What’s New in Acronis Cyber Cloud 9.0
What’s New in Acronis Cyber Cloud 9.0

Groundbreaking, integrated, new service:
Acronis Cyber Protect Cloud

Plus

- New features in Acronis Cyber Backup Cloud
- Multiple Licensing Enhancements
Acronis Cyber Protect Cloud
Solution Overview
Acronis Cyber Protect

Backup and Recovery
Fast and reliable recovery of your apps, systems and data on any device from any incident

Anti-Malware
Next-generation, full-stack, AI/ML-based protection against malware, including ransomware and cryptominers

Security and Management
Comprehensive yet simple endpoint management toolkit, which saves IT resources

One solution integrates backup, disaster recovery, AI-based protection against malware and ransomware, remote desktop, and security tools in a single agent
## Acronis Cyber Protect: Key Features

You don’t need a zoo to cover all capabilities

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure and devices auto-discovery</td>
<td>Remote agent installation</td>
<td>Defenses against malware / ransomware</td>
<td>Patch management integrated with backup</td>
<td>Backup and Disaster Recovery</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>Backup and Disaster Recovery</td>
<td>Hard drive health control</td>
<td>Malware quarantine</td>
<td>Forensic information in backups</td>
</tr>
<tr>
<td>Data protection map</td>
<td>Unified protection policies management</td>
<td>Dashboards and reports</td>
<td>Rescue with bootable media</td>
<td>Remote desktop</td>
</tr>
</tbody>
</table>

Function areas are grouped according to the NIST Cybersecurity Framework
Overview of Key Features
One Protection Plan

Covers all cyber protection aspects:

- 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? Better protection with less effort, automated
Devices 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
- Importing a list of computers from the file
- Protection plan auto apply
- Batch remote installation of agents with a discovery wizard

Why? Easier and faster onboarding, less resources required, completeness of protection
Vulnerability Assessment and Patch Management

1. Scan for vulnerabilities
2. Prioritize vulnerabilities by severity (critical to low)
3. Implement dedicated patch cycles based on vendor releases and updates
4. When vulnerabilities are found, respond and remediate (install needed patches and updates)
Vulnerability Assessment and Patch Management

Key features:

- Continuous, daily updates of Acronis’ vulnerability and patch management database
- Local-network-traffic optimization, by using peer-to-peer update technology
- Patch testing and quality control with auto-approval capability
- Windows and Linux support
Vulnerability Assessment

Discover an issue before an issue happens

- Continuous, daily update of our own vulnerability and patch management database
- **Support for:**
  - Microsoft:
    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
  - Browsers and other software

**Why?** Mitigates potential threats, prevents attacks
Patch Management

Fix an issue before an issue happens
Large common vulnerabilities and exposures 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? Automationates protection, mitigates potential threats, prevents attacks (e.g. Equifax, WannaCry)
Significantly Extended Anti-Malware Capabilities

**Acronis Cyber Backup**
- Acronis Active Protection
  - Anti-ransomware, anti-cryptojacking, AI- and ML-enabled

**Acronis Cyber Protect**
- 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
Anti-Malware Protection

Full-stack anti-malware 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
• 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
Acronis Machine Learning Infrastructure

External Services
- New samples
- Services, storage

Acronis Labs
- Infected processes farm
  - Provides ransomware behavior data
- Clean processes farm
  - Provides clean processes behavior data

Acronis Cloud AI
- Updated knowledge base data
  - Model training, parameters optimization

Acronis KB

Customers
- Unknown events
URL Filtering Controls Access to Malicious URLs

URL filtering allows you to control access to internet websites by permitting or denying access to specific websites based on information contained in an URL list.

