Acronis Cyber Protect Cloud: Advanced Disaster Recovery

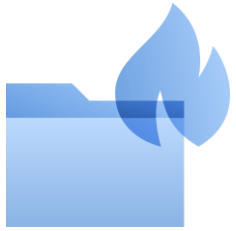
A interrupção dos negócios acontece

25%

Das violações de dados em 2019 foram causadas pela exclusão ou substituição acidental de arquivos ou pastas[1]

51%

Das violações de dados em 2019 foram causadas por ataques criminosos e maliciosos[1]



70%

Das organizações provavelmente sofrerão interrupções nos negócios até 2022 devido à perda irrecuperável de dados[2]

93%

Das empresas sofreram ataques nos últimos três anos[3]

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.

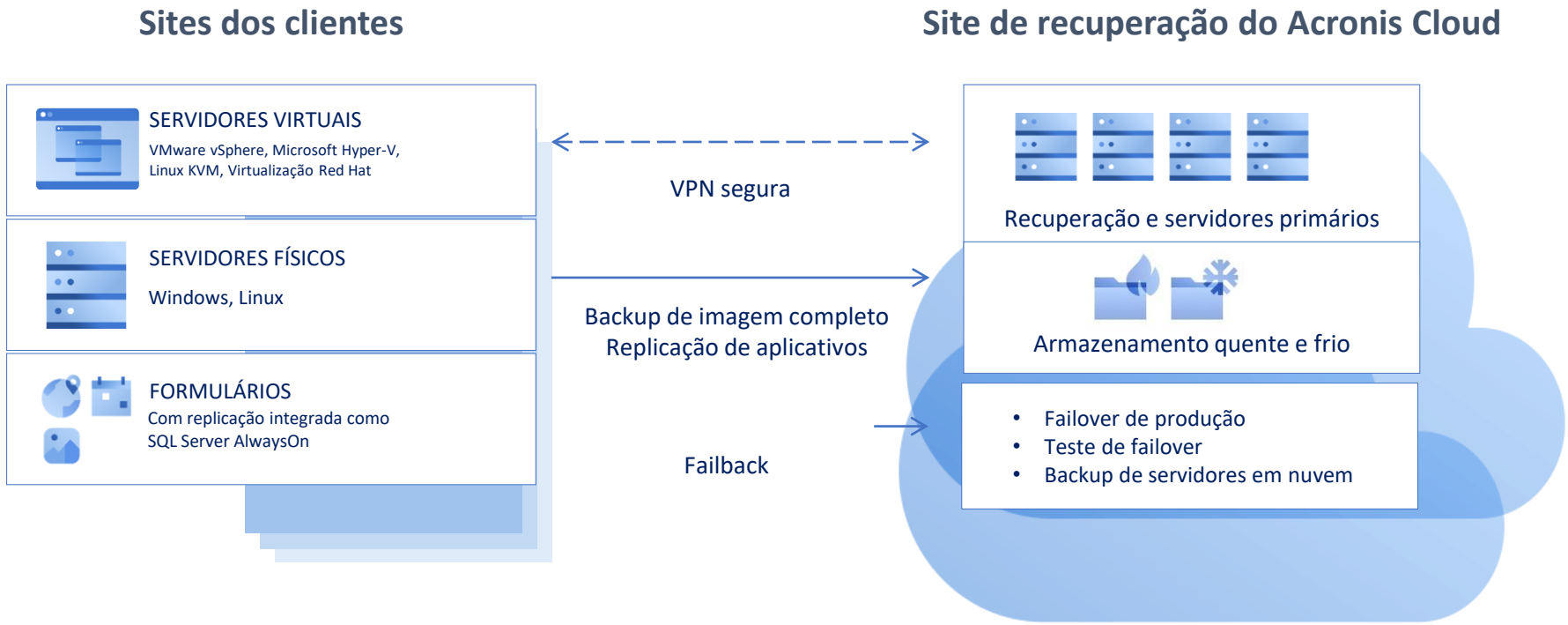
Minimize a complexidade

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

