



# Acronis Cyber Protect Cloud: Advanced Disaster Recovery

## A interrupção dos negócios acontece



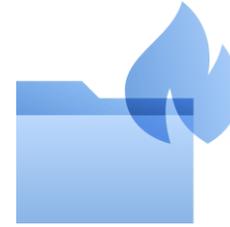
25%

Das violações de dados em 2019 foram causadas pela exclusão ou substituição acidental de arquivos ou pastas<sup>1</sup>



51%

Das violações de dados em 2019 foram causadas por ataques criminosos e maliciosos<sup>1</sup>



70%

Das organizações provavelmente sofrerão interrupções nos negócios até 2022 devido à perda irrecuperável de dados<sup>2</sup>



93%

Das empresas sofreram ataques nos últimos três anos<sup>3</sup>

**FONTES:** 1 PONEMON INSTITUTE, 2019; 2 GARTNER, 2019; 3 IDC, 2019

# Acronis Cyber Protect Cloud com recuperação avançada de desastres



## Menos tempo de inatividade

Coloque os clientes em operação em poucos minutos, ativando sistemas de TI na nuvem da Acronis com conectividade total entre sites e a capacidade de recuperá-los para hardware semelhante ou diferente.



## Minimize a complexidade

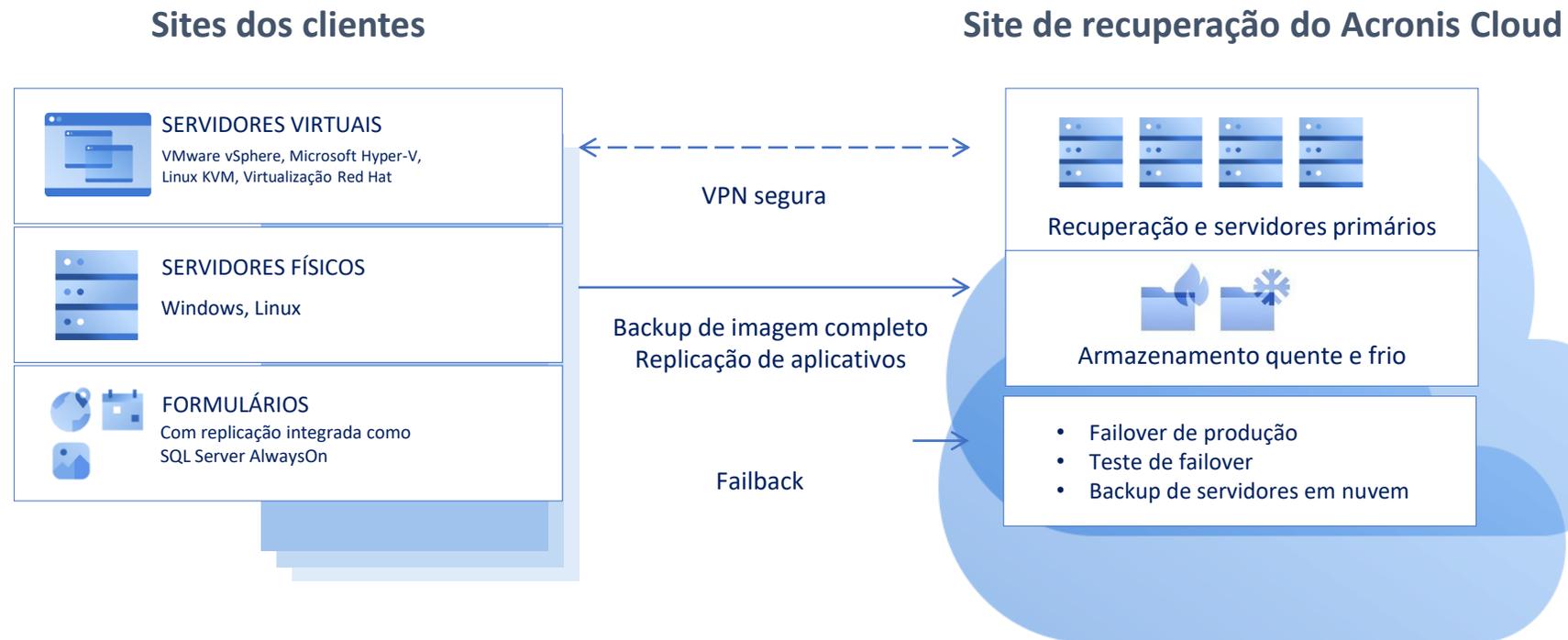
Não há necessidade de adicionar, aprender ou gerenciar outra plataforma. É uma solução para qualquer carga de trabalho gerenciada a partir de uma única interface que permite criar um serviço completo de proteção cibernética.



