

Protected Infrastructure

Resiliência cibernética nativamente inteegrada para servidores e VMs

A ciber-resiliência vai além da cibersegurança tradicional. Não se trata apenas de prevenir ataques, mas também de garantir que as empresas possam continuar operando mesmo quando incidentes ocorrem. Resiliência cibernética é a capacidade de antecipar, resistir, recuperar e adaptar-se a condições adversas, estresses, ataques ou comprometimentos de sistemas." – NIST

Quão rápido o seu negócio pode se recuperar? Sem planos de resposta a incidentes claros, ferramentas adequadas e objetivos definidos de tempo e ponto de recuperação (RTOs e RPOs), cada interrupção corre o risco de causar perda de receita, redução da confiança dos clientes e danos duradouros à reputação.

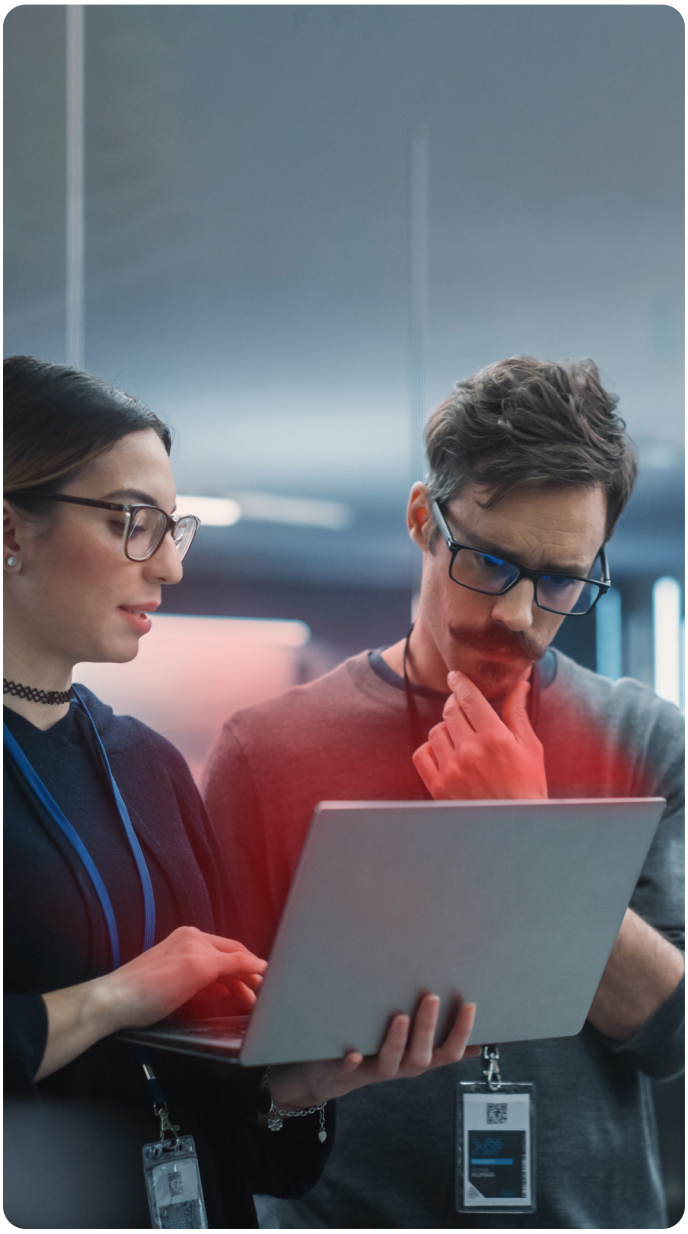


Pontos de dor da resiliência

Empresas de todos os tamanhos estão descobrindo que o tempo de inatividade custa muito mais do que apenas a perda de dados. Eles enfrentam pressões crescentes de conformidade e supervisão regulatória. Qualquer lacuna na preparação os expõe a multas, penalidades e riscos à reputação.