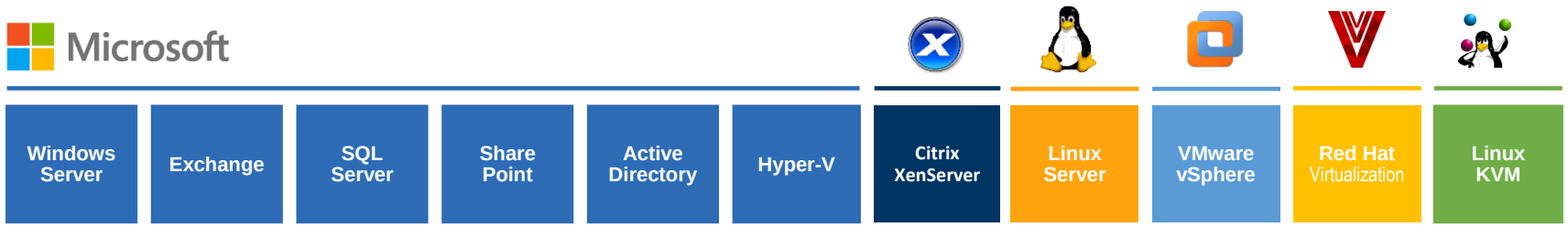
Agregue mais valor, aprofunde o relacionamento com os clientes e aumente a retenção, oferecendo aos clientes os serviços de recuperação de desastres que eles procuram – enquanto aumenta sua receita recorrente mensal.

Recuperação de desastres para o site do Acronis Cloud Recovery



Recuperação de desastres para qualquer carga de trabalho de servidor

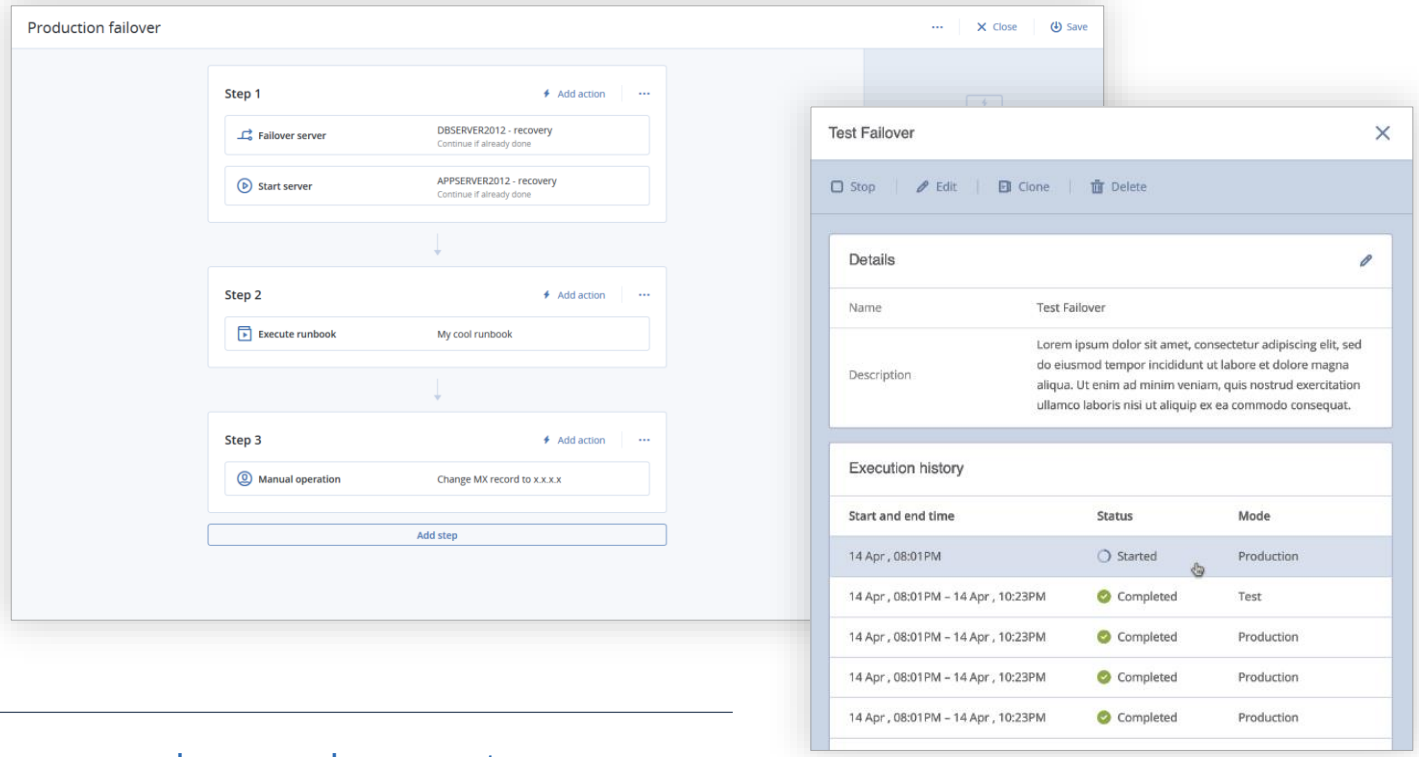
Máquinas físicas e virtuais	Windows	Linux
Plataformas de virtualização	▪ VMware vSphere ▪ Microsoft Hyper-V ▪ Linux KVM	▪ Red Hat Virtualization ▪ Citrix XenServer
Servidores em nuvem para replicação de aplicativos em tempo real	Para aplicativos com replicação integrada, como SQL Server AlwaysOn	



