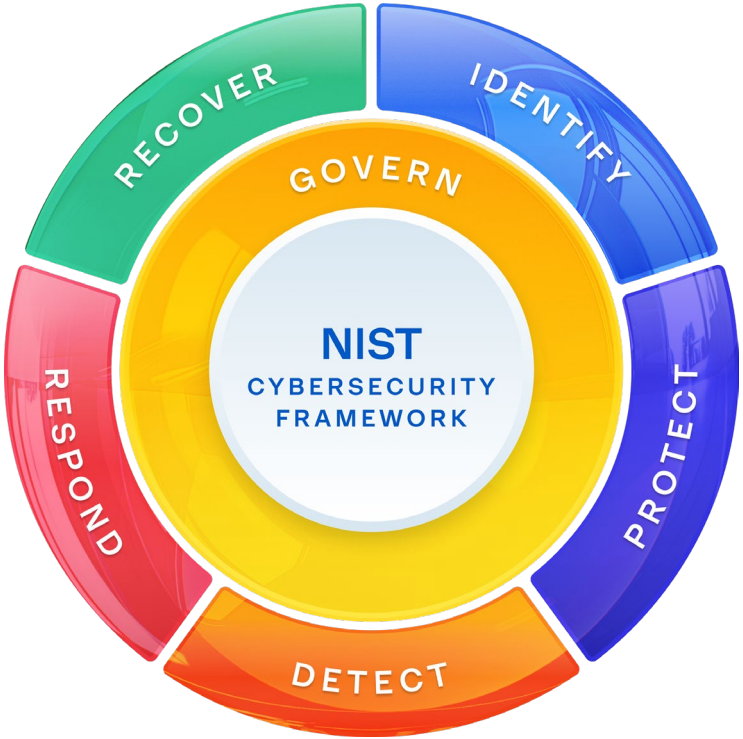
Acronis

Acronis Cyber Protect Local

Complete, end-to-end cyber resilience and endpoint management with cloud-hosted and on-premises management console for business

Make your business cyber resilient with a single platform



Govern

- Provisioning via a single agent and platform
- Centralized policy management
- Role-based management
- Information-rich dashboard
- Schedulable reporting

Identify

- Software and hardware inventory
- Unprotected endpoint discovery
- Content discovery
- Data classification
- Vulnerability assessments

Protect

- Security configuration management
- Patch management
- Device control
- Data loss prevention
- Security training

Detect

- AI- and ML-based behavioural detection
- Exploit prevention
- Anti-malware and anti-ransomware
- Email security
- URL filtering

Respond

- Rapid incident prioritization
- Incident analysis
- Workload remediation with Isolation
- Forensic backups
- Remote access for investigation

Recover

- Rapid rollback of attacks
- One-click mass recovery
- Self-recovery
- Backup integration
- Disaster recovery Integration

Maintain business uptime despite cyberthreats and outages

Build defense-in-depth against attacks and recover fast from any system failure.

Natively integrated

- Data protection, endpoint security and management that work together.
- Delivered with a single agent, single management console, and single policy.
- Maximizing coverage across compliance and insurance requirements.

Highly efficient

- Easy, intuitive management with a short learning curve.
- Fast onboarding with easy deployment.
- Low impact on performance via a single, low-resource agent for all services.

Built for IT teams and OT environments

- Role-based access across controls and to various features.
- Centralized dashboard and scheduled reporting.
- Simplified self-service with one-click recovery for IT and non-IT users.

License one way, deploy your way

Acronis Cyber Protect

Cloud-based management console

Ideal for:

- Microsoft 365 backup and archiving
- Endpoint detection and response
- Cloud disaster recovery

NEW

Acronis Cyber Protect Local

On-premises management server

Ideal for:

- Sovereign private cloud (e.g., public sector)
- Air-gapped operational technology (OT)
- Enterprise edge / remote and offshore locations

Why Acronis Cyber Protect Local

- **Dedicated focus** on organizations running on-premises, private cloud or air-gapped environments.
- Delivers **integrated cyber resilience** (backup and recovery including immutable storage, natively integrated with endpoint security and management).
- Supports **compliance and data sovereignty** requirements.
- Provides a **modern, unified alternative** to fragmented or legacy on-premises tools.

Top use cases for Acronis Cyber Protect Local

Cybersecurity

Zero-day and malware protection

Remote work protection

Detect and respond to security incidents

Data protection

Backup data across your all environments

Post-attack recovery and disaster recovery

Real-time protection of critical data

Administration

Streamlined management

Reduced costs and complexity

Compliance and forensics investigations

Top use cases for business

Feature	Acronis Cyber Protect Local: Capabilities
Enterprise-level backup and recovery	Delivers secure, fast recovery across multisite, multigenerational IT environments with AI and ML proactive protection against all forms of malware.
User-driven recovery	Empowers users with one-click recovery for distributed endpoints, including bare-metal recovery, reducing IT dependency.
Reduced total cost of ownership	Reduces TCO via support for broad, multigenerational OS and enables vendor consolidation while providing comprehensive protection.
Management and autonomy	Simplifies operations with centralized management that retains local control, integrating seamlessly with third-party tools.
Data sovereignty and compliance	Utilizes a global data center network to ensure data is managed according to regional laws, offering compliance and peace of mind.
Legacy system support	Rapidly restores any computer, including legacy systems, with options for bare-metal recovery to new hardware if necessary.
Industrial equipment downtime reduction	Local recovery options for special-purpose industrial equipment minimize downtime in critical operations.
Remote work protection	Extensive remote work protection capabilities, including remote wipe and tools for secure remote access.

Acronis

Native integration reveals new cyber protection capabilities

Innovative data protection scenarios

Continuous data protection
Avoid even the smallest data loss in key applications.

Forensic backup
Image-based backup with valuable, additional data added to backups.

Data protection map
Monitor the protection status of files with classification and reporting.

Better protection with fewer resources
Offload and enable more aggressive scans and vulnerability assessments in central storage, including the cloud.

Safe endpoint recovery
Anti-malware updates integrated into the recovery process.

Fail-safe patching
Automatically back up endpoints before installing any patches to roll back immediately.

Smart protection plan
Auto-adjust patching, scanning and backup to current CPOC alarms.

Global and local whitelists
To support more aggressive heuristics and preventing false detections.

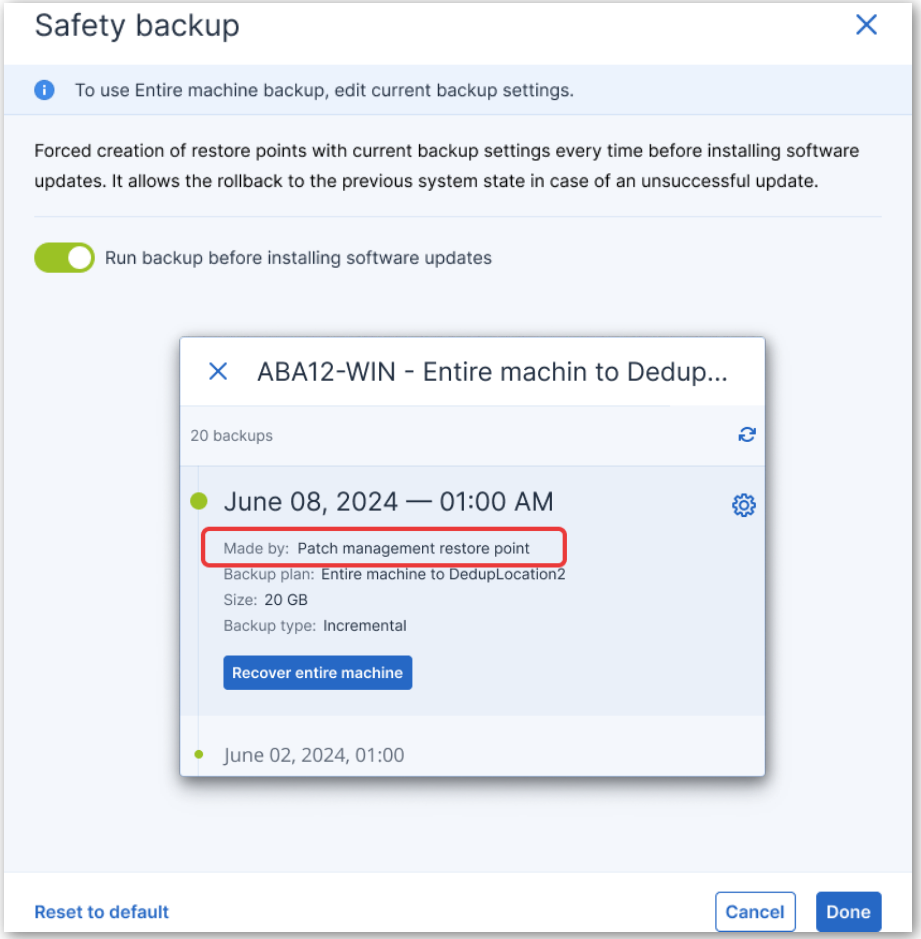
1. Fail-safe patching

Back up endpoints before patching to enable quick rollback to a working state.

A bad system patch can render a system unusable. Patch management rollbacks have limitations and can be slow. Create
an image backup of selected machines before installing a system or application patch.

Why

- Save time by accelerating the patching process.
- Eliminate patching difficulties and delays.
- Reduce breach rates caused by improper patching.
- Support faster and more reliable operations.

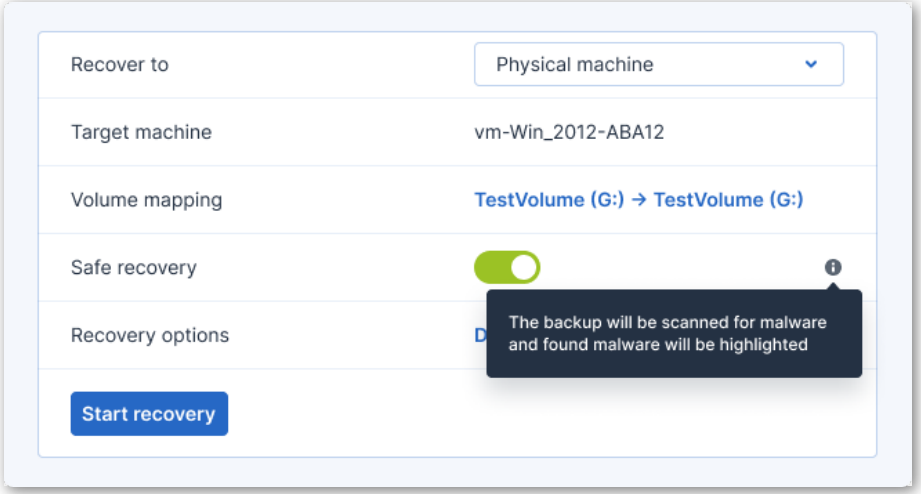


2. Safe recovery

Removing detected malware during the recovery process.

An OS image or application in a backup that is infected with malware can cause continuous reinfection if it is used for recovery without removing the malware.

Removing the detected malware and applying the latest anti-malware definitions during the recovery allows users to restore the OS image safely, reducing the chance of reinfection.



Why

- Ensure the system you are recovering into production is malware free.
- Reduce the chance of reinfection.
- Automate and speed up the recovery process.

3. Malware scan in centralized locations

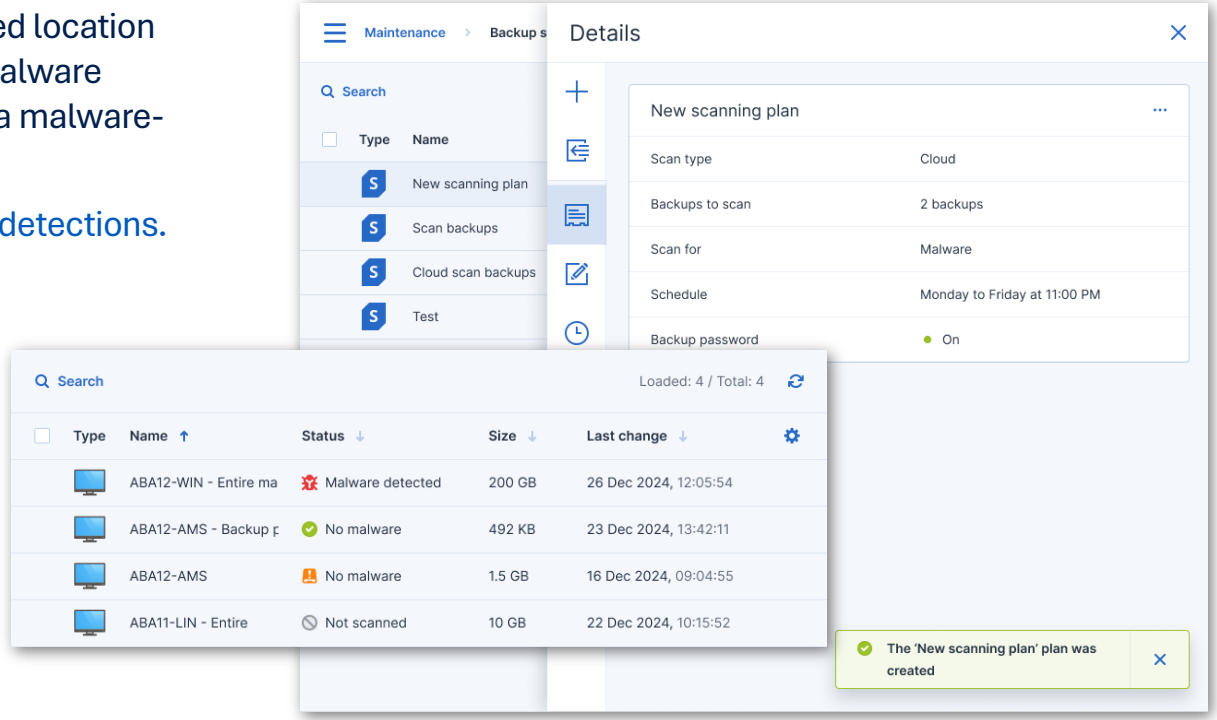
Anti-malware scanning of backups provides additional security.

