

Acronis

#CyberFit

Acronis Cyber Protect

The most secure backup
and fastest recovery



Acronis Cyber Protect



Secure Backup

The industry standard for secure backup, leveraging AI, ML and immutability to ensure your backups remain impenetrable.



Fast Recovery

Lightning-fast recovery of entire systems or individual files. Acronis One Click Recovery automates the recovery process, making it simple for regular users.



Increased Efficiency

Dramatically reduce TCO and simplify protection with a single pane of glass. Streamline administration and training.

Top SMB Use Cases for Acronis Cyber Protect

Cybersecurity



Zero-day and malware protection



Remote work protection



Detect & Respond to security incidents

Data protection



Backup data across your all environments



Post-attack recovery & disaster recovery



Real-time protection of critical data

Administration



Streamlined management



Reduced costs & complexity



Compliance & forensics investigations

Top Enterprise Use Cases

Feature

Acronis Cyber Protect v16 Capabilities

Enterprise-level Backup and Recovery

Delivers secure, fast recovery across multi-site, multi-generational 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, multi-generational 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

#CyberFit

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

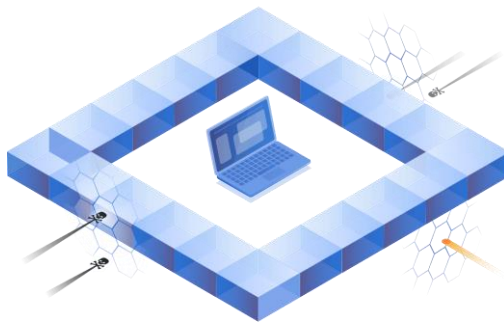


Data Protection Map: Monitor the protection status of files with classification, reporting, and unstructured data analytics



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.

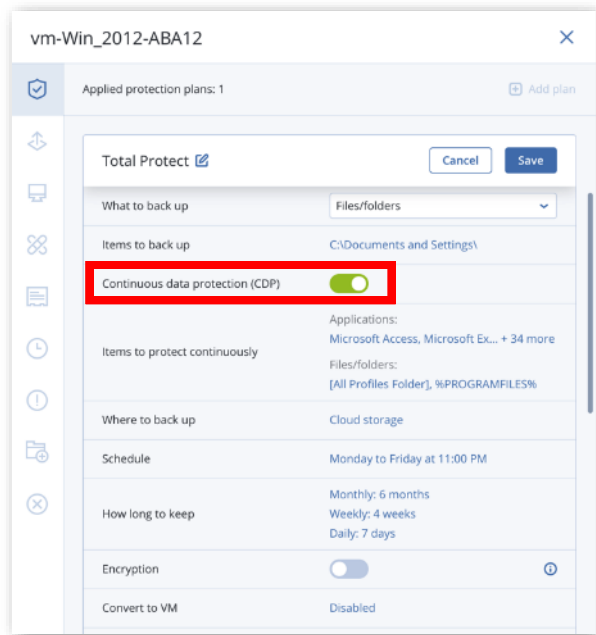
In the event of a malware infection, you can restore the data from the last backup and apply the latest collected changes so no data is lost.

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



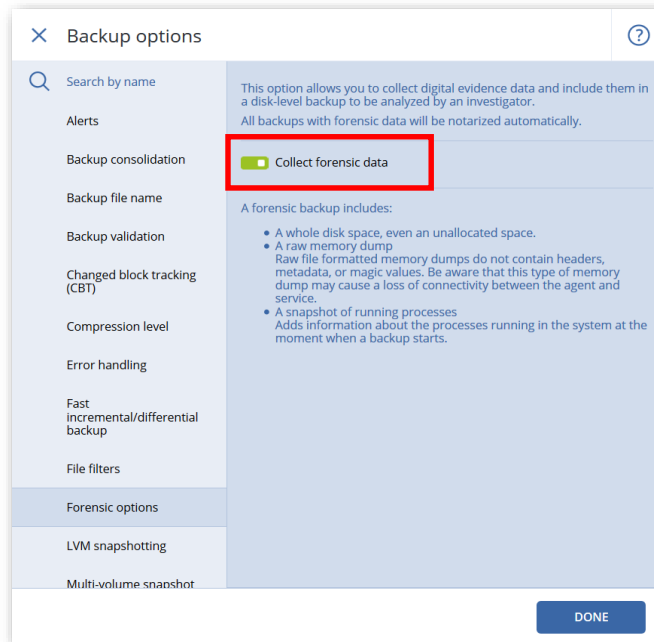
2. Include Backup Information for Forensic Investigation

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



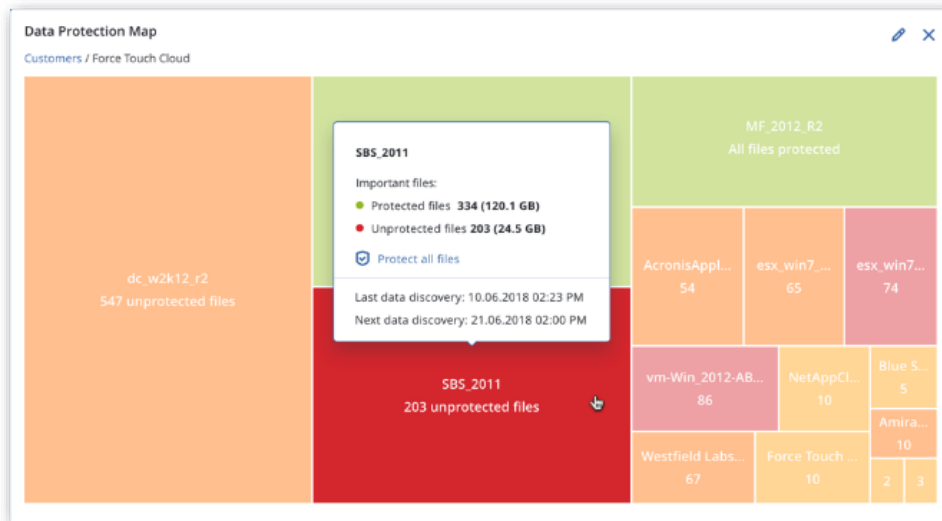
3. Data Compliance Reporting and Data Protection Map

