

Acronis

#CyberFit

Acronis Cyber Protect

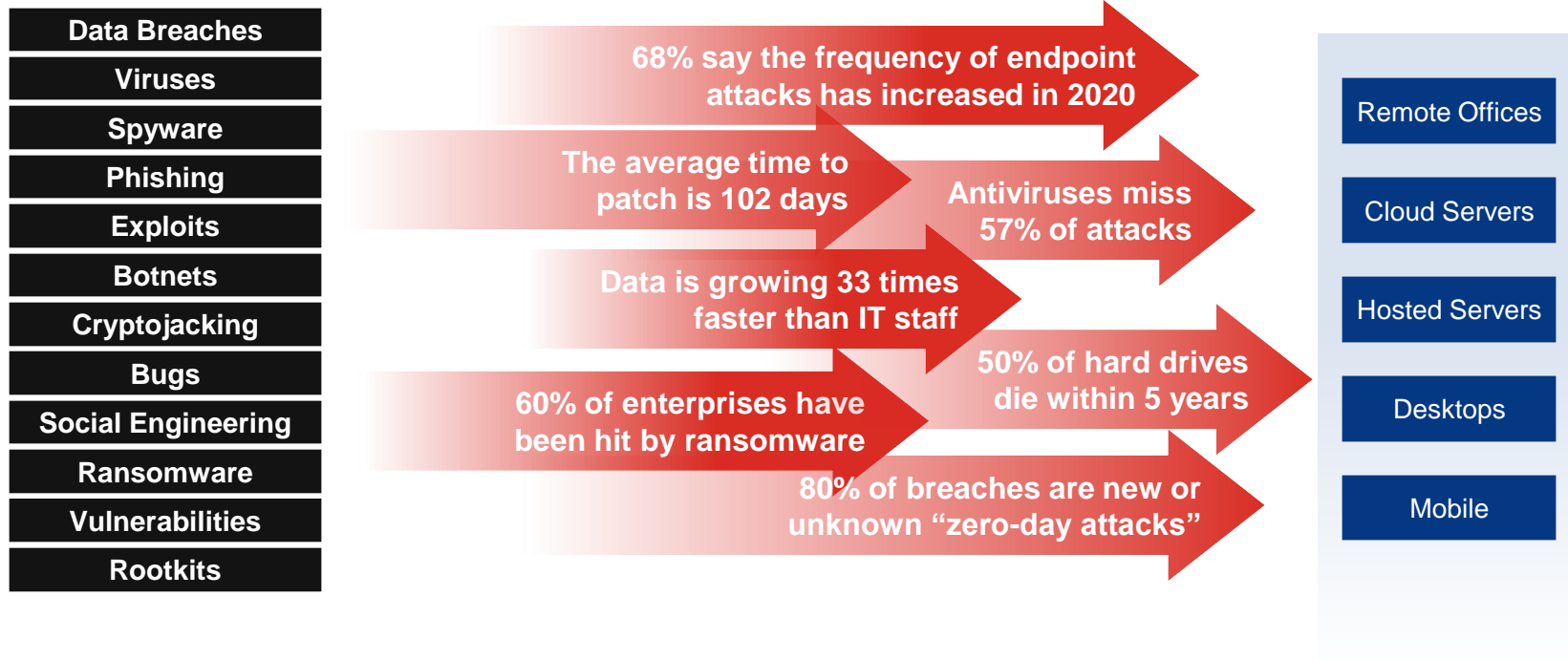
Modernize Your Cybersecurity and Backup
with Integrated Cyber Protection



Dual headquarters
in Switzerland and Singapore

Endpoints and Edge Devices are Under Attack

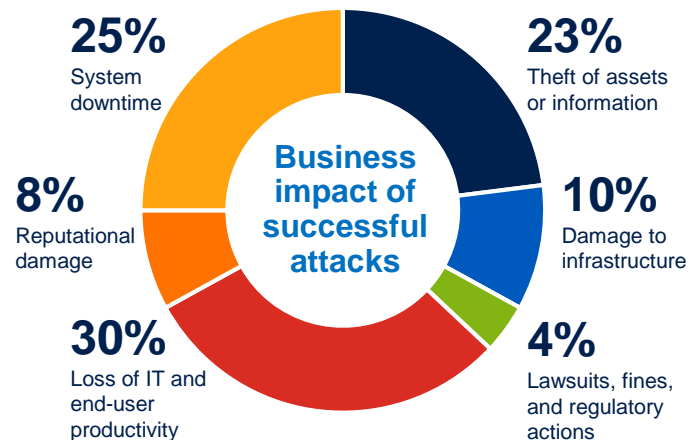
Data amounts are growing fast. It's not as secure as corporate data centers.



Sources: The State of Endpoint Security Risk, Emerson Network Power-sponsored study by the Ponemon Institute, PWC US CEO Survey, The Annual Study of the State of Endpoint Security Risk, Ponemon Institute, 2020

Every Business is Under Attack

- **66%** of the world's SMBs are now experiencing cyberattacks
- **45%** still feel their security posture is ineffective
- **69%** lost some sort of sensitive information
- **39%** still don't have an incident response plan in place



**Each successful attack costs
\$7.1 million for a large organization,
or an average of \$301 per employee or \$440
per endpoint**

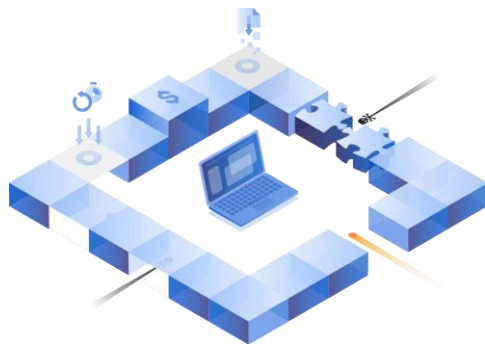
Staying Protected is Complex

Relying on too many protection tools is complex, expensive, and ineffective

More tools add complexity

- 69% report that IT currently spends more time managing security tools than effectively defending against threats
- 71% are adding security tools faster than they are adding the capacity to productively use them

Complex



Companies are buying more and more security tools

- 70% of businesses have invested in more than five technologies in the last year alone

Expensive

Management burden compromises security

- 60% admit most of their security tools are underutilized
- 53% admit that the number of security tools is so burdensome that it adversely impacts security and increases risk

Ineffective

Source: Reliaquest Security Tech Report

Acronis Cyber Protect



Next-generation cybersecurity

Advanced AI-based behavioral detection engine for zero-day attack prevention



Reliable backup and recovery

Full-image and file-level backup, disaster recovery, and metadata collection for security forensics



Enterprise protection management

URL filtering, vulnerability assessments, patch management, remote management, drive health



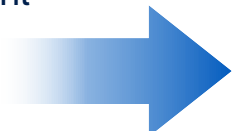
Integration provides unmatched manageability for IT managers – increasing security and productivity while decreasing operating costs

Acronis Cyber Protect Benefits

Eliminate Complexity

- ✗ The traditional stack of endpoint protection products lacks integration and requires much more time for management – maintaining licenses, installing updates and patches, verifying compatibility after updates, and managing multiple policies using a variety of different user interfaces.

- ✓ **Acronis Cyber Protect offers one agent, one management interface, and one license** – removing the complexity and risks associated with non-integrated solutions.



Customer Value:

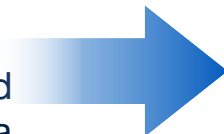
- ✓ Easily manage all protection aspects via a single pane of glass
- ✓ Eliminate performance and compatibility issues
- ✓ Quickly and easily identify and fix issues
- ✓ Save time and hassle associated with managing multiple vendors

Minimize Incidents

- ✗ Traditional antivirus and backup solutions are can't stop modern cyberthreats.

With Acronis Cyber Protect, an AI-based threat detection engine leverages backup data to **improve detection rates and avoid false-positives.**

The integration of advanced antimalware and backup allows the recovery of corrupt data automatically. Backups are protected against attacks on the agent and backup files, ensuring data is clean.



Customer Value:

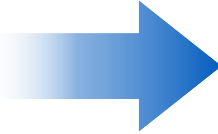
- ✓ Proactively avoid costly downtime
- ✓ Keep your systems up and running
- ✓ Respond to incidents quickly and efficiently
- ✓ Block ransomware attacks before they happen
- ✓ Allow employees to work safely
- ✓ Inspire customer confidence and trust

Increase Productivity

✗ A complex, non-integrated stack of endpoint solutions requires more time to learn and support, and does not offer the benefits of integration and automation.

✓ Unifying multiple protection technologies into one solution not only increases its reliability, it also decreases the time needed to learn, deploy, and maintain the solution.

With Acronis Cyber Protect, you get one integrated solution that delivers complete protection from today's threats – enabling you to streamline management, cut unnecessary administrative time, and reduce TCO.



