Acronis

#CyberFit

Acronis Cyber Protect Cloud: Advanced Disaster Recovery

The new world of threats

Natural disasters

- Only 6% of outages are caused by natural disasters[1]
- Affects facilities and infrastructure

Pandemics

- Requires a different kind of planning scenario
- Affects people

Natural

Hardware failure, software corruption

Up to 30M SMBs are vulnerable to IT failure without comprehensive monitoring[2]

Accidental data deletion

14% of data loss is caused by human error, such as deleting or overwriting files[3]

Cyberattacks

- 93% of businesses were attacked within the past three years[2]
- Malware attacks increased by 25%[4]
- By 2021 cybercrimes will cost $6 trillion per year[4]

Human

(1) Actual Tech Media, (2) IDC, (3) Tech Radar, (4) Symantec 2019 ISTR

Business disruption happens

25%

Of data breaches in 2019 were caused by accidentally deleting or overwriting files or folders[1]

51%

Of data breaches in 2019 were caused by criminal and malicious attacks[1]

70%

Of organizations are likely to suffer business disruption by 2022 due to unrecoverable data loss[2]

93%

Of businesses experienced attacks within the past three years[3]

[1] PONEMON INSTITUTE, 2019
[2] GARTNER, 2019
[3] IDC, 2019

Clients can’t afford downtime

4/10
businesses **suffered a data breach** in 2020

14.1 hours
average **annual downtime** for businesses

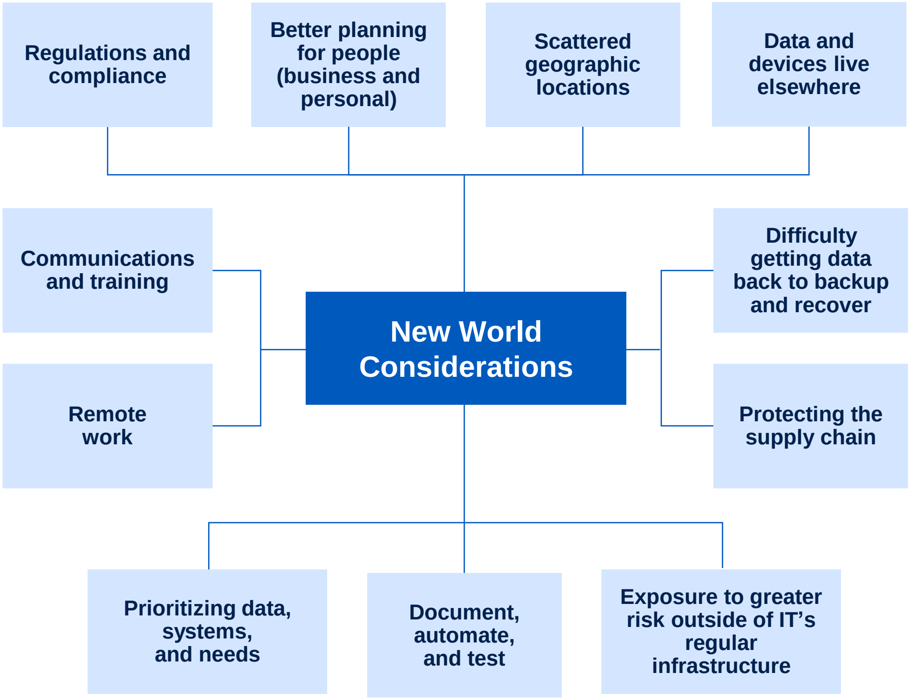
$8,600
average hourly cost of **unplanned downtime** for an SMB

545 hours
average annual hours of **lost staff productivity**

Consider the expected, and unexpected

Traditionally, managing this scenario wouldn't be possible.

When you have a comprehensive platform, you have true power – no matter where your clients are or which devices they're using.



New World Considerations

Regulations and compliance

Better planning for people (business and personal)

Scattered geographic locations

Data and devices live elsewhere

Communications and training

Remote work

Difficulty getting data back to backup and recover

Protecting the supply chain

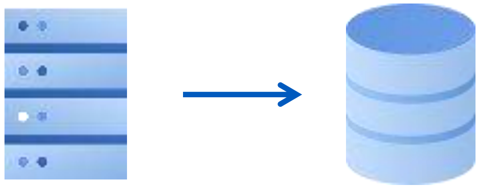
Prioritizing data, systems, and needs

Document, automate, and test

Exposure to greater risk outside of IT's regular infrastructure

Backup is not disaster recovery

Backup



Your data

Backed up
data

Disaster Recovery

Your data

Backed up
data

Cloud infrastructure
to run servers
up data

Backup vs. disaster recovery

	Backup	Disaster Recovery
Key functions	Protection of data from loss	▪ High availability of critical applications ▪ Rapid recovery after a disaster
Target devices	Servers, workstations, mobile devices	Physical or virtual servers
Recovery requirements	▪ Data loss avoidance ▪ Ability to restore/access single items fast	▪ Failover critical workloads quickly to an offsite, malware-free environment ▪ Fail back to a primary site
Required infrastructure	Local and offsite backup tier storage	▪ High-performance offsite storage ▪ Compute and networking resources ▪ DR orchestration software
Storage type	Cold storage	Warm/Hot storage
Applications recovery time	Hours to days	Minutes to hours
Usage frequency	Often	Critical times

Forwarding-thinking SPs Grow Revenue with DRaaS

Protect your clients' data, applications, and systems beyond backup

Increase ARPU

- Sell more cyber protection services
- Get more margin on in-demand services
- Improve attach rate and sell more

Improve SLAs

- Proactively avoid downtime
- Faster remediation with improved endpoint and data protection
- Win more clients with better SLAs

Control Costs

- Reduce expenses by using one tool for all your daily tasks:
  - Onboarding
  - Monitoring
  - Management
  - Assistance
- No new HW/staff required

Decrease Churn

- Improve client satisfaction and keep them coming back for more
- Demonstrate value and simplify renewals
- More services mean stickier clients

Offer DRaaS

- Easy additional revenue:
  - Little investment
  - Turn-key solution for Acronis Cyber Protect Cloud protected endpoints
- Better protection for your clients

Disaster recovery has evolved

1990s → 2000s → 2010s

Company data center or co-location cage

- Depreciated hardware
- Networking
- Licensing
- Replication platforms
- Massive amounts of storage

Hybrid approach

- Costly licensing
- Complicated
- Limited coverage

Modern hybrid and cloud-based DR

- Cost-effective
- Ease-of-use
- Ready-made

Who needs DR?