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

Why? Prevent attacks through malicious/hacked websites, gain better compliance and productivity
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? Windows Defender needs proper configuration, centralized management is complicated
Disk 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 allows 98.5% predictions accuracy (and we keep improving it)
- Once a drive alert is raised, you can take action, for example backup critical files from the failing drive

Why? Avoid unpredictable customer data loss, proactively improve uptime, differentiate yourself
Flexible Monitoring and Reporting

- Hardware health monitoring (HDD, SSD)
- Active alert control
- Missing updates control
- Customizable dashboard widgets
- Quickly identify problems
- Fast access to management actions

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

Also in Acronis Cyber Backup Cloud
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. It uses outgoing connections (443 port).

<table>
<thead>
<tr>
<th>All devices</th>
<th>+ Add</th>
<th>Protect</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Name</td>
<td>Account</td>
<td>Status</td>
</tr>
<tr>
<td>VM</td>
<td>DESKTOP-HHNKBMQ</td>
<td>GreenTorch</td>
<td>Suspicious activity...</td>
</tr>
<tr>
<td>VM</td>
<td>Win81</td>
<td>GreenTorch</td>
<td>Malware is detected...</td>
</tr>
</tbody>
</table>

Why? Fewer tools, less effort to connect, faster reaction
Remote Desktop

Administrator

Acronis Cyber Cloud
Connection broker

Endpoint
Upselling Cybersecurity Features Easily

Because partners can enable/disable the cybersecurity functionalities for Acronis Cyber Backup Cloud clients on a customer tenant level, they can easily show their customers the advantages Acronis Cyber Protect Cloud offers – or, what a simple upgrade includes.

The unique, integrated capabilities the new service offers are easily visible – and readily available – via the Cyber Protection Console (the features are labeled “CYBER PROTECT”).
New Welcome Wizard

During onboarding, give your prospects and existing customers an overview of the key capabilities of Acronis Cyber Protect Cloud and Acronis Cyber Backup Cloud.
API Clients

To boost security and convenience while accessing the Acronis Cyber Cloud API, the standard authentication mechanism (login and password) have been replaced with API clients. Now:

- Users can access publicly available APIs of Acronis Cyber Cloud, including:
  - Account Management API
  - Cyber Protection’s alert service API
  - File Sync and Share API
  - Notary API
- The API client is not tied to a user account
- The API client is compatible with 2-factor authentication (2FA)
- API client-management is available on all tenant levels (incl. partner and customer)
- All API client-related activities are recorded in the audit log

In 9.0, the API client has full-fledged administrator privileges for the specific tenant level it was created on. (We plan to add management privileges in the future as well).
Brand Management in Account Management APIv2

Some APIv1 methods do not have customization alternatives in Account Management APIv2 (e.g. Branding Management). Often this means partners looking to cover branding customization scenarios must use both APIv1 and APIv2 integrations.

Version 9.0 delivers these missing APIv2 Branding Management functionalities – including customization of color schemes, logo type, URLs, etc. – with the following endpoints now available:

- api/2/brands/{brand}
- api/2/tenants/{tenant_id}/brand
Integration Scenarios: Anti-Malware and Backup
Five Levels of Integration

Unique cyber protection capabilities are enabled by integration

One integrated solution:
- Eliminates complexity
- Delivers new security capabilities
- Keeps costs down
- Improves uptime

☑ One license
☑ One user interface
☑ One management console
☑ One shared information about protected system
☑ One data destination
Innovative Data Protection Scenarios

Next-gen Continuous Data Protection: Avert even the smallest data loss in key apps

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 backup to current CPOC alarms

Forensic backup: Image-based backup with valuable, additional data in backups

Better protection with less resources: Offload and enable more aggressive scans and vulnerability assessments in central storage, including cloud

Fail-safe patching: Automatically backup endpoints before installing any patches to roll-back immediately

Global and local whitelists from backups support more aggressive heuristics by preventing false detections
1. Continuous Data Protection

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

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

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

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

Why? Protects customer data even between backups
2. Safe Recovery

Integration of AV updates and patch management into recovery process

A backed-up OS image can have malware that can reinfect a machine after recovery.