Customer Value:

- ✓ Streamline protection management
- ✓ Cut unnecessary administrative time
- ✓ Avoid new expenses
- ✓ Manage all aspects of cyber protection with ease
- ✓ Reduce TCO

Need Backup? Upgrade to Acronis Cyber Protect

Superior Backup: The most secure, easy, and reliable backup for businesses

Proactive Protection

- Vulnerability assessments 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 and RPO
- Metadata storage for forensics and investigation of incidents

Productivity Improvements

- Maximum number of workloads protected per support engineer
- Integrated remote management for quick access to protected workloads
- Pre-configured protection plans for remote workers

Need Security? Move to Acronis Cyber Protect

Unique Capabilities: The most complete cyber protection for businesses

Protection

- Protection for collaboration applications – Zoom, WebEx, Microsoft Teams
- AI-based hard-drive failure prediction

Security

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

Performance

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

Productivity Benefits

- Data protection map to discover and protect important data
- RDP connection to corporate devices for end-customers

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



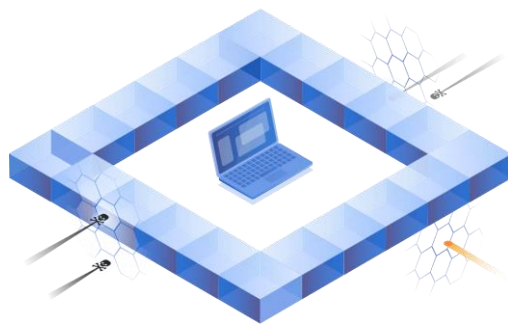
Data Protection Map:

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



Fail-safe Patching:

Automatically back up endpoints before installing any patches to roll-back immediately



Safe Endpoint Recovery:

Integrate antimalware updates and patches into the recovery process



Better Protection with Fewer Resources:

Offload and enable more aggressive scans and vulnerability assessments in central storage, including the cloud



Smart Protection Plan: Auto-adjust patching, scanning, and backup to current CPOC alarms



Global and Local Whitelists:

Built from backups to support more aggressive heuristics and 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, frequently used apps for every device. Acronis' agent monitors every change made in the listed applications.

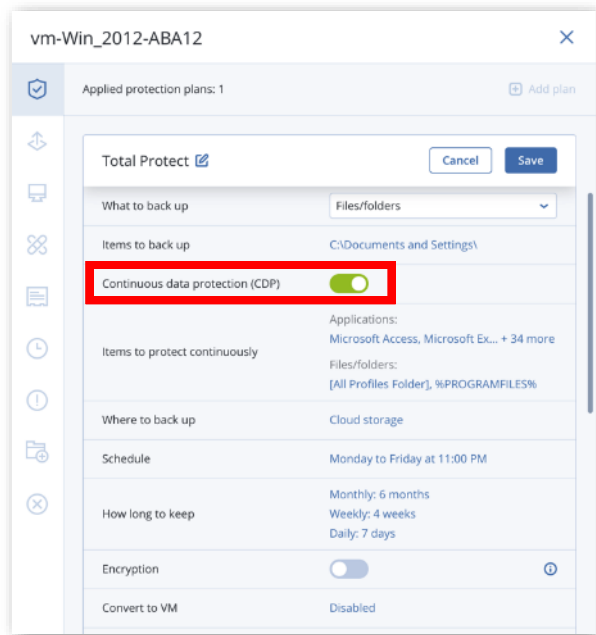
In the event of a malware infection, you can restore the data from the last backup and apply the latest collected changes so no data is lost.

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



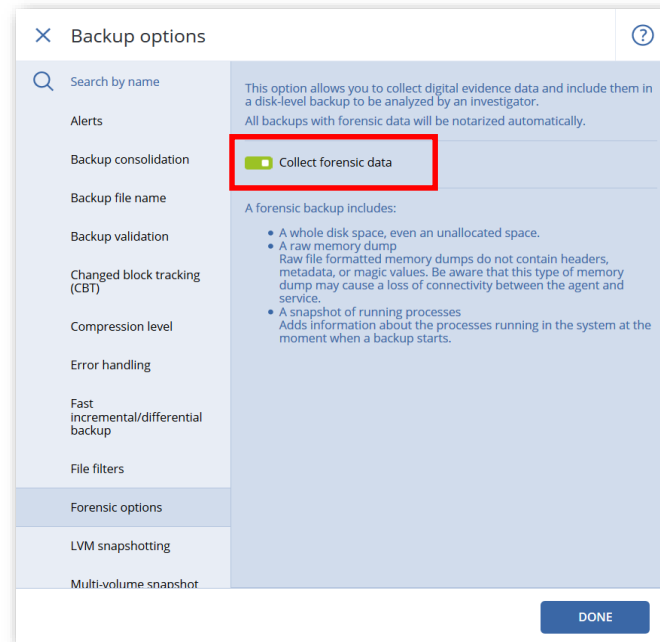
2. Include Backup Information for Forensic Investigation

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.

! Why

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

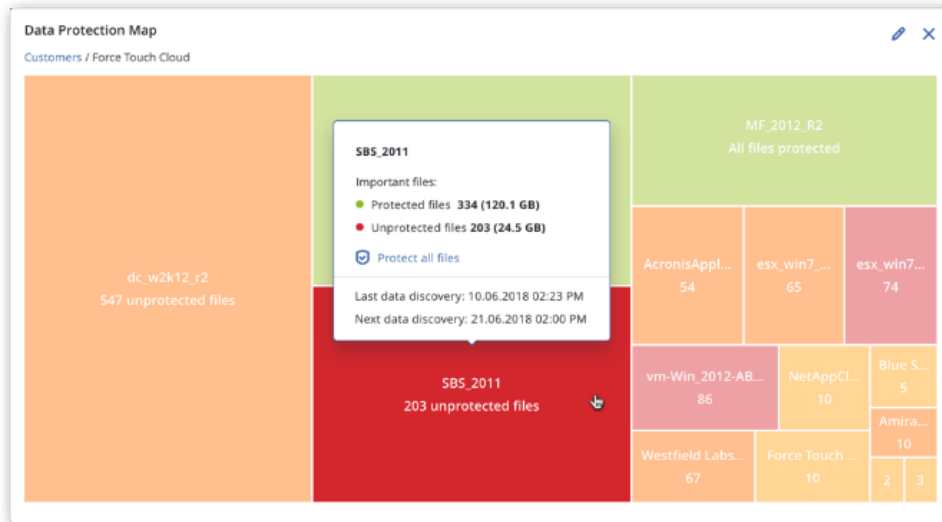


3. Data Compliance Reporting and Data Protection Map

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



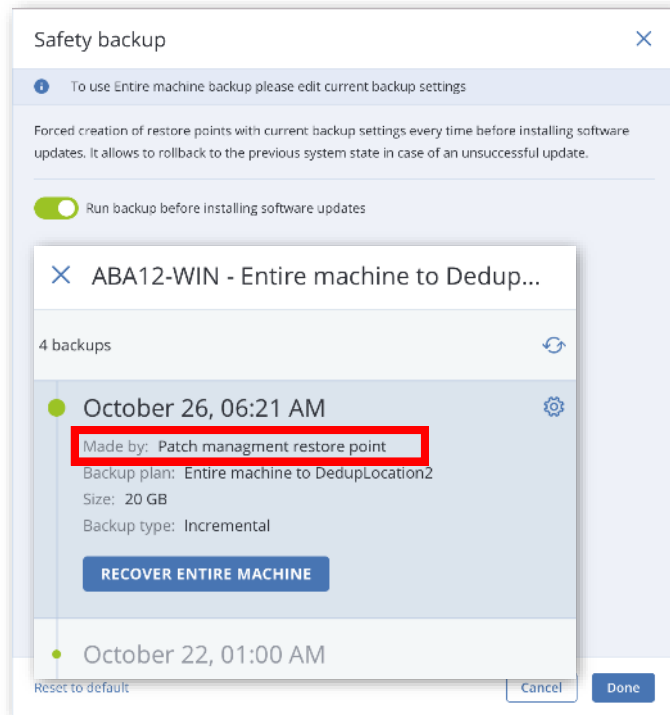
4. Fail-safe Patching

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



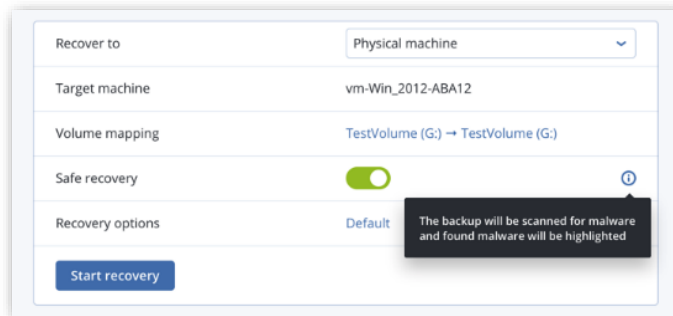
5. Safe Recovery

Integration of AV updates and patch management into the recovery process

The OS image or applications in the backup can have vulnerabilities.

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

- Updates the antimalware database
- Installs the latest security patches



! Why

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

6. Malware Scan in Centralized Locations

Antimalware 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

The screenshot displays the Acronis Backup software interface. The top window, titled 'Details', shows the configuration for a 'New scanning plan'. The settings are as follows:

Property	Value
Scan type	Cloud
Backups to scan	2 backups
Scan for	Malware
Schedule	Monday to Friday at 11:00 PM
Backup password	On

The bottom window shows a table of scanned backups:

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

A notification box on the right states: 'The 'New scanning plan' plan was created'.