Companies that:

- Rely on mission-critical applications and data
- Are subject to regulated compliance requirements
- Are partners in stringent supply chains
- Are located in disaster-prone areas
- Lack technical resources
- Have heavy reliance on IT for business functions
- Lack disaster recovery experience

Key industries

Financial Services

Healthcare

Legal

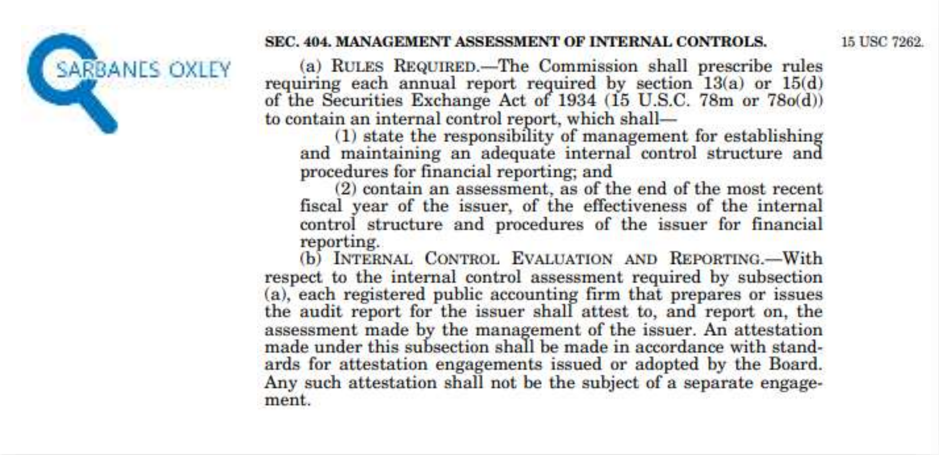
Transportation

Business Services

Manufacturing

Construction

Regulatory requirements and controls for backup and DR


SARBANES OXLEY

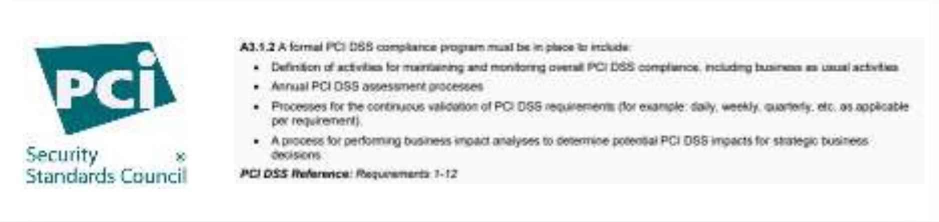
SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS. 15 USC 7262.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

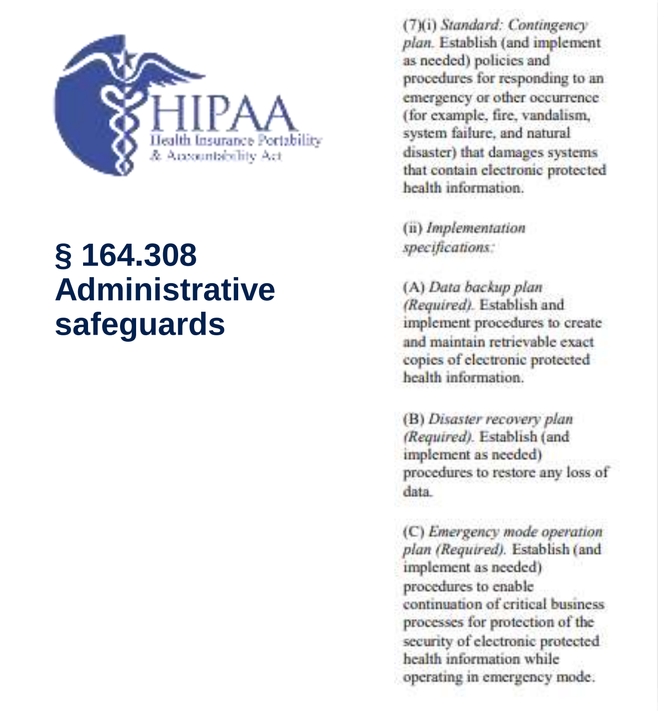
(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.


PCI
Security Standards Council

A3.1.2 A formal PCI DSS compliance program must be in place to include:

- Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business as usual activities
- Annual PCI DSS assessment processes
- Processes for the continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement).
- A process for performing business impact analyses to determine potential PCI DSS impacts for strategic business decisions

***PCI DSS Reference**: Requirements 1-12*


HIPAA
Health Insurance Portability & Accountability Act

§ 164.308 Administrative safeguards

(7)(i) *Standard: Contingency plan.* Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan (Required).* Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan (Required).* Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan (Required).* Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Acronis

#CyberFit

Advanced Disaster Recovery

At-a-glance

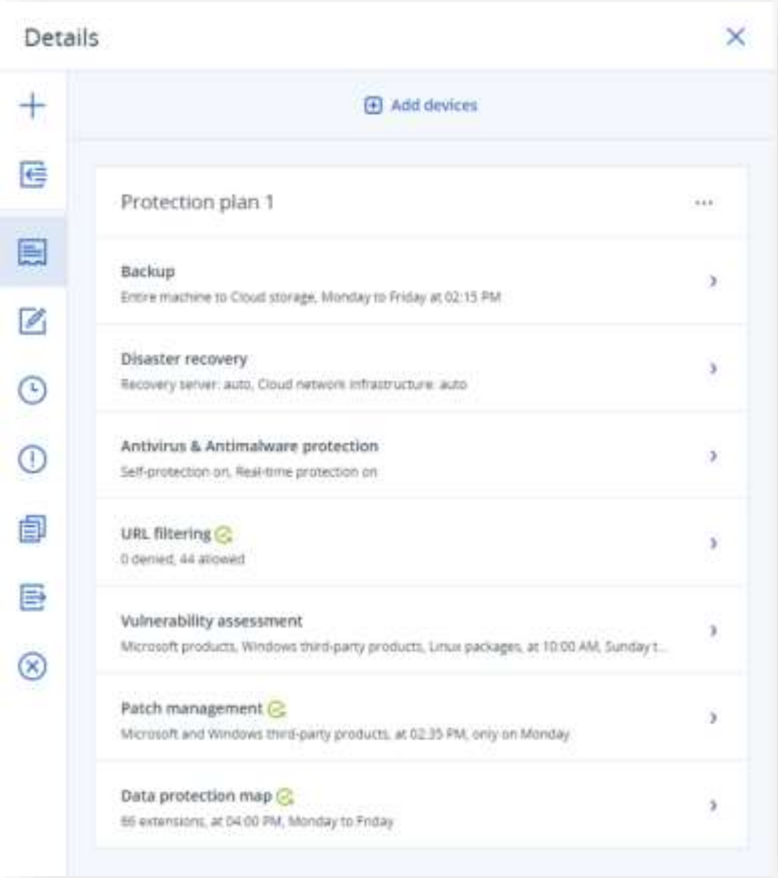
Deep integration enables new capabilities

Integration at all levels: management, products, technology

Harness the power of ONE:

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

One Agent ● Policy ● UX/UI ● License ● Vendor



Protection plan 1

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

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

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

URL filtering
0 denied, 44 allowed

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

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

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

Acronis Cyber Protect Cloud with Advanced Disaster Recovery

Less downtime

Get clients running in mere minutes by spinning up IT systems in the Acronis cloud with full site-to-site connectivity and the ability to recover them to similar or dissimilar hardware.