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

- Increases potential rootkit and bootkit detections.
- Reduces loads of client endpoints.

Why

- Increase security by restoring only clean data.
- Avoid performance degradation by avoiding endpoint overload.



4. Continuous data protection

Gain safe and instant remediation without data loss and close-to-zero RPOs.

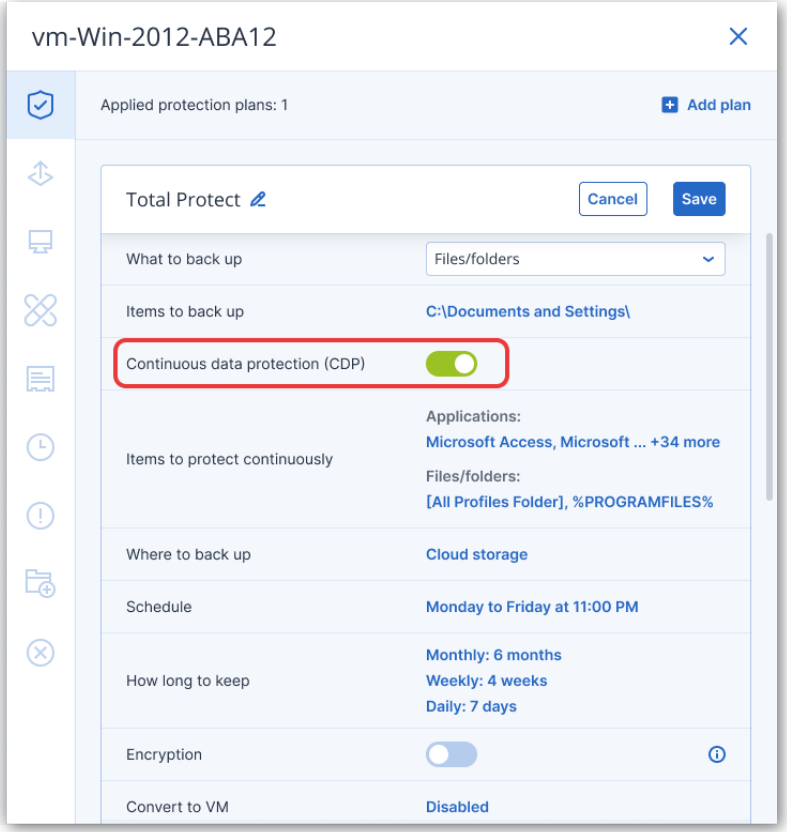
Define the list of critical, frequently used apps for every device. Acronis' agent monitors every change made in the listed applications.

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

IT controls what is continuously backed up: office documents, financial forms, logs, graphic files, etc.

Why

- Ensure all your essential work in progress is safe as data is protected even between the backups.



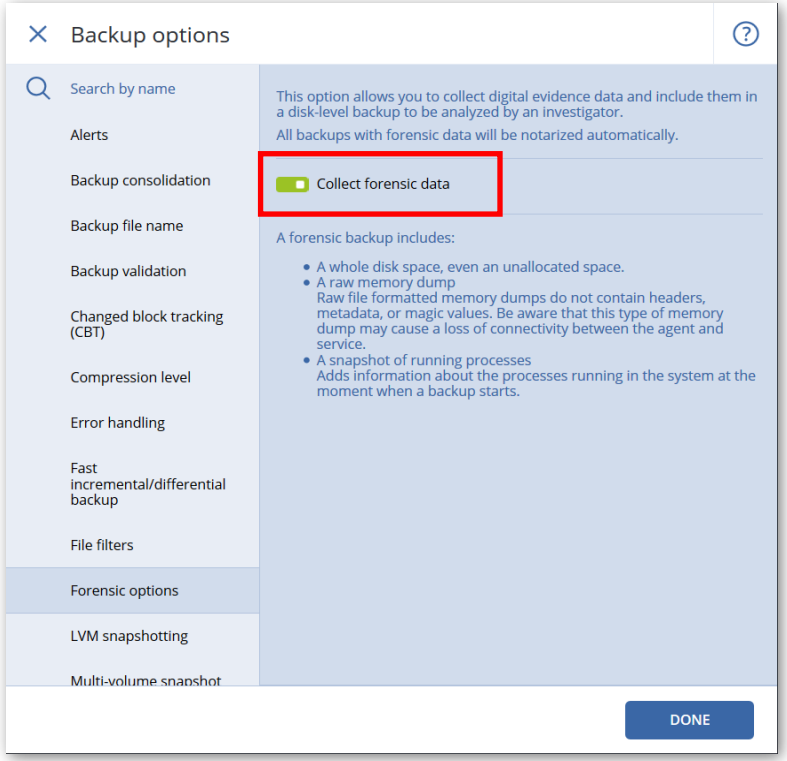
5. Forensic backup

Back up vital data as well as information that's useful for future analysis.

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

Why

- Investigate 'insider' attacks against corporate data (IP theft, information leaks, etc.).
- Simplify and speed up the investigation process.
- Improve internal security.

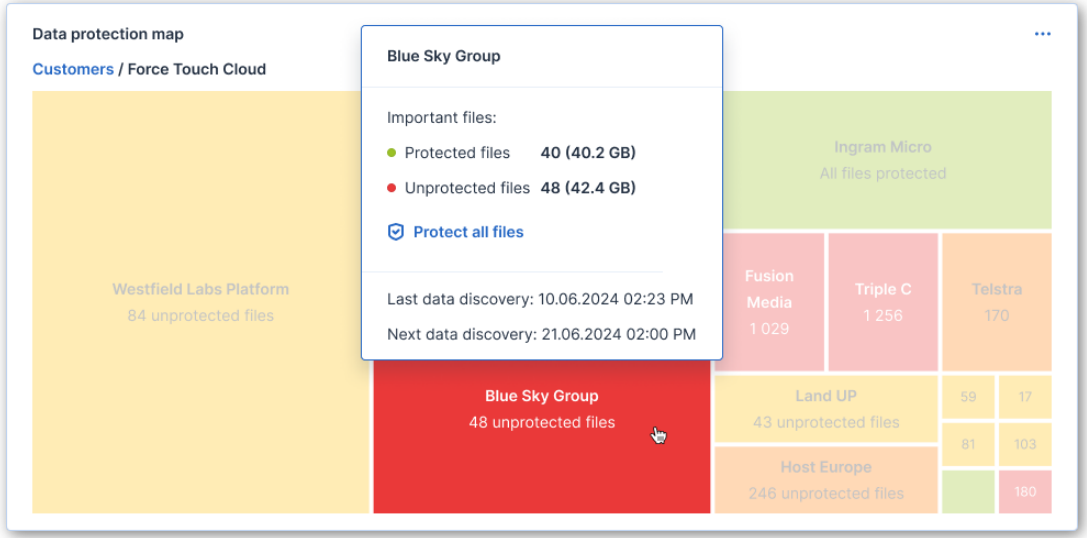


6. Data compliance reporting and data protection map

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

Why

- Make sure all important data is backed up.
- Quickly uncover failed backups and highlight threats.
- Get actionable insights to execute risk mitigation steps.
- Satisfy compliance requirements by proving data is backed up regularly.



7. Smart protection plan

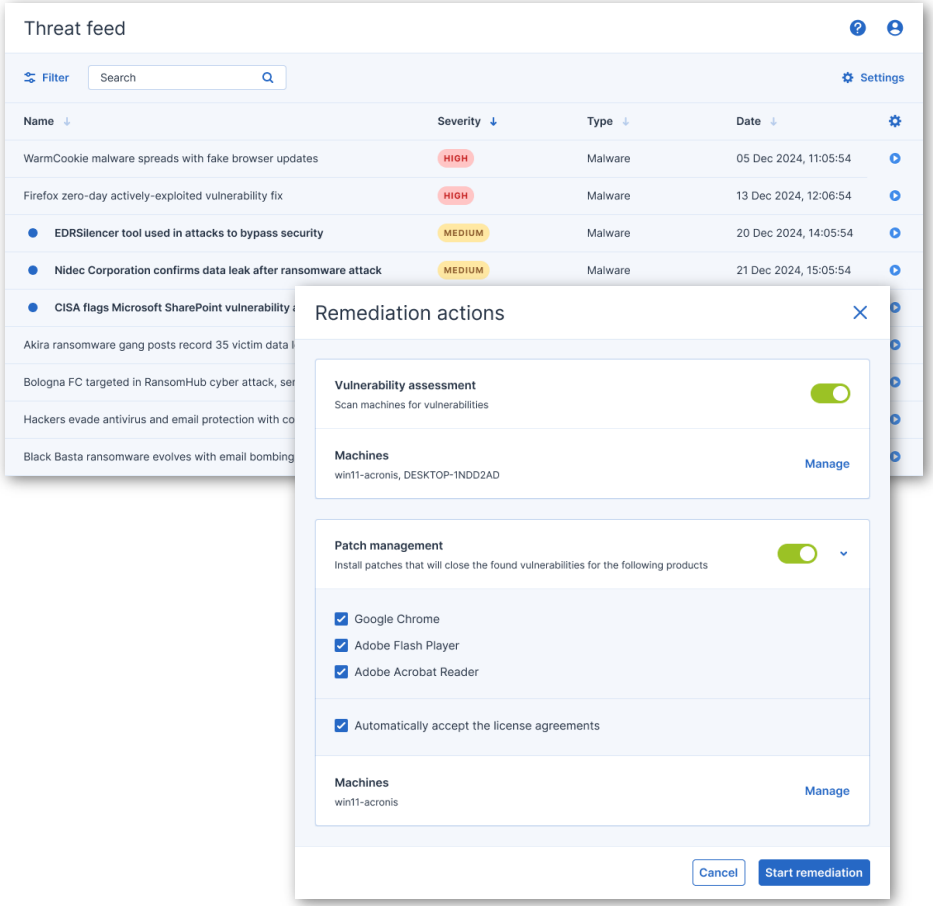
Ensure your protection is up to date.

Acronis CPOCs* monitor the cybersecurity landscape and release 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.

Protection plans will be restored when the situation is back to normal.

Why

- Mitigate risks from upcoming and existing threats.
- Reduce reaction times through automation.



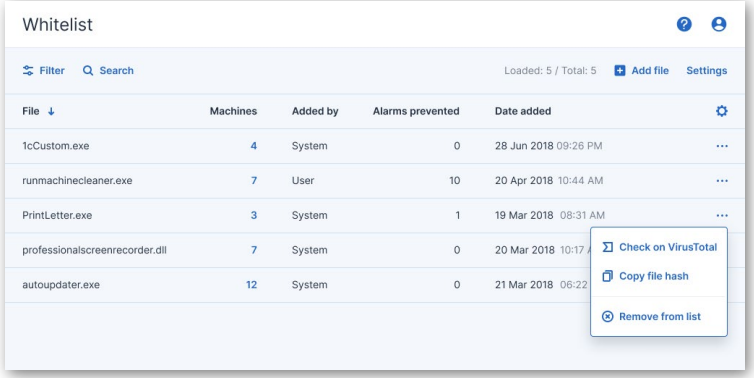
8. Global and local whitelists from backups prevent false detections

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

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

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

- Improves detection rate via improved heuristics.
- Supports manual whitelisting.



Why

- Reduce false positives and ensure legitimate data is always accessible.
- Save time by eliminating time-consuming manual whitelisting of unique apps.

Acronis

New features overview: Acronis Cyber Protect Local

Cloud innovation, delivered locally

NEW

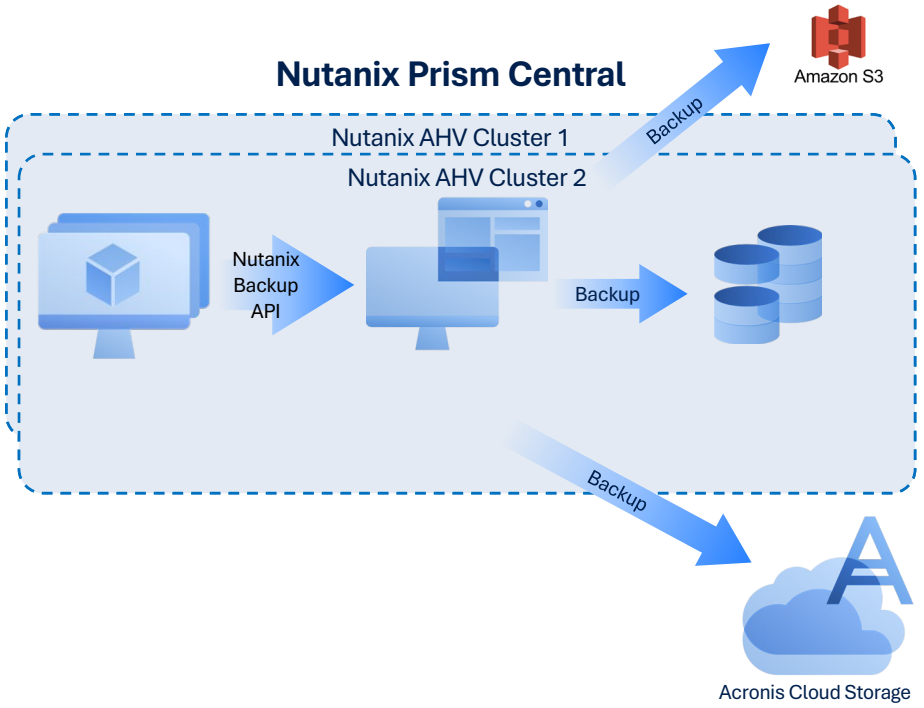
- Nutanix AHV
- Role-based access
- Network discovery
- Proxmox VE
- Hardware inventory
- Software inventory

Agentless backup for Nutanix AHV

New in Local (on premises)

Fast and reliable backup capability built in tight cooperation with Nutanix.

