IBM FlashSystem Cyber Vault

Destaques

- Detecção antecipada de ciberataques para minimização de danos
- Recuperação rápida após um ataque
- Menor tempo de recuperação, de dias ou semanas para apenas algumas horas
- Possibilidade de análise forense de um ataque

Os efeitos comerciais e financeiros dos ataques cibernéticos continuam a aumentar. Os ataques cibernéticos podem ocorrer de várias maneiras: podem assumir formas diferentes e evoluir. Quer o objetivo do invasor seja roubar dados confidenciais de clientes ou reter informações para fins de resgate, as organizações devem manter uma estratégia geral de segurança cibernética.

O armazenamento tem um papel fundamental nesse sentido, tanto na detecção de ataques quanto na recuperação rápida. O IBM® Safeguarded Copy gera snapshots de dados imutáveis isolados, para ajudar a proteger contra ataques cibernéticos, malware, ações maliciosas de funcionários e corrupção de dados. E como esses snapshots do Safeguarded Copy ficam no mesmo local de armazenamento do FlashSystem e dados operacionais, sua recuperação é mais rápida do que a restauração de cópias armazenadas separadamente.

A solução IBM FlashSystem® Cyber Vault complementa o IBM Safeguarded Copy. O FlashSystem Cyber Vault analisa automaticamente as cópias criadas pelo Safeguarded Copy quanto a sinais de corrupção de dados introduzida por malware ou ransomware. Essa varredura tem duas finalidades. Primeiro, ela ajuda a identificar rapidamente um ataque clássico de ransomware após iniciado. Segundo, ela ajuda a identificar quais cópias de dados não foram afetadas por um ataque. Munidos dessas informações, os clientes podem identificar mais rapidamente um ataque em andamento, bem como recuperar mais rapidamente uma cópia não corrompida de seus dados.

Visão Geral

O cibercrime continua a ser uma grande preocupação para as empresas. Quase diariamente ouvimos relatos de novos ataques. O custo médio é de US$ 4,24 milhões, e a recuperação pode levar dias ou semanas. Os ataques cibernéticos têm um impacto imediato nos negócios, além de um impacto duradouro na reputação da empresa se esta permanecer inoperante por um longo período.[1]

Infelizmente, é muito provável que os ataques cibernéticos continuem sendo uma ameaça significativa para 2022 e além. Não se trata de uma simples questão se a empresa foi atacada, mas sim quando.

Mediante um ataque cibernético, a resposta da organização será a diferença entre danos financeiros e de reputação ou distúrbios de relativamente curto prazo.

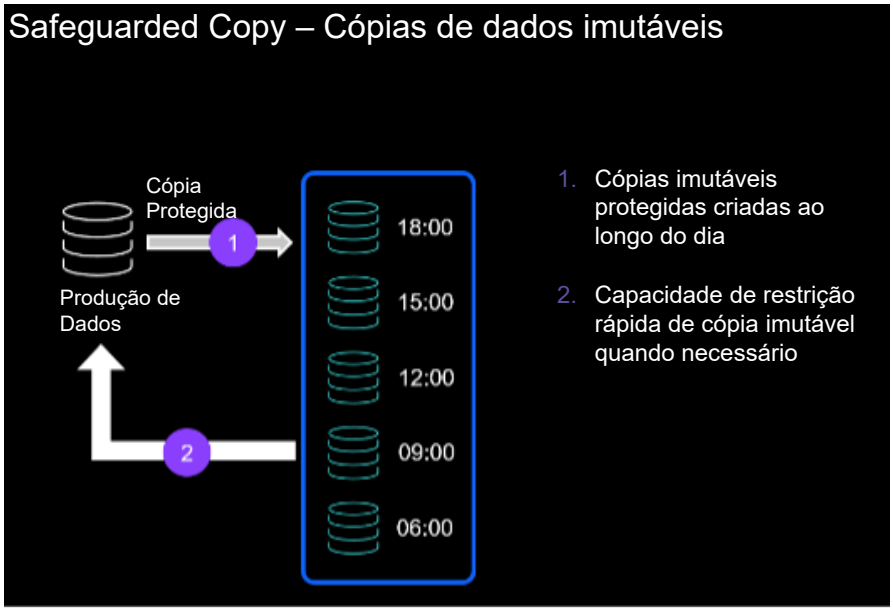
As soluções tradicionais de continuidade de negócios que a maioria das organizações aplica são: alta disponibilidade (HA) e recuperação de desastres (DR), para proteger seus dados contra ameaças convencionais (mas ainda relevantes). Infelizmente, essas soluções são incapazes de proteger contra a crescente variedade de ataques cibernéticos.

