COHESITY

UM GUIA EXECUTIVO PARA AVALIAR COFRES CIBERNÉTICOS

Resumo executivo: por que os cofres cibernéticos são essenciais para a resiliência cibernética

Nenhuma empresa está imune a ataques cibernéticos; por isso, uma resposta e uma recuperação eficazes são essenciais para todas as organizações. Os invasores não medem esforços para obrigá-lo a pagar um resgate, chegando até mesmo a atacar os próprios sistemas destinados a proteger seus dados. As estratégias tradicionais de backup, concebidas para proteger contra falhas de hardware e desastres naturais, pouco contribuem para proteger sua organização contra ataques cibernéticos direcionados e em várias etapas. Quando um ransomware ataca, as cópias de backup dos dados conectados às redes de produção podem ser criptografadas ou excluídas, tornando praticamente impossível uma recuperação rápida e completa. Para os líderes de TI, não se trata de saber se um ataque ocorrerá, mas sim quando. A sua organização está preparada para se recuperar com segurança quando esse ataque ocorrer?

À medida que organizações como a sua repensam como proteger e recuperar dados, o cofre cibernético tornou-se um elemento fundamental de uma estratégia moderna de resiliência cibernética. Um cofre cibernético garante que você tenha uma cópia intacta dos seus dados para recuperar quando tudo mais falhar. O cofre oferece a segregação, a verificação e o controle necessários para garantir dados limpos e recuperáveis, mesmo diante de ataques cibernéticos destrutivos. É por isso que seus pares estão adotando o cofre cibernético como um imperativo para a resiliência.

O desafio: a recuperação cibernética é muito mais complexa do que a recuperação de desastres

Durante anos, as organizações criaram sistemas de backup para lidar com falhas de hardware, exclusões acidentais e desastres naturais. Esses sistemas muitas vezes cumpriam bem seu propósito. Mas eles não são suficientes para garantir a segurança e a proteção dos dados contra os ataques cibernéticos destrutivos que predominam atualmente.

Como resultado, surgiu um fator de risco crítico: os dados de backup podem ser tão vulneráveis quanto os dados de produção. Os agentes maliciosos já não se concentram exclusivamente em criptografar dados de produção. Eles se infiltram em repositórios de backup, desativam agendamentos de snapshots, instalam malware e corrompem metadados para eliminar caminhos de recuperação.

Esses riscos existem mesmo que você já tenha uma plataforma moderna de proteção de dados em funcionamento.

Por que seu ambiente de dados está em risco

Você deve estar pensando: "Tenho uma plataforma de dados segura para todos os meus backups, com todos os complementos de segurança ativados. Isso não é suficiente?" Resposta curta: Não.

Essa plataforma reduz significativamente o risco e a superfície de ataque. Mas, por si só, não elimina a exposição.

Veja por quê:

- **Conectividade compartilhada**: a maioria dos sistemas de backup permanece conectada à rede de produção. Se esse ambiente de produção for comprometido, os invasores já terão acesso aos dados de backup.
- **Sobreposição de credenciais**: as credenciais administrativas costumam ser compartilhadas entre diferentes ambientes. Assim que um invasor obtém acesso privilegiado, ele pode excluir ou criptografar backups com a mesma facilidade com que o faz com os dados de produção.
- **Imutabilidade falsa**: alguns backups "imutáveis" são bloqueados apenas por software. Se o plano de controle de armazenamento ou a API forem violados, o sinalizador de imutabilidade pode ser desativado.
- **As ameaças latentes podem permanecer**: muitas organizações realizam a restauração a partir de backups sem validar a integridade dos dados nem verificar a presença de malware latente, o que aumenta o risco de reinfecção durante a recuperação.

O impacto nos negócios

O resultado é uma lacuna de confiança: a percepção da integridade dos dados de backup é muito superior à realidade. As consequências negativas se propagam:

- **Tempo de inatividade prolongado**: backups não verificados ou comprometidos prolongam a recuperação de horas para dias ou semanas.
- **Tensão operacional**: as equipes gastam tempo recriando sistemas ou conjuntos de dados em vez de executar planos de recuperação.
- **Custos cumulativos**: cada hora de inatividade aumenta a perda de receita, o risco de violação de regulamentações e os danos à marca.
- **Erosão da confiança**: quando a equipe de TI não consegue garantir uma recuperação rápida e sem falhas, a confiança dos executivos e do conselho na resiliência da organização diminui.