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



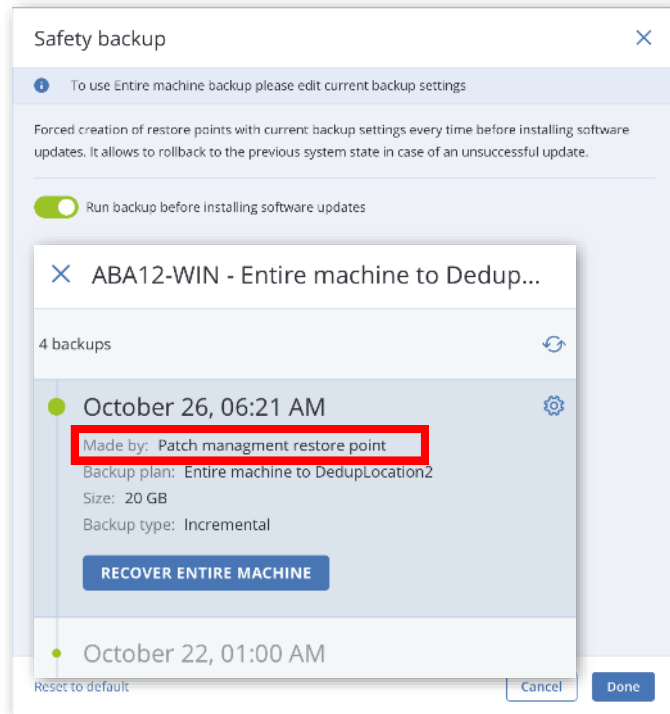
4. Fail-safe Patching

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

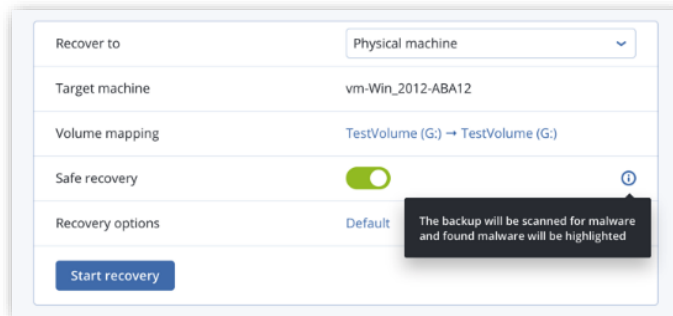


5. Safe Recovery

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

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 scan results. The table has columns for Type, Name, Status, Size, and Last change. The data is as follows:

Type	Name	Status	Size	Last change
Computer	ABA12-WIN - Entire machine	Malware detected	200 GB	Oct 27, 2018 09:00 AM
Backup plan	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

The screenshot displays two overlapping windows from the Acronis Cyber Protection interface. The background window is the 'Threat Feed' panel, which lists various security alerts. The foreground window is the 'Remediation actions' panel, which provides options to manage vulnerabilities and patches.

Threat Feed

Name	Severity	Type	Date
Snatch ransomware reboots PCs into Safe Mode L...	HIGH	Malware	Dec 10, 2019
Acronis discovers new AutoIt Cryptominer campai...	HIGH	Malware	Dec 11, 2019
Town hit by ransomware: System shut down to li...	MEDIUM	Malware	Dec 9, 2019
Caution! Ryuk ransomware decrypter damages lar...	MEDIUM	Malware	Dec 10, 2019
		Malware	Dec 13, 2019
		Malware	Dec 2, 2019
		Malware	Dec 2, 2019
		Malware	Dec 4, 2019
		Malware	Dec 4, 2019

Remediation actions

Vulnerability assessment
Scan machines for vulnerabilities

Patch management
Install patches on affected machines

☒ Google Chrome
☒ Adobe Flash Player
☒ Adobe Acrobat Reader

☒ Automatically accept the license agreements

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

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

Buttons: Cancel, Start remediation

*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

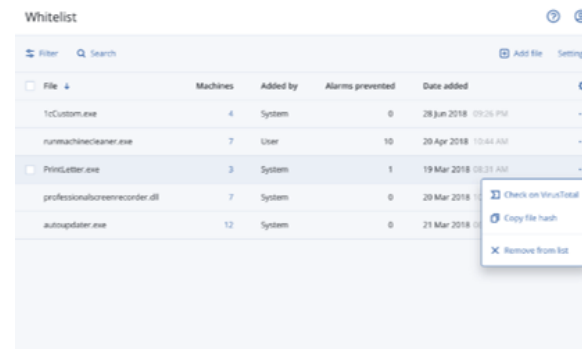
Improved detection rates may lead to more false positive alerts. Traditional, global whitelisting does not support custom applications.

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



File	Machines	Added by	Alarms prevented	Date added
1cCustom.exe	4	System	0	28 Jun 2018 09:26 PST
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

Acronis

#CyberFit

Key Features Overview

New capabilities in v16

Backup

- **Immutable storage**
- **One Click Recovery ***
- LTO-9 support
- Backup and Recovery for Synology NAS
- Local backup with replication to cloud
- Recovery of workloads protected by BitLocker

Security

- **Endpoint Detection and Response (EDR) ****
- Intel TDT (Threat Detection Technology) – enhanced fileless attack protection
- Email notification for alerts
- Encryption of archives enabled by default

Platform

- **Centralized dashboard for multiple management servers**
- Allow agent installation without Antimalware components

* Requires Advanced edition

** Requires cloud deployment model

Error-proof immutable backups

New in v16

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 2 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.

One-click recovery

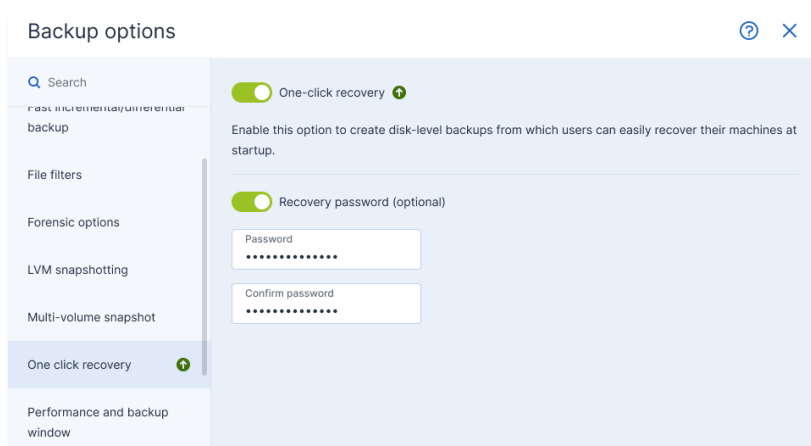
New in v16

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 non-technical end users with a simplified, automated recovery of an entire workload.