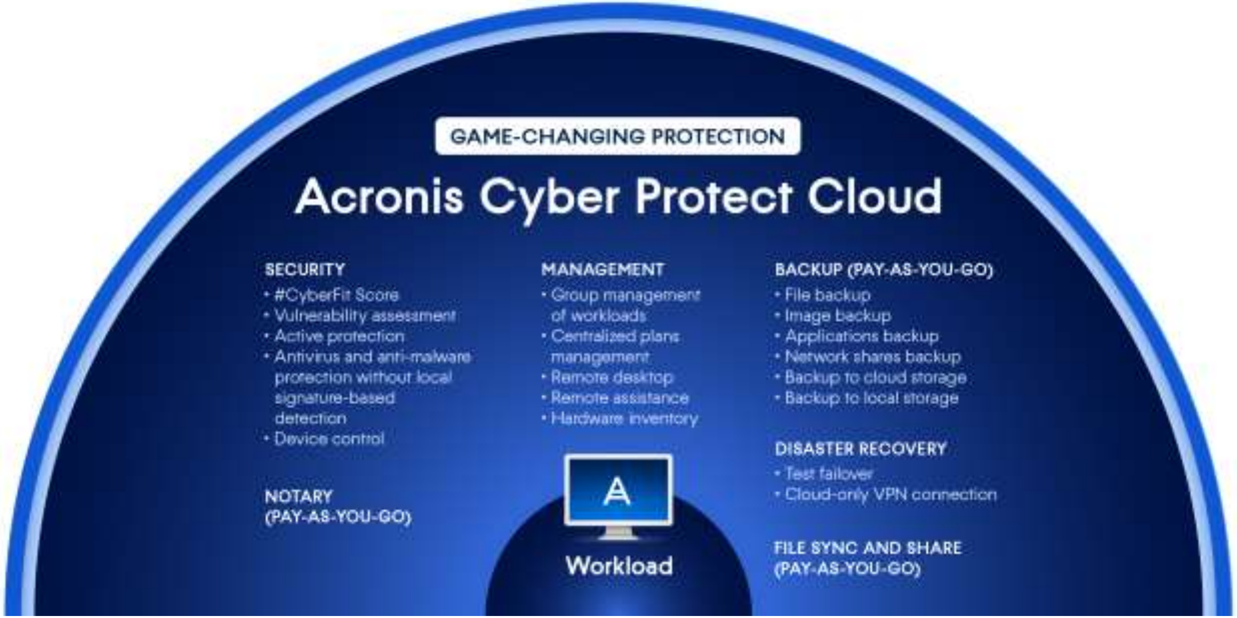
Minimize complexity

No need to add, learn, or manage another platform. It’s one solution for any workload managed from a single interface that enables you to build a complete cyber protection service.

Grow recurring revenue

Deliver more value, deepen client relationships, and increase retention by offering clients the disaster recovery services they are looking for – while increasing your monthly recurring revenue.

Best-in-breed backup
with integrated security and management



GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

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

NOTARY (PAY-AS-YOU-GO)

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

BACKUP (PAY-AS-YOU-GO)
- File backup
- Image backup
- Applications backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY
- Test failover
- Cloud-only VPN connection

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

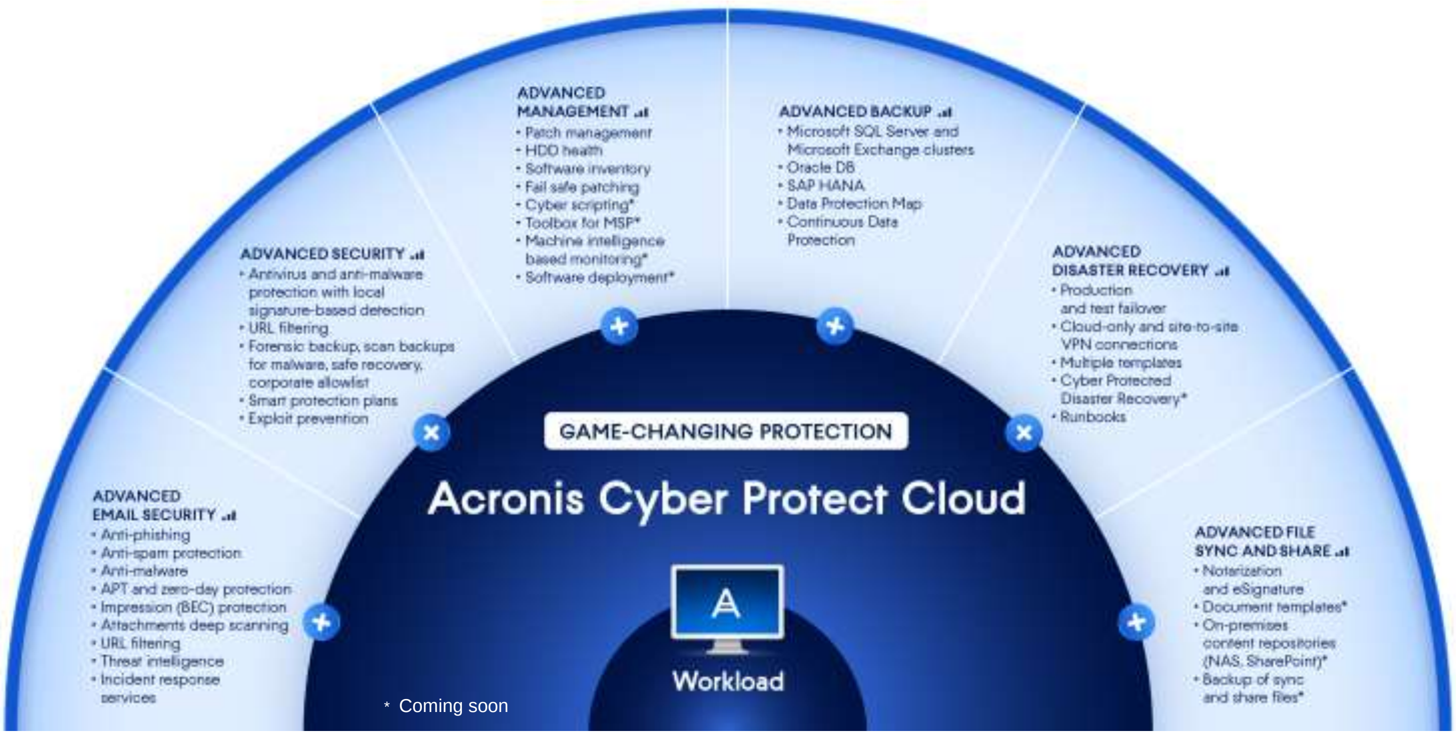
Protect every workload at no charge

Best-in-breed backup included

Strengthens your AV against zero-day threats

Accelerate security and manageability

Add Advanced Disaster Recovery Pack



GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

Workload

ADVANCED EMAIL SECURITY
- Anti-phishing
- Anti-spam protection
- Anti-malware
- APT and zero-day protection
- Impression (BEC) protection
- Attachments deep scanning
- URL filtering
- Threat intelligence
- Incident response services

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

ADVANCED MANAGEMENT
- Patch management
- HDD health
- Software inventory
- Fail safe patching
- Cyber scripting*
- Toolbox for MSP*
- Machine intelligence based monitoring*
- Software deployment*

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

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

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

* Coming soon

Optimize for every workload **Increase your service offerings** **Consolidate vendors**