A única solução é investir em tecnologia atualizada e processos automatizados para proteção contra um evento cibernético, além de ajudar a recuperar rapidamente as operações comerciais críticas. Durante um evento cibernético, a recuperação rápida é a maior prioridade para qualquer organização. Seja de pequeno ou grande porte, e independentemente do setor, toda organização deve manter uma estratégia de resiliência bem definida de dados, incluindo resiliência cibernética, para permitir a recuperação rápida ante uma violação de dados ou ataques semelhantes.

IBM Safeguarded Copy

O IBM Safeguarded Copy gera snapshots de dados imutáveis (não podem ser alterados) isolados (separados de servidores), para ajudar a proteger contra ataques cibernéticos, malware, ações maliciosas de funcionários e corrupção de dados. E como esses snapshots do Safeguarded Copy ficam no mesmo local de armazenamento do FlashSystem e dados operacionais, sua recuperação é mais rápida do que a restauração de cópias armazenadas separadamente.

Nesse exemplo, uma política Safeguarded Copy gera automaticamente cópias imutáveis de snapshots a cada três horas.



Operação do IBM Safeguarded Copy

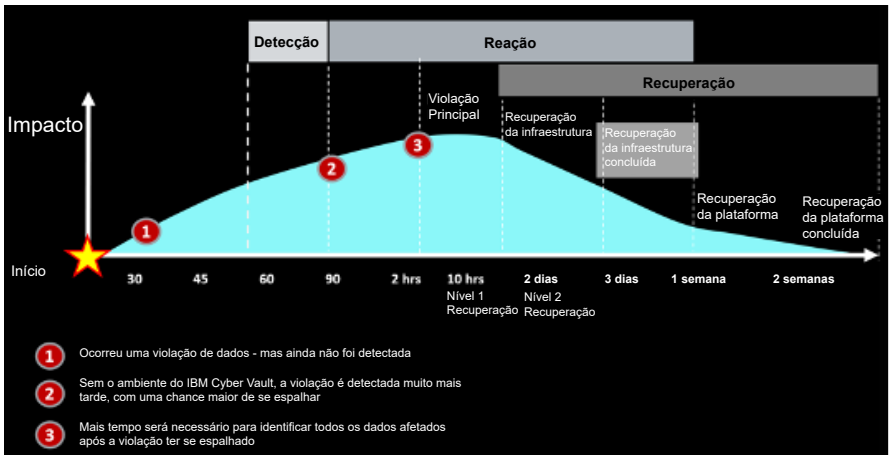
IBM FlashSystem Cyber Vault

A resiliência cibernética total requer detecção de invasão e monitoramento de atividade incomum em todos os níveis de sua infraestrutura, incluindo indivíduos, programas e sistemas interconectados, incluindo fornecedores externos e recursos de nuvem. Para essa detecção, a geração de relatórios e painéis de alerta para as equipes sobre atividades e comportamentos incomuns é fundamental.

Todos os funcionários, contratados e pessoas que trabalham com ferramentas ou sistemas de TI devem atualizar regularmente seus recursos e treinamento sobre como evitar pontos de ataque comuns, como phishing, smishing, vishing ou engenharia social. Eles também devem se comprometer e reconhecer os eventos para reportar comportamentos incomuns, pois isso é realmente um esforço de equipe.

Em resumo, será tarde demais se a detecção de um ataque de ransomware ocorrer após esse evento. Investimentos, uso e implementação de tecnologias, ferramentas, processos, monitoramento, educação e comunicação adequados são essenciais antes que um incidente ocorra. Essas medidas são fundamentais para obter a cibersegurança e a resiliência de nível empresarial.