## Aumente a receita recorrente

Agregue mais valor, aprofunde o relacionamento com os clientes e aumente a retenção, oferecendo aos clientes os serviços de recuperação de desastres que eles procuram – enquanto aumenta sua receita recorrente mensal.

# Recuperação de desastres para o site do Acronis Cloud Recovery



# Recuperação de desastres para qualquer carga de trabalho de servidor

Máquinas físicas e virtuais

Windows

Linux

Plataformas de virtualização

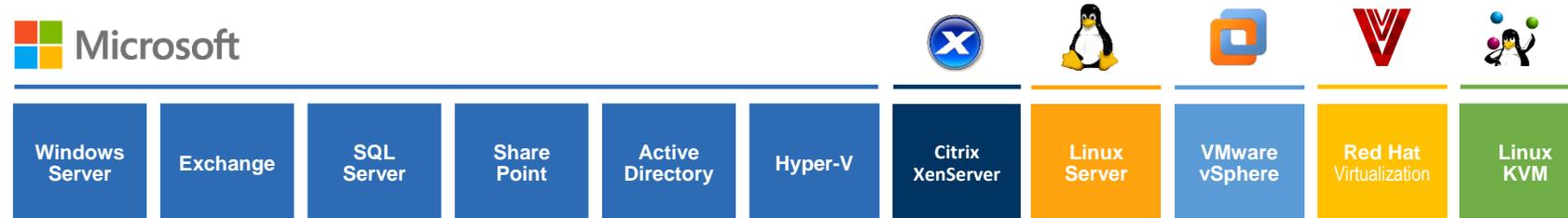
- VMware vSphere
- Microsoft Hyper-V
- Linux KVM

- Red Hat Virtualization
- Citrix XenServer

Servidores em nuvem para replicação de aplicativos em tempo real

Para aplicativos com replicação integrada, como SQL Server AlwaysOn

 Microsoft



# Melhore os RTOs e automatize a recuperação de desastres com runbooks

O recurso de runbooks simplifica e acelera o failover de várias máquinas para um site de recuperação na nuvem.

Ele permite operações eficientes para automatizar failover e testes e garante que os sistemas sejam recuperados na ordem certa para resolver interdependências entre aplicativos em máquinas diferentes.

The image displays two screenshots from the Acronis Cyber Protect Cloud interface. The left screenshot shows a 'Production failover' runbook with three sequential steps:

- Step 1:** Contains two actions: 'Failover server' (DBSERVER2012 - recovery) and 'Start server' (APPSERVER2012 - recovery).
- Step 2:** Contains one action: 'Execute runbook' (My cool runbook).
- Step 3:** Contains one action: 'Manual operation' (Change MX record to x.x.x.x).

The right screenshot shows the 'Test Failover' execution history. It includes a 'Details' section and a table of execution records.

Start and end time	Status	Mode
14 Apr, 08:01 PM	Started	Production
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Test
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Production
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Production
14 Apr, 08:01 PM - 14 Apr, 10:23 PM	Completed	Production

**Por que?** Garante que todos os sistemas sejam recuperados na ordem correta

# Failback automatizado para máquinas virtuais e físicas

Obtenha os melhores tempos de failback e proteja os dados de seus clientes transferindo-os para o site local, enquanto a máquina virtual na nuvem ainda está em execução. Receba atualizações do progresso do sistema e estimativas de tempos de inatividade esperados para planejar com eficácia o processo de failback.

- Simplifique seus esforços gerenciando todo o processo em um painel
- Beneficie-se de um dos tempos de inatividade de transição mais baixos do mercado
- Elimine a confusão com instruções fáceis de usuário na interface

The screenshot displays the Acronis Cyber Cloud interface. On the left is a navigation sidebar with options: DASHBOARD, DEVICES, PLANS, DISASTER RECOVERY (selected), Runbooks, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, and INFRASTRUCTURE. The main area shows a 'Servers' list with columns for RECOVER SERVERS and PRIMARY SERVERS. A search bar is present. Below the list, a 'Failback' window is open for 'DR\_Server\_W2K3\_SP2\_x64'. This window has tabs for Details, Activities, Backup, and Failback. The 'Failback parameters' section includes a progress bar with stages: Planning, Data transfer, Switchover, and Validation. Below the progress bar, there is a text box explaining the process: 'Data is being transferred to the local site and the virtual machine is running. To reduce downtime, start the switchover after at least 90% of the data is transferred to the local site. After the switchover starts, the virtual machine is powered off.' A 'Switchover' button is visible. Below this, a table titled 'How the failback works' provides details:

Progress	16 GB of 2 TB
Downtime estimation	7 h 15 m
Target	Virtual machine
Target machine location	Hypervisor: VMware ESXi Host: 10.250.194.69
Agent	125Acronis-Backup-WA-ESXi-host82
Target machine settings	Virtual processors: 1 Memory: 1 GB Network adapters: 2
Datastore	2TB_HDD_Datastore_117
Provisioning mode	Thin
Target machine name	DR_Server_W2K3_SP2_x64

## Por que?

Obtenha tempo de inatividade próximo de zero, garanta a continuidade dos negócios e proteja os dados dos seus clientes

# Failover de teste automatizado

Economize tempo e esforço com testes de failover automatizados e simplificados.

Com o pacote de recuperação avançada de desastres, você pode realizar testes programados e automatizados para qualquer servidor, semanal ou mensalmente, dando-lhe a confiança de que poderá se recuperar com rapidez e sucesso.

- A verificação de captura de tela com tecnologia de IA é usada para verificar se as cargas de trabalho estão funcionando na nuvem
- Um relatório consolidado é criado após cada sessão de teste com os detalhes dos testes para cada carga de trabalho

### Create recovery server

General | Cloud Firewall Rules

**Server configuration**

CPU and RAM  
1 vCore.4 GB RAM

The cost of running this server is 1 compute point per hour.

Type:  Warm  Cold

Retention (last recovery point)  
- 1 +

**Production network**

Cloud network  
192.168.244.0/24

DHCP:  Provided by cloud site  Custom

IP address in production network  
192.168.244.100

**Test network**

External test IP address

IP address  
192.168.244.56

**Automated test failover**

Schedule  
Monthly

Screenshot timeout / Min  
5  Save as default timeout

In automated test failover, the system takes a screenshot of the latest recovery point and validates if the operating system of the recovery server can be started. The process starts automatically at scheduled intervals.

Each automated test failover that is performed consumes compute points.

### DR\_Server\_W2K3\_SP2\_x64

Fallover | Edit | Delete

Details | Activities

**Server details**

Original server	vm-Win-2012-ABA12
Description	-
Type	Warm
Status	OK
State	Standby
Last recovery point	Ready
Actual RPO	Compliant

**Automated test failover**

Schedule: Monthly  
Screenshot timeout: 5 min  
Last start: Jul 9, 2022 12:00 AM + 02:00  
Last status: Success  
Next start: Jul 10, 2022  
[Show screenshot](#)

# Suporte VPN multisite IPsec

Reforce a segurança dos seus clientes

Integra protocolos e algoritmos seguros, para que você possa oferecer suporte facilmente a clientes com vários sites que hospedam cargas de trabalho críticas com requisitos mais elevados de segurança, conformidade e largura de banda.

Status transparente de conexões e túneis e solução automática de problemas.

The image displays two screenshots of the Acronis Cyber Cloud interface. The top screenshot shows the 'Connectivity' section with three options: 'Cloud-only', 'Site-to-site Open VPN', and 'Multi-site IPsec VPN'. Each option includes a brief description and a 'Configure' button. The bottom screenshot shows a detailed view of the 'Connectivity' section, displaying 'Local sites' (Irvine\_Cisco\_ASA and Las\_Vegas\_Sophos\_XG Firewall) connected to a 'VPN tunnel' (1 of 1 up), and a 'Cloud site' (VPN gateway) with status 'Online' and internet access 'Enabled'. It also shows two IP addresses (172.16.1.0/24 and 192.168.1.0/24) and an 'Add network' button.