- Works with any backup location supported by the product
- Supports recovery passwords for enhanced security



Why? Eliminate IT bottlenecks and save time and money by reducing downtime in case of a cyberattack

Centralized dashboard for multiple Management Servers

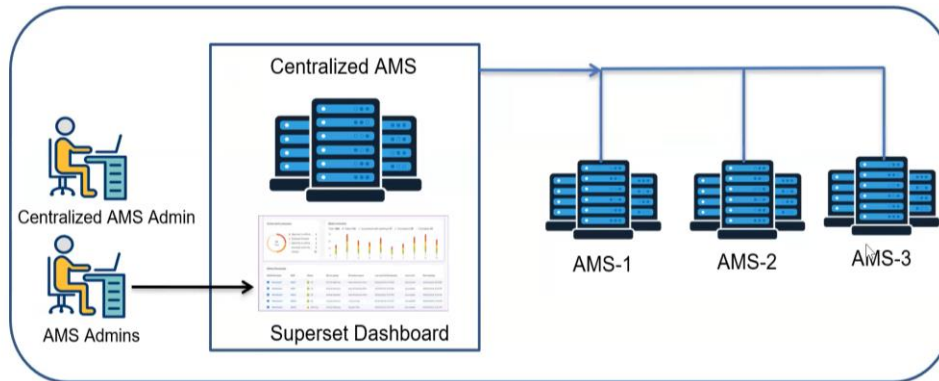
New in v16

A single consolidated view to monitor all Management Servers in an organization.

Simpler administration of thousands of devices for larger enterprises.

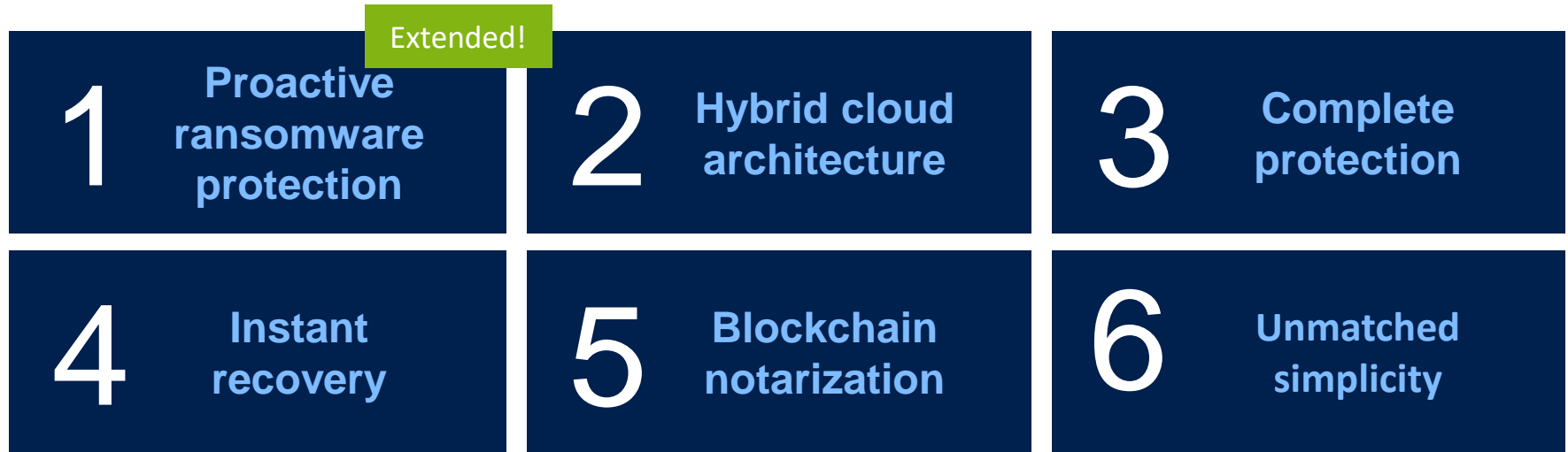
Widgets available:

- Devices
- Alerts
- Activities



On-premise deployment

Includes All Data Protection Advantages



Why? Faster recovery, better RTOs

Significantly Extended Antimalware Capabilities

Acronis Cyber Protect

Acronis Active Protection



Antiransomware, anticryptojacking, AI- and ML-enabled



Acronis static AI analyzer

On-access and on-demand detection



Acronis antimalware engine

Any malware (cloud and local detection)



Acronis behavioral engine

On-access detection

Native integration with Windows Security Center

Why? 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

The need for EDR



Only advanced security can combat advanced attacks

More than 60% of breaches **involve some form of hacking**

On average, it takes organizations **207 days to** identify a breach



Breach is inevitable – you need to be prepared

70 days to contain a breach

USD 4.35 million – average total cost of a data breach

76% of security and IT teams struggle with **no common view** over applications and assets



For many – compliance is mandatory

Regulations require organizations to **report security incidents** within a strict time-frame – e.g. 72 hours for GDPR

70% of breaches involve PII (post-incident analysis required for reporting for regulatory purposes)