O diagrama abaixo mostra as médias de tempo para uma organização recuperar suas operações comerciais. Perceba que o tempo de 2-3 semanas é o mais comum.



Duração típica da recuperação cibernética

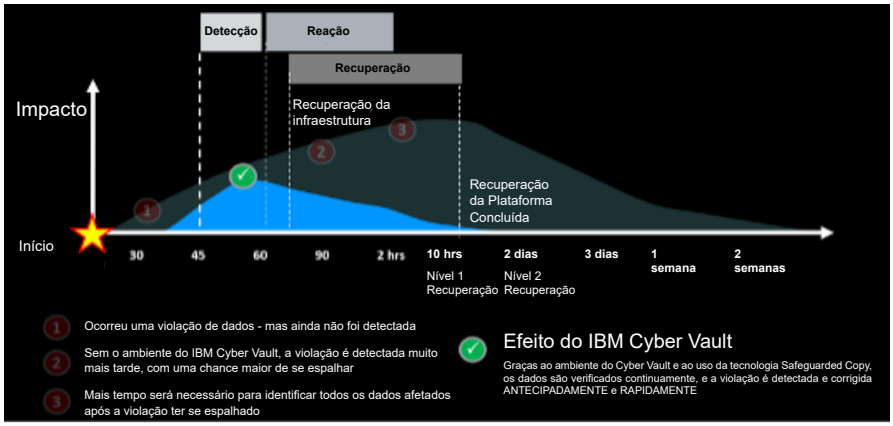
De acordo com um estudo, enquanto 41% das empresas atingidas por um ataque de ransomware conseguiu se recuperar em um mês, mais da metade (58%) afirmou que levou mais de um mês para se recuperar, 29% reportou mais de três meses, e 9% reportou mais de cinco a seis meses.[2]

Uma solução de armazenamento de resiliência cibernética deve permitir recursos para proteção contra os desafios de um ataque cibernético. O primeiro é a necessidade absoluta de isolamento virtual ou físico; cópias imutáveis de dados que não podem ser corrompidas ou apagadas por um invasor cibernético.

Em segundo, ferramentas necessárias para validar continuamente esses dados, para detectar um ataque e criar confiança na qualidade e validade de um backup de recuperação após a ocorrência de um ataque cibernético. Essas ferramentas também ajudarão a equipe de TI a realizar a análise forense do incidente; formular estratégias e opções de recuperação ideais; e determinar o escopo de recuperação, arquivos, bancos de dados ou sistemas completos.

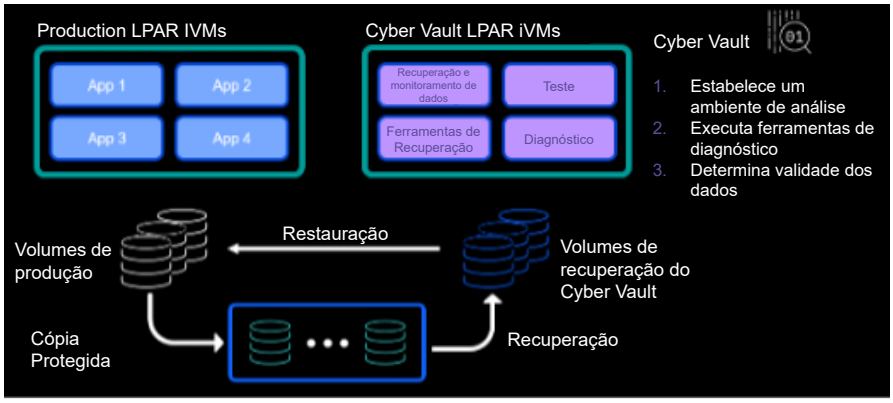
A solução IBM FlashSystem Cyber Vault é um blueprint implementado pelo IBM Lab Services ou IBM Business Partners, desenvolvida para acelerar a detecção e a recuperação contra ataques cibernéticos. A solução Cyber Vault é executada continuamente, monitorando os snapshots à medida que são criados pelo Safeguarded Copy. Através das ferramentas de banco de dados padrão e software de automação, o FlashSystem Cyber Vault verifica os snapshots do Safeguarded Copy quanto a violações.