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.

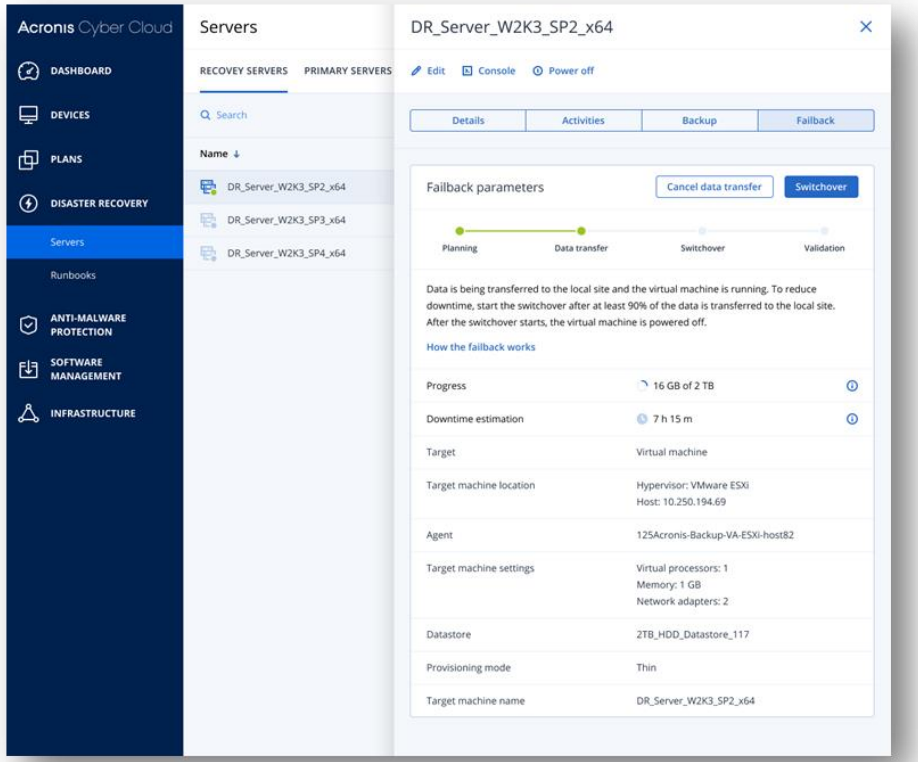
Ele permite operações eficientes para automatizar failover e testes e garante que os sistemas sejam recuperados na ordem certa para resolver interdependências entre aplicativos em máquinas diferentes.