- **Flexible storage options:** Acronis Cloud, Azure Storage / AWS S3 and other public clouds.
- **Cross-platform recoveries** to Nutanix AHV VMs from anywhere (Any-to-Nutanix recovery), including **migration from VMware**.
- "**Nutanix Ready**" certification planned right after initial release.

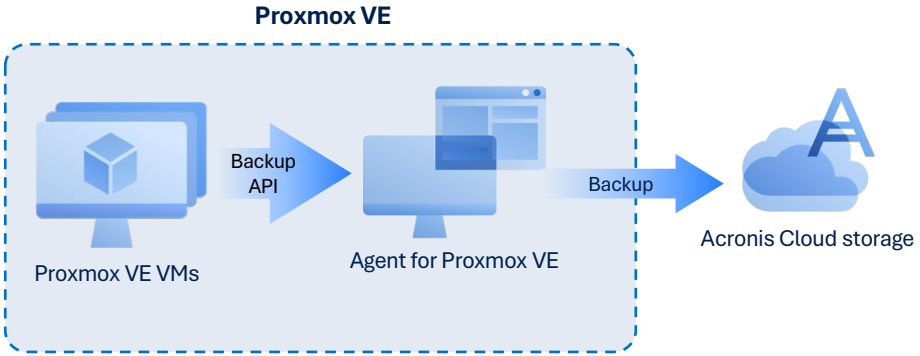


Agentless backup for Proxmox VE

New in Local (on premises)

Efficient protection for Proxmox VE environments.

- **Seamless user experience:** Manage backups of your entire environment from a single console, including Proxmox VE.
- **Efficient management**: No need to install agent inside each VM.
- **Cross-platform**: Recover your physical machines backups as Proxmox VE VMs.



User role-based management

New in Local (on premises)

Introducing new granular roles for enterprise flexibility.

Designed for large and midsized organizations with distributed IT responsibilities:

- Minimize risk: Limit access based on roles to reduce human error and insider threats.
- Align with compliance: Support internal policies through clear separation of duties.
- Streamline operations: Empower specialized teams without granting full administrative control.

New user roles:

- **Backup administrator:** Configures and manages backup policies and schedules.
- **Restore operator:** Initiates and manages data recovery without full admin rights.
- **Security administrator:** Controls security settings and policies. Isolates sensitive controls for InfoSec or SecOps teams.

Purpose-built access control for secure, efficient IT operations.

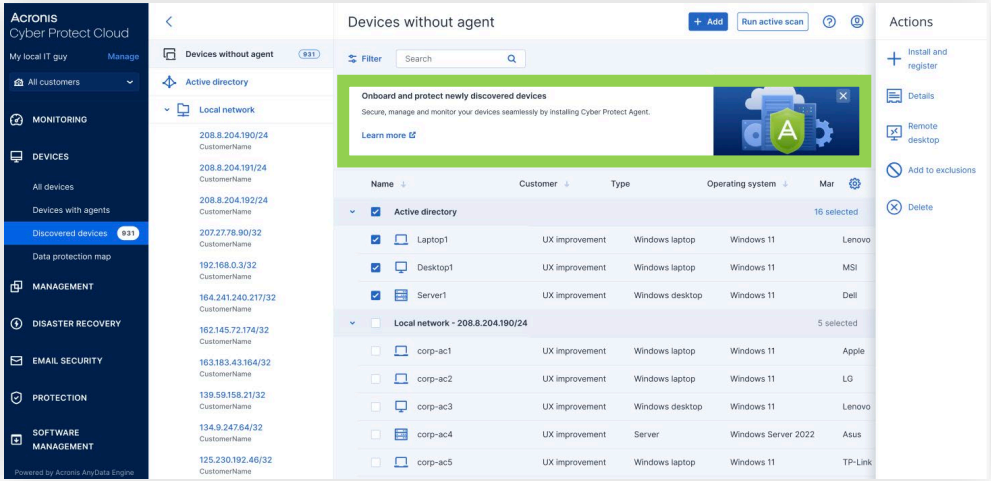
Device Sense™ Device Discovery

New in Local (on premises)

Eliminate uncertainty: Gain better visibility of environment.

- **Automatically discover** and secure every device on your network.
- **Instant discovery**
  Uncover all connected devices, including hidden or unmanaged ones.
- **Close protection gaps**
  Identify and secure unprotected endpoints before they become risks.
- **Strengthen security posture**
  Gain full visibility to stay compliant, secure and in control.

No more blind spots. No manual effort.
Just smarter protection.



Software inventory

New in Local (on premises)

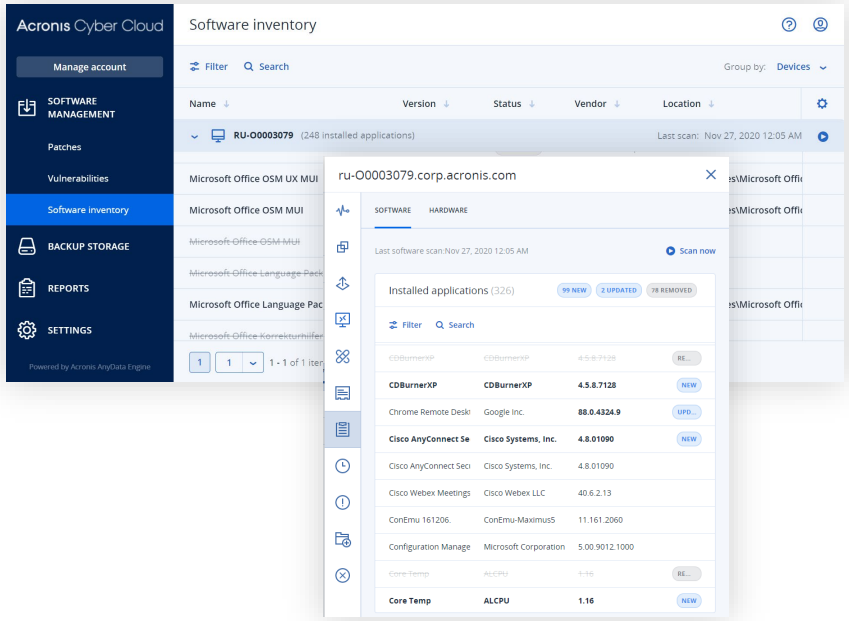
Complete list of software used by customers to efficiently plan and track updates

Increase visibility with up-to-date information about all software assets:

- Discover all software assets on all registered machines in the organization.
- Search and filter software assets by multiple criteria (e.g., software name, software vendor, status).
- Schedule automated scans or run scanning on-demand.

Reduce time spent on maintenance by:

- Tracking changes in software inventory since previous scans.
- Generate software inventory reports.



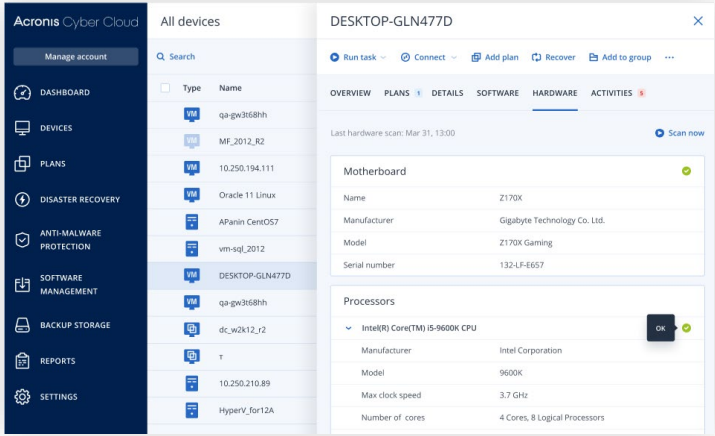
Hardware inventory

New in Local (on premises)

Keep up-to-date information on hardware assets to properly plan replacement.

Increase visibility with up-to-date information about hardware assets:

- Discover all hardware assets on all registered machines of the organization (e.g., CPU, GPU, motherboard, RAM, network adapters, etc.).
- Search and filter hardware assets by multiple criteria: processor model, processor cores, disk total size, memory capacity, etc.
- Schedule automated scans or run scanning on demand.



Reduce time spent on maintenance by:

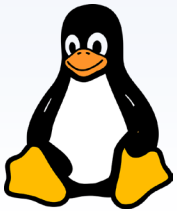
- Tracking changes in hardware inventory since previous scans.
- Generate hardware inventory reports.

Support for new OS systems

New in Local (on premises)

Backup and recovery for new versions of operating systems:

- Windows Server 2022/2025 Essentials support
- Ubuntu 24.10
- Fedora 39, 40, 41
- Oracle Linux 9.5
- CloudLinux 9.5
- AlmaLinux 9.5
- Rocky Linux 9.4, 9.5
- Red Hat 9.5



Acronis

Key features overview

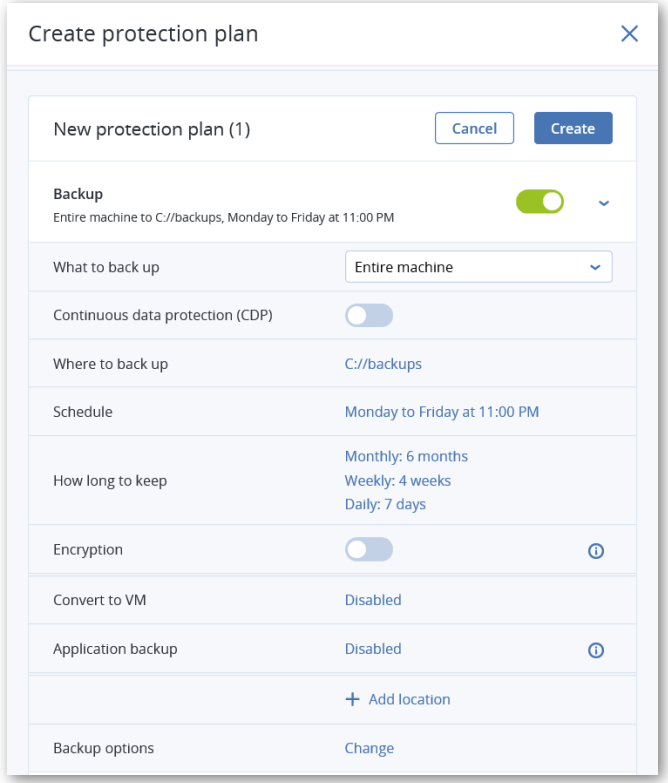
Acronis

Backup

Full-image and file-level backup

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

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



Why

- Ensure business continuity with flexible backup options.
- Avoid costly downtime and data loss.

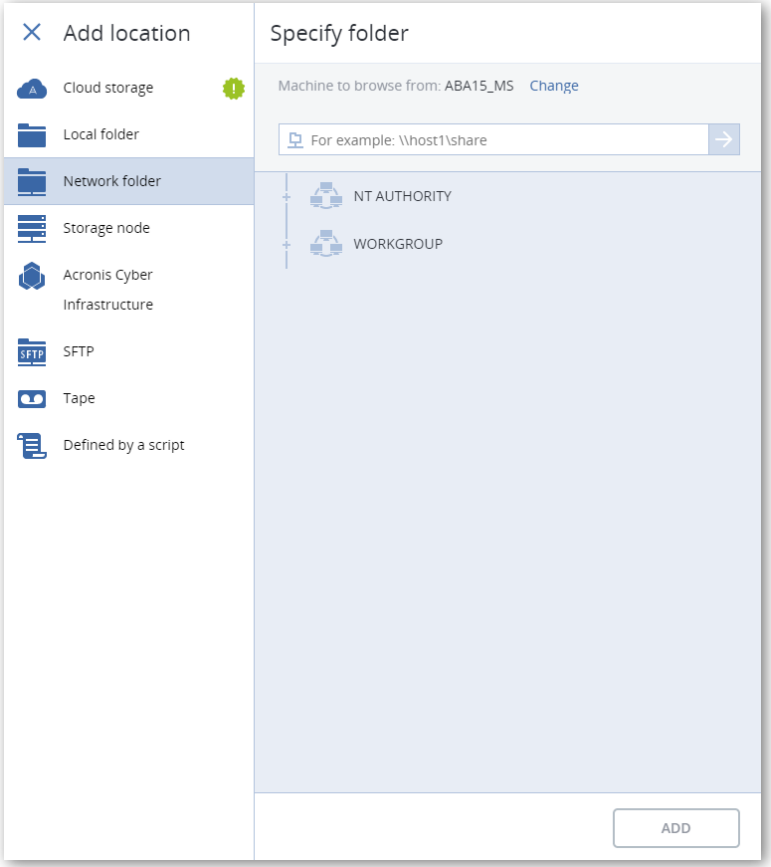
Flexible storage options

Grow with ease using the storage that fits your needs.