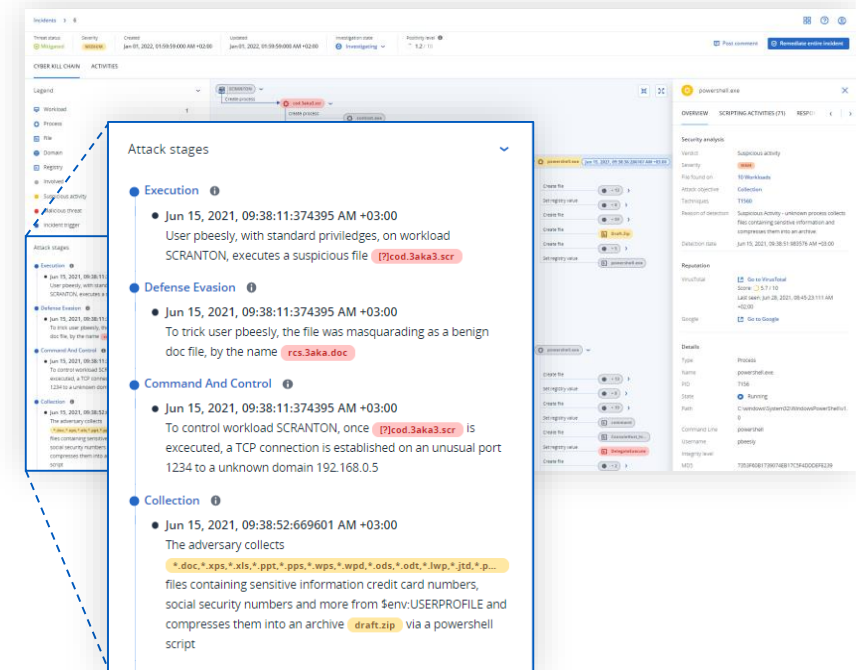
Sources: "Data Breach Investigations Report", Verizon, 2022"; "Cost of data breach report", 2022, IBM Security & Ponemon Institute; "Costs and Consequences of Gaps in Vulnerability Response," ServiceNow, 2020, Investigation or Exasperation? The State of Security Operations", iDC

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 a **prioritized visibility of suspicious activities** across endpoints – rather than 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 trainings 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 rollback, file- or image-level recovery, and disaster recovery

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

Remediate entire incident

Analyst verdict

☒ True positive ☐ False positive

Remediation actions

☒ Step 1 – Stop threats
Stops all processes related to the threat.

☒ Step 2 – Quarantine threats
After being stopped, all malicious or suspicious processes and files are quarantined.

☒ Step 3 – Rollback changes
Rollback first deletes any new registry entries, scheduled tasks or files created by the threat (and any of its children threats). Next, rollback reverts any modifications made by the threat (or its children) to the registry, scheduled tasks and/or files existing on the workload prior to the attack. To optimize speed, rollback tries to restore items from the local cache. Items that fail to be restored will be restored by the system from backup images.
Affected items: 20

☐ Recover workload
If any of the above selected remediation steps fail completely or partially.

Prevention actions

☒ Add to blocklist
Adds all threats from the incident to the blocklist in the selected protection plans. This action will prevent these threats from future executions.

Protection plan

☐ Patch workload
Prevents further attacks by patching software that contains vulnerabilities used by attackers in order to get a foothold on the workload.

☒ Change investigation state of the incident to: Closed

Comment

Cancel Remediate

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

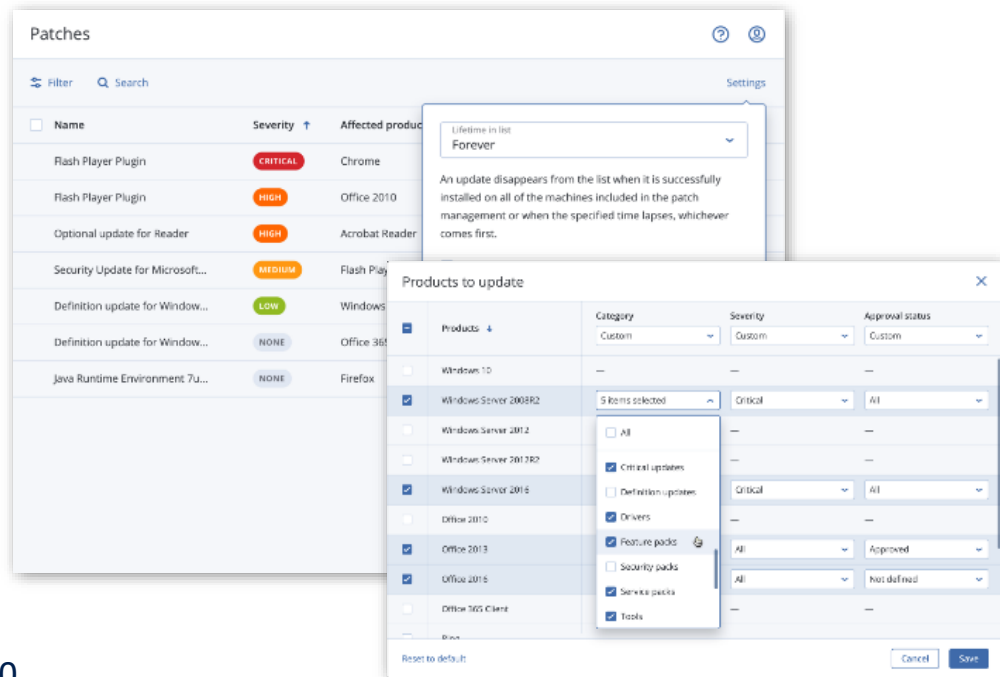
Vulnerabilities					
 Install patches			4 items selected 		
<input type="checkbox"/>	Name	Affected products	Machines	Severity ↑	Patches
<input checked="" type="checkbox"/>	CVE-2018-209654	Chrome, Firefox	12	CRITICAL	—
<input checked="" type="checkbox"/>	CVE-2018-1000016	Office 2010	3	HIGH	2
<input type="checkbox"/>	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	NONE	3
<input checked="" type="checkbox"/>	CVE-2018-337894	Firefox	3	NONE	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