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

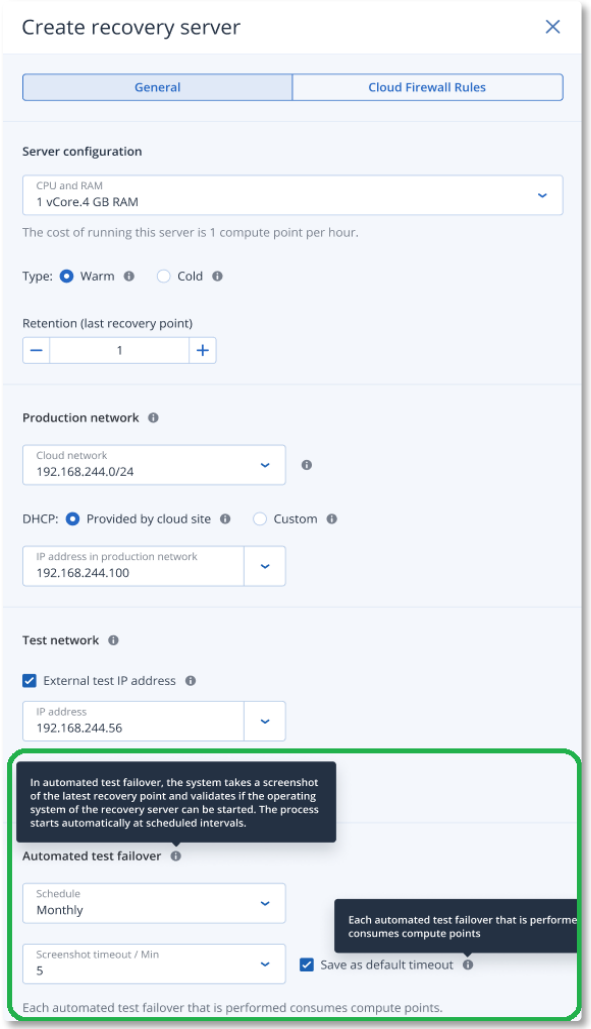
Por que? Obtenha tempo de inatividade próximo de zero, garanta a continuidade dos negócios e proteja os dados dos seus clientes