Balance the value of data, infrastructure, and any regulatory requirements with flexible storage options:

- Local and network folder***
- Acronis Cloud***
- Any S3-compatible cloud storage (e.g. AWS/Wasabi/Impossible Cloud)*
- Azure Storage*
- Acronis Storage Node (including tapes)**
- Tapes directly attached to backed up device**
- Acronis Cyber infrastructure**

* Only with cloud deployment
** On premises
*** Cloud deployment and on premises



Error-proof immutable backups

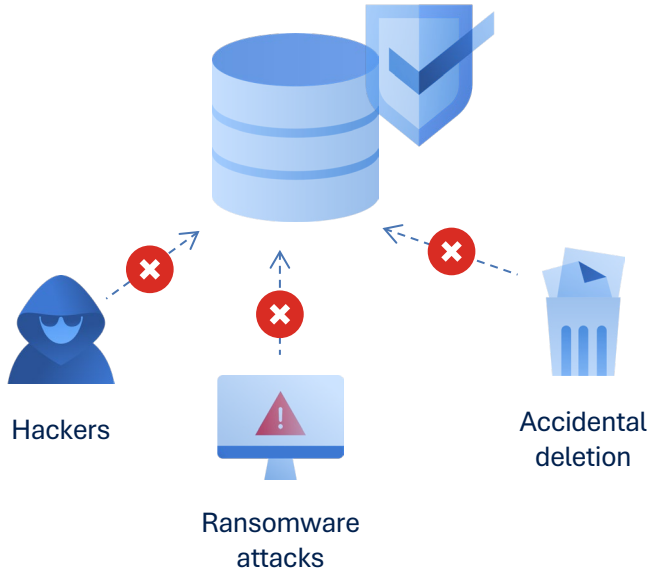
Prevent accidental and malicious data loss.

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 available in two modes: governance and compliance, 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). Governance mode can still be disabled by an administrator.

The **compliance mode** cannot be disabled once activated.



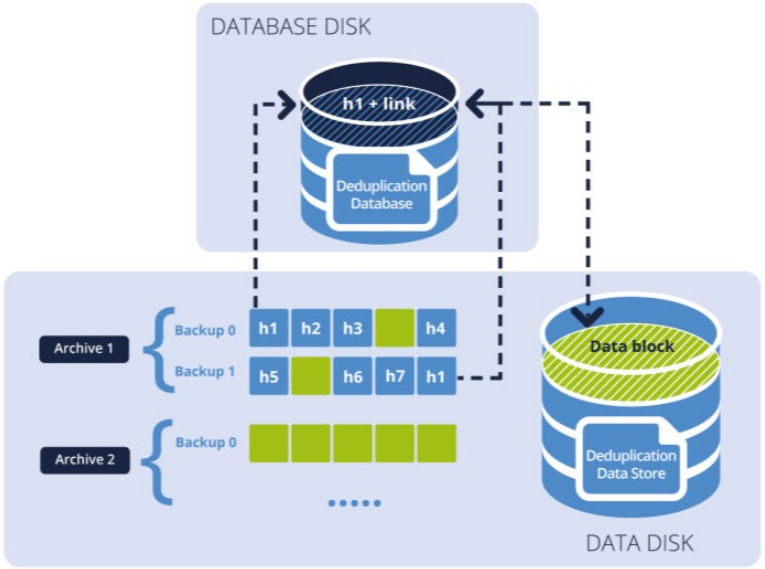
Why

- Prevent backups from being deleted by malware or malicious users.

Deduplication

Protect more systems while reducing the impact on disk-storage and network capacity.

- Detect data repetition.
- Eliminate duplicate data blocks when you back up and transfer data.
- Store the identical data only once.



Why

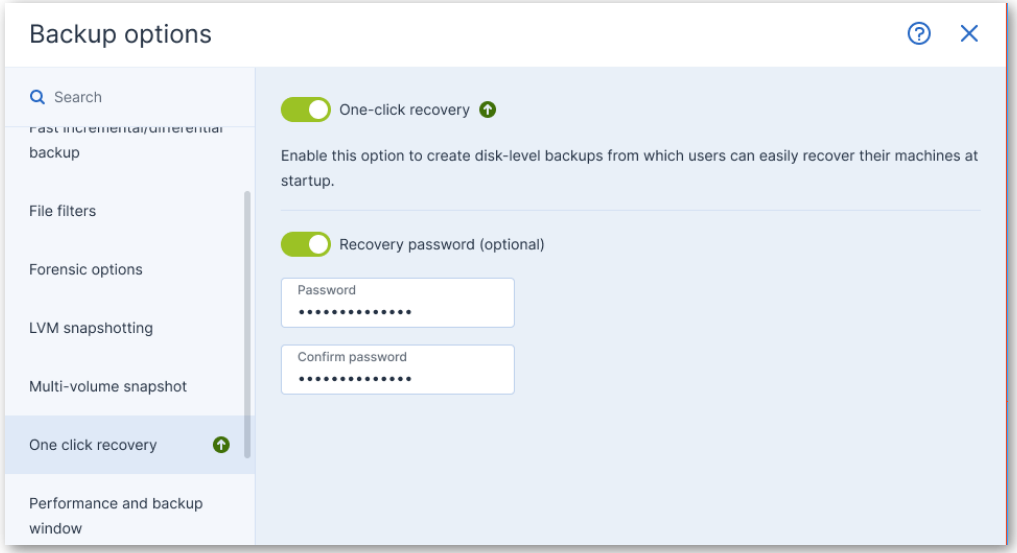
- Reduce storage space usage by storing only unique data.
- Eliminate the need to invest in data deduplication-specific hardware.
- Reduce network load because less data is transferred, leaving more bandwidth for your production tasks.

One-click recovery

Enable quick and easy mass recovery with minimal IT intervention.

Speed up the recovery process of multiple workloads and minimize IT efforts by offloading the recovery to end users.

By enabling one-click recovery in the protection plan, you can easily empower nontechnical end users with a simplified, automated recovery of an entire workload.



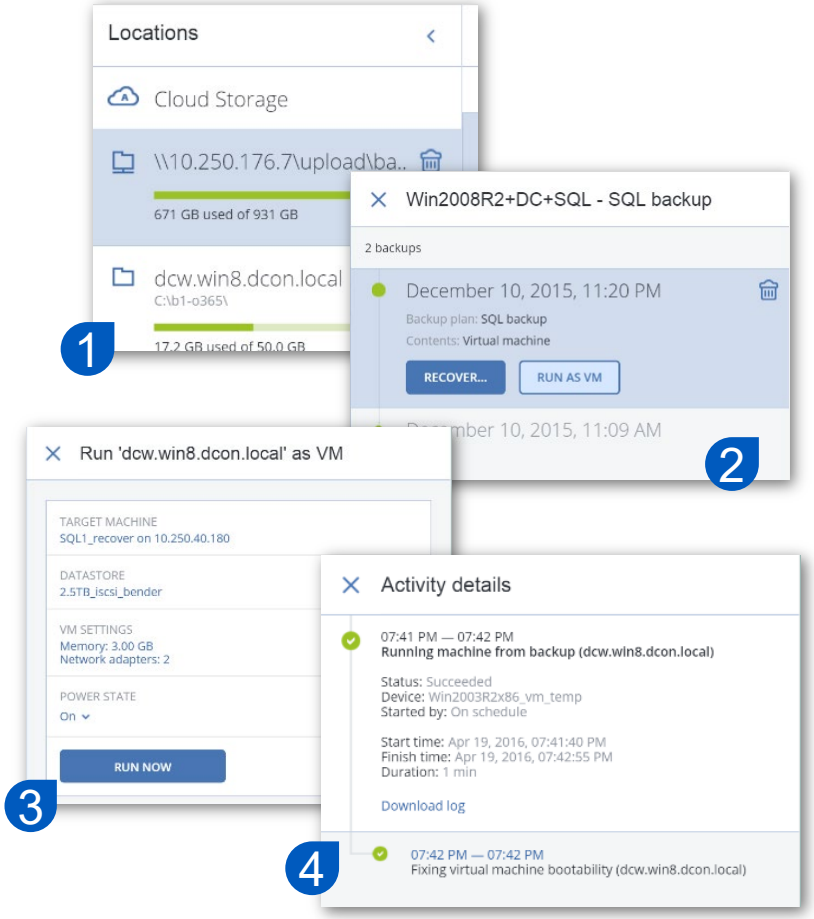
Why

- Eliminate IT bottlenecks and save time and money by reducing downtime in case of a cyberattack.

Acronis Instant Restore

Get running again in seconds.

- Immediately start your backup as a Windows or Linux virtual machine directly from storage.
- Have your VM up and running in mere seconds, while Acronis Instant Restore technology invisibly moves your data to the host in the background.
- Recover any virtual, physical or cloud server, Windows or Linux.



Why

- Reduce network consumption.
- Reduce recovery times with best-in-industry RTOs.

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 your 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 and easy system migration with a few clicks.
- Reduce RTOs.
- Minimize expensive downtime.

Any-to-any migration

Easily recover to any platform.

- Acronis stores data in a unified backup format so that you can easily recover to any platform, regardless of the source system.
- Migrate between different hypervisors and to and from physical machines (P2V, V2V, V2P, and P2P) or the cloud (P2C, V2C, C2C, C2V, and C2P).

Why

- Ensure data integrity by safeguarding against data loss.
- Reduce risk and IT overload.

Join machine to domain after recovery

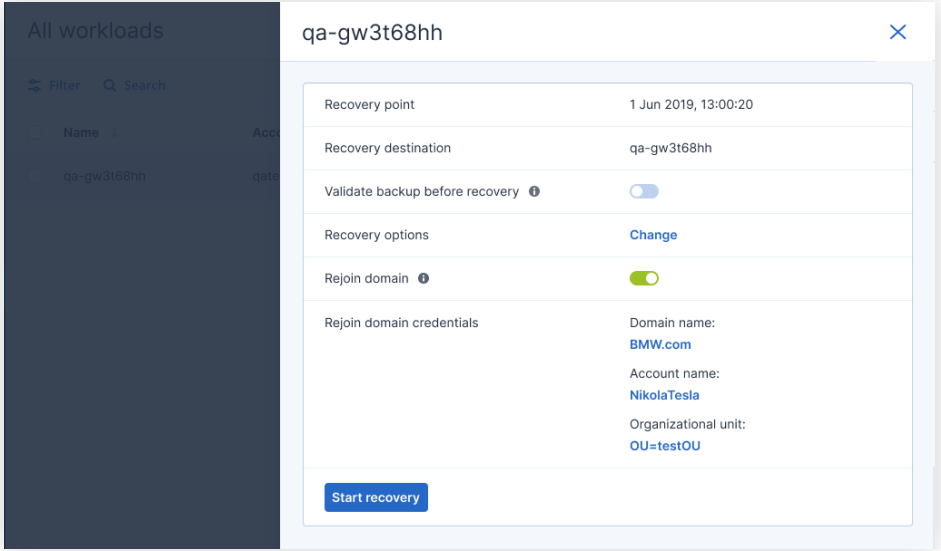
Streamline recovery operation by rejoining machines to the domain.

No need to manually rejoin the machine to the domain after recovery. You can configure this directly as a part of the recovery operation:

1. Enable the “Rejoin domain” in recovery options.

2. Provide domain credentials with permissions to add machines to the domain, including:

- Domain name
- Account name
- Organizational unit (optional)

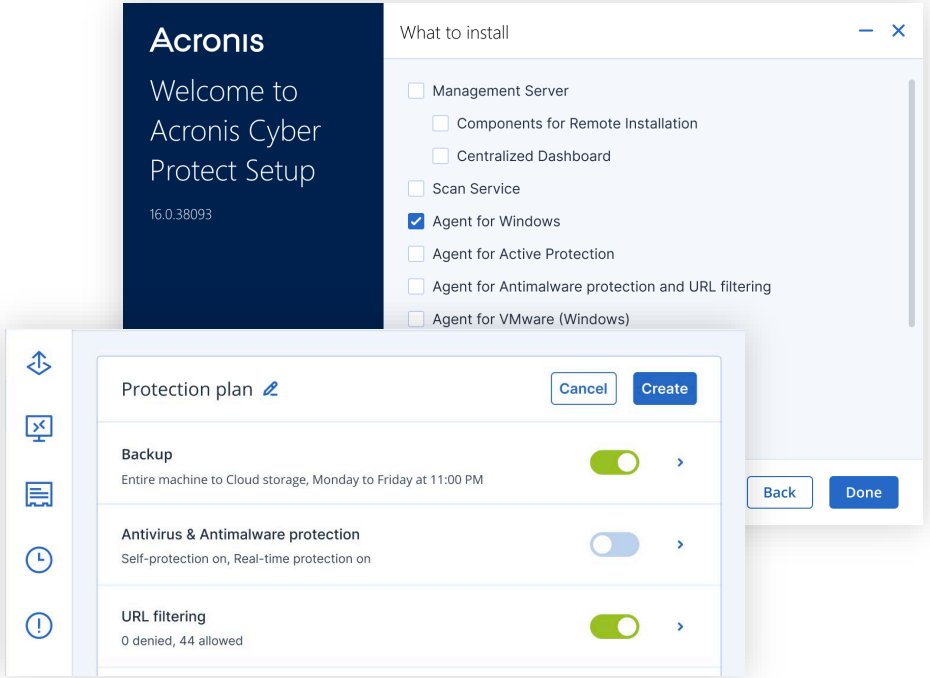


Agent installation without Active Protection

More flexibility — Install only what you need.