7. Smart Protection Plan

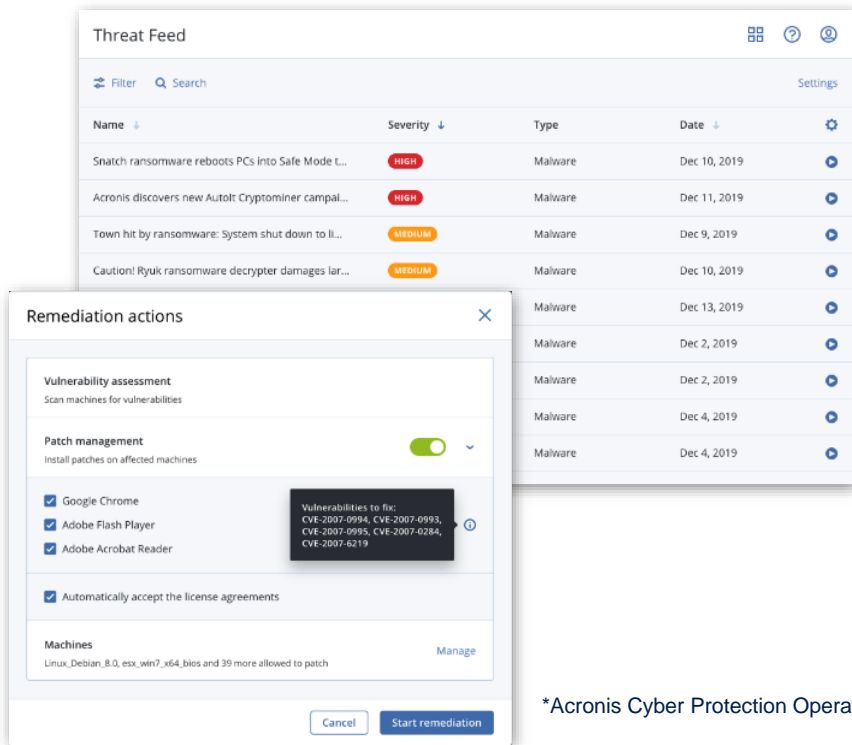
Ensure your protection is up to date

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



*Acronis Cyber Protection Operation Centers

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

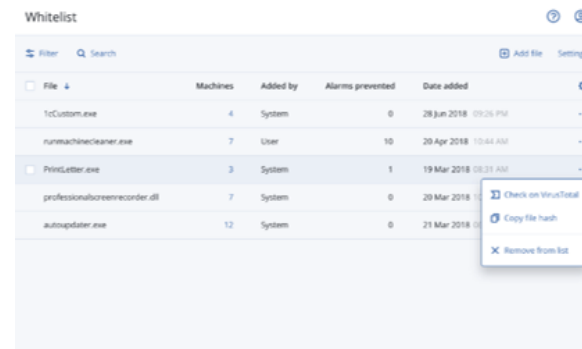
Improved detection rates may lead to more false positive alerts. Traditional, global whitelisting does not support custom applications.

Acronis Cyber Protect scans backups with antimalware 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



The screenshot shows the 'Whitelist' interface with a table of whitelisted applications. The table has columns for File, Machines, Added by, Alarms prevented, and Date added. A context menu is open for 'PrintLetter.exe', showing options: 'Check on VirusTotal', 'Copy file hash', and 'Remove from list'.

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

Top Use-Cases for Acronis Cyber Protect

- **Remote work protection.** Protect remote workers with multiple remote work protection capabilities – remote wipe, protection for remote work tools, remote connection, and others.
- **Simplified administration.** Discover all devices that require protection and remotely install just one agent – instead of many – for antimalware, backup, remote desktop, patch management, etc.
- **Zero-day malware and ransomware protection.** The industry-leading, AI-based Acronis Active Protection has been extended with a static analyzer and behavioral analysis.
- **Compliance and forensic investigations.** The right solution for strict compliance requirements – Acronis equips you with image-based backup and forensic data like free space and memory dump.
- **Post malware-attack recovery.** Lower your risk of reinfection and ensure fewer operations with antimalware 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.
- **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 antimalware scans, based on real-time alerts from Acronis Cyber Protection Operation Centers.
- **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, plus real-time improved Acronis Active Protection.

Key Features Overview

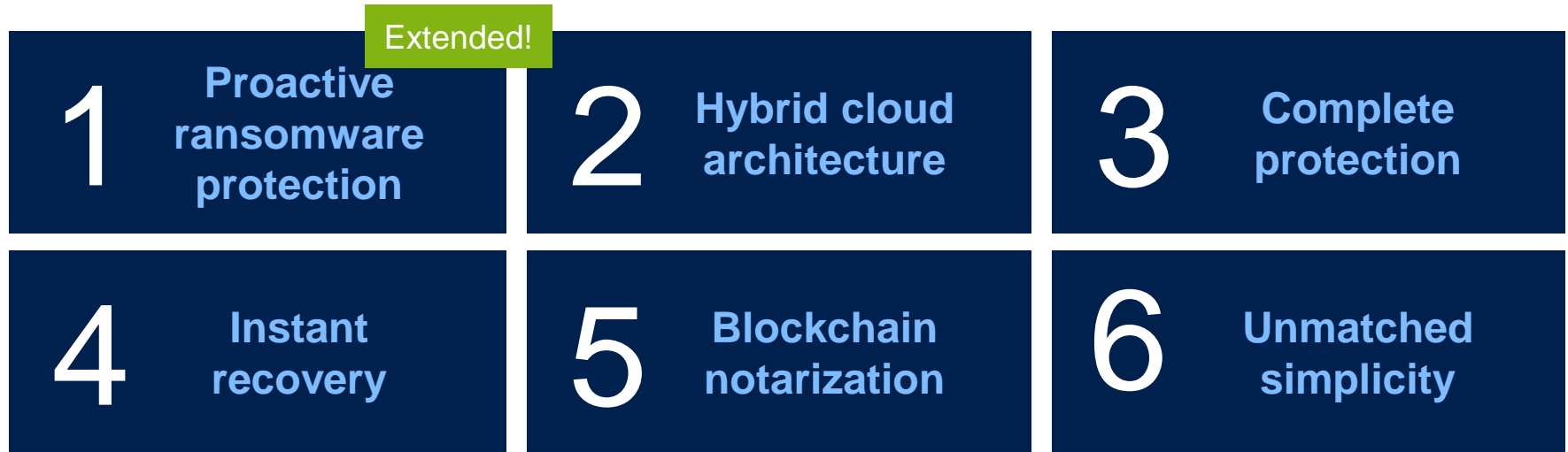
Acronis Cyber Protect: Key Features

Identify	Protect	Detect	Respond	Recover
Infrastructure and device auto-discovery	Remote agent installation	Defenses against malware and exploits	Patch management integrated with backup	Backup and disaster recovery
Vulnerability assessments	Backup and disaster recovery	Hard drive health control	Malware quarantine	Forensic information in backups
Data protection map	Unified protection policy management	Dashboards and reports	Rescue with bootable media	Remote desktop

Function areas are grouped according to the NIST Cybersecurity Framework

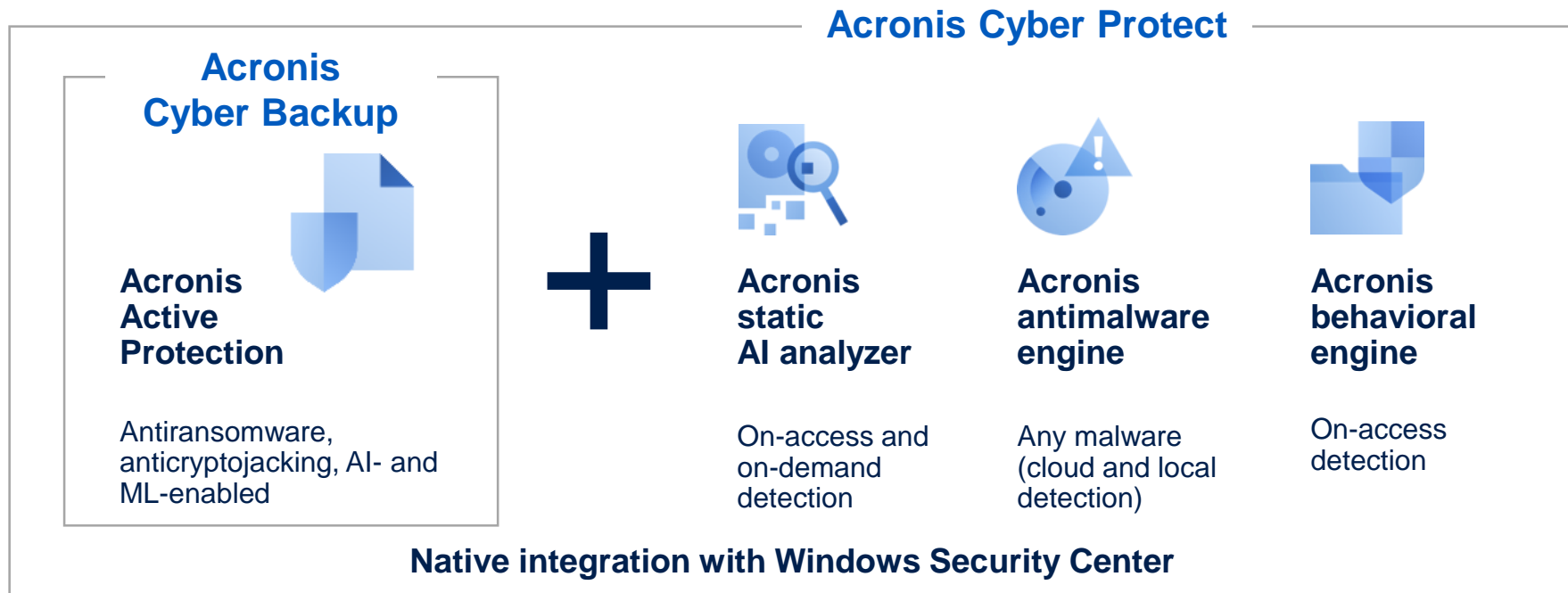


Includes All Acronis Cyber Backup Advantages



Why? Faster recovery, better RTOs

Significantly Extended Antimalware Capabilities



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


Antimalware 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; 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

Protection plan  Cancel Save


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

 **Malware is detected and blocked (RTP)**

Real-time anti-malware protection has detected and blocked malware.