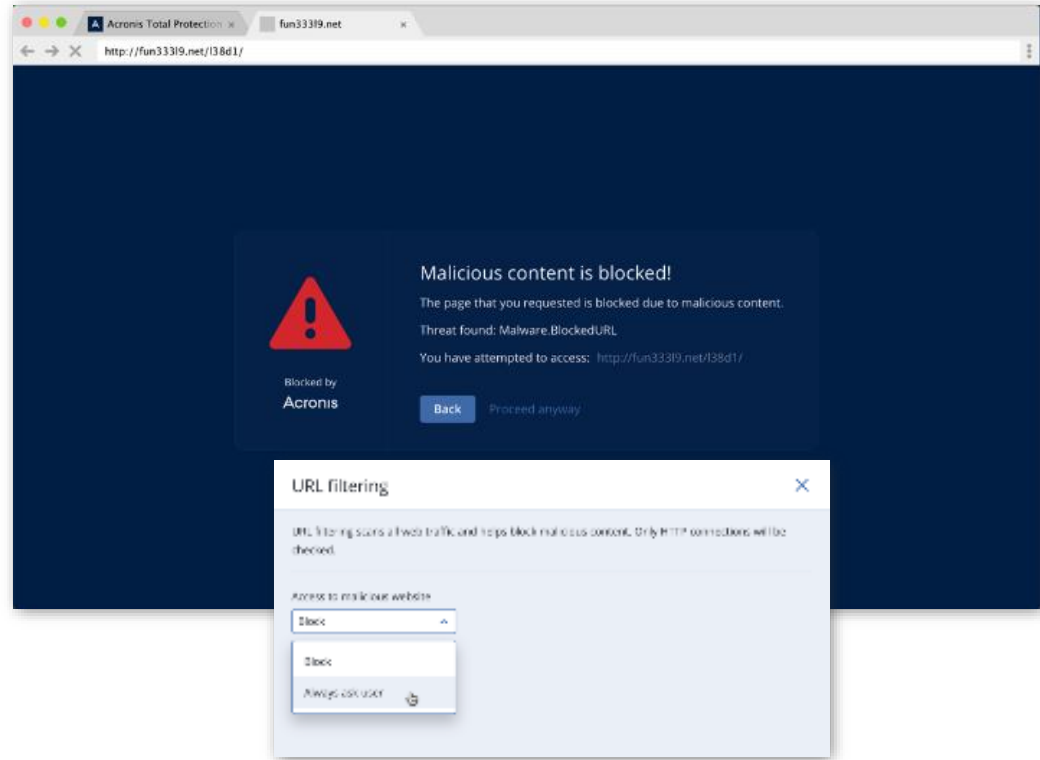
- HTTP/HTTPS interceptor
- Black/whitelists for URLs
- Payload analysis for malicious URLs

Acronis URL Filtering List:

- Acronis' own signatures
- AI-based detection

Why?