Active Protection components are now modular and customizable, allowing customers to install only what they need, resulting in greater efficiency and optimized performance.

- **Flexible installation:** Install only backup components when Active Protection is not required.
- **Seamless management:** Enable or disable Active Protection along with antivirus and anti-malware protection anytime via the Protection Plan.



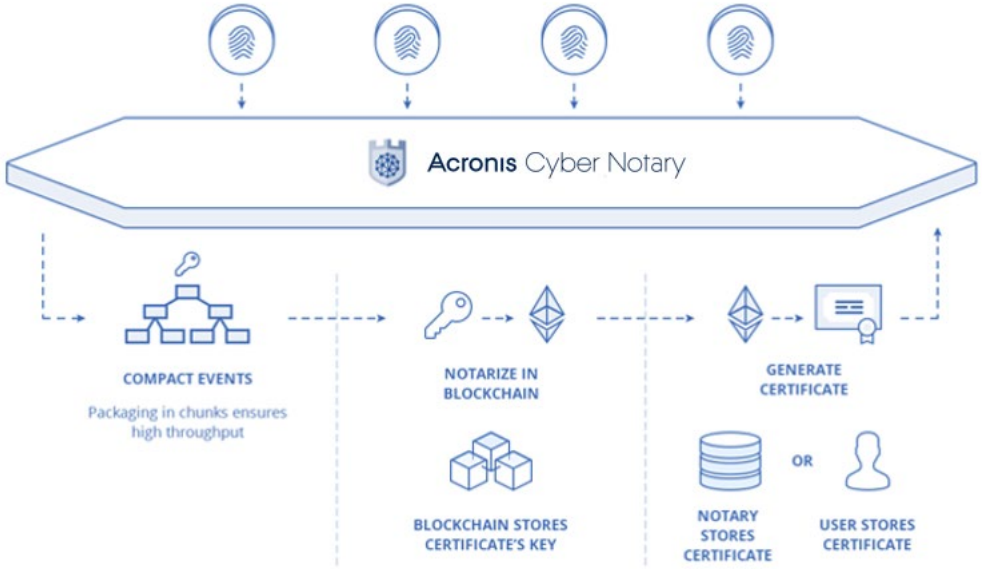
Blockchain notarization

Ensure data integrity with innovative blockchain-based Acronis Cyber Notary technology.

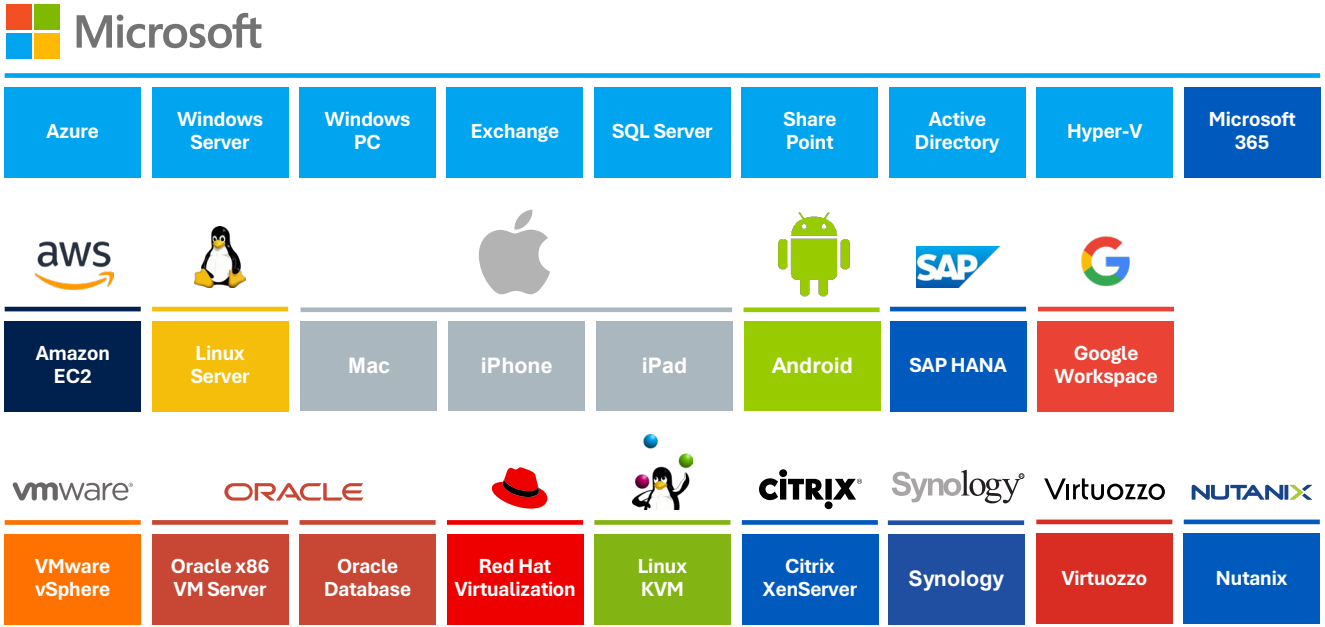
- Highly scalable micro-service architecture.
- API interface (REST), queue interface (AMPQ) for integration.
- High throughput (xx10,000 objects per blockchain transaction).
- Notarization certificates with built-in verification.

Why

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



Provides protection for 30+ workload types from infrastructure to SaaS apps



New features:

- Proxmox

New OS support:

- Windows Server 2022/2025 Essentials Support
- Ubuntu 24.10
- Fedora 39, 40, 41
- Oracle Linux 9.5
- CloudLinux 9.5
- AlmaLinux 9.5
- Rocky Linux 9.4, 9.5
- Red Hat 9.5

Every workload covered

Industry best coverage of various OSes and hypervisors.

Windows

- Windows Server 2003 SP1, R2 and later, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022 except Nano Server, 2025
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows XP Professional SP1, SP2, SP3
- Windows 7 , 8/8.1, 11 (all editions), 10, – all editions, except Windows RT

Microsoft SQL Server

- 2022, 2019, 2017, 2016, 2014, 2012, 2008 R2, 2008, 2005

Microsoft Exchange Server

- 2019, 2016, 2013, 2010, 2007

Hypervisors

VMware vSphere

- 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server

- 2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer/Citrix Hypervisor

- 8.2 - 4.1.5

Linux KVM

- 8 - 7.6

Scale Computing Hypercore

- 8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)

- 3.6-2.2

Red Hat Virtualization

- 4.0, 4.1, 4.2, 4.3, 4.4

Virtuozzo

- 7.0.14 - 6.0.10

Virtuozzo Infrastructure Platform

- 3.5

Nutanix Acropolis Hypervisor (AHV)

- 20160925.x through 20180425.x

MacOS

- **OS X** Mavericks 10.9, Yosemite 10.10, El Capitan 10.11
- **macOS** Sierra 10.12, High Sierra 10.13, Mojave 10.14, Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13, Sonoma 14, Sequoia 15

Linux: Kernel 2.6.9-5.19, 6.7-6.11

- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*, 9.5*
- Ubuntu 9.10 - 23.04, 24.10
- Fedora 11 – 31, 39, 40, 41
- SUSE Linux Enterprise Server 10, 11, 12, 15
- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4-7.7, 8.0-8.8, 8.11, 9.0- 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*, Stream 8*,9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*, 9.5*
- CloudLinux 5.x, 6.x, 7.x, 8.x*, 9.5*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*, 9.3*, 9.5*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*, 9.5*
- ALT Linux 7.0

Tape multiplexing and multistreaming

Maximize the effective use of tape drives during backup and recovery.

- Multiplexing: Enables multiple clients to back up to a single tape drive simultaneously.
- Use this method when a tape drive is faster than the backup source as it allows the tape drive to keep spinning, avoiding writing interruptions.
- Multistreaming: Enables the backup of a single client to run simultaneously to multiple tape drives.
- Use this method when you have multiple destination devices and would like a single backup job to utilize them all simultaneously at the time of backup.

Why

- Maximize the effective use of tape drives during backup and recovery.
- Avoid writing interruptions.

VMware vSphere Web Client plugin

Backup management for vSphere users.

Seamless user experience:

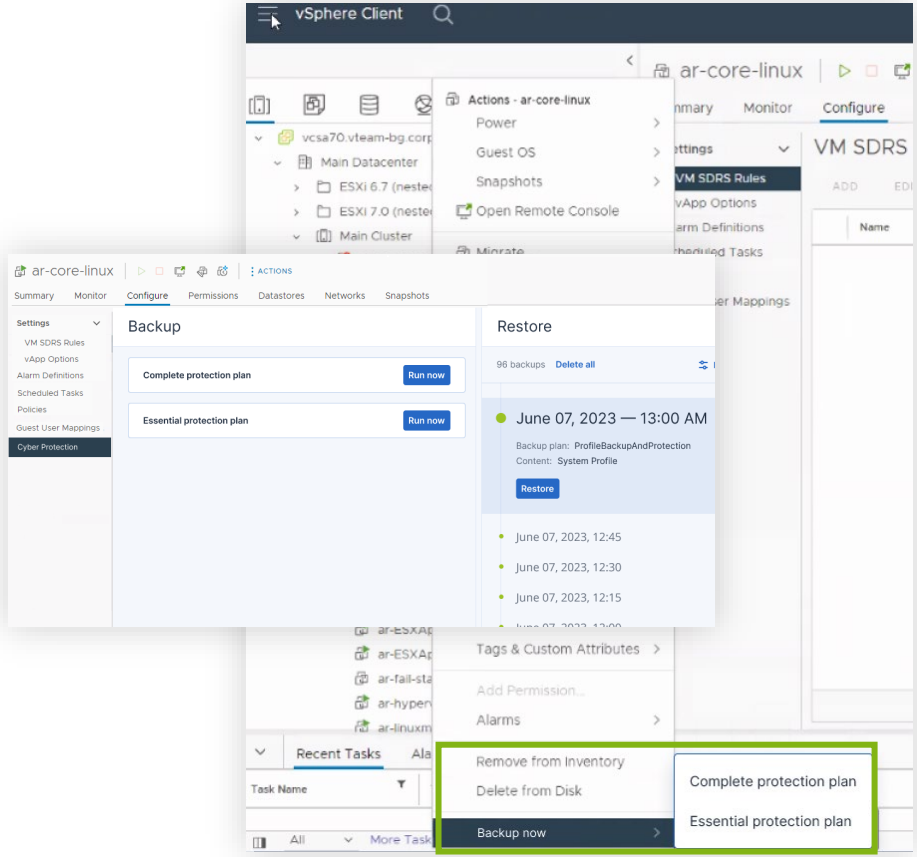
- Manage backups of your VMware environment within a vSphere web client.

Efficient management:

- Run VM backups and recoveries with context menu.
- Monitor backup status across all VMs with embedded Acronis Dashboard.

Secure solution:

- Only users who have special vSphere privileges will be able to perform backup management.



Acronis

Cybersecurity

Significantly extended anti-malware capabilities

Acronis Cyber Protect

Acronis Active Protection

Anti-ransomware, anti-cryptojacking and 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.

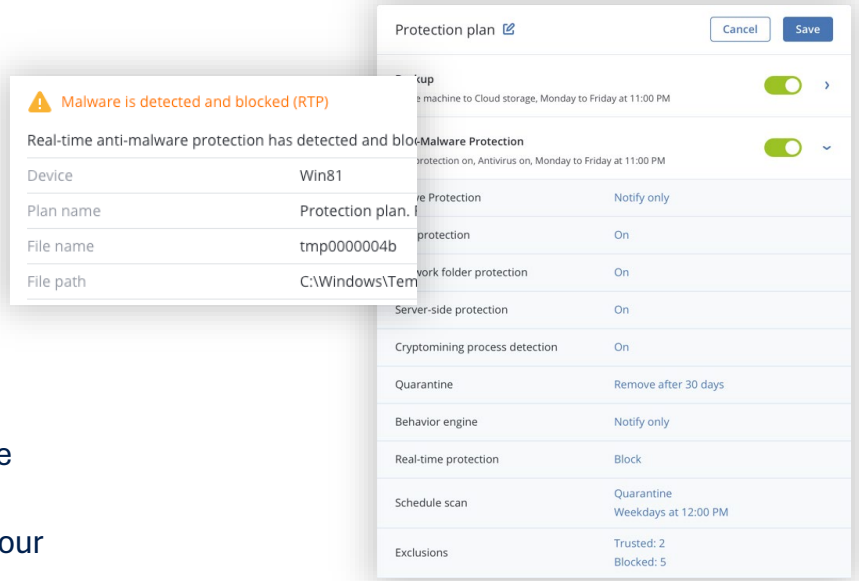
Native integration with Windows Security Center

Why Actively prevent downtime and data loss, don't just recover information after an attack.