Device	Win81
Plan name	Protection plan. 1
File name	tmp0000004b
File path	C:\Windows\Temp

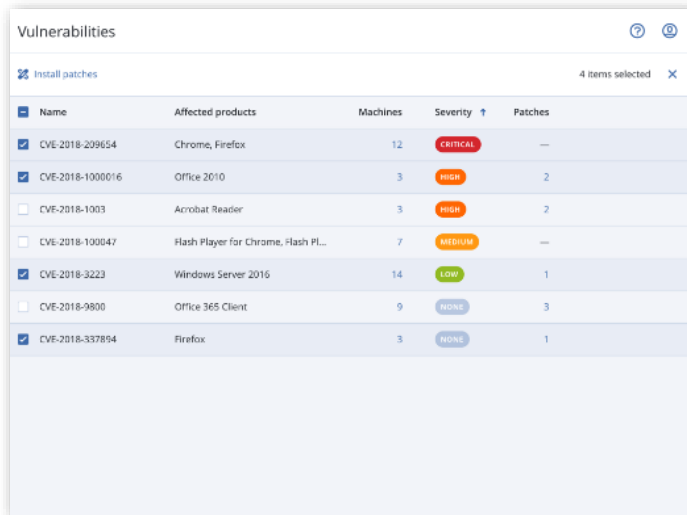
Vulnerability Assessment

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



The screenshot shows the 'Vulnerabilities' section of the Acronis console. It features a table with the following data:

<input checked="" type="checkbox"/>	Name	Affected products	Machines	Severity ↑	Patches
<input checked="" type="checkbox"/>	CVE-2018-209654	Chrome, Firefox	12	CRITICAL	—
<input checked="" type="checkbox"/>	CVE-2018-1000016	Office 2010	3	HIGH	2
<input type="checkbox"/>	CVE-2018-1003	Acrobat Reader	3	HIGH	2
<input type="checkbox"/>	CVE-2018-100047	Flash Player for Chrome, Flash PL...	7	MEDIUM	—
<input checked="" type="checkbox"/>	CVE-2018-3223	Windows Server 2016	14	LOW	1
<input type="checkbox"/>	CVE-2018-9800	Office 365 Client	9	MEDIUM	3
<input checked="" type="checkbox"/>	CVE-2018-337894	Firefox	3	MEDIUM	1

Patch Management

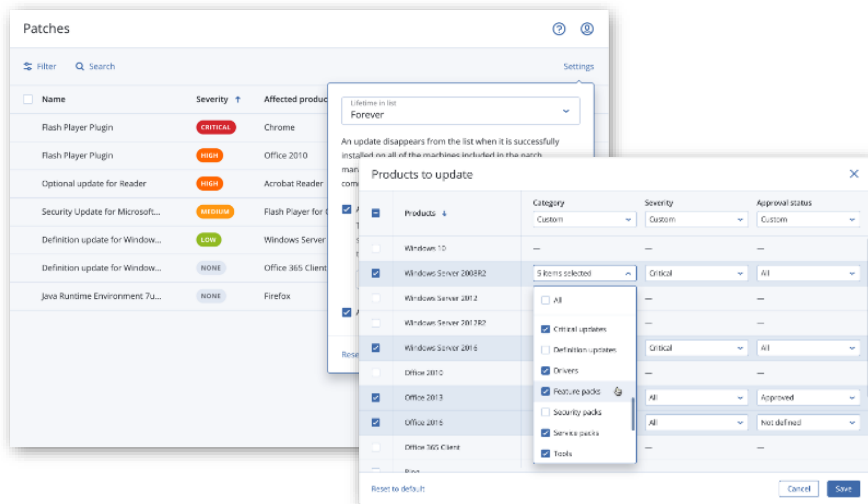
Fix an issue before it happens

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

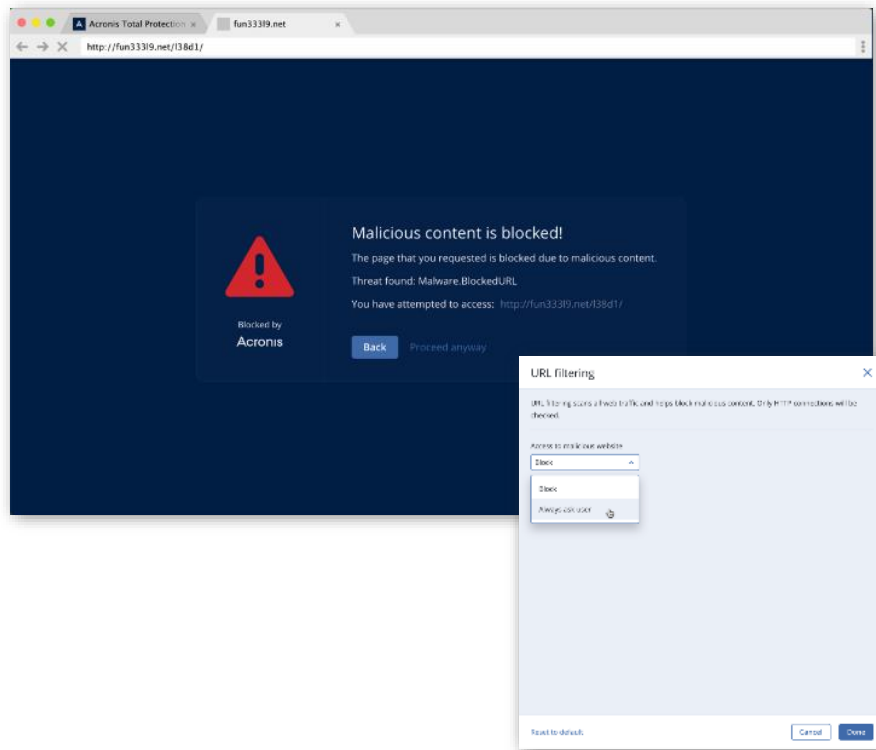
- HTTP/HTTPS interceptor
- Black/whitelists for URLs
- Payload analysis for malicious URLs

Acronis URL Filtering List:

- Acronis' own signatures
- AI-based detection

Why?

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

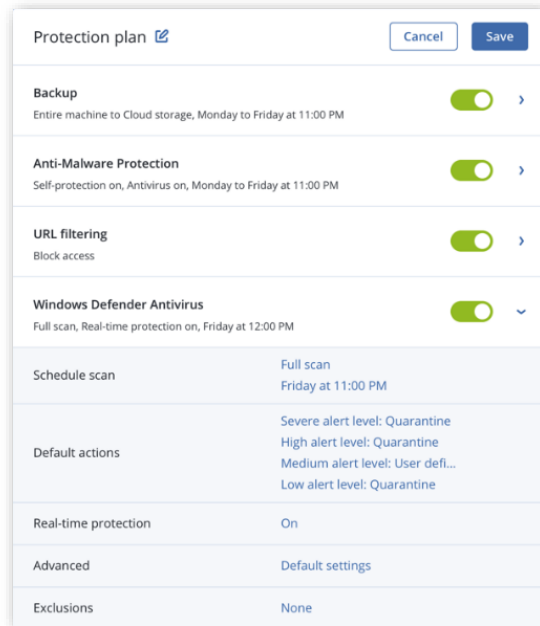


Windows Defender Antivirus or Microsoft Security Essentials Management

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

Why?

- Streamline management
- Save time and effort



The screenshot shows the 'Protection plan' settings for Windows Defender Antivirus. It includes a 'Cancel' button and a 'Save' button. The settings are as follows:

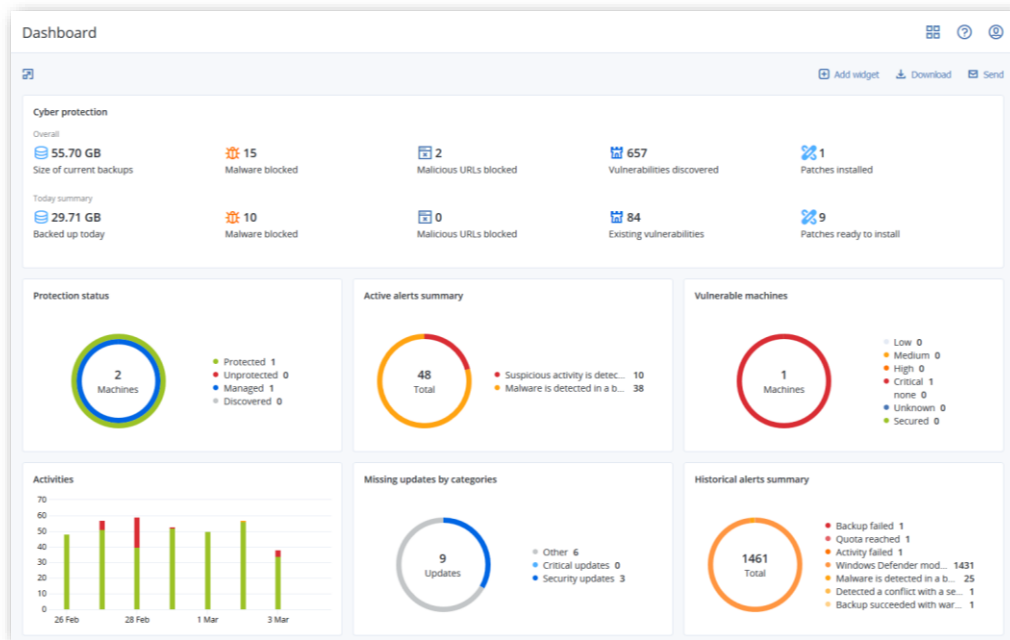
Setting	Value
Backup	Entire machine to Cloud storage, Monday to Friday at 11:00 PM
Anti-Malware Protection	Self-protection on, Antivirus on, Monday to Friday at 11:00 PM
URL filtering	Block access
Windows Defender Antivirus	Full scan, Real-time protection on, Friday at 12:00 PM
Schedule scan	Full scan Friday at 11:00 PM
Default actions	Severe alert level: Quarantine High alert level: Quarantine Medium alert level: User defi... Low alert level: Quarantine
Real-time protection	On
Advanced	Default settings
Exclusions	None

