Acronis Protected Server

Proteção 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

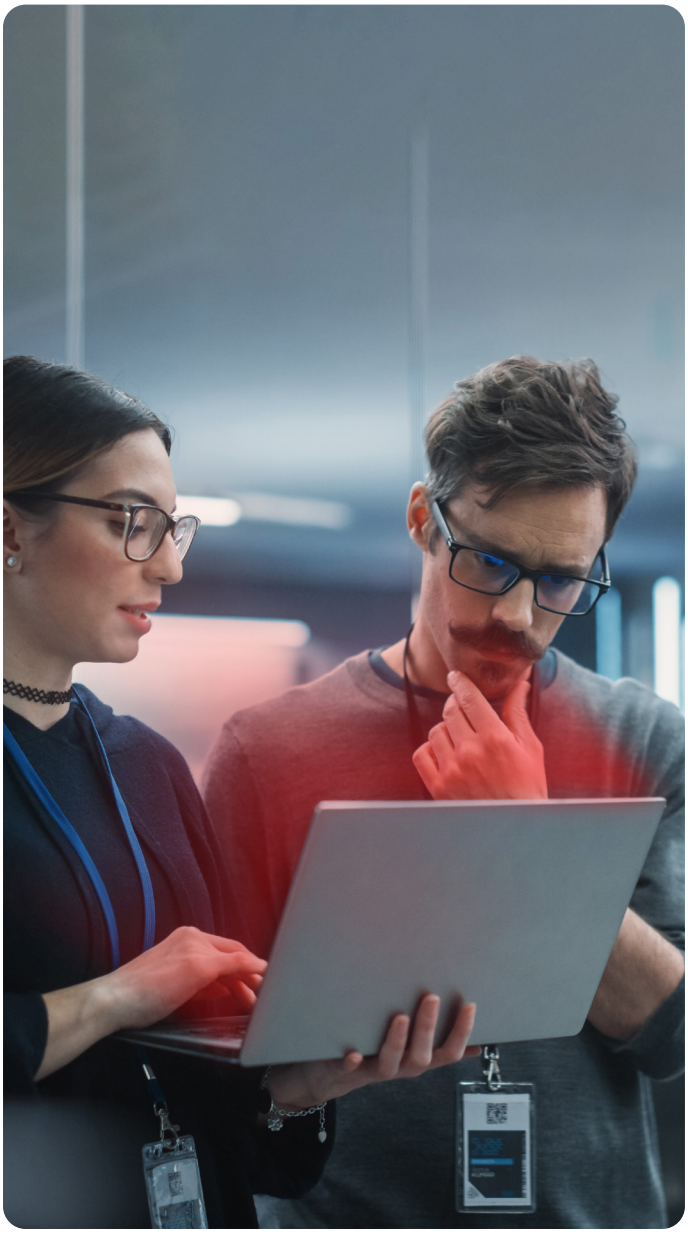
Para provedores de serviços e empresas, a verdadeira questão é: Quão rápido o seu negócio pode se recuperar? Sem planos de resposta a incidentes claros, ferramentas adequadas e objetivos definidos de tempo e ponto de recuperação (RTOs e RPOs), cada interrupção corre o risco de causar perda de receita, 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. Provedores de serviços enfrentam o risco adicional de perda de clientes, pois estes rapidamente mudam de provedor se as interrupções recorrentes minam a confiança.

As empresas, por outro lado, enfrentam crescentes pressões de conformidade e supervisão regulatória. Qualquer lacuna na preparação os expõe a multas, penalidades e riscos à reputação.

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. Elas também devem ser capazes de **resistir** às ameaças, detectando e contendo-as em tempo real com recursos avançados, como detecção e resposta em endpoints (EDR), detecção e resposta estendida (XDR) e prevenção contra perda de dados (DLP). 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.

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.

A solução Acronis Protected Server

A solução Acronis Protected Server unifica backup, recuperação de desastres, segurança de endpoint, avaliação de risco e prevenção de perda de dados em uma única plataforma. Essa abordagem elimina silos, reduz a proliferação de ferramentas e garante a resiliência sem adicionar complexidade. Desenvolvida para empresas e provedores de serviços, a plataforma abrange todos os estágios 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 resposta para endpoints (EDR) • Detecção e Respostas Estendidas (XDR) • Prevenção de perda de dados (DLP) • 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 remotos (RMM) • Security Awareness Training (SAT) • Detecção e resposta gerenciadas (MDR) • Modelos de resposta a incidentes consultivos

Por que as empresas escolhem a Acronis?

Para provedores de serviços, a Acronis oferece um caminho para receitas recorrentes aceleradas. Ao adicionar serviços de proteção cibernética de alta margem ao seu portfólio, os MSPs não apenas ampliam suas ofertas, mas também se destacam em um mercado cada vez mais comoditizado. A plataforma unificada simplifica as operações, reduzindo a proliferação de ferramentas, enquanto um modelo de licenciamento direto maximiza as margens e escala perfeitamente com o crescimento do cliente final.

Para empresas e PMEs, a Acronis garante a continuidade dos negócios, possibilitando a recuperação rápida e sem malware, que minimiza o tempo de inatividade e as perdas financeiras. O suporte integrado para geração de relatórios e conformidade facilita a realização de auditorias regulatórias. Capacidades robustas de proteção também aumentam a elegibilidade para seguro cibernético, frequentemente resultando na redução dos prêmios. Além disso, demonstrar uma estratégia de resiliência robusta constrói confiança com clientes, parceiros e reguladores.

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