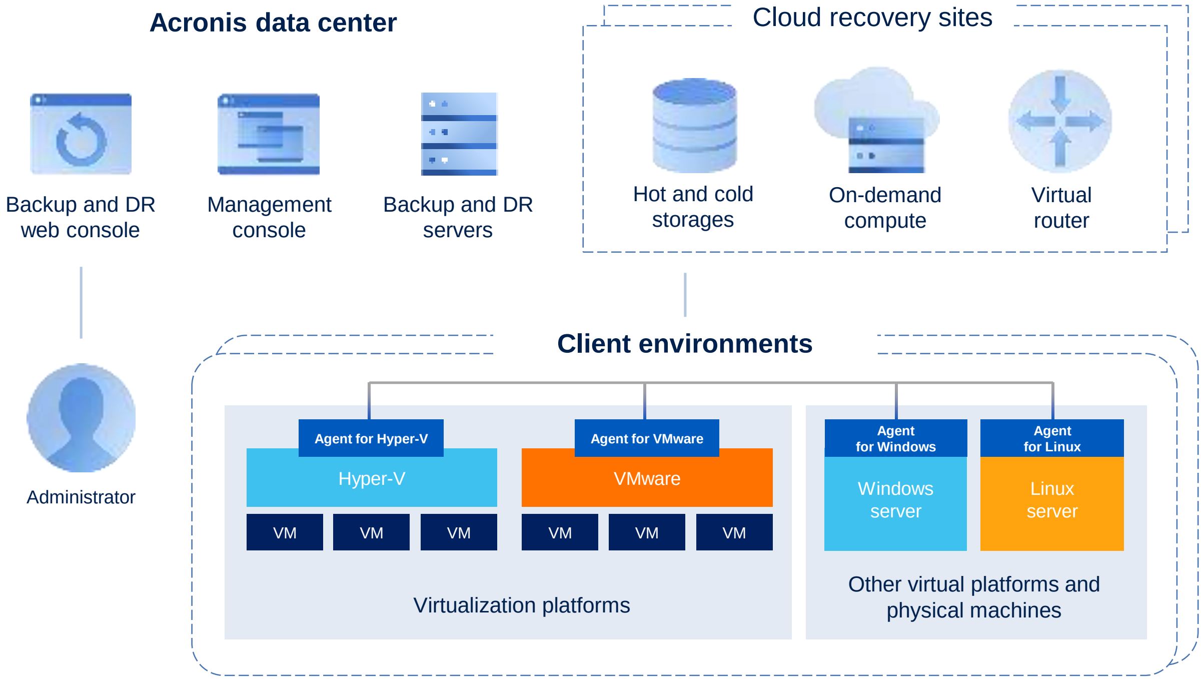
Disaster Recovery for Any Server Workload

Physical and virtual machines	Windows	Linux
Virtualization platforms	▪ VMware vSphere ▪ Microsoft Hyper-V ▪ Linux KVM	▪ Red Hat Virtualization ▪ Citrix XenServer
Cloud servers for real-time application replication	For applications with built-in replication like SQL Server AlwaysOn	

Microsoft

- Windows Server
- Exchange
- SQL Server
- Share Point
- Active Directory
- Hyper-V
- Citrix XenServer
- Linux Server
- VMware vSphere
- Red Hat Virtualization
- Linux KVM

Sample High-Level Architecture



All DRaaS components out-of-the-box.

Easier and quicker PoC and deployment stages.

All key DR operations done from a single web console.

Acronis

#CyberFit

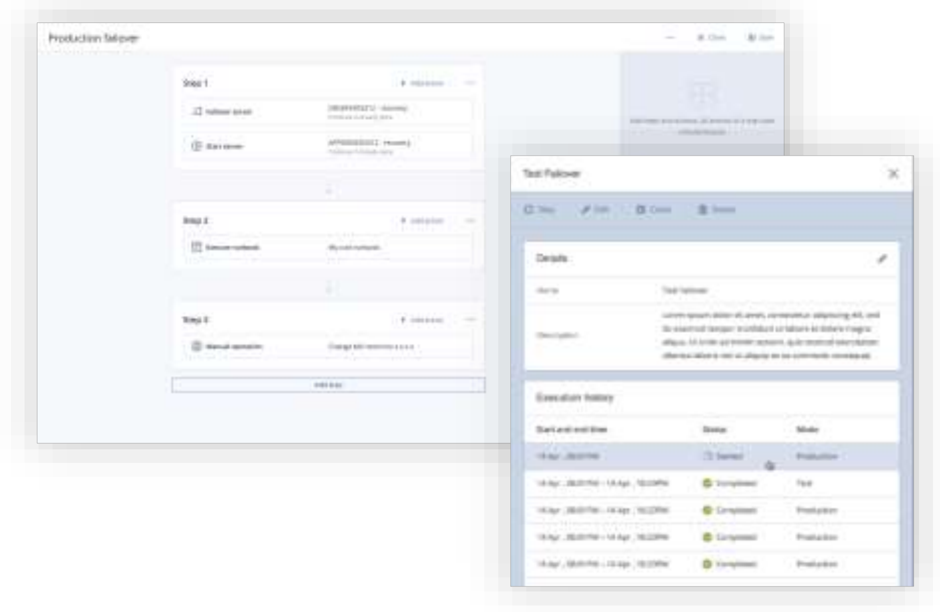
Advanced Disaster Recovery

Features

Improve RTOs and automate disaster recovery with runbooks

The runbooks feature simplifies and speeds up failover of multiple machines to a cloud recovery site.

It allows efficient operations to automate failover and testing and ensures the systems are recovered in the right order to address interdependencies between applications on different machines.



Why? Ensures that all systems are recovered in the right order

Improve RTOs and automate recovery with runbooks

Design

Use the intuitive **drag-and-drop editor** to define groups of machines and sequences of action with these groups

Test

Verify the integrity of your disaster recovery plans by executing runbooks in the **test mode** in the web console

Execute

Execute runbooks in a few clicks when the real disaster strikes and minimize RTOs with fast failover and failback of multiple servers

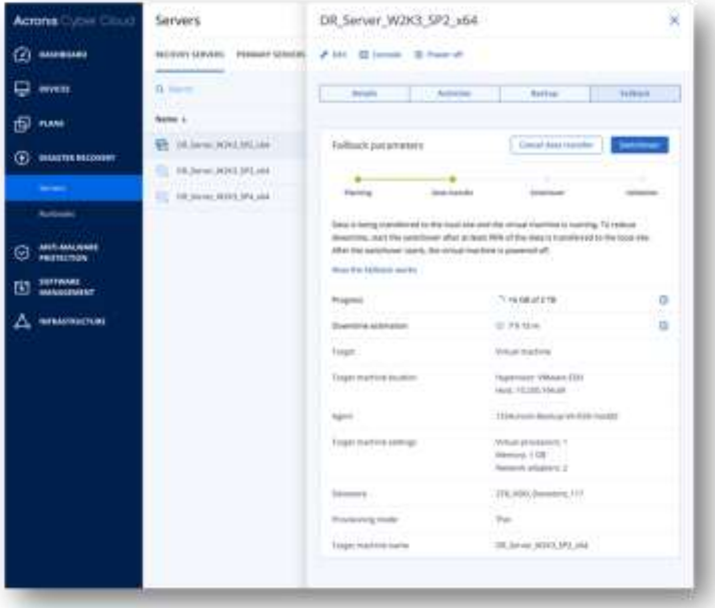
Monitor

Gain disaster recovery orchestration visibility with a detailed **runbook execution real-time view** and **execution history**

Automated failback for virtual machines

Achieve best-in-class failback times and safeguard your clients’ data by transferring it to the local site, while the virtual machine in the cloud is still running. Receive system progress updates and expected downtimes estimates to effectively plan the failback process.