**Por que?** Dê suporte facilmente a clientes com vários sites que hospedam cargas de trabalho críticas

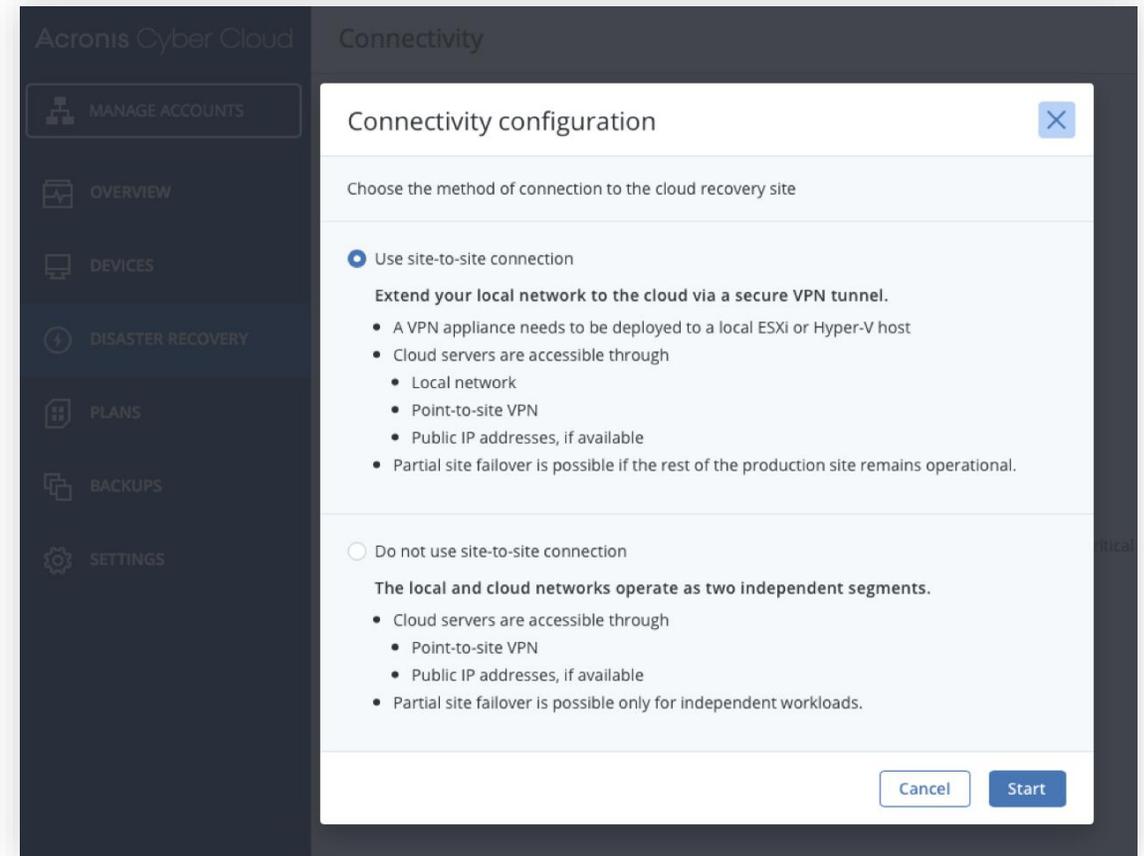
# Opção de implantação sem VPN

## Integre clientes mais rapidamente e facilmente

O dispositivo virtual VPN não é necessário para conectividade “ponto a site”.

Mude do modo “ponto a site” para “site a site” conforme desejar.

Esta opção é especialmente útil para clientes que desejam avaliar rapidamente o serviço ou não precisam estender a rede local até o site na nuvem.