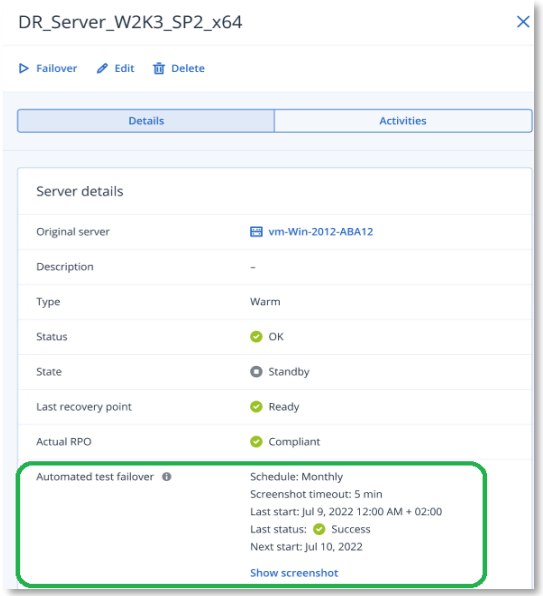
Failover de teste automatizado

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



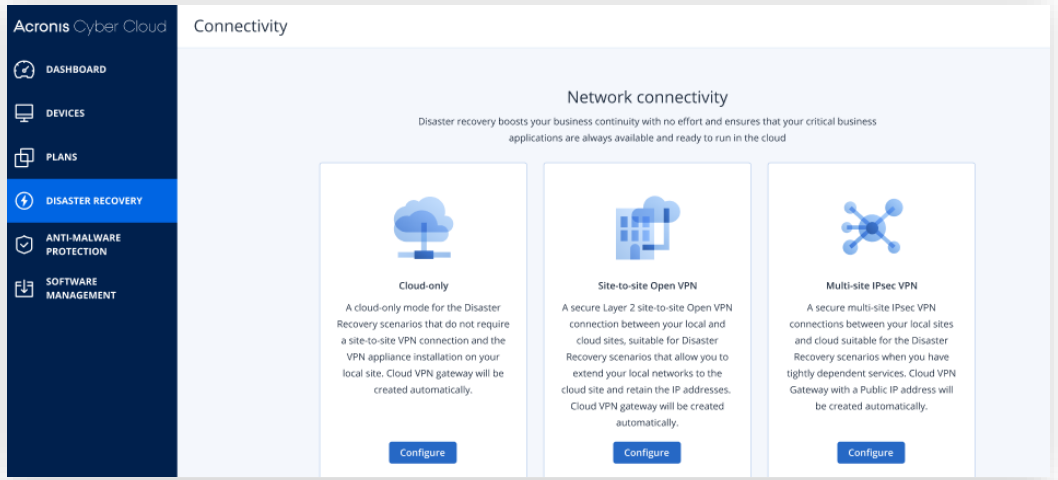


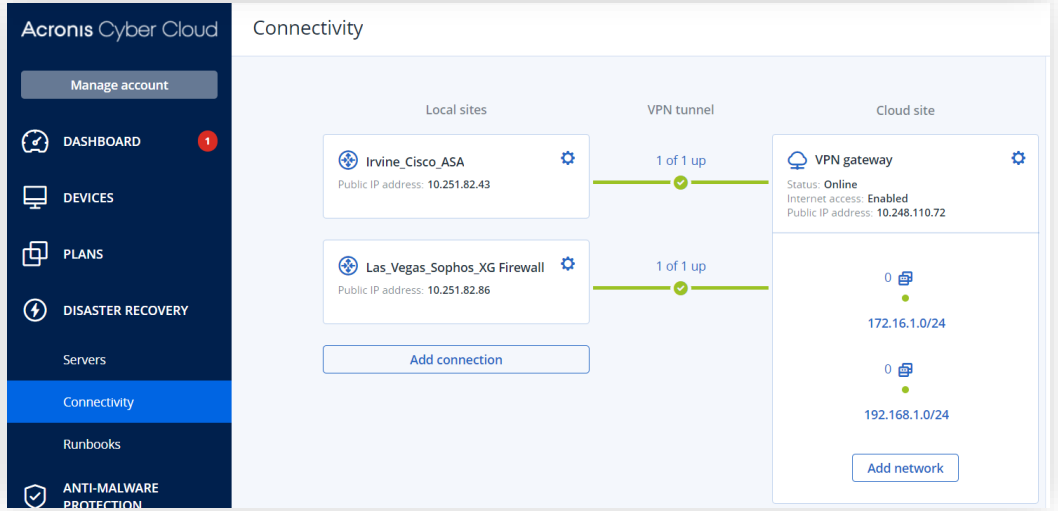
Suporte VPN multisite IPsec

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.