Anti-malware protection

Full-stack antimalware protection for Windows and macOS.

- Real-time protection against malware.
- Cryptomining process detection.
- Ransomware detection.
- 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.
- File quarantine.
- Exclusions management: Specify processes that will not be considered malware; exclude folders where file changes will not be monitored; and select files and folders where scheduled scanning will not be executed.



Why

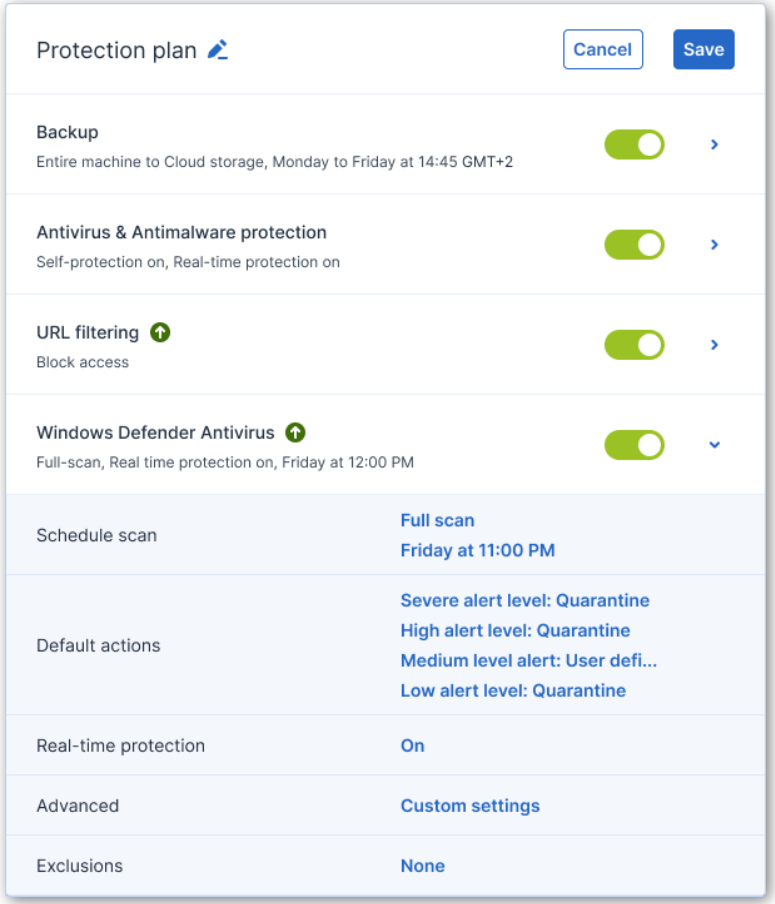
- Block malware before it affects your data
- Ensure business continuity
- Enable employees to work uninterrupted

Windows Defender Antivirus or Microsoft Security Essentials Management

- Enforce settings across multiple machines.
- Collect all Windows Defender Antivirus and Microsoft Security Essentials detection events and display them in the management console.

Why

- Streamline management.
- Save time and effort.



Vulnerability assessment

Discover a vulnerability before it's exploited.

Continuous, daily updates of Acronis' vulnerability and patch management database.

Support for:

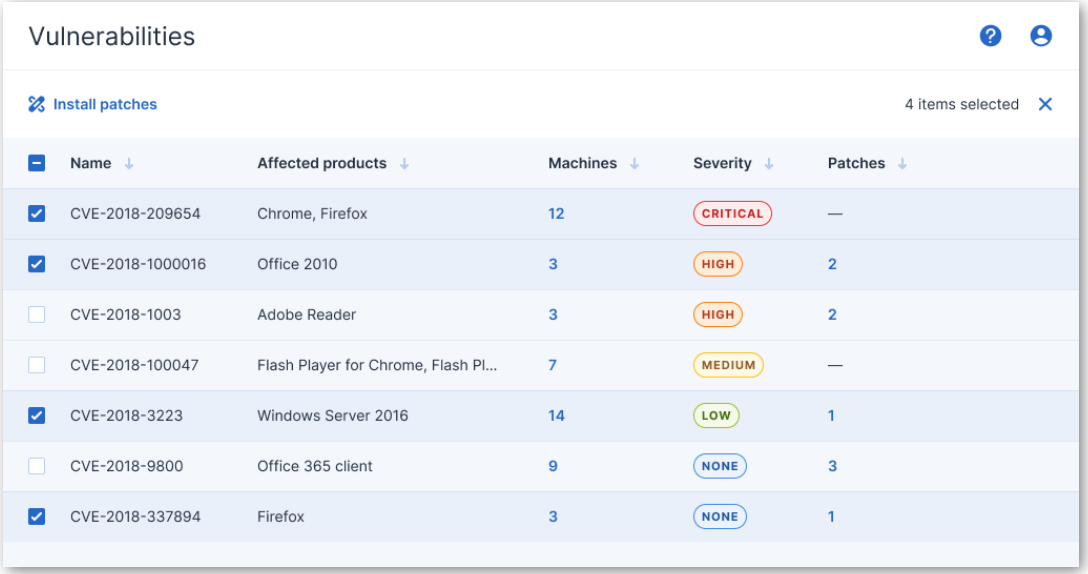
Microsoft:

- Workstations – Windows 7 and later.
- Server – Windows Server 2008R2 and later.
- Microsoft Office (2010 and more) and
- related components.

.NET Framework and server applications.

Adobe, Oracle, Java.

Browsers and other software.



Why

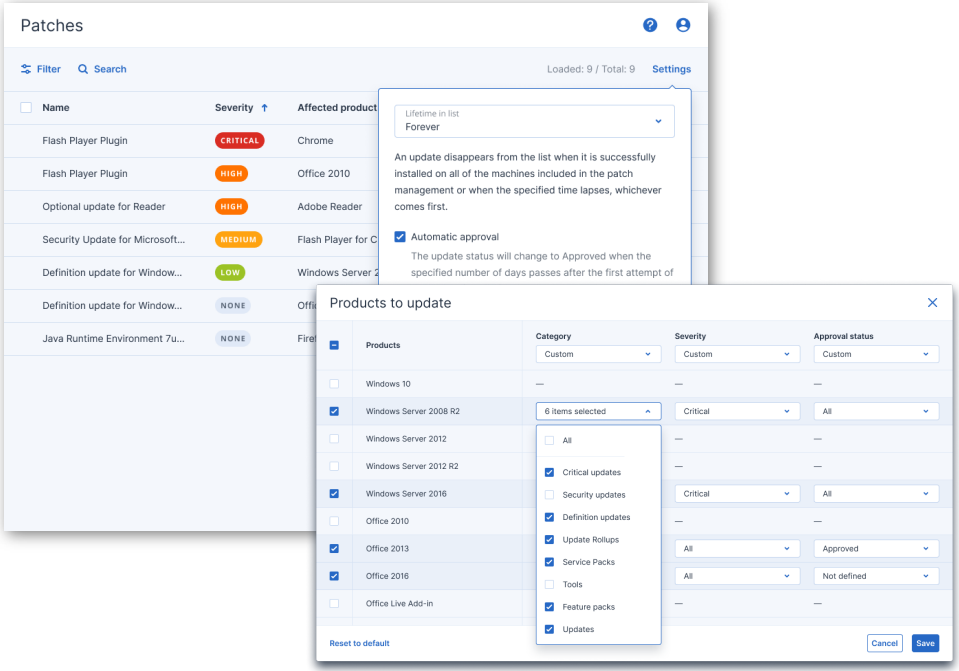
- Identify vulnerabilities before attackers find them.
- Identify the level of risk on your systems.
- Mitigate potential threats.
- Optimize security investments.

Patch management

Fix an issue before it happens.

Large common vulnerabilities and exposure database, 250-300 new CVEs weekly.

- **Auto-approval** of patches.
- Deployment on a **schedule**.
- **Manual** deployment.
- **Flexible** reboot and maintenance window options.
- **Staged** deployment.
- **All Windows updates** including MS Office, and Win10 apps.
- Support for patch management of **Microsoft and third-party software** on Windows.

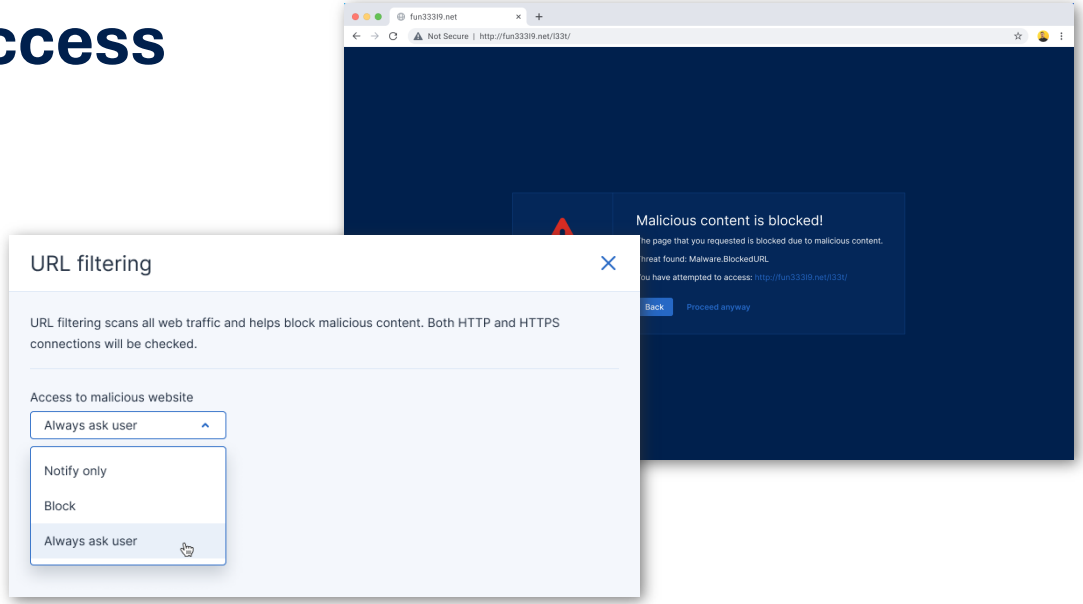


Why

- Automate your protection.
- Reduce potential risks.
- Prevent attacks (e.g., Equifax, WannaCry).

URL filtering controls access to malicious URLs

Control access to the internet by permitting or denying access to specific websites based on information contained in a URL list.



- HTTP / HTTPS interceptor.
- Black / whitelists for URLs.
- Payload analysis for malicious URLs.

Acronis URL Filtering List:

- Acronis' own signatures.
- AI-based detection.

Why

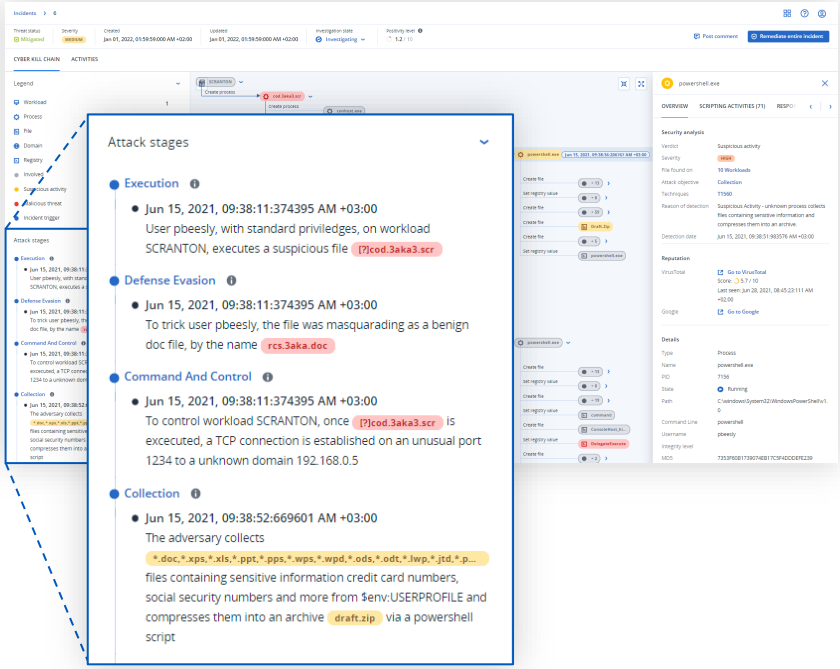
- Prevent attacks through malicious or hacked websites.
- Gain better compliance.
- Increase employee productivity.

Analyze attacks in minutes to unlock rapid response

Leverage AI-based, human-friendly interpretation of attacks and prioritized visibility.

Enable your team to effortlessly analyze attacks with ease and speed:

- Get **prioritized visibility of suspicious activities** across endpoints rather than a flat list of all alerts.
- **Gain complete visibility into the attack chain:**
  The attack evolution is mapped to the MITRE framework (industry-standard)
  - How did it get in?
  - How did it hide its tracks?
  - How did it cause harm?
  - How did it spread?
- **Save money and time, removing the need for** rigorous training or highly skilled personnel doing operational tasks.
- **Focus on what matters** using an emerging threat intelligence feed to search for IoCs.