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

All devices + Add ≡ ⌘ ? 👤

Search Selected: 1 / Loaded: 2 / Total: 2

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

🛡️ Protect
↕ Recovery
🖥️ Connect via RDP client
🌐 Connect via HTML5 client

Single Protection Plan

Covers all aspects of cyber protection:

- Backup
- Antimalware 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

Cyber Protection Plan

Cancel

Save

Backup Disks/volumes to Cloud storage, Monday to Friday at 10:30 AM + CDP	<div><div></div></div>	>
Anti-malware Protection Self-protection on, Real-time protection on, at 02:20 PM, Sunday through Saturday	<div><div></div></div>	>
URL filtering Always ask user	<div><div></div></div>	>
Windows Defender Antivirus Full scan, Real-time protection on, at 12:00 PM, only on Friday	<div><div></div></div>	>
Microsoft Security Essentials Full scan, at 12:00 PM, only on Friday	<div><div></div></div>	>
Vulnerability assessment Microsoft products, Windows third-party products, at 01:40 PM, only on Monday	<div><div></div></div>	>
Patch management Microsoft and other third-party products, at 02:35 PM, only on Monday	<div><div></div></div>	>
Data protection map 66 extensions, at 04:00 PM, Monday through Friday	<div><div></div></div>	>

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

The screenshot displays the 'Add machines' wizard in Acronis software. The 'Select discovery method' step is active, showing three options: 'Search Active Directory' (selected), 'Scan local network', and 'Specify manually or import from file'. A tooltip message states: 'If the discovery agent cannot access some machines due to the network topology, select an agent that has'. The 'Post-discovery actions' step is also visible, showing options to 'Install agents and register machines', 'Register machines with installed agents', and 'Add as unmanaged machines'. The 'Actions after registration' section shows the 'Apply protection plan' toggle is turned on, with a chosen plan of 'Total Protect'. The 'Backup' section shows 'Weekdays at 11:00 PM. Entire machine to Cloud'. The 'Active Protection' section shows 'Notify only. Self-protection on'. The 'Back' and 'Next' buttons are at the bottom right.

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



Tape multiplexing and multistreaming

Maximize the effective use of tape drives during backup and recovery

- **Multiplexing:** allows **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:** allows 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

Full-Image and File-Level Backup

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

- **File-level backup:** use this option to protect specific data, reduce backup size, and save storage space
- **Full-image backup:** easily back up the entire system as a single file, ensuring a bare metal restore
- 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

Create protection plan



New protection plan (1)

Cancel>Create

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

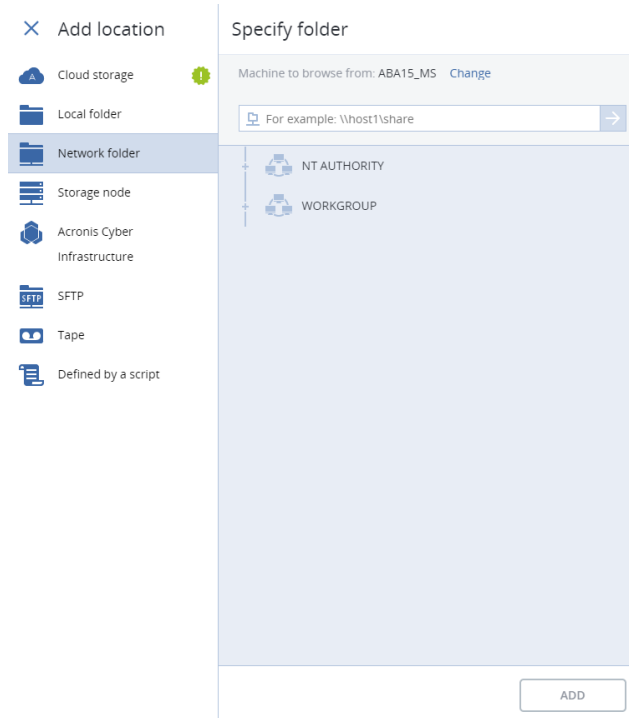
Change

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:

- Disk
- Tape
- NAS
- SAN
- Partner Cloud
- Private Cloud
- Acronis Cloud
- Public cloud (Azure, AWS Google)



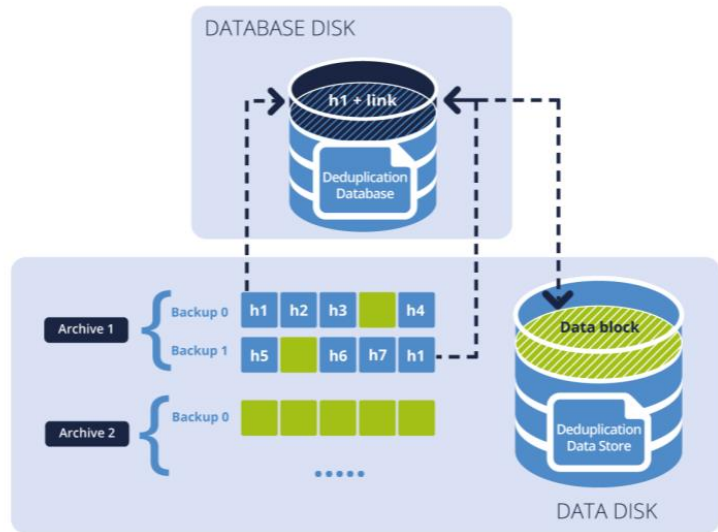
Deduplication

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



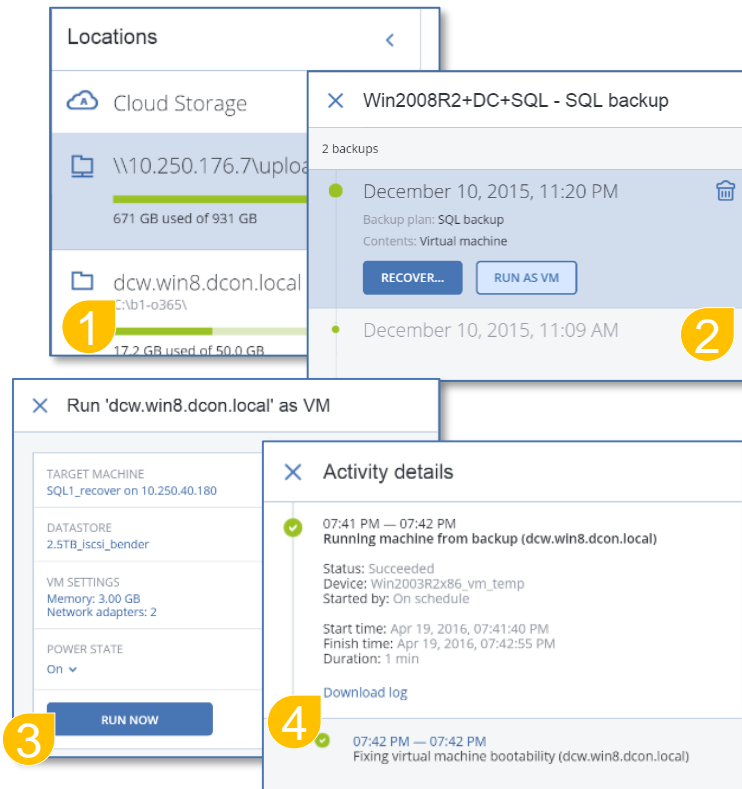
Acronis Instant Restore

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



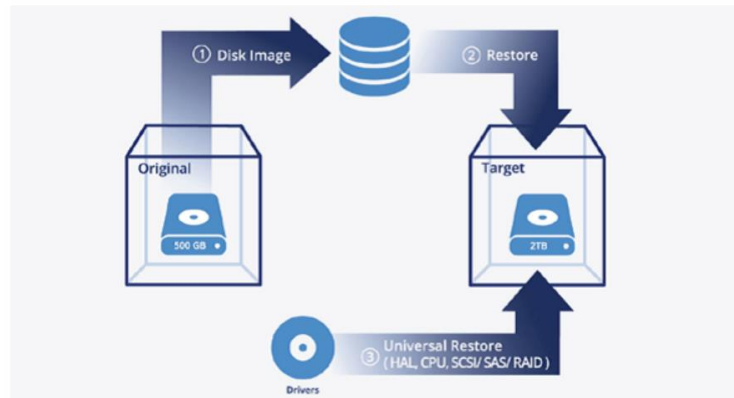
Acronis Universal Restore

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/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

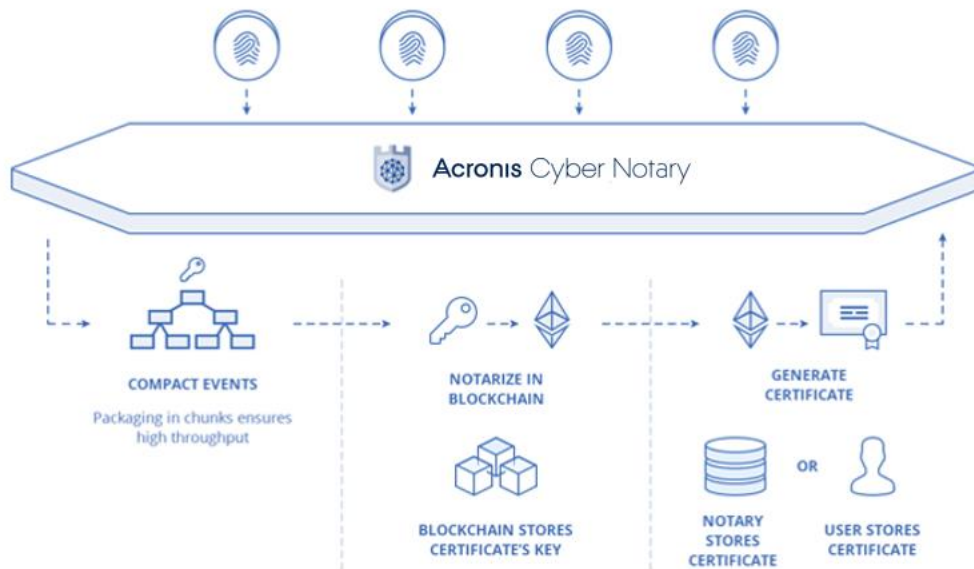
Blockchain Notarization

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

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

Why?