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

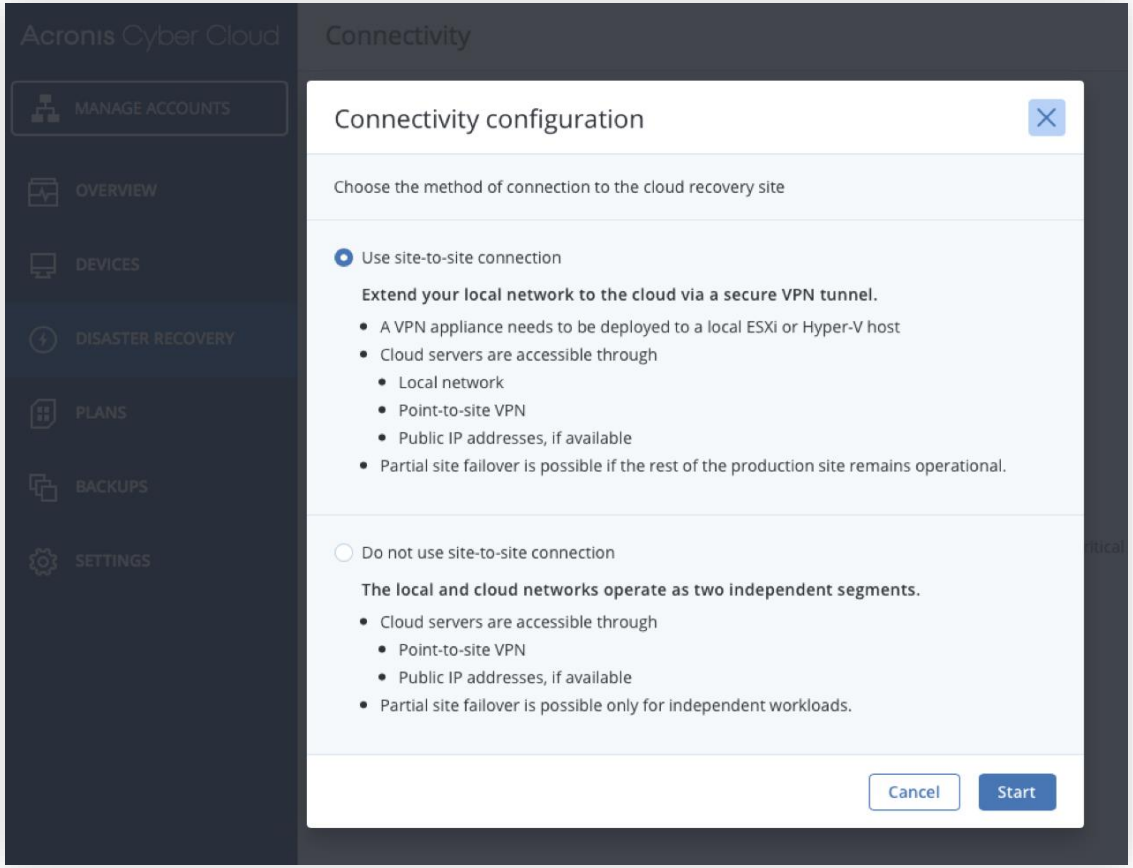
Opção de implantação sem VPN

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

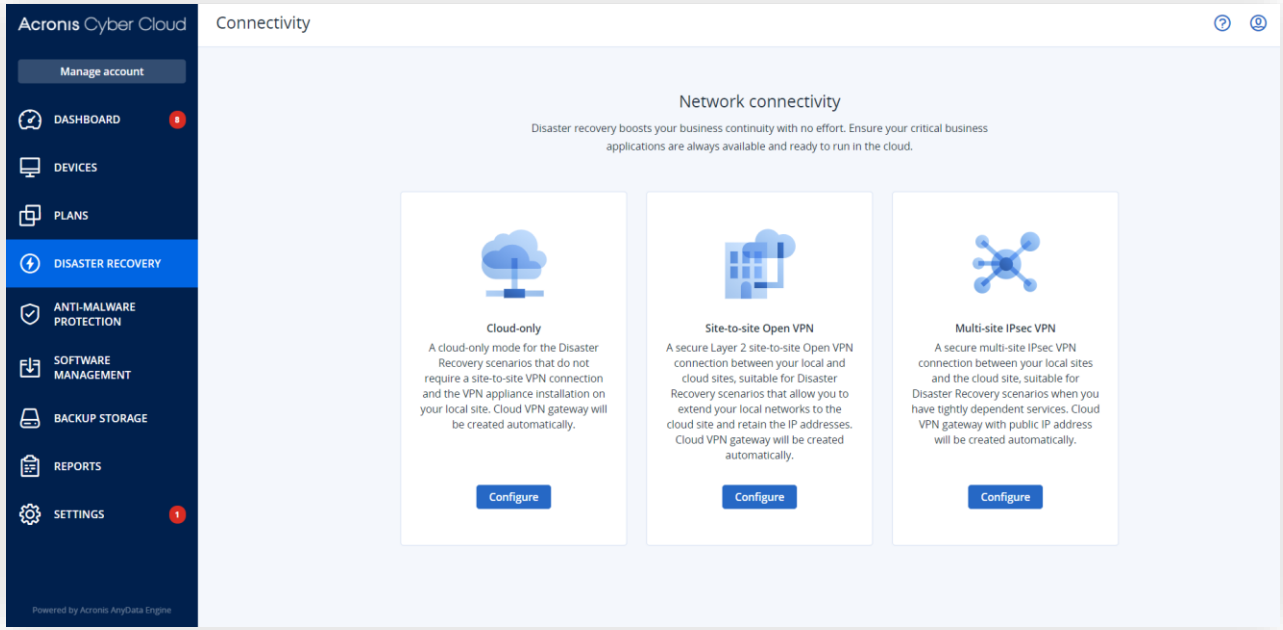
Suporte a múltiplas redes

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

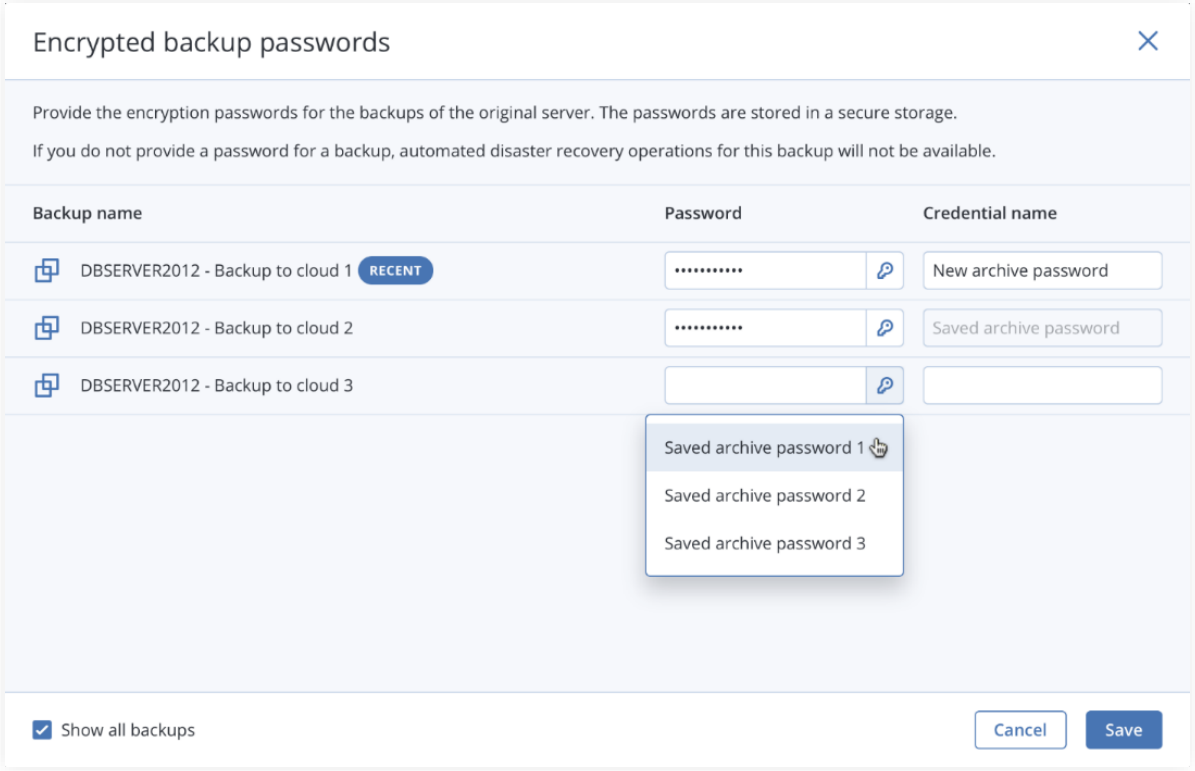
Suporte de backup criptografado