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

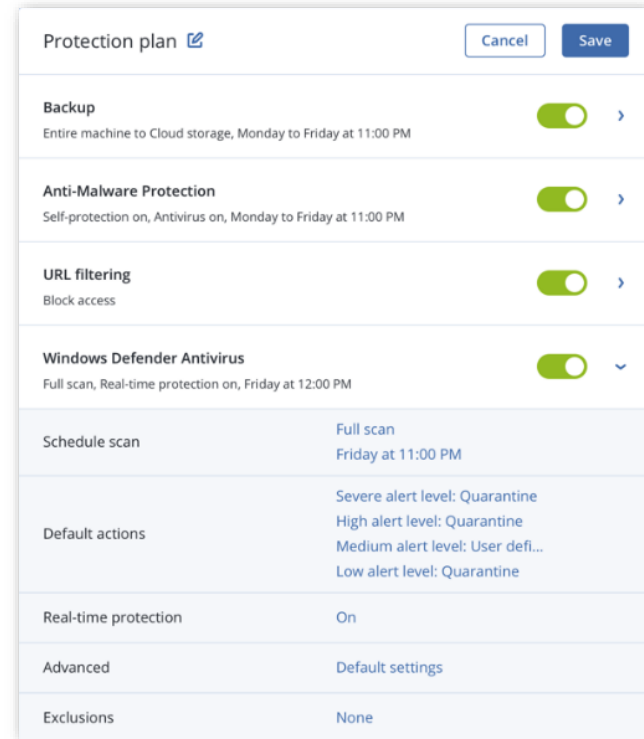


Windows Defender Antivirus or Microsoft Security Essentials Management

- 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

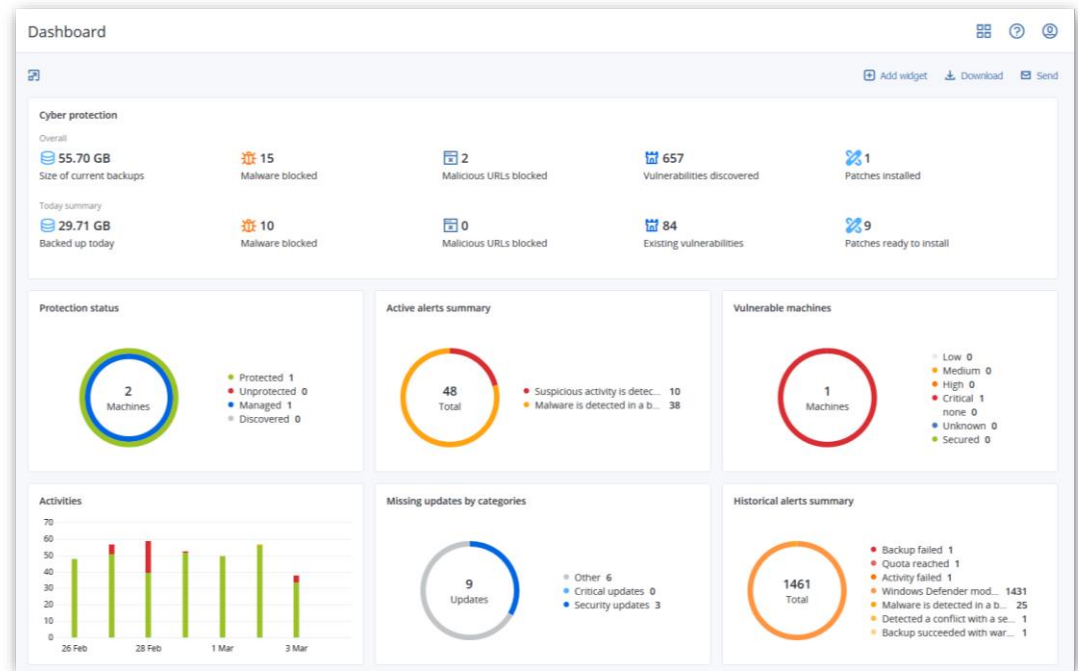


Flexible Monitoring and Reporting

- 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	<input checked="" type="checkbox"/>	>
Anti-malware Protection Self-protection on, Real-time protection on, at 02:20 PM, Sunday through Saturday	<input checked="" type="checkbox"/>	>
URL filtering Always ask user	<input checked="" type="checkbox"/>	>
Windows Defender Antivirus Full scan, Real-time protection on, at 12:00 PM, only on Friday	<input type="checkbox"/>	>
Microsoft Security Essentials Full scan, at 12:00 PM, only on Friday	<input type="checkbox"/>	>
Vulnerability assessment Microsoft products, Windows third-party products, at 01:40 PM, only on Monday	<input checked="" type="checkbox"/>	>
Patch management Microsoft and other third-party products, at 02:35 PM, only on Monday	<input checked="" type="checkbox"/>	>
Data protection map 66 extensions, at 04:00 PM, Monday through Friday	<input checked="" type="checkbox"/>	>

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 image shows two overlapping screenshots of the 'Add machines' wizard in Acronis software. The background window is at the 'Select discovery method' step, with 'Discovery agent' set to 'AMS-125252'. It offers three options: 'Search Active Directory' (selected), 'Scan local network', and 'Specify manually or import from file'. A tooltip indicates that if the discovery agent cannot access some machines, the user should select an agent that has network access. The foreground window is at the 'Post-discovery actions' step, showing 6 machines selected. It offers three options: 'Install agents and register machines' (selected), 'Register machines with installed agents', and 'Add as unmanaged machines'. Below these, the 'Actions after registration' section shows 'Apply protection plan' (checked), 'Chosen plan: Total Protect', 'Backup' (Weekdays at 11:00 PM, Entire machine to Cloud), and 'Active Protection' (Notify only, Self-protection on). '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

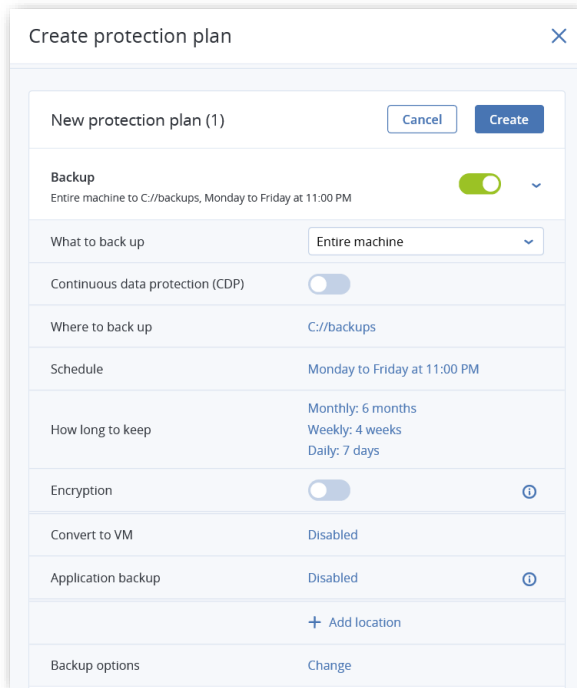
Full-Image and File-Level Backup

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



The screenshot shows the 'Create protection plan' dialog box. It has a title bar with a close button (X). Below the title bar, there's a section 'New protection plan (1)' with 'Cancel' and 'Create' buttons. The main area contains several settings:

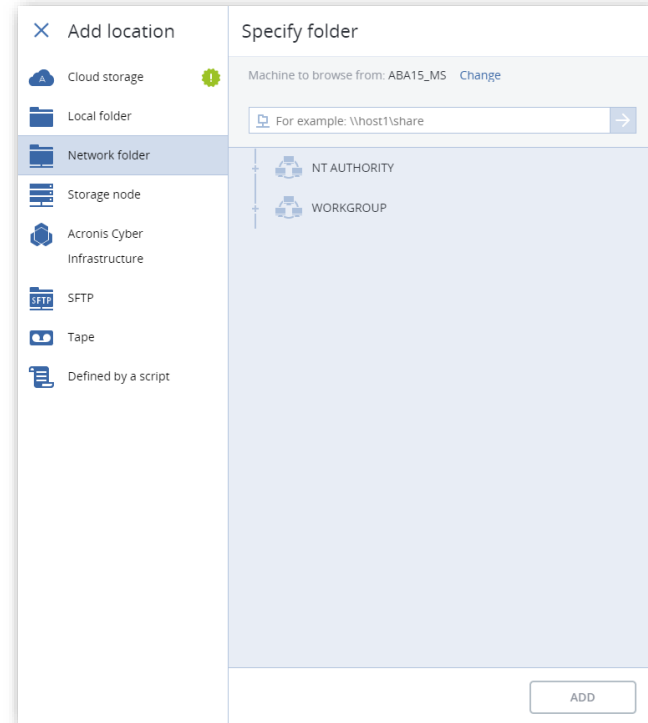
- Backup:** A toggle switch is turned on (green). Below it, the text reads 'Entire machine to C://backups, Monday to Friday at 11:00 PM'.
- What to back up:** A dropdown menu is set to 'Entire machine'.
- Continuous data protection (CDP):** A toggle switch is turned off (grey).
- Where to back up:** The text is 'C://backups'.
- Schedule:** The text is 'Monday to Friday at 11:00 PM'.
- How long to keep:** A dropdown menu shows 'Monthly: 6 months', 'Weekly: 4 weeks', and 'Daily: 7 days'.
- Encryption:** A toggle switch is turned off (grey). To its right is an information icon (i).
- Convert to VM:** The text is 'Disabled'.
- Application backup:** The text is 'Disabled'. To its right is an information icon (i).
- Below these, there is a '+ Add location' button.
- Backup options:** The text is '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)



