Email Security (Q2)	Anti-malware and anti-phishing protection, impersonation protection, attachments scan, content disarm and reconstruction, graph of trust	Included (Q2)
Advanced Data Loss Prevention (Q3)	Network control	Included (Q3)
	User activity monitoring	Included (Q3)
	Content control	Included (Q3)
	Content discovery*	Included (Q3)
Advanced Security + EDR (Q4)	All Advanced Security features + Endpoint Detection and Response (events collection, automated response, security incident management)	Included (Q4)
Advanced Automation (Q4)	Sales and billing automation	Included (Q4)
	Service desk and time tracking	Included (Q4)
	CRM with leads and opportunities management	Included (Q4)
	Integrations with accounting and payment systems	Included (Q4)
Advanced Protection (Q4)	All Advanced Security, Advanced Backup, Advanced Management, Advanced Security + EDR, and Advanced Data Loss Prevention	Included (Q4)

ℹ **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 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 Cloud management console

New vs. Old SKUs: Per-GB

Service	Model	Product Name	SKU	New/Old	Price level	Functionality
Acronis Cyber Protect Cloud	Per-GB	Acronis Cyber Protect Cloud - Acronis Hosted Storage (per GB)	SPBAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Google Hosted Storage (per GB)	SP3AMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Azure Hosted Storage (per GB)	SQ2AMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Hybrid Storage (per GB)	SPBBMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Local Storage (per GB)	SP4BMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Files Cloud - Acronis Hosted Storage (per GB)	SP1AMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Files Cloud - Hybrid Storage (per GB)	SP2AMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Notary Cloud - eSignature (per file)	SQ5AMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Notary Cloud - Notarization (per notarization)	SQ4AMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Notary Cloud - Acronis Hosted Storage (per GB)	SQ6AMSENS	Reused SKU from 20.08	Same	Same
Advanced Functionality		Advanced Backup - Server	SRDAMSENS	New SKU	new price	new
		Advanced Backup - VM	SREAMSENS	New SKU	new price	new
		Advanced Backup - Workstation	SRFAMSENS	New SKU	new price	new
		Advanced Backup - Hosting Server	SRGAMSENS	New SKU	new price	new
		Advanced Management	SRHAMSENS	New SKU	new price	new
		Advanced Security	SRIAMSENS	New SKU	new price	new
		Advanced Disaster Recovery - Acronis Hosted Storage (per GB)	SVEAMSENS	Reused SKU from 20.08	Same	Same
		Advanced Disaster Recovery - Hybrid Storage (per GB)	SVFAMSENS	Reused SKU from 20.08	Same	Same
		Advanced Disaster Recovery - Acronis Hosted - 1 compute point (per running hour)	SQYAMSENS	Reused SKU from 20.08	Same	Same
		Advanced Disaster Recovery - Acronis Hosted Public IP address	SEDAMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Files Cloud Advanced - eSignature (per file)	SR1AMSENS	New SKU	new price	new
		Acronis Cyber Files Cloud Advanced - Notarization (per notarization)	SR2AMSENS	New SKU	new price	new

New vs. Old SKUs: Per-workload

Service	Model	Product Name	SKU	New/Old	Price level	Functionality
Acronis Cyber Protect Cloud	Per-workload	Acronis Cyber Protect Cloud - Server	SPEAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - VM	SPFAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Workstation	SPGAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Hosting Server	SQ7AMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Microsoft 365 seat	SRAAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Microsoft Hosted Exchange	ST6AMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Google Workspace	SQ8AMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Mobile	SRBAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Website	SEAAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Acronis Hosted Storage for per Workload model (per GB)	SPDAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Google Hosted Storage for per Workload model (per GB)	SPXAMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Protect Cloud - Azure Hosted Storage for per Workload model (per GB)	SQ1AMSENS	Reused SKU from 20.08	Same	+ cyber protection functionality
		Acronis Cyber Files Cloud - User (per user)	SPIAMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Files Cloud - Acronis Hosted Storage (per GB)	SUVAMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Notary Cloud - eSignature (per file)	SQ5AMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Notary Cloud - Notarization (per notarization)	SQ4AMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Notary Cloud - Acronis Hosted Storage (per GB)	SQ6AMSENS	Reused SKU from 20.08	Same	Same
Advanced Functionality		Advanced Backup - Server	SRDAMSENS	New SKU	New price	new
		Advanced Backup - VM	SREAMSENS	New SKU	New price	new
		Advanced Backup - Workstation	SRFAMSENS	New SKU	New price	new
		Advanced Backup - Hosting Server	SRGAMSENS	New SKU	New price	new
		Advanced Management	SRHAMSENS	New SKU	New price	new
		Advanced Security	SRIAMSENS	New SKU	New price	new
		Advanced Disaster Recovery - Acronis Hosted Storage (per GB)	SVEAMSENS	Reused SKU from 20.08	Same	Same
		Advanced Disaster Recovery - Hybrid Storage (per GB)	SVFAMSENS	Reused SKU from 20.08	Same	Same
		Advanced Disaster Recovery - Acronis Hosted - 1 compute point (per running hour)	SQYAMSENS	Reused SKU from 20.08	Same	Same
		Advanced Disaster Recovery - Acronis Hosted Public IP address	SEDAMSENS	Reused SKU from 20.08	Same	Same
		Acronis Cyber Files Cloud Advanced - eSignature (per file)	SR1AMSENS	New SKU	New price	new
		Acronis Cyber Files Cloud Advanced - Notarization (per notarization)	SR2AMSENS	New SKU	New price	new

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

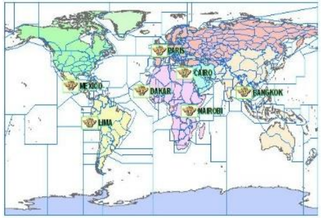
Dual Headquarters for Dual Protection

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

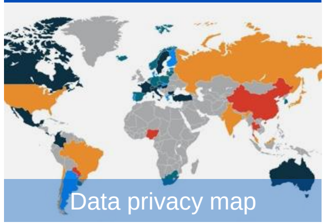
Accessibility

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

Building a more knowledgeable future

#CyberFit

CREATE, SPREAD AND PROTECT KNOWLEDGE WITH US!

www.acronis.org

Building new schools • Providing educational programs • Publishing books