Cofre cibernético: sua última linha de defesa quando todo o resto falha

Um cofre cibernético aborda essa lacuna de confiança. Um cofre cibernético é um repositório seguro, isolado e imutável que armazena cópias limpas de dados críticos. O cofre é deliberadamente desconectado das redes de produção e dos sistemas de backup primários.

A adoção de um cofre cibernético atualiza a regra de backup 3-2-1: manter três cópias dos dados em dois tipos diferentes de mídia, com uma cópia externa isolada e imutável.

Na prática, as organizações implementam essa regra moderna de backup da seguinte forma:

- **Três cópias de dados devem ser imutáveis:** as cópias devem ser protegidas por meio de bloqueio do tipo "grave uma vez, leia várias vezes" (WORM) ou bloqueio no nível do objeto, e devem ser continuamente validadas por meio de detecção de anomalias baseada em IA e varreduras regulares contra ameaças, a fim de confirmar que os dados estão limpos.
- **Duas mídias diferentes significam armazenar dados em duas plataformas diferentes ou limites de confiança:** as cópias devem estar alojadas em sistemas distintos que não compartilhem o mesmo plano de controle nem a mesma superfície de ataque. Isso pode incluir combinações de armazenamento em disco, fita ou nuvem projetadas para o isolamento de dados.
- **Uma cópia externa deve ser isolada:** a cópia final deve ser separada por uma barreira física ou lógica e protegida por um modelo de segurança isolado e por custódia de terceiros. Essa cópia também deve ser protegida por autenticação multifatorial (MFA), quórum e verificações de integridade de dados.

Juntos, esses avanços transformam a regra 3-2-1 em um pilar fundamental da resiliência cibernética. O cofre cibernético serve como ponto de recuperação final e limpo para dados críticos. Ao combinar imutabilidade, isolamento, diversos domínios de armazenamento e uma rigorosa validação de integridade, o cofre cibernético permite que as organizações se recuperem com segurança de ataques cibernéticos destrutivos, mesmo no pior dos cenários, em que seu ambiente de backup tenha sido comprometido.

Avaliação de soluções de cofre cibernético

Ao selecionar uma solução de cofre cibernético, os líderes de TI devem avaliar tanto a arquitetura de segurança quanto a prontidão operacional. Com base no feedback de centenas de líderes de TI, os cinco pilares a seguir representam capacidades essenciais:

1. **Isolamento e controle de acesso:** os dados do cofre devem estar inacessíveis a partir das redes de produção. Procure por barreiras de isolamento de rede, domínios de identidade independentes, autenticação multifatorial (MFA) e aprovações administrativas baseadas em quórum.
2. **Imutabilidade e integridade:** os dados devem ser à prova de adulteração, com políticas de armazenamento WORM e bloqueio de retenção que impeçam a modificação ou exclusão, mesmo por parte dos administradores.
3. **Automatização e orquestração:** a replicação, validação e recuperação do cofre devem ser automatizadas. A orquestração baseada em políticas reduz o erro humano e acelera a recuperação.
4. **Proteção contra ameaças:** a detecção de anomalias e a verificação de malware baseadas em IA identificam possíveis ameaças nos instantâneos, ajudando a garantir que apenas dados limpos e não comprometidos sejam armazenados e restaurados.
5. **Conformidade e relatórios:** os registros de auditoria imutáveis, a criptografia e o gerenciamento de retenção devem estar em conformidade com normas como a NIST SP 800-209, a ISO 27040 e a DORA, a fim de comprovar a capacidade de recuperação e a preparação para a resiliência.

Cartão de pontuação de avaliação: use este cartão de pontuação durante suas conversas com fornecedores.

Instruções:

1. Para cada categoria, atribua uma nota de 1 a 5 a cada fornecedor, sendo que 1 significa que não atende aos requisitos e 5 que atende plenamente aos requisitos.
2. Multiplique a pontuação de cada fornecedor pelo **Peso** atribuído a essa categoria e registre o resultado na célula correspondente de Pontuação ponderada.
3. Para cada fornecedor, some todas as **Pontuações ponderadas** da coluna e registre o total na linha **Total ponderado**, na parte inferior da tabela.
4. Use o **Total ponderado** para comparar fornecedores no geral e registrar quaisquer observações qualitativas ou riscos separadamente.