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

Why? Saves time, efforts and data: recover infected/vulnerable images quickly with no efforts
Safe Recovery

Restores from infected backups

Other Vendors

Safe recovery – look for malware in Acronis Cyber Cloud, and remove found malware during recovery

Any malware found is deleted, so machine can't be re-infected
3. Anti-Malware Scanning of Backups in the Acronis Cloud

Prevent restoring infected files from backups

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

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

Why? Better protection with less effort and resources: offload endpoints, more aggressive scans
4. Smart Protection Plan

Use Acronis’ Cyber Protection Operations Center (CPOC) alerts to mitigate risks from upcoming/existing threats

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.

- Minimize business downtime when facing issues like a malware epidemic, natural disaster, etc.
- Reduce reaction times and avoid data loss

Why? Faster reaction, prevention of downtime and data loss
5. 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.

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

Why? Saves resources, faster and more reliable operations
6. Include Backup Information for Forensic Investigation

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.

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

Why? Enables investigation, better compliance
7. 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.

- 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 the basis for compliance reports

Why? Complete protection that’s easy, with no important data missed
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”.

- Eliminates time-consuming manual whitelisting of unique apps
- Improves detection rate via improved heuristics
- Supports manual whitelisting

Why? “False positives” can prevent access to data or apps. Automation saves time, improves protection
Acronis Cyber Cloud 9.0: Changes in Licensing
New Service – Three Editions

**Acronis Cyber Cloud 8.0**
- Acronis Cyber Backup Cloud
  - Standard edition
  - Advanced edition
  - Disaster Recovery edition
- Acronis Cyber Files Cloud
- Acronis Cyber Notary Cloud

**Acronis Cyber Cloud 9.0**
- Acronis Cyber Backup Cloud
  - Standard edition
  - Advanced edition
  - Disaster Recovery edition
- Acronis Cyber Protect Cloud NEW
  - Standard edition
  - Advanced edition
  - Disaster Recovery edition
- Acronis Cyber Files Cloud
- Acronis Cyber Notary Cloud
Acronis Cyber Protect Cloud Editions Overview

**Standard**
Includes all features in the Acronis Cyber Backup Cloud Standard edition, plus advanced cybersecurity functionality in Acronis Cyber Protect Cloud

**Advanced**
Includes all features in the Standard edition, plus several “advanced” features for scalable management of larger infrastructures and support for additional workloads

**Disaster Recovery**
Includes all features in the Advanced edition, plus all available features in Acronis Cyber Disaster Recovery Cloud

Both per-GB and per-device models are available.
## Editions – New Features

<table>
<thead>
<tr>
<th>New Features</th>
<th>Acronis Cyber Backup Cloud</th>
<th>Acronis Cyber Protect Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standard</td>
<td>Advanced</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>▪ Basic auto-discovery and remote agent installation</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Advanced auto-discovery and remote agent installation</td>
<td>❌</td>
<td>✔️</td>
</tr>
<tr>
<td>Patch management</td>
<td>❌</td>
<td>✔️</td>
</tr>
<tr>
<td>▪ Anti-malware protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ URL filtering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Continuous data protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Anti-malware scanning of backups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Safe recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Safe patching</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>▪ Smart protection plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Windows Defender Antivirus and Microsoft Security Essentials management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Drive health monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Remote desktop</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Forensic data backup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Data protection map</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Acronis 2020
Meeting Customer Cyber Protection and Solution Scalability Requirements

<table>
<thead>
<tr>
<th></th>
<th>Small Business</th>
<th>Medium Business, Enterprise, and Partners</th>
<th>High RTO/RPO requirements</th>
</tr>
</thead>
</table>

Completeness of protection

Infrastructure size and RTO/RPO requirements
Acronis
Cyber Foundation
Building a more knowledgeable future

CREATE, SPREAD AND PROTECT KNOWLEDGE WITH US!

www.acronis.org

Building new schools • Providing educational programs • Publishing books