Quatro principais maneiras de proteger seus dados para uma recuperação limpa e confiável

Os dados são vulneráveis a inúmeras ameaças, de ataques cibernéticos e falhas de hardware a desastres naturais. Uma estratégia de backup robusta e multicamadas protege seus dados, garante a continuidade dos negócios, reduz o risco de perda de dados e fortalece sua postura geral de segurança.

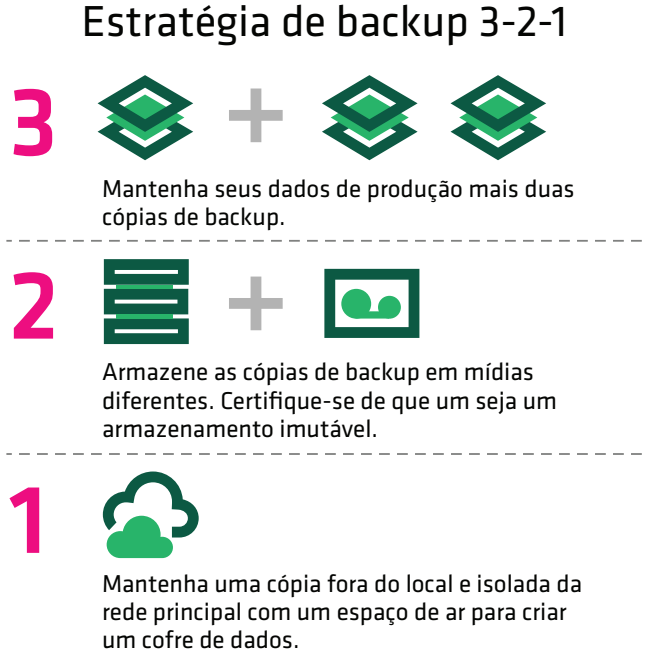
Aqui estão quatro medidas de postura de segurança que ajudam a garantir que seus dados estejam sempre limpos e recuperáveis.

1. Implemente controles de acesso e autenticação

- **Certifique-se de que apenas usuários autorizados possam acessar seus dados.** Adicionar uma camada extra de segurança é essencial para proteger contra ameaças internas e externas. Habilitar a autenticação multifator (multifactor authentication, MFA) em todos os lugares é um meio eficaz de proteger contra essas ameaças, além de manter suas políticas existentes de gestão de identidade e acesso.
- **Limite o acesso e as permissões com base nas funções do usuário.** Aplique o controle de acesso baseado em funções (role-based access control, RBAC) para fornecer acesso e permissões limitados e granulares aos usuários em seu ambiente de backup com base em sua função específica. Isso ajuda a garantir que cada pessoa tenha apenas os privilégios mínimos de acesso necessários para cumprir suas responsabilidades.

2. Priorize a proteção e a integridade dos dados

- **Implemente um cofre de dados imutável.** Para manter seus dados protegidos contra adulteração, considere usar o Cohesity NetBackup Flex Appliance ou o Cohesity FortKnox para armazenamento imutável seguro e resistente à adulteração no local ou na nuvem.
- Implemente uma estratégia de backup 3-2-1 para cargas de trabalho críticas. Manter três cópias de dados em duas mídias diferentes, com pelo menos uma cópia armazenada fora do local em armazenamento imutável e indelével, fornece redundância de dados e ajuda a garantir que seus dados sejam sempre recuperáveis.
- Evite a exfiltração de dados com criptografia forte. Proteja os dados contra acesso não autorizado durante a transmissão e o armazenamento. Para evitar acesso não autorizado e roubo de dados, use criptografia forte para todos os seus dados, estejam eles armazenados no local ou na nuvem.



3. Aproveite o monitoramento e a detecção de segurança

- Use a automação para detecção inteligente de ameaças de usuários. Nosso mecanismo de risco adaptável monitora continuamente o comportamento do usuário em busca de atividades suspeitas. Ao detectar anomalias ou outras ações suspeitas do usuário, a plataforma iniciará ações de segurança de forma autônoma, como autenticação multifatorial, para bloquear o acesso aos dados de backup.

- Acelere a identificação e a resposta a ameaças. A Cohesity fornece recursos rápidos de caça a ameaças que pesquisam proativamente indicadores de comprometimento e respondem a ameaças. Também oferecemos uma análise completa do raio de explosão das áreas afetadas em todo o ambiente, até 93% mais rápida do que a varredura tradicional de malware.

4. Fortaleça a configuração do seu sistema

- **Crie uma Digital Jump Bag.**™ Uma Digital Jump Bag é um repositório protegido e confiável que fornece acesso rápido às ferramentas necessárias para aquisição e análise remotas. Ela contém as ferramentas, software, arquivos de configuração e documentação necessários para responder a um incidente em um armazenamento imutável em cofre, muito além do alcance dos adversários.
- **Reduza a exposição da rede.** Implemente controles de acesso à rede para restringir o acesso de rede a sistemas e dados de backup e impedir o acesso não autorizado. Segmente facilmente sua rede e crie um ambiente de sala limpa para aumentar a segurança e ajudar a minimizar o impacto de possíveis violações de segurança.
- **Implemente a recuperação de dados em sala limpa**. Crie um ambiente separado e seguro para operações forenses e de recuperação para minimizar o risco de contaminação.
- **Mantenha todos os sistemas e software atualizados.** Atualize regularmente o software e instale patches de segurança para aproveitar os novos recursos e medidas de segurança aprimoradas.

Compartilhe essas diretrizes com sua equipe e incentive-a a implementar essas etapas cruciais para proteger os dados da sua organização e fortalecer sua postura de segurança.

Para obter esquemas e melhores práticas para arquitetar um ambiente de backup para sua organização, leia *Topologias modernas de segurança e gestão de dados: um guia para líderes de TI*.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100085-001-EN 6-2025