- Streamline your efforts by managing the whole process in one panel
- Benefit from one of the lowest switchover downtimes on the market
- Eliminate confusion with easy user instructions in the interface



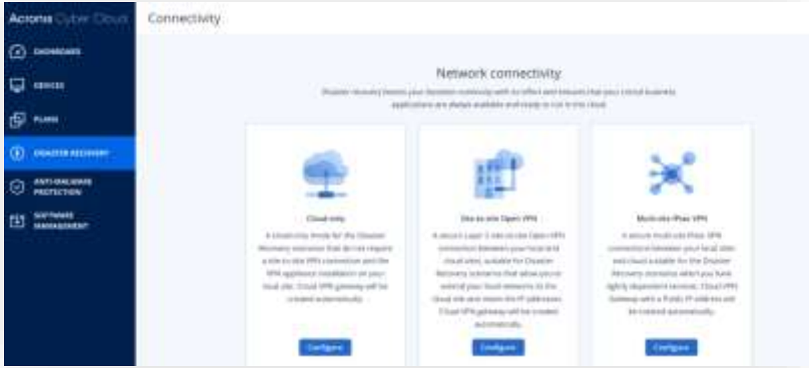
Why? Achieve near-zero downtime, ensure business continuity, and safeguard your clients’ data

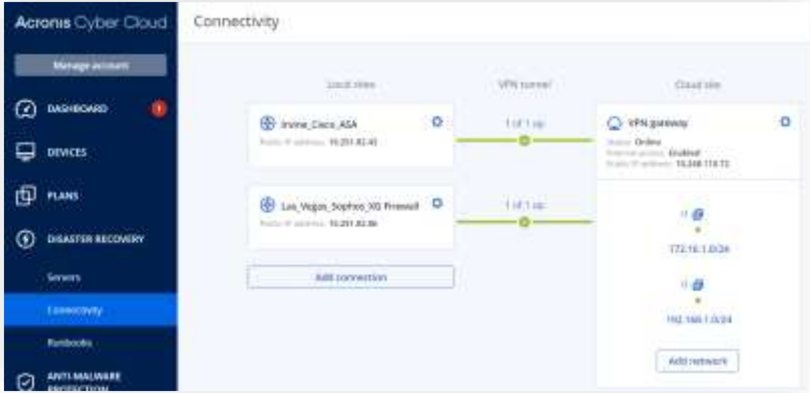
IPsec Multisite VPN Support

Strengthen security for your clients

Integrates secure protocols and algorithms, so you can easily support clients with multiple sites that are hosting critical workloads with higher requirements for security, compliance, and bandwidth.

Transparent connections and tunnels status and self troubleshooting.





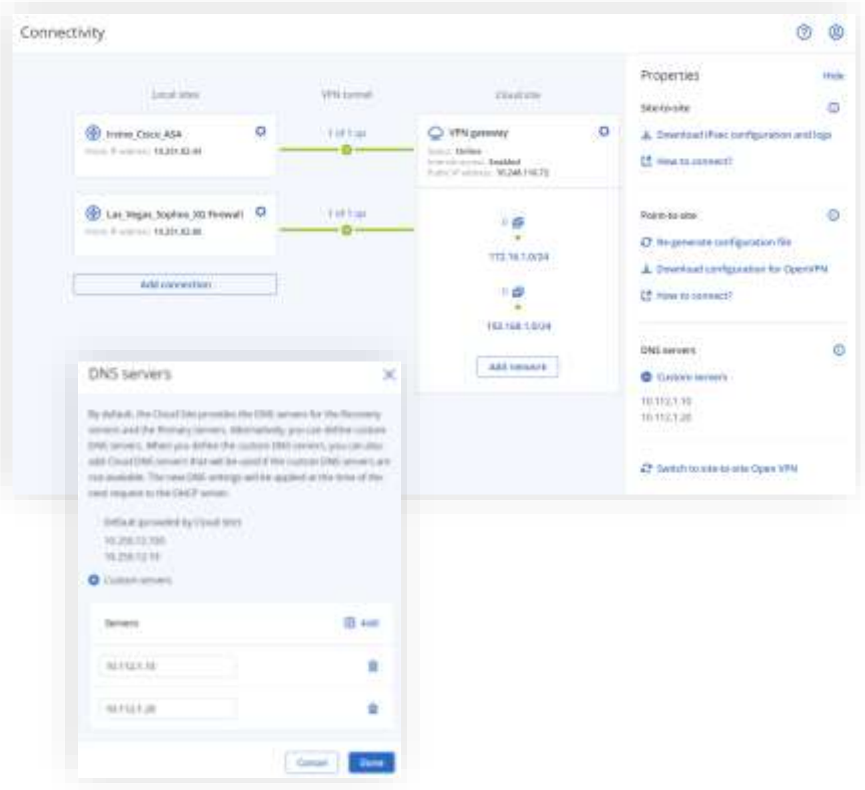
Why? Easily support clients with multiple sites that are hosting critical workloads

Custom DNS configuration

Provide flexibility by setting up custom DNS configurations

Easily adjust DNS settings for your cloud servers, that are dependent on your own DNS services.

Set up custom DNS settings for Disaster recovery cloud servers for the whole disaster recovery infrastructure in the Acronis cloud.



DNS servers

By default, the Cloud Site provides the DNS servers for the Recovery servers and the Primary servers. Alternatively, you can define custom DNS servers. When you define the custom DNS servers, you can also add Cloud DNS servers that will be used if the custom DNS servers are not available. The new DNS settings will be applied at the time of the next request to the DHCP server.

○ Default (provided by Cloud Site)
10.250.12.100
10.250.12.10

● Custom servers

Servers
10.112.1.10
10.112.1.20

Why? Makes it even easier for you to support your clients

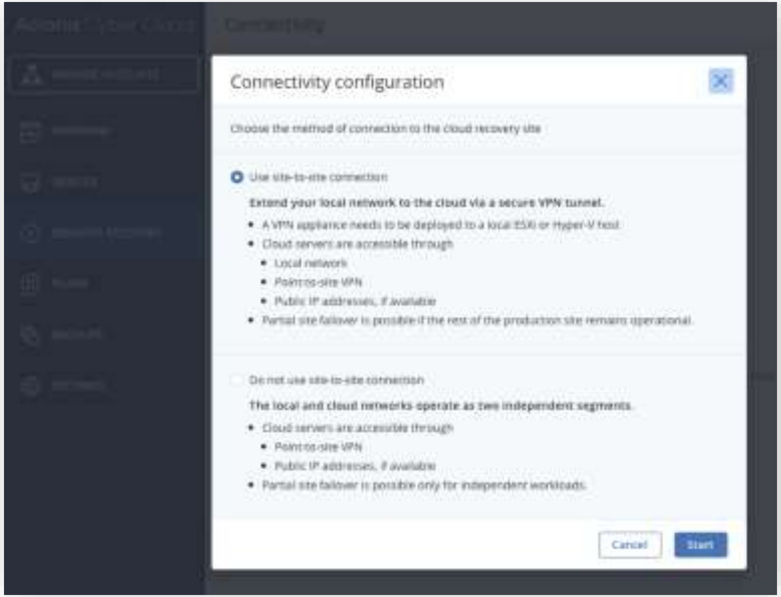
VPN-less deployment option

Onboard clients more quickly and easily

VPN virtual appliance is not necessary for “point-to-site” connectivity.

