OBJECT FIRST

Lista de verificação

Lista de verificação de resiliência para ataques de ransomware

Identifique armazenamento de backup com imutabilidade absoluta

Os ataques de ransomware se tornaram mais sofisticados do que nunca. 66% das organizações sofreram pelo menos um ataque nos últimos dois anos, e 96% deles tiveram dados de backup como alvo*.

Sendo assim, quando (e não se) uma violação ocorrer e sua empresa, reputação e carreira estiverem em jogo, o armazenamento de backup imutável será a melhor e última linha de defesa.

No entanto, dados "imutáveis" que podem ser sobrescritos por um administrador de backup ou armazenamento, um fornecedor ou um invasor, não são uma solução de armazenamento absolutamente imutável.

Use esta lista de verificação de três etapas para conferir se sua solução de backup atual (ou buscada) é de fato resiliente contra ataques de ransomware.

*ESG Research 2025

Prepare-se

1.ª etapa: Use armazenamento de objetos S3

- ☐ Sua solução de armazenamento utiliza bloqueio e controle de versões de objetos S3 para garantir a imutabilidade e preservar o histórico de backups?
- ☐ Ela aplica o modo de conformidade (não de governança) e permite criptografia de ponta a ponta desde o momento em que os dados são criados?
- ☐ A imutabilidade pode ser verificada de forma independente por meio de padrões abertos e testes de penetração realizados por terceiros independentes?

Somente o armazenamento de objetos S3, com a imutabilidade nativa estabelecida diretamente em seu protocolo e APIs, proporciona segurança inerente. Esse design de base assegura que os dados não possam ser alterados ou excluídos depois de registrados. O armazenamento de objetos S3 é baseado em uma arquitetura aberta padrão de mercado que segue as práticas mais recomendáveis de TI e permite testes realizados por terceiros.

2.ª etapa: Garanta imutabilidade com tempo zero

- ☐ Sua solução torna os dados de backup imutáveis desde o exato momento em que são registrados sem nenhum atraso ou "zona de aterrissagem"?
- ☐ Ela evita a imutabilidade fundamentada em imagens instantâneas ou camadas de deduplicação, modelos que aplicam proteções somente depois que a operação é finalizada?
- ☐ Os dados de backup são registrados diretamente no armazenamento de objetos com bloqueio de objetos S3 ativado?

Garantir que os dados de backup sejam imutáveis desde o momento em que são registrados é fundamental para evitar alterações não autorizadas, manter a integridade dos dados e defender-se contra ataques de ransomware. A forma comprovadamente mais segura de conseguir isso é utilizar controle de versões S3 combinadas com bloqueio de objetos, o que garante a imutabilidade quando um objeto é criado no sistema de armazenamento.

3.ª etapa: Use um dispositivo de destino feito sob medida

- ☐ Sua configuração faz total separação entre software de backup e armazenamento de backup para limitar o raio de impacto de uma violação?
- ☐ Sua organização utiliza um dispositivo de destino exclusivo e gerenciado pelo fornecedor, em lugar de uma configuração de armazenamento de produção própria que requeira atualizações, correções e monitoramento manuais?
- ☐ Sua solução oferece proteção verificável, ou ela depende de um sistema de arquivos exclusivo de um fornecedor que impede a realização de testes independentes e oculta o modo como a imutabilidade é garantida?

Um armazenamento de backup feito sob medida envolve um dispositivo de armazenamento independente configurado e otimizado para armazenar dados de backup. Existem dois tipos: dispositivos integrados, que combinam software e armazenamento de backup em um único sistema; e dispositivos de destino, que fornecem um dispositivo de armazenamento pronto para uso com um software de backup externo, como o Veeam. Somente um dispositivo de destino S3 para backup pronto para uso e desenvolvido sob medida oferece resiliência de dados Zero Trust ao separar adequadamente software e armazenamento, e possibilitar a realização de testes de segurança independentes.

Imutabilidade absoluta: a melhor defesa contra ataques de ransomware

Se você não puder marcar todos os campos da lista, seus backups podem estar vulneráveis a ataques de ransomware. **Imutabilidade absoluta** significa zero acesso para ações destrutivas. Ninguém – nem mesmo o melhor administrador ou invasor com acesso a armazenamento de backup – pode modificar ou excluir os dados depois de armazenados.

Atingir a imutabilidade absoluta por meio de acesso zero requer o cumprimento de **três princípios fundamentais:**

1. **Armazenamento de objetos S3:** Um padrão aberto e totalmente documentado com imutabilidade integrada de forma nativa que permite testes de penetração e verificações independentes.
2. **Imutabilidade com tempo zero:** Os dados de backup devem ser imutáveis desde o exato momento em que são registrados.
3. **Dispositivo de armazenamento de destino:** Um dispositivo de armazenamento de destino exclusivo separa o armazenamento do software de backup e elimina os riscos associados ao armazenamento de backup de desenvolvimento próprio e autogerenciados durante operações.

Baixe nosso white paper e saiba por que a **imutabilidade absoluta** é a melhor resiliência para ataques de ransomware.

Leia o documento branco ↗

Sobre a Object First

A Object First fornece armazenamento de backup seguro, simples e poderoso, feito sob medida para a Veeam e absolutamente imutável. Com a melhor defesa contra ataques de ransomware, você e sua organização se tornam resilientes de maneira simples.

Demotermin vereinbaren ↗