Copyright © 2003-2026 Acronis International GmbH.

Gerenciar incidentes com ferramentas fragmentadas também cria complexidade desnecessária. Sem uma estratégia unificada, as equipes de TI enfrentam o caos operacional, lutando para unir detecção, resposta e recuperação em vários consoles e agentes. Essas ineficiências aumentam os custos, retardam os tempos de resposta e expandem a responsabilidade. O aumento dos prêmios de seguros cibernéticos adiciona mais uma camada de preocupação, e a baixa resiliência pode até mesmo resultar na negação da cobertura.



Barreiras tecnológicas para a resiliência

À medida que as empresas aceleram a transformação digital, a conquista da resiliência torna-se mais desafiadora. Os ambientes de TI híbridos se estendem por sistemas locais, plataformas de nuvem e endpoints remotos, criando uma superfície de ataque em constante expansão. Isso resulta em mais interdependências e pontos únicos de falha. Ao mesmo tempo, as ameaças se tornaram mais sofisticadas. Ransomware, comprometimentos de cadeias de suprimento e riscos internos estão explorando as brechas deixadas por soluções isoladas. Ferramentas pontuais podem reduzir riscos específicos, mas também criam pontos cegos, processos manuais e lacunas que os invasores exploram rapidamente.

O caminho para a ciber-resiliência

Alcançar a verdadeira resiliência cibernética exige mais do que defesas fortes. Trata-se de garantir a continuidade, independentemente da interrupção. As empresas podem alcançar a resiliência ao adotar uma abordagem estruturada que começa com a **antecipação** dos riscos por meio do mapeamento de ativos, avaliação de vulnerabilidades e gerenciamento de patches. Eles devem então ser capazes de **resistir** ameaças, detectando-as e contendo-as em tempo real com recursos avançados, como proteção de endpoints com inteligência artificial e monitoramento baseado em aprendizado de máquina. Essas medidas proativas só são eficazes quando combinadas com uma estratégia de recuperação eficiente.

A recuperação é o próximo passo crítico. Restaurar dados e sistemas rapidamente, de forma confiável e livre de malware mantém o tempo de inatividade ao mínimo. Em uma falha grave, o mais importante é manter a continuidade dos negócios. Com o Acronis Cloud Disaster Recovery, as empresas podem transferir suas cargas de trabalho de forma imediata para a nuvem da Acronis ou para o Microsoft Azure, garantindo continuidade das operações mesmo em caso de falhas. Esse failover imediato garante a continuidade das operações mesmo durante as interrupções mais graves e atua como um ambiente de contingência seguro até que a restauração completa dos sistemas primários seja concluída.

Por fim, a resiliência não é estática. As organizações devem **se adaptar**, aprendendo com os incidentes, treinando suas equipes e aprimorando suas defesas ao longo do tempo.

Copyright © 2003-2026 Acronis International GmbH.

O espectro da recuperação de desastres

Em última análise, essas estratégias não se limitam a recuperar os dados após um desastre, mas a garantir a resiliência operacional para continuar as funções essenciais do negócio em qualquer adversidade. A capacidade de recuperar serviços em minutos, em vez de dias, é a chave para minimizar perdas financeiras e manter a confiança dos clientes.

As estratégias de recuperação de desastres são tipicamente categorizadas pelos RPOs e RTOs que podem alcançar. Duas das estratégias mais adotadas são:

DR de recuperação rápida

Essa abordagem oferece um equilíbrio entre custo e velocidade de recuperação. Ele utiliza sistemas pré-estagiados que podem ser colocados rapidamente em funcionamento, alinhando-se com o objetivo de "recuperação" de minimizar o tempo de inatividade, mantendo um RPO e um RTO definidos.

DR a frio

Focado exclusivamente na reconstituição e restauração de dados, o DR frio depende da recuperação completa a partir de backups, o que resulta em tempos de recuperação mais longos, mas custos operacionais mais baixos.