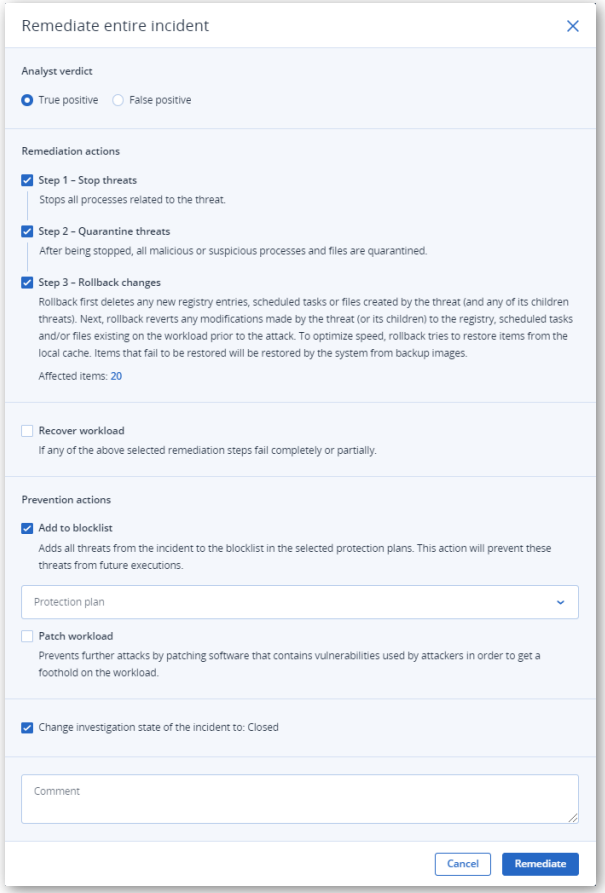


Stop the breach and ensure business continuity

Succeed where point solutions fail. Unlock the full power of a platform with integrated capabilities for unmatched business resilience.

- **Investigate further** using remote connection and forensic backup.
- **Contain threats** by network isolating the affected workload.
- **Remediate** by killing malware processes, quarantining threats and rolling back changes.
- **Prevent** incidents from reoccurring with software patch management and by blocking analyzed threats from execution.
- **Ensure unmatched business continuity** with integrated recovery capabilities, including attack-specific rollbacks, file- or image-level recovery, and disaster recovery.

Select the actions you want to take and respond with a single click.

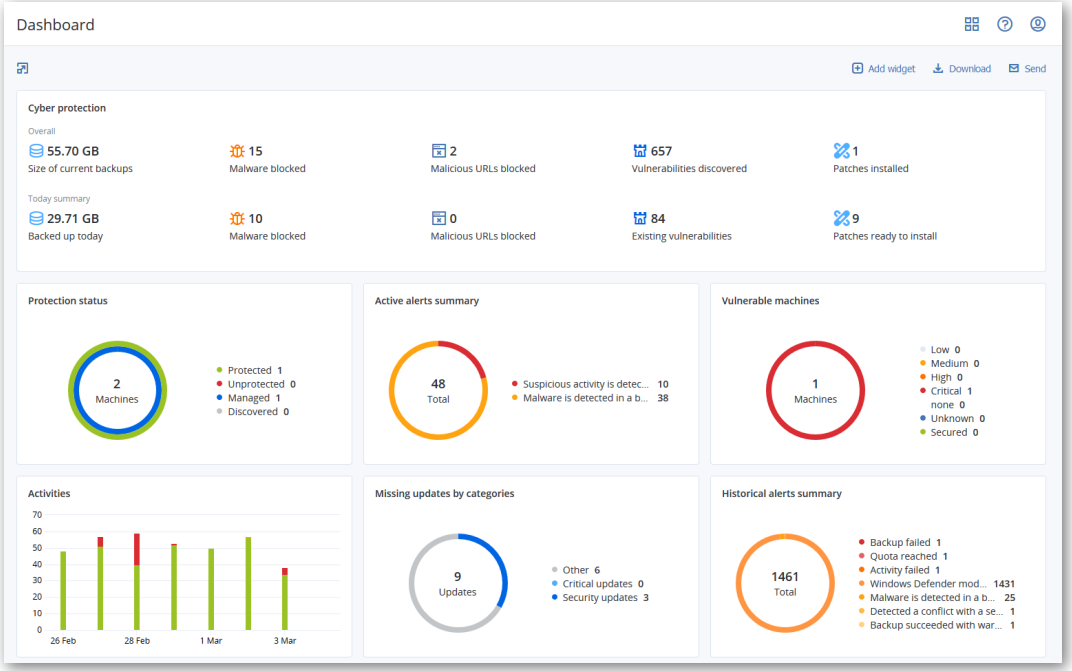


Acronis

Management / administration

Flexible monitoring and reporting

- Hardware health monitoring (HDD, SSD).
- Active alert control.
- Missing updates control.
- Customizable dashboard widgets.



Why

- Easily manage your data.
- Quickly identify any issues.
- Obtain actionable information.
- Get quick access to management actions.

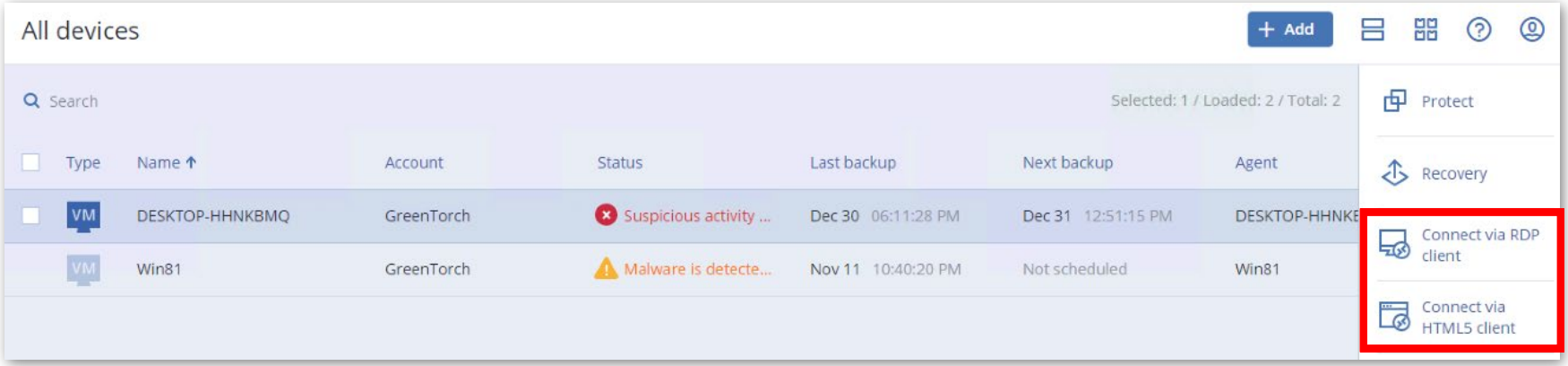
Remote desktop

Remotely operate any endpoint as if you are near the device.

- Assist remote users and avoid a gigantic waste of time.
- Reach systems that are sitting in a private network without changing firewall settings or establishing additional VPN tunnels by using outgoing connections (443 port).

Why

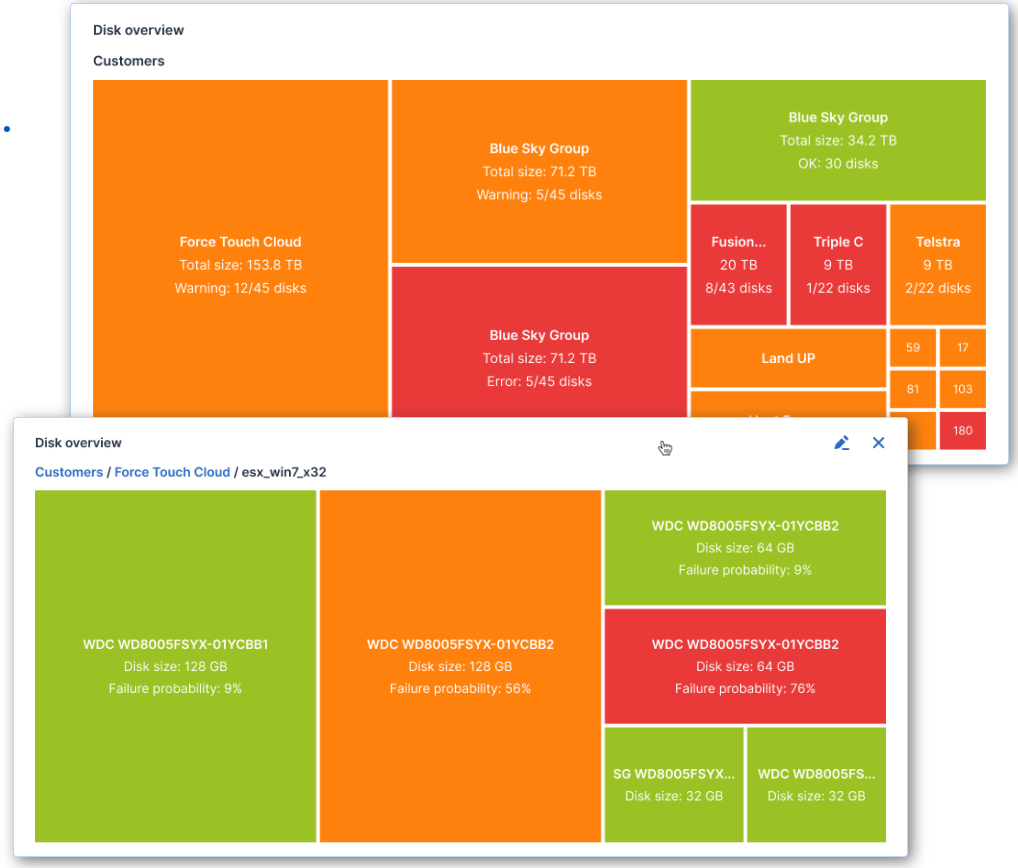
- Save time.
- Easily manage and access data.
- Solve issues quickly and easily.



Drive health monitoring

Know about a disk issue before it 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 allows 98.5% prediction accuracy (and we keep improving it).
- Once a drive alert is raised, you can take action; for example, back up critical files from the failing drive.



Why

- Easily detect potential failures.
- Avoid unpredictable data loss.
- Proactively improve uptime.
- Reduce risk of unexpected downtime.

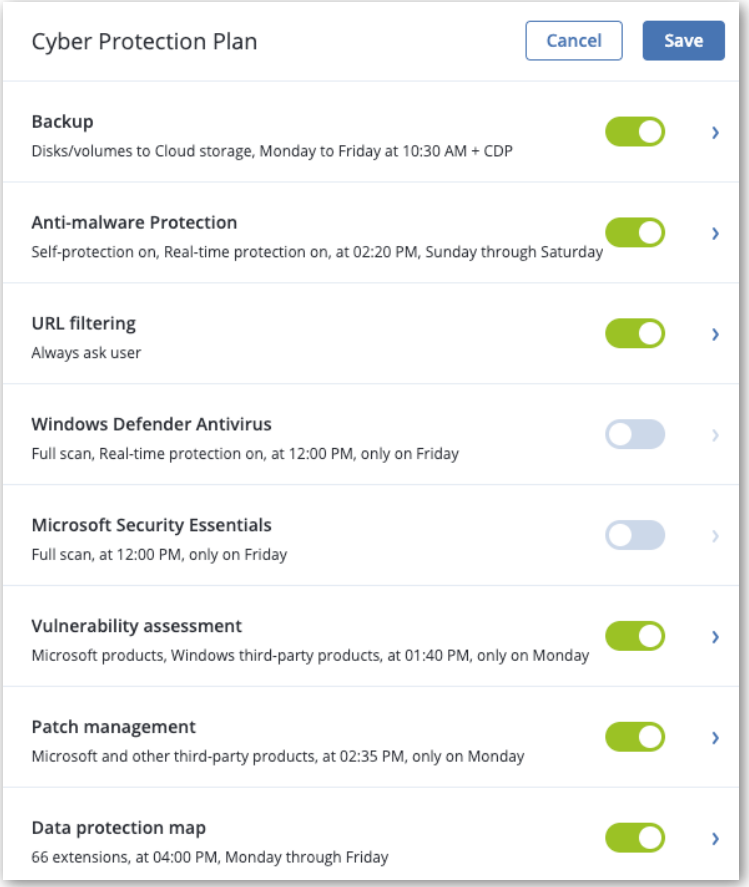
Single protection plan

Covers all aspects of cyber protection:

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

Why

- Streamline cyber protection management.
- Get an actionable, unified view.
- Save time and effort.