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.



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

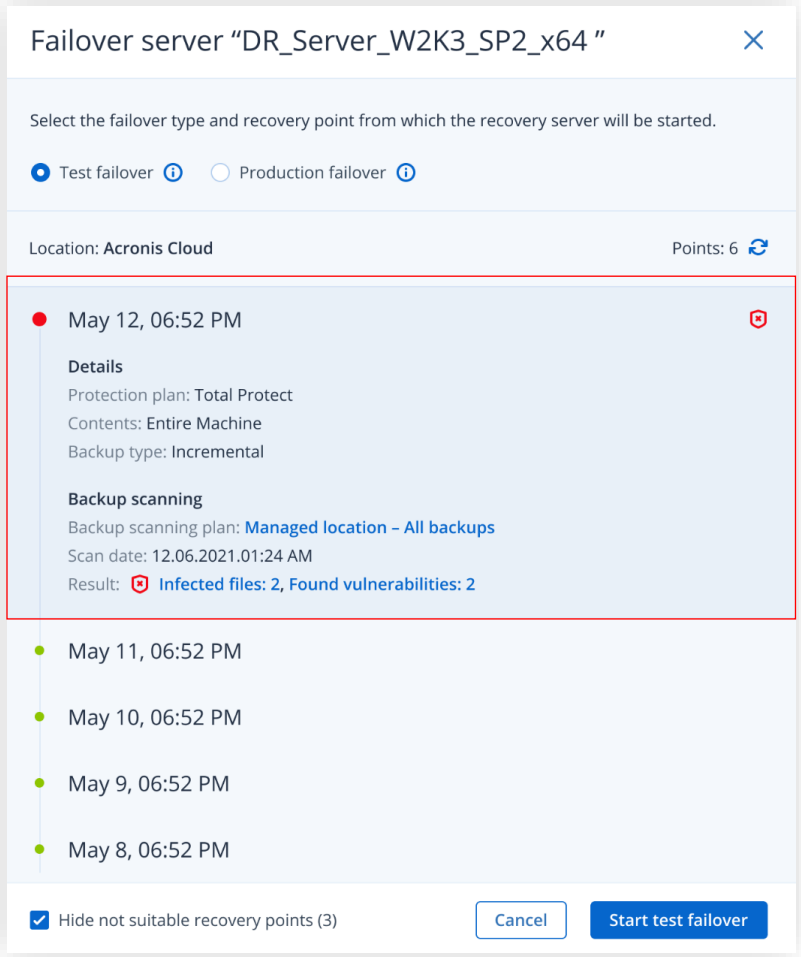
Failover para um ponto de recuperação livre de malware

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.



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.

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.