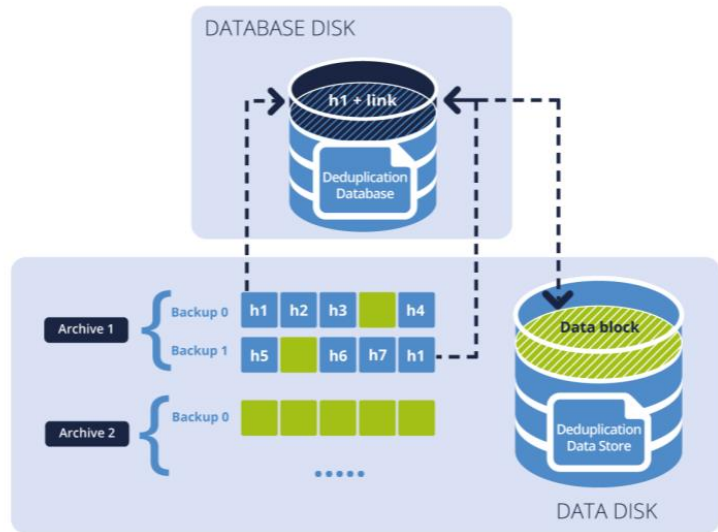
Deduplication

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



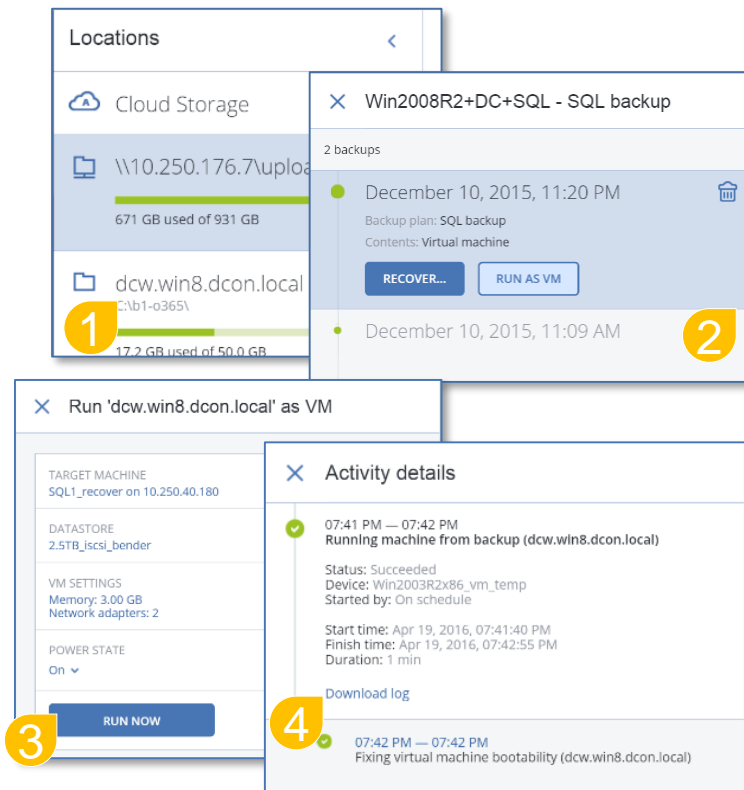
Acronis Instant Restore

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

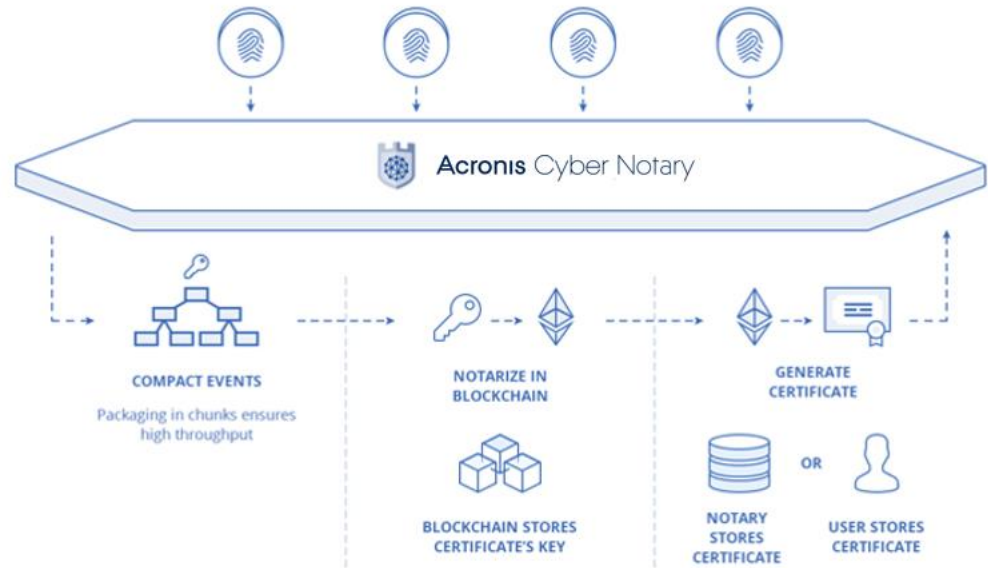
Blockchain Notarization

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

- Highly scalable micro-service architecture
- API interface (REST), queue interface (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