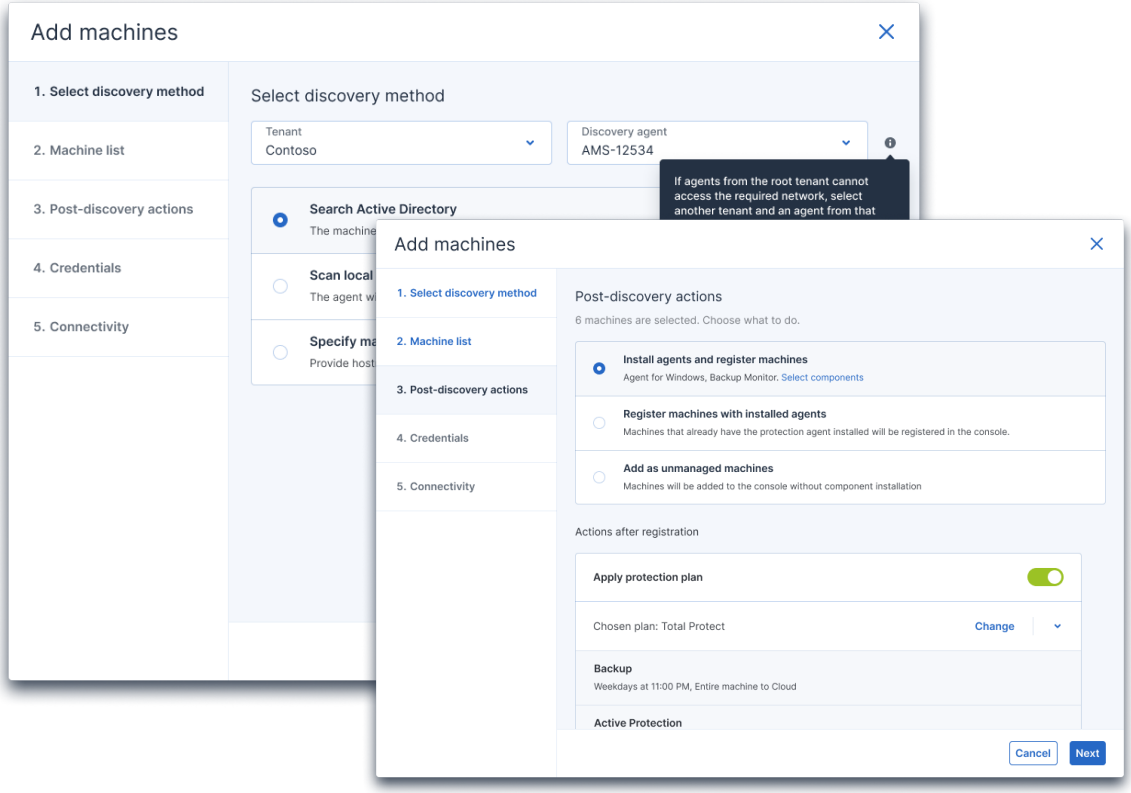
Device auto-discovery and remote agent installation

Simplify the process of installing multiple agents at once: 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 installation with a discovery wizard.

Why

- Simplify installation processes.
- Save time and resources.



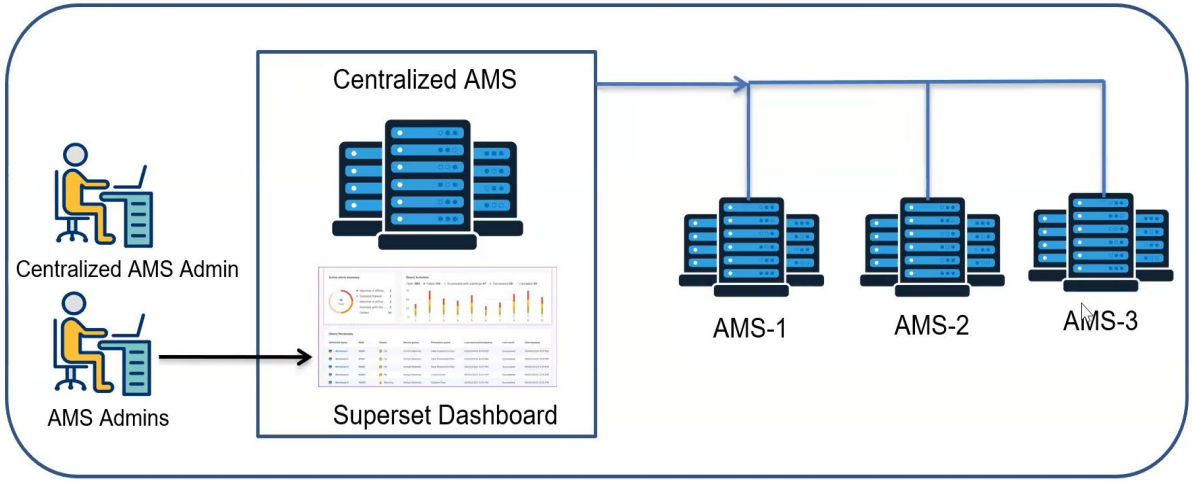
Centralized dashboard for multiple management servers

A single, consolidated view to monitor all management servers in an organization.

Simpler administration of thousands of devices for larger enterprises.

Widgets available:

- Devices
- Alerts
- Activities



On-premise deployment

Acronis

Acronis Cyber Protect editions and licensing

Acronis Cyber Protect editions

Acronis Cyber Protect is available in **three different editions**.

Knowing the difference between them is important; it enables you to tailor and differentiate your cyber protection offerings, while providing the functionality that best meets customers' needs and budget.

Acronis Cyber Protect editions	
Acronis Cyber Protect Standard	Provides complete data protection and cybersecurity for small and medium environments.
Acronis Cyber Protect Advanced	Provides advanced data protection and cybersecurity for large IT environments.
Acronis Cyber Protect Backup Advanced	Provides advanced data protection for large IT environments.

Available licenses

	Acronis Cyber Protect Standard	Acronis Cyber Protect Advanced	Acronis Cyber Protect Backup Advanced
Workstation	✓	✓	✓
Windows Server Essentials	✓	–	–
Server	✓	✓	✓
Virtual host	✓	✓	✓
Public cloud VM	✓	✓	✓
Universal license	–	✓	–
Microsoft 365	–	–	✓
Google Workspace	–	–	✓

✓ **Subscription** license is available both in **on-prem** and **cloud deployment** - License is not available

Free Acronis Cloud Storage per workload

- All Acronis Cyber Protect subscription licenses include **free cloud storage.**
- Free cloud storage is enabled automatically for any purchased license.
- Quota per license is defined in licensing configuration file, so update of the value will require data center update.
- **Free space** = Free_GB_per_licence * Number_of_licences_acquired.
- **Total space** = Paid space + free space
- The total space is visible in the web console UI (locations).
- The amount of free space per workload is shown in the Acronis Customer Portal.

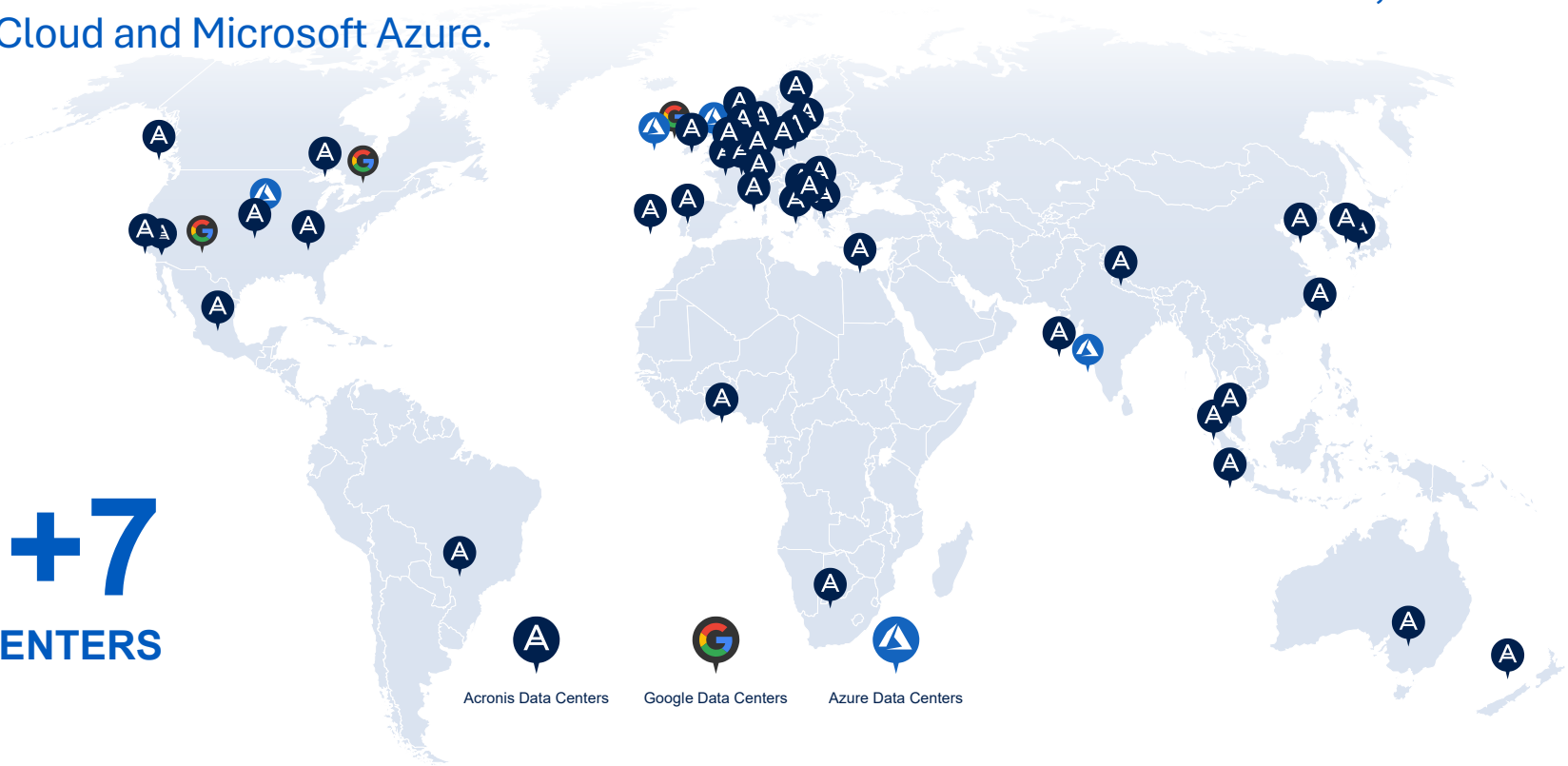
Licences	Free Cloud storage, GB
Acronis Cyber Protect Standard – Workstations	50
Acronis Cyber Protect Standard – Windows Server Essentials	150
Acronis Cyber Protect Standard – Servers	250
Acronis Cyber Protect Standard – Virtual hosts	250
Acronis Cyber Protect Standard – Public Cloud VMs (pack of 3)	40 per VM
Acronis Cyber Protect Advanced – Workstations	50
Acronis Cyber Protect Advanced – Servers	250
Acronis Cyber Protect Advanced – Virtual hosts	250
Acronis Cyber Protect Advanced – Public Cloud VMs (pack of 3)	40 per VM
Acronis Cyber Protect Advanced – Universal	250
Acronis Cyber Protect Backup Advanced – Workstations	50
Acronis Cyber Protect Backup Advanced – Servers	250
Acronis Cyber Protect Backup Advanced – Virtual hosts	250
Acronis Cyber Protect Backup Advanced – Public Cloud VMs (pack of 3)	40 per VM
Acronis Cyber Protect Backup Advanced – Universal	250

Acronis

Acronis expertise

Master data sovereignty

Choose to store data inhouse or utilize 54 data centers worldwide – Acronis Hosted, Google Cloud and Microsoft Azure.



47+7

DATA CENTERS

Acronis Cyber Protection Operation Centers

Stay alert with global threats monitoring 365/7/24

Top-level compliance
GDPR Art. 33, NIS Directive Art. 16 (4), Telecom Framework Directive Art. 13a, eIDAS regulation Art. 19

Up-to-date protection
Provides threat and vulnerability awareness, proactive detection, and the ability for Acronis to enhance products

Support and threat investigation
Advanced security experts help to speed up remediation and provide additional security services

Proven by the security experts

Tests, certifications, alliances and memberships.

- AV-Test certified and test winner
- AV-Comparatives approved business security product
- MRG Effitas participant and test winner
- ICSA Labs certified
- OPSWAT Platinum anti-malware certified
- M3AAWG member
- MVI member
- VIRUSTOTAL member
- Anti-Phishing Working Group member
- Anti-Malware Testing Standards Organization
- Cloud Security Alliance member
- GDPR compliant
- FIPS 140-2 certified cryptographic library
- ISO 27001:2013 certified information management
- PCI DSS compliant
- GLBA compliant
- HIPAA compliant
- SOC 2 Type 2 compliance

We believe that Acronis Cyber Protect is among the most comprehensive attempts to provide data protection and cyber security to date … Acronis shows potential to disrupt traditional IT security vendors by delivering integrated components for backup/recovery and malware detection and protection.

Phil Goodwin

Research Director, Cloud Data Management and Protection, IDC

Local recovery of computers controlling special-purpose industrial equipment

Minimizes costly downtime on automated factory floors, in oil and gas operations, and in pharma drug research and production.

Acronis partners and OEM

Power generation

Westinghouse

ABB System 800xA

OVATION

Oil / life sciences

YOKOGAWA

DELTAV

Honeywell EXPERION PKS Process Knowledge System

Manufacturing

Rockwell Automation

SIEMENS

Allen-Bradley

BOSCH

Proven compatibility with every major OT and ICS vendor

Acronis is a leader in cybersecurity and data protection for MSPs and IT departments

Swiss

Corporate HQ in Schaffhausen, Switzerland
Founded in Singapore in 2003

Global

1,800+ employees in 45 countries
Products in 26 languages

Cybersecurity

195+ million threats and 61+ million malicious emails blocked in 2023

20,000+

Service provider partners

750,000+

Business customers

54

Data centers worldwide

Acronis
Education

Grow your business with MSP Academy

Short modules.
Big impact.
Enroll today!