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



Complete Microsoft 365 protection



**Backup for
Microsoft
Exchange Online**



**Backup for
Microsoft OneDrive
for Business**



**Backup for
Microsoft SharePoint
Online**



**Backup for
Microsoft Teams**
Including call protection

- Back up from Microsoft data centers directly to cloud storage
- Automatically protect new Microsoft 365 users, groups, and sites
- Search through Microsoft 365 backups to get quick access to your backed-up data
 - Support for Microsoft 365 data centers in Germany

20+ Platforms Protected

Backup that outpaces technology: new platforms with every release



Remote Work Support Anti-Pandemic Features

Remote Work and Anti-Epidemic Features

Acronis Cyber Protect

- Easy Remote Desktop access from Windows or Mac
- Mission critical telecommute apps priority patching
- URL filtering that protects from COVID-19 scams
- Easy remote Windows-based machine wipe
- Remote desktop connectivity
- Additional CPOC alerts related to public health
- Keep germs away via the voice-controlled Cyber Console

Acronis Remote Device Wipe

Remote wipe

Administrators can wipe Windows machines remotely from the Acronis Cyber Protect console. **Administrators rights on the endpoint machine are required.**

The "Wipe data" action restores a machine to its factory default settings. All data, applications, and settings will be removed. For example, if the machine gets lost or stolen.

Status	Description	Device	Started by
✓ Succeeded	Remote wipe of 'qa-gw3t68hh' data	qa-gw3t68hh	ABA12-AMSVAdministrator
✓ Succeeded	Logging in account 'qa-gw3t68hh\Administrator'	—	ABA12-AMSVAdministrator

Wipe device data

Wipe data cannot be reversed, therefore review carefully the selected device before entering the credentials of the user with administrator rights to qa-gw3t68hh to proceed.

DOMAIN\username

jacob.jones

Password

Cancel

Wipe Data

Why?

- Prevent unauthorized access
- Get greater control over sensitive data
- Reduce the risk of data loss

Ensure the Safety of Remote Work Tools

Prioritized patch management and antimalware protection

Patches				
Filter Search				
<input type="checkbox"/> Name ↑	Severity ↓	Product ↓	Installed ver...	Version ↓
2018-05 Cumulative Update for Wind.	MEDIUM	Windows 10 L...	—	—
2020-03 Servicing Stack Update for ...	CRITICAL	Windows 10 L...	—	—
Microsoft Silverlight (KB4481252)	MEDIUM	Silverlight	—	—
TeamViewer GmbH TeamViewer	MEDIUM	TeamViewer	15.3.2682	15.3.8497
Windows Malicious Software Remov...	MEDIUM	Windows 10 L...	—	—

Patches		
Approval status	Not defined	Install patches
<input checked="" type="checkbox"/> Name ↓	Severity ↓	Product ↓
<input checked="" type="checkbox"/> Update for Skype for Business 2016 (KB4484245) 64-Bit Edition	CRITICAL	Office 2016
<input type="checkbox"/> Update for Microsoft Project 2016 (KB4484253) 64-Bit Edition	CRITICAL	Office 2016
<input type="checkbox"/> Update for Microsoft OneNote 2016 (KB4092450) 64-Bit Edition	CRITICAL	Office 2016
<input type="checkbox"/> Update for Microsoft Office 2016 (KB4484247) 64-Bit Edition	CRITICAL	Office 2016

Collaboration tools

Zoom

Webex

Microsoft Teams

Skype

Slack

TeamViewer

VPNs

OpenVPN

NordVPN

Why?

- Eliminate potential cybersecurity weaknesses
- Enable employees to work securely
- Increase productivity

CPOC Alerts on COVID-19-related Malware

Don't let malware hide behind coronavirus news

Threat feed

Q Search

Name	Severity
Covid-19 drug advice from the WHO disguised as HawkEye infostealer	
New RedLine Stealer distributed using Coronavirus-themed email campaign	
Trickbot, Emotet malware use Coronavirus news to evade detection	
A new variant of Pysa ransomware is infecting French governments	
Netwalker Ransomware Infecting Users via Coronavirus Phishing	
Windows Adobe Type Manager Library RCE	
BlackNET RAT spreads using bogus Corona Antivirus application campaign	
Malware disguised as Google Updates pushed via compromised WordPress w...	
Security update available for Creative Cloud Desktop Application	
HPE Warns of New Bug That Kills SSD Drives After 40,000 Hours	
Security flaws in Cisco, Citrix, Zoho devices targeted by APT41	
FIN7 hackers target enterprises with weaponized USB drives via USPS	

Netwalker Ransomware Infecting Users via Coronavirus Phishing

Remediate

Remediation actions

antiMalwareScan	new
runBackupUnprotected	new

Details

More

The new Netwalker phishing campaign is using an attachment named CORONAVIRUS_COVID-19.vbs contains an embedded Netwalker Ransomware executable and obfuscated code to extract and launch the computer.

Type	—
Category	—
Severity	
Date	Mar 23, 2020

New CoronaVirus ransomware acts as cover for Kpot infostealer

Remediate

Remediation actions

antiMalwareScan	new
runBackupUnprotected	new

Details

More details

A new ransomware called CoronaVirus has been distributed through a fake web site pretending to promote the system optimization software and utilities from WiseCleaner. With the increasing fears and anxiety of the Coronavirus (COVID-19) outbreak, an attacker has started to build a campaign to distribute a malware cocktail consisting of the CoronaVirus ransomware and the Kpot infostealer trojan.

Type	—
Category	—
Severity	
Date	Mar 18, 2020

Block COVID-19 Fake News Sites with URL Filtering

Fact checking by Acronis analysts and communities



How It Works Resources Licensing Partners News Literacy About Feedback English

Coronavirus Misinformation Tracking Center

As a new strain of coronavirus that causes COVID-19 spreads across the globe, so does disinformation and misinformation. Follow the spread of this dangerous information with NewsGuard's new Coronavirus Misinformation Tracking Center.

Listed below are all the news and information sites in the U.S., the U.K., France, Italy, and Germany that we have identified — 146 so far — as publishing materially false information about the virus. You'll find websites that are notorious for publishing false health content, and political sites whose embrace of conspiracy theories extends well beyond politics. Among the hoaxes these sites publish are that swallowing bleach or colloidal silver will prevent the coronavirus — when in fact these "treatments" can be harmful. Troublingly, you'll also see some sites that generally stick to the facts but in this case have published unvetted, poorly sourced stories that turned out to be false.

To read our full review of each website, click on its name to see its NewsGuard Nutrition Label (some labels include highlighted sections of coronavirus-related content). You can also see these ratings and thousands of others in our browser extension, which is [free to all users](#) during the COVID-19 crisis.

Needless to say, this is a work in progress about a story that has new developments daily. If you have come across a false story about the COVID-19 virus on a site we have not listed below, [please report it here](#) or contact us via our [misinformation hotline](#).

For more information about NewsGuard's approach to tracking coronavirus misinformation, read [this piece](#) on the topic from our lead health analyst, listen to [this story](#) on NPR, or [watch this segment](#) with the BBC.

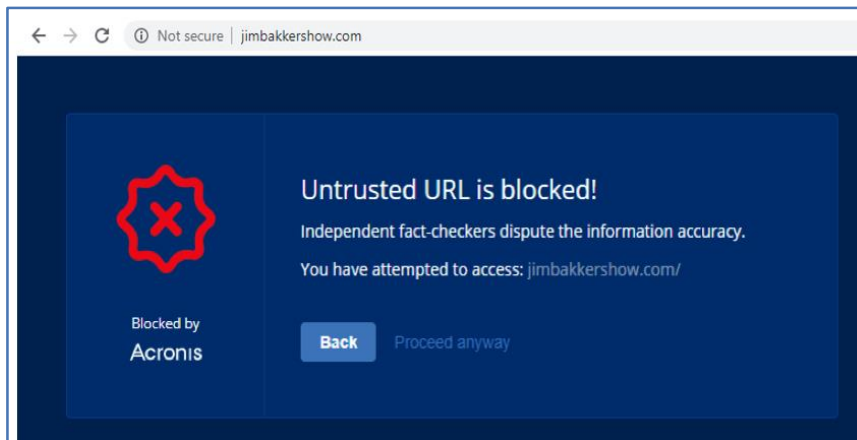
For reliable information on the COVID-19 virus, consult the websites of public health institutions such as the [U.S. Centers for Disease Control and Prevention](#) and the [World Health Organization](#).