Switch from the “point-to-site” to “site-to-site” mode as you wish.

This option is especially useful for customers who want to quickly evaluate the service or don’t need to extend the local network to the cloud site.



Connectivity configuration

Choose the method of connection to the cloud recovery site

● Use site-to-site connection

Extend your local network to the cloud via a secure VPN tunnel.

- A VPN appliance needs to be deployed to a local ESXi or Hyper-V host.
- Cloud servers are accessible through
  - Local network
  - Point-to-site VPN
  - Public IP addresses, if available
- Partial site failover is possible if the rest of the production site remains operational.

○ Do not use site-to-site connection

The local and cloud networks operate as two independent segments.

- Cloud servers are accessible through
  - Point-to-site VPN
  - Public IP addresses, if available
- Partial site failover is possible only for independent workloads.

Why? Connect clients’ quickly and easily with point-to-site or site-to-site connectivity

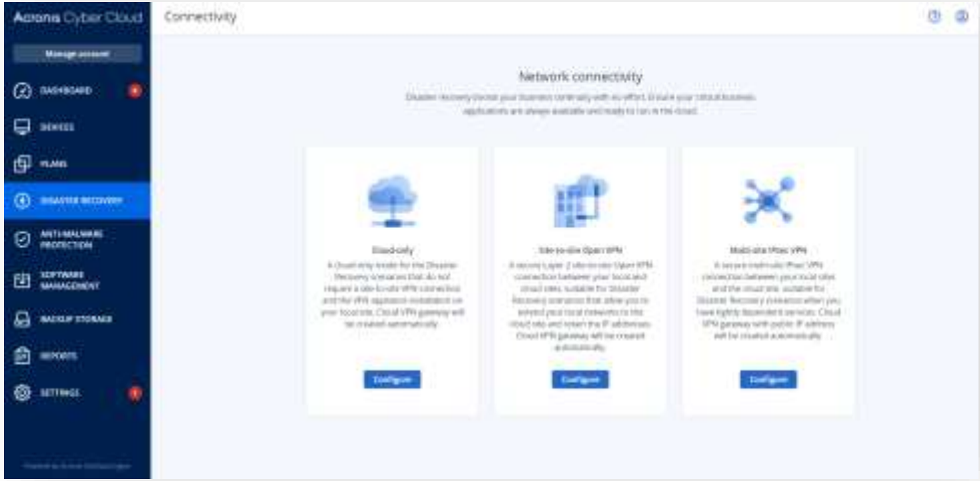
Multiple networks support

Support more complex customer infrastructures

Extend up to five local networks to the Acronis Cloud Recovery Site through the single site-to-site connection.

Failover complex environments where protected servers are distributed across several network segments.

See connectivity statuses of all five networks in one view.



Network connectivity

Disaster recovery. Boost your business continuity with no effort. Ensure your critical business applications are always available and ready to run in the cloud.

Cloud-only

A cloud-only mode for the Disaster Recovery scenarios that do not require a site-to-site VPN connection and the VPN appliance installation on your local site. Cloud VPN gateway will be created automatically.

Configure

Site-to-site Open VPN

A secure Layer 2 site-to-site Open VPN connection between your local and cloud sites, suitable for Disaster Recovery scenarios that allow you to extend your local networks to the cloud site and retain the IP addresses. Cloud VPN gateway will be created automatically.

Configure

Multi-site IPsec VPN

A secure multi-site IPsec VPN connection between your local sites and the cloud site, suitable for Disaster Recovery scenarios when you have tightly dependent services. Cloud VPN gateway with public IP address will be created automatically.

Configure

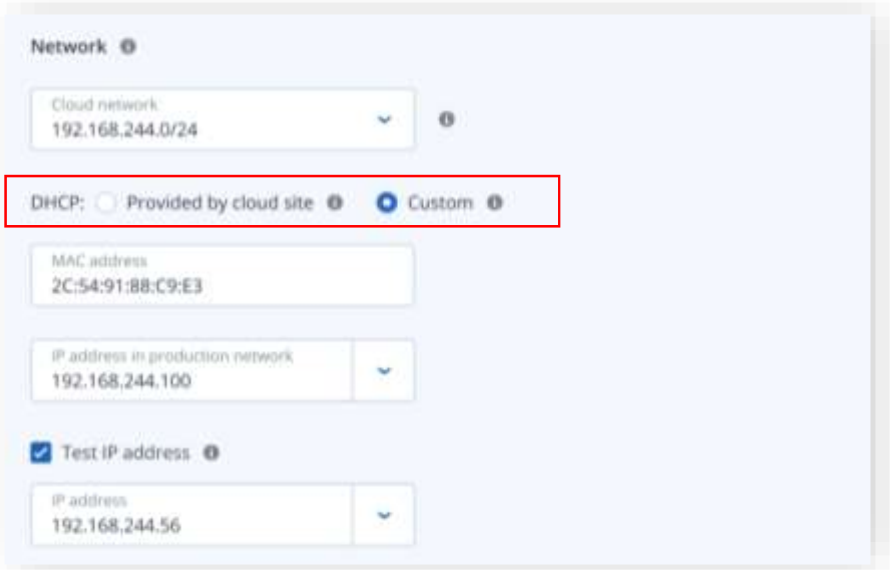
Why? Assist different kinds of clients by supporting more complex infrastructures

Disaster recovery for DHCP servers

Unlock more failover scenarios for licensed applications

By running your own DHCP service on a recovery server during failover or test failover, you can gain more control over network configurations and IP address leases.

Additionally, clients can run applications where the license is bounded to a MAC address.



Network

Cloud network
192.168.244.0/24

DHCP: ○ Provided by cloud site ● Custom

MAC address
2C:54:91:88:C9:E3

IP address in production network
192.168.244.100

☑ Test IP address

IP address
192.168.244.56

Why? Gain broader failover control and more failover scenarios

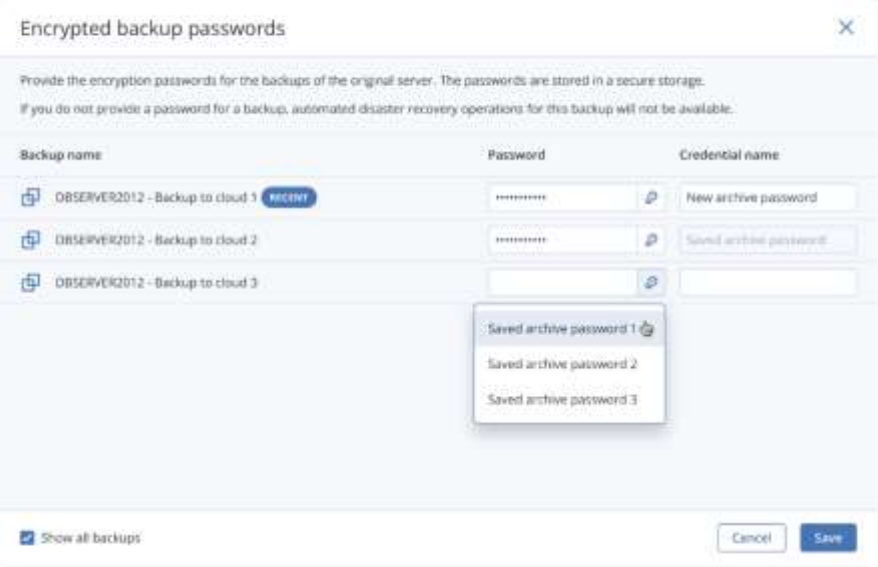
Encrypted backup support

Comply with data security requirements

Perform failover using encrypted backups and allow the system to use the securely stored passwords for automated disaster recovery operations.