		Fornecedor 1		Fornecedor 2		Fornecedor 3		Fornecedor 4	
Categoria	**Peso**	**Pontuação**	**Pontuação ponderada**	**Pontuação**	**Pontuação ponderada**	**Pontuação**	**Pontuação ponderada**	**Pontuação**	**Pontuação ponderada**
Isolamento/Air Gap	10								
Imutabilidade/WORM	10								
Separação dos controles de acesso	10								
Autenticação forte (MFA/quórum)	8								
Detecção de ameaças/anomalias	8								
Bloquear a recuperação de instantâneos infectados	8								
Orquestração da recuperação	8								
Sala limpa/validação	8								
Conformidade/auditabilidade	8								
Simplicidade de SaaS/TTV	7								
Flexibilidade híbrida/multinuvem	8								
TCO/Sobrecarga operacional	7								
Total ponderado									

O cofre cibernético moderno oferece resultados de negócios mensuráveis:

- **Resiliência**: uma cópia de recuperação isolada física ou logicamente que permanece intacta mesmo quando as plataformas de backup são comprometidas.
- **Continuidade**: os backups em cofre garantem que as organizações tenham uma cópia dos dados para recuperação, independentemente da magnitude do ataque.
- **Conformidade**: o armazenamento imutável e a aplicação de políticas de retenção fornecem evidências auditáveis da proteção dos dados e da prontidão para a recuperação.
- **Confiança**: os pontos de recuperação são mantidos fora do raio de ação operacional e podem ser validados antes do uso, garantindo que os dados restaurados estejam intactos e não tenham sido comprometidos.

O cofre cibernético integra operações de TI, segurança e conformidade; assim, quando ocorre uma crise, a recuperação sem falhas é garantida, e não uma aposta.

Da dependência de backup à recuperação resiliente: Bethany Children's Health Center

Muitas organizações estão integrando o cofre cibernético como um componente padrão de sua estratégia de proteção de dados. Um exemplo é o Bethany Children's Health Center, em Oklahoma, que fornece cuidados para crianças com necessidades médicas complexas. Para garantir a continuidade dos cuidados, o centro deve proteger os dados confidenciais de saúde e restaurá-los rapidamente em caso de um ataque cibernético ou desastre. O Bethany atende a esses requisitos armazenando backups imutáveis tanto no local quanto no Cohesity FortKnox, um cofre isolado na nuvem.

Para aumentar a resiliência, Bethany segue o princípio 3-2-1, mantendo três cópias dos dados em dois suportes diferentes, com uma cópia armazenada fora do local. Duas cópias de segurança imutáveis são mantidas no local, enquanto a terceira é armazenada no Cohesity FortKnox.

O Cohesity FortKnox oferece um serviço gerenciado de cofre cibernético, disponível para ambientes DataProtect e NetBackup, fornecido na AWS, no Azure e no GCP, bem como em soluções locais para os ambientes mais seguros. O FortKnox combina isolamento, imutabilidade e automação para oferecer recuperação rápida, limpa e verificada em escala empresarial.

O FortKnox adiciona uma nova camada de defesa: um cofre seguro e isolado que garante que os dados críticos permaneçam protegidos, em conformidade com as normas e recuperáveis.

Próximas etapas para avaliar sua resiliência cibernética

Seu plano de resiliência não pode depender de suposições que não se aplicam mais. À medida que os ataques cibernéticos se tornam mais agressivos, a continuidade dos negócios depende cada vez mais da robustez da sua última cópia de dados, a mais segura. O cofre cibernético representa uma abordagem proativa que fortalece a recuperação cibernética e reduz o tempo de inatividade.

Comece avaliando:

- **Você faz backup de dados no SaaS, no local e na nuvem de todas as suas fontes de dados em uma única plataforma moderna?**
- **Você já reforçou a segurança da sua plataforma com autenticação multifatorial (MFA), imutabilidade e controle de acesso baseado em funções (role-based access control, RBAC)?**
- **Você segue a regra de backup 3-2-1?**
- **Que medidas de isolamento separam seus dados de backup das redes de produção?**
- **Com que frequência você verifica seus backups em busca de ameaças?**
- **Com que frequência você testa seu plano de resposta cibernética?**
- **Durante seu último teste de resposta cibernética, com que rapidez você se recuperou?**

Agora é a hora de elevar a resiliência cibernética de um objetivo técnico para um imperativo estratégico. A prontidão, não a suposição, é a vantagem competitiva definitiva.

Veja como o cofre cibernético moderno pode proteger seus dados, fortalecer sua capacidade de recuperação e proporcionar a confiança necessária para operar com segurança, independentemente da ameaça. Saiba mais em https://www.cohesity.com/pt-br/platform/fortknox/

COHESITY

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

4500065-001-PT 2-2026