Websites Publishing False Coronavirus Information:

Listed By Country (in alphabetical order)

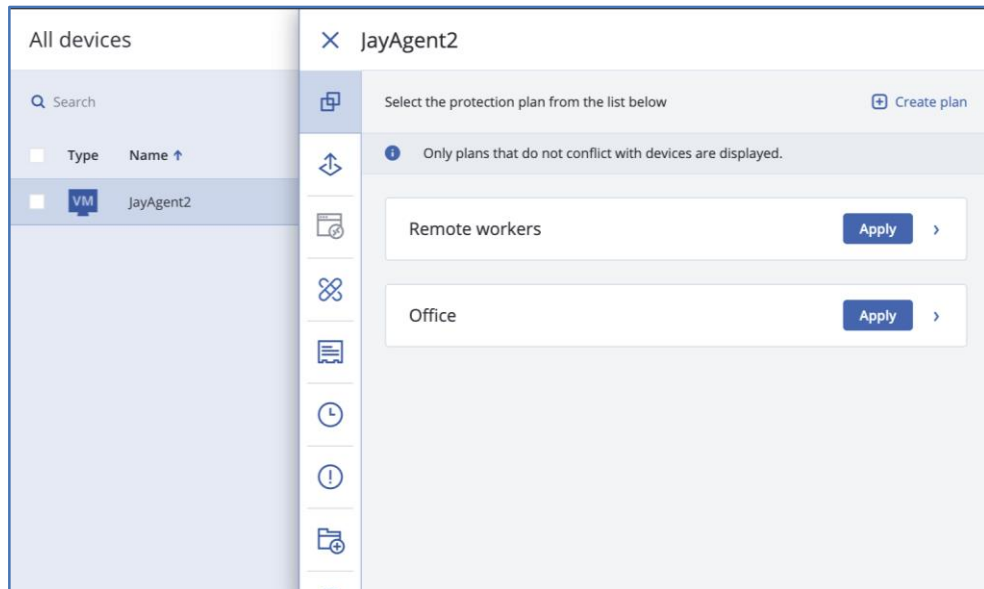
United States

- [ActivistPost.com](#)
- [AmericanThinker.com](#)
- [BeforeItsNews.com](#)
- [RealEstatePolitics.com](#)



Protection Plans for Office and Remote Workers

Simplify security management for remote environments



- **More frequent** backups, antimalware, and vulnerability assessments
- Stricter **actions** (Block vs Ask)
- Restrict backup destinations to **corporate locations** only (block USB, local shares)
- Enable **Battery power** as backup condition

Why?

- Simplify security management
- Reduce security risks
- Make sure your team is protected

Acronis Cyber Protect Editions and Licensing

Editions Overview

Acronis Cyber Backup		Acronis Cyber Protect		
Standard	Advanced	Essentials	Standard	Advanced
Designed for backing up data in on-premises or cloud Windows, Linux, VMware, Hyper-V, or mixed heterogeneous small and medium environments.	Designed for larger environments, includes advanced backup features, such as: <ul style="list-style-type: none"> • Group management • Shared protection plans • Off-host data processing • Tape support • Deduplication • Customizable reporting 	Includes basic file-level backup capabilities and essential cyber protection features, such as: <ul style="list-style-type: none"> • Antivirus and antimalware protection • Vulnerability assessment • Patch management • URL filtering 	Includes the Acronis Cyber Backup Standard and the Acronis Cyber Protect Essentials features, plus additional cybersecurity functionality, such as: <ul style="list-style-type: none"> • Data protection map • URL filtering with categorization • Continuous data protection • HDD health 	Includes advanced backup and cyber protection capabilities for larger infrastructures, such as <ul style="list-style-type: none"> • Support for additional workloads • Shared protection plans • Backup notarization • Safe recovery of backups • Backup scan for malware • Dashboard configuration

Editions: Feature Comparison

Features	Acronis Cyber Backup		Acronis Cyber Protect		
	Standard	Advanced	Essentials	Standard	Advanced
Acronis Cyber Backup Standard features	✓	✓	Limited	✓	✓
Acronis Cyber Backup Advanced features	—	✓	—	—	✓
<ul style="list-style-type: none"> Vulnerability assessment <small>NEW</small> Basic auto-discovery and remote agent installation <small>NEW</small> 	✓	✓	✓	✓	✓
Essential anti-malware and security management features <ul style="list-style-type: none"> Patch management Anti-virus and anti-malware protection URL filtering Remote desktop Remote device wipe Windows Defender Antivirus and Microsoft Security Essentials management 	—	—	✓	✓	✓
Advanced anti-malware and security management features <ul style="list-style-type: none"> Continuous data protection Anti-malware scanning of backups Safe recovery Smart protection plans Drive health monitoring Forensic data backup Data protection map 	—	—	—	✓	✓

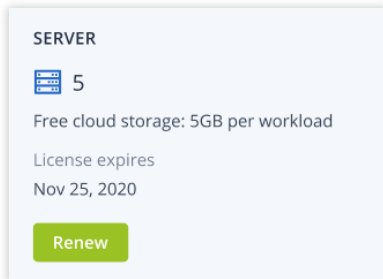
Available Licenses

	Acronis Cyber Backup Standard		Acronis Cyber Backup Advanced		Acronis Cyber Protect Essentials	Acronis Cyber Protect Standard	Acronis Cyber Protect Advanced
Workload type	Subscription	Perpetual	Subscription	Perpetual	Subscription	Subscription	Subscription
Workstation	✓	✓	✓	✓	✓	✓	✓
Windows Server Essentials	✓	✓	✗	✗	✗	✓	✗
Server	✓	✓	✓	✓	✓	✓	✓
Virtual Host	✓	✓	✓	✓	✗	✓	✓
Universal license	✗	✗	✗	✓	✗	✗	✓
Microsoft 365	✓	✗	✓	✗	✗	✗	✗
G Suite	✓	✗	✓	✗	✗	✗	✗

- ✓ - **Subscription** License is available both in **on-prem** and **cloud deployment**
- ✓ - **Perpetual** License is available in **on-prem** only
- ✗ - License is not available

Free Cloud Storage per workload

- Free cloud storage is enabled automatically for any purchased workload license
- Quota per license is defined in licensing configuration file, so update of the value will require datacenter 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
Cyber Protect Essentials - Workstations	5
Cyber Protect Essentials - Servers	5
Cyber Protect Standard - Workstations	50
Cyber Protect Standard - Windows Server Essentials	150
Cyber Protect Standard - Servers	250
Cyber Protect Standard - Virtual hosts	250
Cyber Protect Advanced - Workstations	50
Cyber Protect Advanced - Servers	250
Cyber Protect Advanced - Virtual hosts	250
Cyber Protect Advanced - Universal	250
Cyber Backup Standard - Workstations	50
Cyber Backup Standard - Windows Server Essentials	150
Cyber Backup Standard - Servers	250
Cyber Backup Standard - Virtual hosts	250
Cyber Backup Advanced - Workstations	50
Cyber Backup Advanced - Servers	250
Cyber Backup Advanced - Virtual hosts	250
Cyber Backup Advanced - Universal	250

Acronis Cyber Protect 15 pricing, USD

	Acronis Cyber Backup Standard	Acronis Cyber Backup Advanced	Acronis Cyber Protect Essentials	Acronis Cyber Protect Standard	Acronis Cyber Protect Advanced
Server					
Perpetual	\$999	\$1 529			
1 year	\$469	\$709	\$239	\$539	\$839
2 years	\$729	\$1 119	\$379	\$839	\$1 319
3 years	\$999	\$1 529	\$499	\$1 149	\$1 799
Workstation					
Perpetual	\$89	\$119			
1 year	\$69	\$99	\$59	\$79	\$119
2 years	\$129	\$179	\$109	\$149	\$209
3 years	\$179	\$249	\$149	\$209	\$299
Virtual Host					
Perpetual	\$1 199	\$1 999			
1 year	\$559	\$929		\$639	\$1 069
2 years	\$879	\$1 469		\$1 009	\$1 689
3 years	\$1 199	\$1 999		\$1 379	\$2 299
Server Essentials					
Perpetual	\$499				
1 year	\$229			\$259	
2 years	\$369			\$419	
3 years	\$499			\$569	
Universal					
Perpetual		\$2 199			
1 year					\$1 149
2 years					\$1 799
3 years					\$2 529

Upgrade Options

Existing Licenses After GA

Existing Customers Have	Upgrade Options
Acronis Cyber Backup 12.5 Standard (Perpetual)	<p>Valid maintenance:</p> <ul style="list-style-type: none">Free upgrade of Acronis Cyber Backup 15 Standard via account.acronis.com <p>Expired maintenance:</p> <ul style="list-style-type: none">Buy Version Upgrade SKU
Acronis Cyber Backup 12.5 Advanced (Perpetual)	<p>Valid maintenance:</p> <ul style="list-style-type: none">Free upgrade of Acronis Cyber Backup 15 Advanced via account.acronis.com <p>Expired maintenance:</p> <ul style="list-style-type: none">Buy Version Upgrade SKU
Acronis Cyber Backup 12.5 Standard (Subscription)	<p>Subscription licenses remain unchanged (quota and expiration date). The customer can download the new build and use the subscription with agents updated to version 15.</p>
Acronis Cyber Backup 12.5 Advanced (Subscription)	

Acronis Security Expertise

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

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

Passed



VB100 certified



AV-Test participant and test winner

Current test results combined

Testing laboratory	Real-world detection	Prevalent malware detection	Collection set detection	False positives	Performance
AV-Test.org	NA	100%	NA	0	NA
AV-Comparatives	98%	98.9%	NA	0	Very fast; fast
ICSA Labs	98.23%	99.89%	99.98%	0	NA
VirusBulletin VB100	NA	100%	98.35%	0	NA



“Approved Business Security” certification



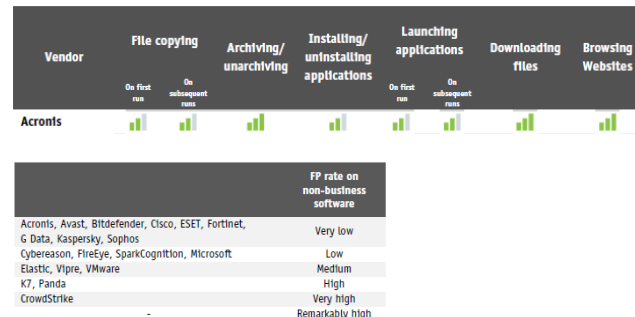
Acronis scored a 98.0% detection rate in a real-world test, but more importantly, it caused **zero false positives** – a distinction held by only three other vendors in the test.