Ao unificar detecção, proteção e recuperação, as empresas obtêm a vantagem crítica de poder não apenas sobreviver a uma crise, mas também sair dela mais fortes. Com o Acronis Cloud Disaster Recovery, as organizações podem selecionar o nível de resiliência adequado para cada carga de trabalho, desde opções de falha de quente a frio que reconstituem serviços após uma interrupção até continuidade quase instantânea com recuperação de desastres de alta disponibilidade integrada. Essa flexibilidade fortalece as defesas em todos os estágios da jornada de ciber-resiliência.



Copyright © 2003-2026 Acronis International GmbH.

A solução Protected Infrastructure

A solução Protected Infrastructure da Acronis unifica backup, recuperação de desastres, segurança de endpoints, avaliação de riscos e prevenção contra perda de dados em uma única plataforma de ciberproteção com integração nativa. Essa abordagem elimina silos, reduz a proliferação de ferramentas e garante a resiliência sem adicionar complexidade. A plataforma abrange cada estágio da jornada de resiliência: antecipar, resistir, recuperar e adaptar. Com uma única plataforma, um único agente e um único console, as empresas podem detectar ameaças mais rapidamente, recuperar operações sem interrupções e adaptar-se continuamente a riscos em evolução.

ANTECIPE	RESISTIR	RECUPERAÇÃO	ADAPTAR
• Descoberta de dispositivos • Mapa de proteção de dados • Inventário de ativos • Avaliação de vulnerabilidades • Gerenciamento de patches	• Detecção de ameaças em tempo real • Detecção e a resposta de endpoint baseada em IA (EDR) • Monitoramento baseado em autoaprendizagem • Contenção rápida de ameaças ativas	• Recuperação de dados automatizada e com segurança • Recuperação de desastres na nuvem (CDR) • Backups imutáveis • Mobilidade de hipervisor • Recupere para pontos sem malware	• Monitoramento e gerenciamento de endpoint • Security Awareness Training (SAT) • Modelos de resposta a incidentes consultivos

Por que as empresas escolhem a Acronis?

Em um ambiente onde os ciberataques são inevitáveis, a Acronis fortalece a ciber-resiliência unificando a proteção contra ameaças com inteligência artificial e a recuperação de desastres orquestrada na nuvem em uma única plataforma. Ao contrário das abordagens fragmentadas que focam apenas na prevenção, a Acronis garante que os dados críticos estejam protegidos e recuperáveis por meio de backups imutáveis, detecção de ransomware baseada em inteligência artificial e validação de recuperação limpa.

Com recuperação de desastres totalmente gerenciada na nuvem, failover instantâneo para a Acronis Cloud, cobrança de computação baseada no uso e testes e execução controlados pelo cliente, a solução Protected Infrastructure da Acronis oferece ciberproteção de nível corporativo sem o custo ou a complexidade das infraestruturas legadas. O resultado é uma operação de recuperação mais rápida, risco operacional reduzido e continuidade de negócios ininterrupta quando mais importa.

Solicite uma reunião com um especialista da Acronis

Sua continuidade de negócios depende de mais do que proteção. Isso exige resiliência. Veja como a Acronis pode ajudar você a antecipar ameaças, resistir a ataques, recuperar-se mais rapidamente e adaptar-se para o futuro.

ENTRE EM CONTATO CONOSCO



Acronis

Saiba mais em
www.acronis.com

Copyright © 2003-2026 Acronis International GmbH. Todos os direitos reservados. A Acronis e o logotipo da Acronis são marcas comerciais da Acronis International GmbH nos Estados Unidos e/ou em outros países. Quaisquer outras marcas comerciais ou registradas são propriedade de seus respectivos donos. Pode haver alterações técnicas e diferenças em relação às ilustrações, bem como erros. 2026-11