The new Credential Store feature (accessible from the web console in the Disaster Recovery > Credential Store tab) allows you to securely store and manage passwords for encrypted server backups.

Comply with various data regulations.



Encrypted backup passwords

Provide the encryption passwords for the backups of the original server. The passwords are stored in a secure storage.

If you do not provide a password for a backup, automated disaster recovery operations for this backup will not be available.

Backup name	Password	Credential name
OBSERVER2012 - Backup to cloud 1 RECENT	••••••••••••	New archive password
OBSERVER2012 - Backup to cloud 2	••••••••••••	Saved archive password
OBSERVER2012 - Backup to cloud 3		

☑ Show all backups

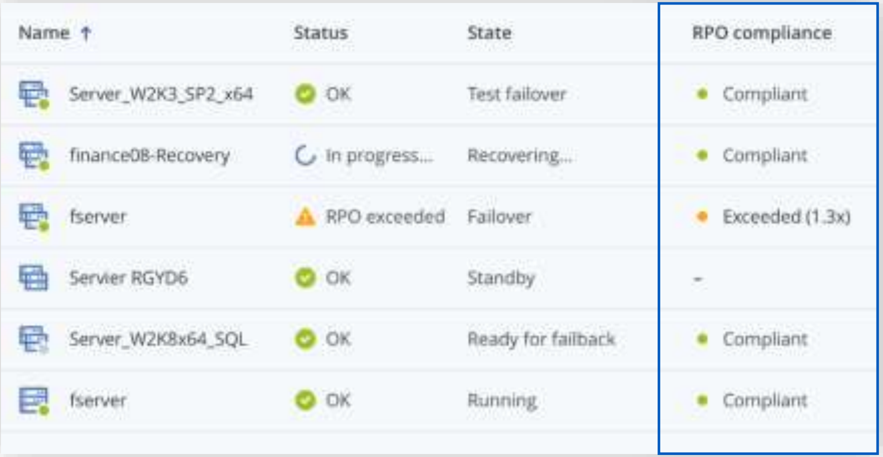
Why? Keep clients' data safe while complying with various data regulations

Recovery servers RPO compliance tracking

Improve SLA compliance

Define recovery point thresholds for the recovery servers to identify how "fresh" the cloud backup of the original machine (to perform failover) should be.

Track recovery point objective (RPO) compliance in real time via the web console.



Name ↑	Status	State	RPO compliance
Server_W2K3_SP2_x64	✓ OK	Test failover	● Compliant
finance08-Recovery	In progress...	Recovering...	● Compliant
fserver	⚠ RPO exceeded	Failover	● Exceeded (1.3x)
Servier RGYD6	✓ OK	Standby	-
Server_W2K8x64_SQL	✓ OK	Ready for failback	● Compliant
fserver	✓ OK	Running	● Compliant

Why? Provide competitive SLAs and ensure you are able to meet them

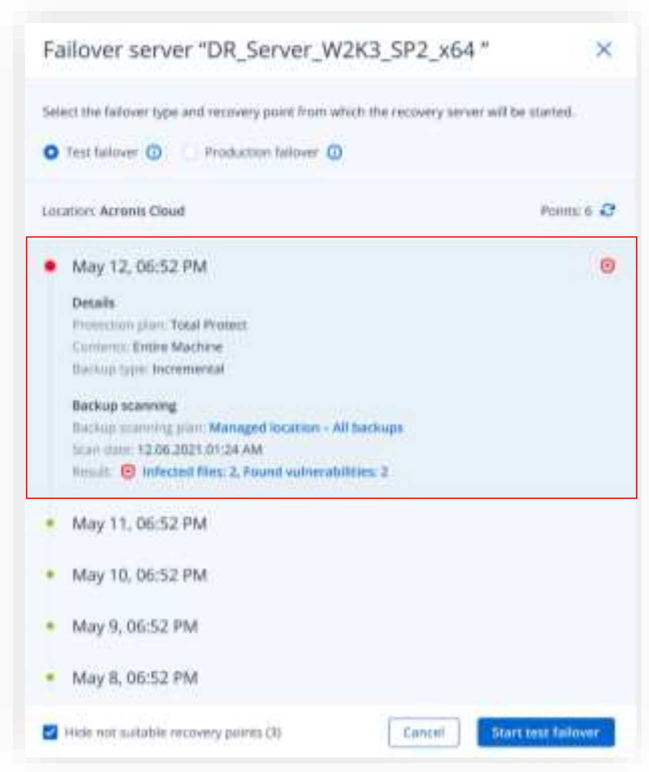
Failover to a malware-free recovery point

Avoid reinfection by being proactive

Check the list of recovery points available for failovers to see if a malware or other indicator of compromise was discovered during the backup scanning process.*

Ensure a faster, safer return to productivity by preventing reinfection via a compromised recovery point.

* To perform anti-malware scanning of backups, Advanced Security must be enabled.



Failover server "DR_Server_W2K3_SP2_x64 "

Select the failover type and recovery point from which the recovery server will be started.

● Test failover ○ Production failover

Location: Acronis Cloud   Points: 6

● May 12, 06:52 PM

Details

Protection plan: Total Protect
Contents: Entire Machine
Backup type: Incremental

Backup scanning

Backup scanning plan: Managed location - All backups
Scan date: 12.06.2021 01:24 AM
Result: Infected files: 2, Found vulnerabilities: 2

● May 11, 06:52 PM

● May 10, 06:52 PM

● May 9, 06:52 PM

● May 8, 06:52 PM

☑ Hide not suitable recovery points (3)

Why? Ensure successful recovery by selecting malware-free recovery points

Acronis

#CyberFit

Advanced Disaster Recovery Licensing

Advanced Disaster Recovery: Licensing Highlights

Advanced Disaster Recovery can be added **to both per-GB and per-workload licensing models** of Acronis Cyber Protect Cloud.

Disaster recovery storage is a single billing item – it is similar to regular backup cloud storage in regards to its unit of measure and usage calculation.

Acronis Hosted cloud storage and service provider cloud storage are the only options available. **The cost is per GB for both storages.**

Acronis

Advanced Disaster Recovery: Costs

When protecting your workloads with advanced disaster recovery features in both per-GB and per-workload models, you also pay for:

DR to Acronis Cloud or Service Provider Cloud

Total DR storage space used in Acronis Cloud or in a service provider cloud. You pay only after a cloud backup is created.