	Blocked	User dependent	Compromised	PROTECTION RATE (Blocked % + (User dependent %)/2) ¹	False Alarms
Fortinet	767	-	-	100%	11
Panda	767	-	-	100%	27
Kaspersky	766	-	1	99.9%	0
Avast	766	-	1	99.9%	5
Microsoft	765	-	2	99.7%	8
ESET	764	-	3	99.6%	0
K7	764	-	3	99.6%	15
Bitdefender, G Data	763	-	4	99.5%	2
Sophos, VIPRE	763	-	4	99.5%	3
VMware	762	-	5	99.3%	2
Elastic	762	-	5	99.3%	41
Cisco	757	-	10	98.7%	1
SparkCognition	754	-	13	98.3%	0
Acronis	762	-	15	98.0%	0
CrowdStrike	747	-	20	97.4%	21
Cybereason	743	-	24	96.9%	20
FireEye	740	-	27	96.5%	1

Acronis Cyber Protect scored a 98.9% detection rate, again with **zero false-positive reactions!**

	Malware Protection Rate	False Alarms on common business software
Cisco, K7, Microsoft, VMware	100%	0
Bitdefender, ESET, G Data, Panda	99.9%	0
Avast, Vipre	99.8%	0
CrowdStrike, Cybereason	99.7%	0
Elastic, FireEye	99.6%	0
Fortinet, Kaspersky	99.5%	0
Sophos	99.4%	0
Acronis	98.9%	0
SparkCognition ⁷	92.7%	0

In all eight performance test categories, Acronis Cyber Protect demonstrated either **Very Fast or Fast performance.**



- If a product is configured in a way that blocks, quarantines, or deletes a potential threat with a false reaction, the endpoint machine can crash and become completely non-operational. This causes a business to experience costly downtime, which is why a cybersecurity solution must not cause any false reactions.

AV-Comparatives July 2020 Test



One of only four solutions with zero false positives for all the tests!

	Blocked	User dependent	Compromised	[Blocked % + (User dependent %)/2] ^a	False Alarms
Fortinet	767	-	-	100%	11
Panda	767	-	-	100%	27
Kaspersky	766	-	1	99.9%	0
Avast	766	-	1	99.9%	5
Microsoft	765	-	2	99.7%	8
ESET	764	-	3	99.6%	0
K7	764	-	3	99.6%	15
Bitdefender, G Data	763	-	4	99.5%	2
Sophos, VIPRE	763	-	4	99.5%	3
VMware	762	-	5	99.3%	2
Elastic	762	-	5	99.3%	41
Cisco	757	-	10	98.7%	1
SparkCognition	754	-	13	98.3%	0
Acronis	762	-	15	98.0%	0
CrowdStrike	747	-	20	97.4%	21
Cybereason	743	-	24	96.9%	20
FireEye	740	-	27	96.5%	1

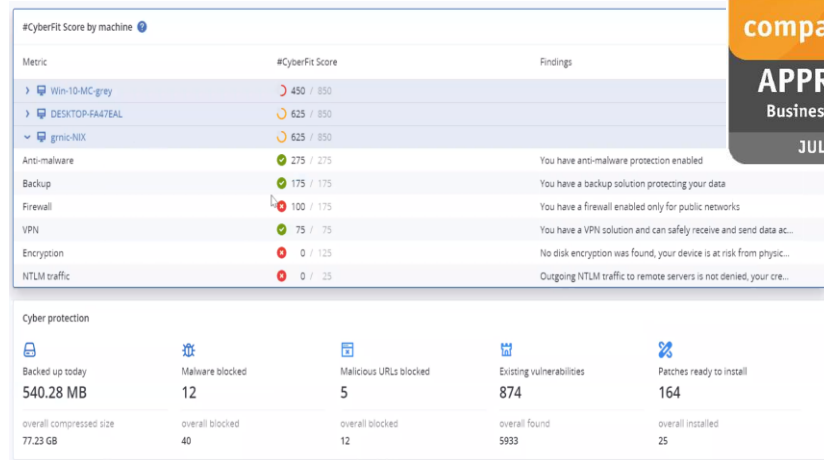
	FP rate on non-business software
Acronis, Avast, Bitdefender, Cisco, ESET, Fortinet, G Data, Kaspersky, Sophos	Very low



Excellent performance: all tests either Very fast or Fast

AV-Comparatives praised Acronis Cyber Protect excellent interface and ease-of-use

- **"Acronis' cloud-based management console stands out for its very clear and clean modern interface.** All of the management functionality is easily accessible via a single menu column on the left-hand side of the window. Individual pages have a simple, uncluttered view, which makes it easy to find the details. In many ways, the console resembles a well-designed smartphone app, and would doubtless scale very well when used on the smaller screen of, say, a tablet. **The product's simplicity and clarity mean that it would be particularly well-suited to smaller businesses and less-experienced administrators."**



<https://www.av-comparatives.org/tests/business-security-test-2020-march-june/>

Acronis Cyber Protect Cloud earns VB100 certification (June)

Certification test, malicious set:

- Total samples: 2029
- Detected samples: 2029
- Missed samples: 0
- Detection rate: 100.00%

Certification test, clean file set:

- Total samples: 99990
- Detected as malicious: 0
- Detected as clean: 99990
- False-positive rate: 0.000%



“Virus Bulletin extends their congratulations to Acronis who are newcomers to the VB100 certification, achieving their first certification at 100% malware detection + 0% false-positive rate on our certification sets.”

<https://www.virusbulletin.com/testing/results/latest/vb100-antimalware>

VB100 certification updated in August

Acronis Cyber Protect Cloud was certified again with the following results:

- **WildList detection – 100%**
- **False positive rate – 0%**
- **Diversity Test rate - 99.74%**

A product achieves a VB100 certification if:

- No more than 0.5% of WildList samples are missed
- No more than 0.01% of legitimate files are blocked



Top results in ICSA Labs Endpoint Anti-Malware Certification

Real Time Protection

June 2020 Test Set

File Infectors			Non-File Infectors		
NA	NA	NA	Detected 1,716	Total 1,747	Eff 98.23%

To pass, products must be at least 92% effective at detecting malicious, non-file infectors known to exist in systems worldwide.

The anti-malware product's ability to detect malicious file infectors was not applicable as there were no file infectors in the June 2020 test set.

On Demand Scanning

June 2020 Test Set

File Infectors			Non-File Infectors		
NA	NA	NA	Detected 1,745	Total 1,747	Eff 99.89%

Acronis detected 99.89% of malicious samples during ICSA Labs' testing of Acronis Cyber Protect Cloud on demand malware scanning capability.

There were no malicious file infectors in the June 2020 test set; therefore ICSA Labs was unable to measure how effective the product's on demand functionality was in detecting malicious file infectors.

ICSA Labs

"Collection 2020" Test Set

Detected 44,717	Total 44,725	Eff 99.98%
--------------------	-----------------	---------------

To meet the requirements, Acronis Cyber Protect Cloud had to be at least 90% effective at detecting malicious threats in ICSA Labs' "Collection" of known malware collected in recent years.

During testing, Acronis Cyber Protect Cloud was nearly perfect having scored much higher than the percentage required by the test criteria.

False Positive Testing

0 False Positives

Acronis's endpoint anti-malware product was tested with 1000s of clean test cases to determine whether or not it would improperly alert or quarantine any innocuous samples. Acronis Cyber Protect Cloud had no false positives during testing, which is very good.



- 0 false positives
- 99.9% on-demand detection rate
- 98.23% real-world new and unknown malware detection rate

https://www.icsalabs.com/sites/default/files/FINAL_Acronis_Endpt_Anti-Malware_Report_20200724.pdf

ICSA comments on Acronis results

Significance of the Test & Results

Readers of certification testing reports often wonder what the testing and results really mean. They ask, “In what way is this report significant?” The statements below sum up what this ICSA Labs Anti-Malware Certification Testing report should indicate to the reader:

1. Acronis’s endpoint anti-malware product provided very good real time protection against malware known to exist on systems worldwide.
2. Acronis Cyber Protect Cloud had no false positives on any of the thousands of innocuous files used in testing.
3. The real time protection provided by Acronis Cyber Protect Cloud was almost equally effective compared to the already very effective on demand scanning provided by the product.
4. While under contract, ICSA Labs will continue to test Acronis Cyber Protect Cloud each month against the then current set of threats reported on systems worldwide and report the results.



What the Experts Say



*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



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 & Rapid Growth

\$300M+ billings
50% business growth
100%+ cloud
business growth



Global Reach

100% of Fortune 1000
50,000+ partners
500,000+ businesses
5,500,000+ prosumers




Global Presence

1,500+ employees
33 locations
Products available in
150+ countries and
40+ languages



Acronis Introduces New Category: Cyber Protection

Acronis Protects all Data, Applications, and Systems (**Workloads**)




Safety

Reliable copy for recovery



Accessibility

Access from anywhere at any time



Privacy

Control over visibility and access



Authenticity

Proof that copy is exact replica of the original



Security

Protection against cyberthreats

Ease of Use

Total Cost of Ownership

Security

Control

Reliability

Acronis Cyber Singularity

Simplified View of Acronis Product Portfolio

Acronis Cyber Protection

For Customers



Acronis Cyber Cloud

For Partners



Acronis Cyber Platform

For Developers



Acronis Cyber Infrastructure

For cyber benefits:
easy, efficient,
secure, controlled,
and reliable



Acronis Cyber Services

For mindshare,
expertise, and wider
reach



Acronis Cyber Foundation

Building a more knowledgeable future

**CREATE, SPREAD
AND PROTECT
KNOWLEDGE WITH US!**

www.acronis.org

#CyberFit

Building new schools • Providing educational programs • Publishing books