**Por que?** Conecte clientes de forma rápida e fácil com conectividade ponto a site ou site a site

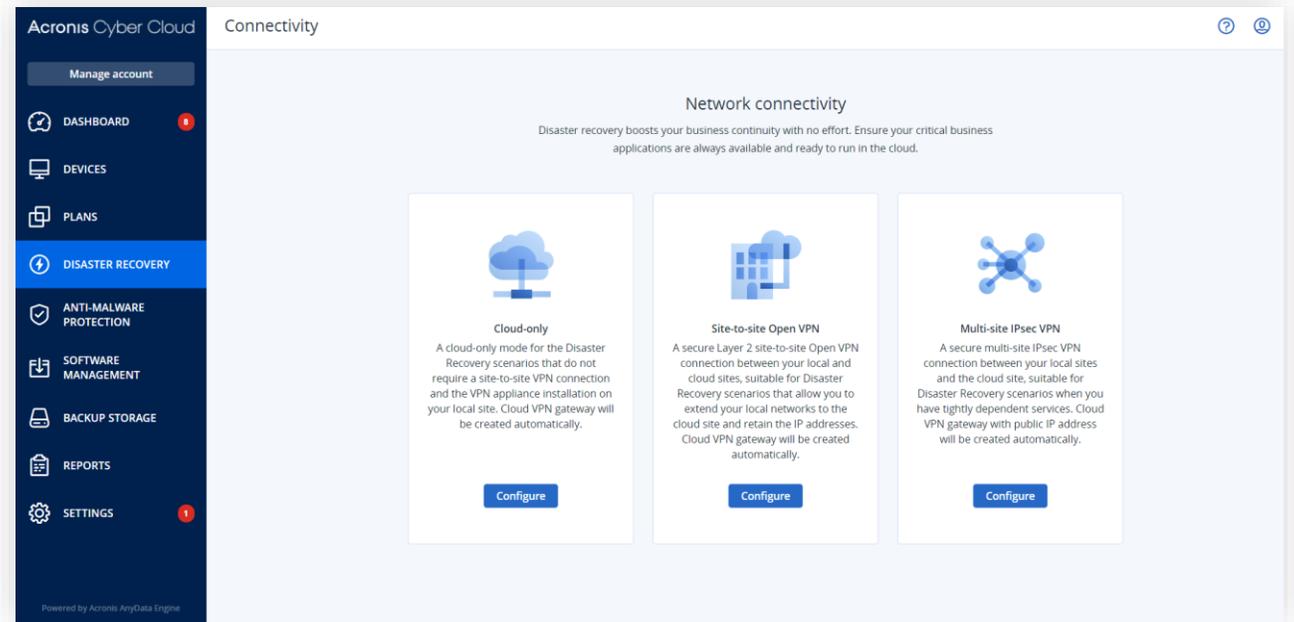
# Suporte a múltiplas redes

Apoie infraestruturas de clientes mais complexas

Estenda até cinco redes locais ao site do Acronis Cloud Recovery através de uma única conexão site a site.

Failover ambientes complexos onde servidores protegidos são distribuídos em vários segmentos de rede.

Veja os status de conectividade de todas as cinco redes em uma única visualização.



**Por que?** Auxiliar diferentes tipos de clientes, apoiando infraestruturas mais complexas

# Suporte de backup criptografado

## Cumpra os requisitos de segurança de dados

Execute o failover usando backups criptografados e permita que o sistema use as senhas armazenadas com segurança para operações automatizadas de recuperação de desastres.

O novo recurso Armazenamento de credenciais (acessível no console da web na guia Recuperação de desastres > Armazenamento de credenciais) permite armazenar e gerenciar com segurança senhas para backups de servidores criptografados.

Cumpra vários regulamentos de dados.

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
 DBSERVER2012 - Backup to cloud 1 <span style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 10px; font-size: 0.8em;">RECENT</span>	..... 	<input type="text" value="New archive password"/>
 DBSERVER2012 - Backup to cloud 2	..... 	<input type="text" value="Saved archive password"/>
 DBSERVER2012 - Backup to cloud 3	<input type="text"/> 	<input type="text"/>

Saved archive password 1 

Saved archive password 2

Saved archive password 3

Show all backups

**Por que?** Mantenha os dados dos clientes seguros enquanto cumpre diversas regulamentações de dados

# Failover para um ponto de recuperação livre de malware

## Evite a reinfecção sendo proativo

Verifique a lista de pontos de recuperação disponíveis para failovers para ver se um malware ou outro indicador de comprometimento foi descoberto durante o processo de verificação de backup.\*

Garanta um retorno à produtividade mais rápido e seguro, evitando a reinfecção por meio de um ponto de recuperação comprometido.

\* Para realizar a verificação antimalware de backups, a Segurança Avançada deve estar habilitada.

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)

**Por que?** Garanta uma recuperação bem-sucedida selecionando pontos de recuperação livres de malware

# Recuperação avançada de desastres: Custos



Ao proteger suas cargas de trabalho com recursos avançados de recuperação de desastres em modelos por GB e por carga de trabalho, você também paga por:

## DR para Acronis Cloud ou Service Provider Cloud

Espaço total de armazenamento DR usado no Acronis Cloud ou em uma nuvem de provedor de serviços. Você paga somente depois que um backup na nuvem for criado.



## Recursos de computação

Os recursos de computação referem-se à quantidade de vCPUs e RAM que você está usando com valores de computação atribuídos por hora.

O custo de computação é por hora e é aplicado somente quando um servidor em nuvem está ativo (por exemplo, em failover, modo de teste ou em execução como servidor primário).



## IP de recuperação de desastres (opcional)

Endereços IP públicos dedicados podem ser adicionados a servidores que requerem acesso à rede externa. Você só será cobrado se um endereço IP externo for adicionado a um servidor.

**i Nota:** Os encargos para recursos de computação e IP de recuperação de desastres são calculados apenas se usados com armazenamento em nuvem hospedado pela Acronis.