Complete Microsoft 365 protection



**Backup for
Microsoft
Exchange Online**



**Backup for
Microsoft OneDrive
for Business**



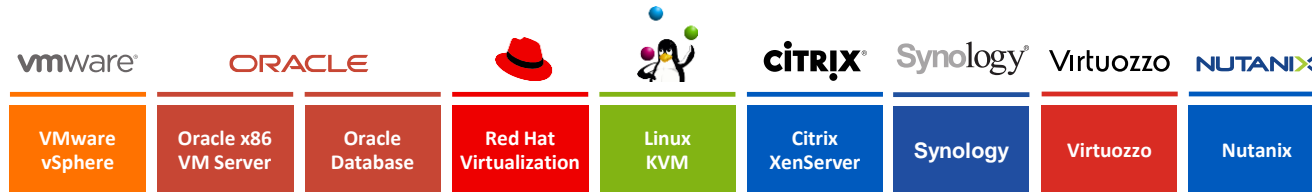
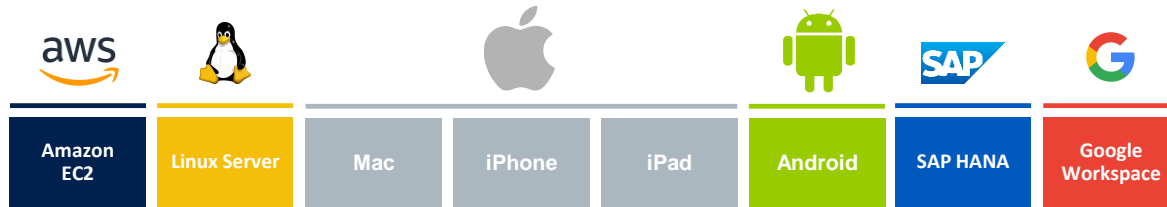
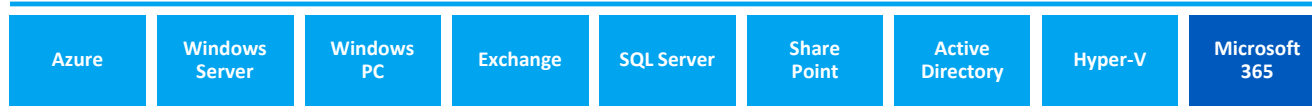
**Backup for
Microsoft SharePoint
Online**



**Backup for
Microsoft Teams**

- 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

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



New features:

- Backup and recovery for Synology NAS

New OS support:

- Red Hat/AlmaLinux 9.0-9.2
- macOS 14 Sonoma
- macOS on ARM CPU support

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
- 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

Linux: Kernel 2.6.9 to 5.19

- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 - 23.04
- Fedora 11 - 31
- 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*
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

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-AMS\Administrator
✓ Succeeded	Logging in account 'qa-gw3t68hh\Administrator'	—	ABA12-AMS\Administrator

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

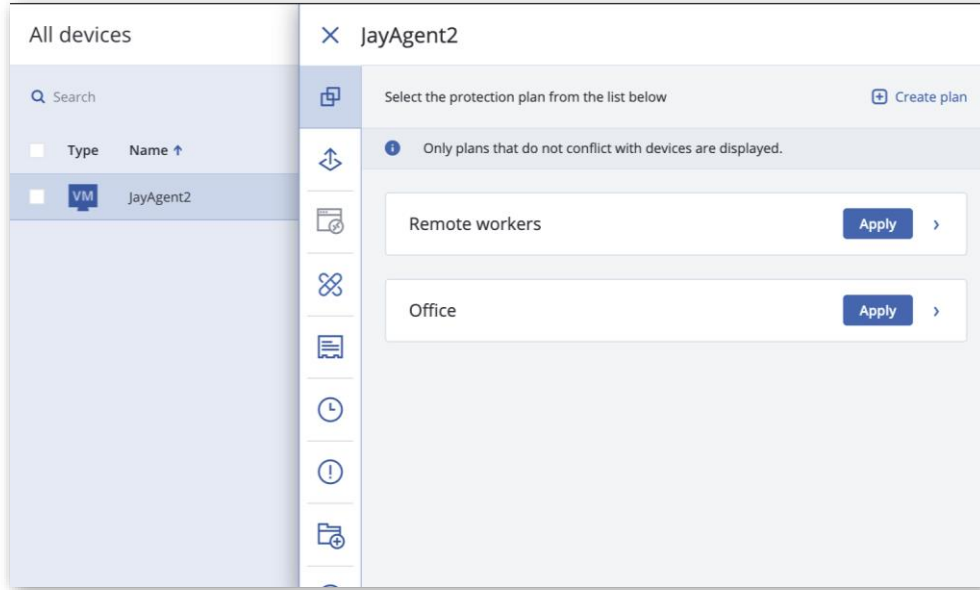
NordVPN

Why?

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

Predefined protection plans

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

#CyberFit

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 allows 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.

Acronis Cyber Protect Features

Features	Acronis Cyber Protect Standard	Acronis Cyber Protect Advanced	Acronis Cyber Protect – Backup Advanced
Basic backup features <ul style="list-style-type: none"> Backup and Recover for Synology NAS New in v16 	✓	✓	✓
Advanced backup features <ul style="list-style-type: none"> One Click Recovery New in v16 	–	✓	✓
<ul style="list-style-type: none"> Vulnerability assessment Basic auto-discovery and remote agent installation 	✓	✓	✓
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"> Anti-malware scanning of backups Safe recovery of backups Corporate allow lists Forensic data backup 	–	✓	–
EDR New in v16 <ul style="list-style-type: none"> Search for IOCs of emerging threats Rapid incident analysis Workload remediation with isolation Rapid rollback of attacks 	–	✓	–

Available Licenses

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


✓ - Subscription license is available both in **on-prem** and **cloud deployment**

✗ - License is not available

Free 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 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
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 Advanced – Workstations	50
Acronis Cyber Protect Advanced – Servers	250
Acronis Cyber Protect Advanced - Virtual hosts	250
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 - Universal	250

SERVER
 5
Free cloud storage: 5GB per workload
License expires
Nov 25, 2020
[Renew](#)

Acronis

#CyberFit

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

Acronis security industry recognition



MVI member



VIRUSTOTAL member



Cloud Security Alliance member



Anti-Malware Testing
Standard Organization
member



Anti-Phishing Working
Group member



2023 Frost Radar™
Leader: EPP



Anti-Malware Test Lab
participant and test winner



ICSA Labs certified



NioGuard Security Lab
participant and test winner



AV-Comparatives approved
business security product



VB100 certified



AV-Test participant and
test winner



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/gas operations, and in pharma drug research/production

Acronis Partners and OEM

Power Generation



Oil/Life Sciences



Manufacturing



Proven compatibility with every major OT and ICS vendor

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



Global-Local Presence

- **2,200+** employees
- **34+** locations
- **150+** countries
- **26** languages
- **750,000** businesses
- **53** DCs globally



Digital World Protection Challenges

- Complexity
- Cost
- Security
- Privacy
- **Cyber protection** is the 5th basic human need



Acronis Cyber Protect

- **2,800,000+** workloads protected
- **1,000,000+** attacks prevented
- **20,000+** service providers

Acronis Cyber Foundation Program

**Share the success of
your growing business
by helping others**



**Get your free
CSR in a Box
training kit**