+

Compute resources

Compute resources refer to the amount of vCPUs and RAM you are using with assigned per-hour compute values.

Compute cost is per hour and is applied only when a cloud server is active (e.g. in a failover, testing mode, or running as a primary server).

+

Disaster Recovery IP (optional)

Dedicated public-facing IP addresses can be added to servers that require external network access. You will only be charged if an external IP address is added to a server.

Note: Charges for compute resources and disaster recovery IP are calculated only if used with Acronis-hosted cloud storage

Compute resources: Pricing

Let’s look more closely at how compute resources are priced:

- Compute resources are priced per hour and if used with Acronis-hosted cloud storage.
- The price depends on the cloud server configuration and is measured in compute points (see the table below).
- Total account compute-resources usage is calculated as the sum of compute points consumed by all cloud servers, then rounded to the next highest integer.

Type	vCPU	RAM	Compute points
F1	1 vCPU	2 GB	1 point
F2	1 vCPU	4 GB	2 points
F3	2 vCPU	8 GB	4 points
F4	4 vCPU	16 GB	8 points
F5	8 vCPU	32 GB	16 points
F6	16 vCPU	64 GB	32 points
F7	16 vCPU	128 GB	64 points
F8	16 vCPU	256 GB	128 points

Example

If you have two cloud servers - an F2 type (2 points) that ran for 15 minutes, and an F5 type (16 points) that ran for 30 minutes, then:

(2 points x 15 minutes) + (16 points x 30 minutes) =
(2 points x 15/60) + (16 points x 30/60) = 0.5 + 8 = 8.5
or 9 points after rounding.

ⓘ **Note:** Pricing for compute resources is the same for both models – per GB and per workload.

Advanced Disaster Recovery: SKUs

SKU	Product name	Description
SVEAMSENS	Advanced Disaster Recovery – Acronis-hosted Storage (Per GB)	Refers to Acronis-hosted cloud storage space
SVFAMSENS	Advanced Disaster Recovery – Hybrid Storage (Per GB)	Refers to a service provider’s cloud storage
SQYAMSENS	Advanced Disaster Recovery – Acronis-hosted – 1 compute point (Per running hour)	Refers to standard preconfigured vCPU and RAM configurations with assigned per-hour compute values
SEDAMSENS	Advanced Disaster Recovery – Acronis-hosted Public IP address	Refers to a public-facing IP addresses added to servers

Acronis

#CyberFit

Hybrid Disaster Recovery

Sometimes where data is matters

When do you need Hybrid Disaster Recovery

1. You want to tune DR hardware to specific client needs (application-specific requirements, etc.).
2. You want to have more control over DR scenarios or offerings.
3. Your clients have stringent data localization requirements *(GDPR, Data Sovereignty, industry-specific regulations, consumer data laws, etc.).*
4. Your clients' requirements dictate faster, full recovery time SLAs for RTO and/or RPO *(reducing or eliminating cloud-based latency factors).*
5. You want to increase margins on client accounts with fault and time-tolerant risk profiles.
6. You need to implement cost-containment strategies for storage and compute-intensive applications.
7. You have any other scenario where data location matters.

Hybrid Disaster Recovery

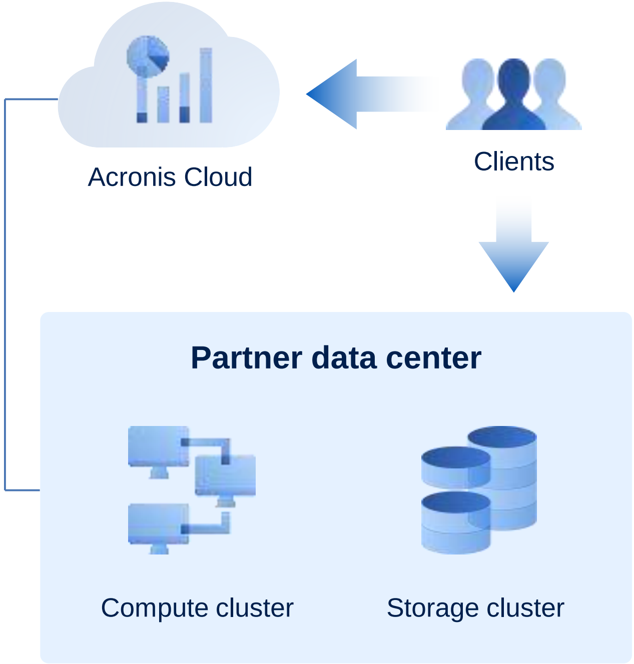
for Acronis Cyber Protect Cloud

Using a combination of Acronis Cloud and your own data center, infrastructure can be tuned to meet specific client requirements.

Whichever deployment option you choose — local or cloud — your clients will benefit from excellent performance, enhanced security and cost optimization, which is not available to them elsewhere.

Adapt to changing client business needs, handle new requirements and control costs.

Learn more



About Acronis

Acronis is a Leader in Cyber Protection

AI-powered Cyber Protection, Cyber Cloud, Cyber Platform

Swiss

Since 2008 Corporate HQ in Schaffhausen, Switzerland

Singaporean

Founded in 2003 in Singapore, currently the International HQ

Dual Headquarters for Dual Protection

Scale, Growth and Reach

$300M+ billings
50% business growth
100%+ cloud growth
100% of Fortune 1000
1,000,000+ businesses
50,000+ partners

Global Local Presence

1,500+ employees
33+ locations
150+ countries
33+ languages
DCs in 100+ countries in the next 24 months

304 Flight Information Regions (FIR)

Acronis Cyber Protect

1,000,000+ workloads protected
1,000,000+ attacks prevented
9,000+ Cloud partners

Solution: Integrated and Autonomous Cyber Protection

Acronis mission is to protect all data, applications and systems (workloads)

S Safety

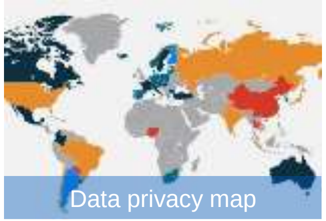
Nothing is lost: there is always a copy for recovery

A Accessibility

Access from anywhere at any time

P Privacy

Control over visibility and access



Data privacy map

A Authenticity

Proof that a copy is an exact replica of the original

S Security

Protection against bad actors

Acronis Cyber Singularity

Autonomous, integrated and modular cyber protection for everybody

Acronis Cyber Protect

Making cyber protection available as a Cloud service and on-premises “Classic” solution

Acronis Cyber Cloud

Control panel for Classic & Cloud: 15k+ resellers and 30k+ service providers by 2022

da Vinci Surgical System

Acronis Cyber Platform

More services for partners, higher margin on more services offered 10k+ certified developers in 2022

Rich ecosystem

Acronis Cyber Infrastructure

Cloud, hardware and software appliances 100+ Acronis DCs, 1,000+ Partner DCs for compute and storage after 2022

Data privacy map

Acronis Cyber Services

Premium support, Acronis #CyberFit Academy, marketing, sales, and development services

Acronis Cyber Foundation

Building a more knowledgeable future

#CyberFit

Create, Spread and Protect Knowledge With Us!

- Building new schools
- Providing educational programs
- Publishing books

www.acronis.org