Se o FlashSystem Cyber Vault detectar essas alterações, ocorre uma indicação imediata de um possível ataque. Ao preparar uma reação, conhecer os últimos snapshots sem evidência de um ataque pode acelerar a determinação de qual snapshot usar. E como esses snapshots do Safeguarded Copy ficam no mesmo local de armazenamento do FlashSystem e dados operacionais, sua recuperação é mais rápida do que a restauração de cópias armazenadas separadamente. Com essas vantagens, o FlashSystem Cyber Vault foi criado para reduzir o tempo de recuperação de ataques cibernéticos de dias para apenas algumas horas.



Efeito do IBM Cyber Vault

A solução IBM FlashSystem Cyber Vault permite um ambiente seguro e isolado, no qual uma réplica do ambiente de produção é mantida. O ambiente IBM FlashSystem Cyber Vault não afeta o ambiente de produção, pois aproveita um ambiente sandbox/sala limpa (partições lógicas ou VMs) para executar processos de validação de dados sem comprometer a produção. Esse ambiente de sandbox também é o local para treinar suas equipes, realizar análises forenses após a detecção de uma violação de dados e, com base na análise, realizar procedimentos de recuperação com a tranquilidade de que, se algo der errado em qualquer etapa, suas equipes podem sempre voltar para a Cópia Protegida original.



Ambiente do IBM Cyber Vault

O IBM FlashSystem Cyber Vault é composto pelos quatro elementos principais abaixo:

Operações do IBM Cyber Vault

Vejamos individualmente esses elementos.

Cópias Imutáveis de Dados

O IBM Safeguarded Copy é o mecanismo de proteção mais recente para dados nos sistemas de armazenamento da família IBM FlashSystem e IBM SAN Volume Controller. Assim como nos sistemas IBM DS8000®, o Safeguarded Copy ajuda a proteger seus dados contra incidentes acidentais ou deliberados. Ele também permite a recuperação rápida de cópias pontuais protegidas após um ataque cibernético.

O Safeguarded Copy permite cópias ou snapshots seguros e pontuais de dados de produção ativos, os quais não podem ser alterados ou excluídos (cópias imutáveis). Essas Cópias Protegidas geralmente são criadas em um ambiente de armazenamento separado da produção, e acessadas apenas pelo sistema de recuperação IBM FlashSystem Cyber Vault.

Monitoramento Proativo

Detectar uma ameaça antes que ela ocorra é fundamental para acelerar a recuperação e a disponibilidade operacional.

O IBM Security® QRadar® é uma solução Security Information and Event Management (SIEM), para monitorar, inspecionar, detectar e derivar insights para identificação de ameaças potenciais aos dados armazenados no IBM FlashSystem e no IBM Spectrum® Virtualize. Ele oferece recursos avançados de resiliência cibernética e detecção de ameaças, como visualização centralizada, implementação flexível, inteligência automatizada, aprendizado de máquina, busca proativa de ameaças e muito mais.

O IBM QRadar pode detectar padrões maliciosos através de diferentes fontes de dados e ferramentas e técnicas de análise, incluindo logs de acesso, heurística, correlação com logs de outros sistemas (como logs de rede ou logs de servidor), fluxo de rede e dados de pacote, incluindo detecção de vetor de ameaça desconhecida por meio de recursos do IBM Watson® for Security. O IBM QRadar tem integração com o IBM Safeguarded Copy para obter um snapshot protegido de dados ao primeiro sinal de um possível ataque.

O IBM Security Guardium® Data Protection detecta e classifica automaticamente dados confidenciais de toda a empresa, com monitoramento de atividade de dados em tempo real. Ele é aprimorado pelo Guardium Vulnerability Assessment, que detecta vulnerabilidades comportamentais, como xcsharing de contas, logins administrativos eessive e atividades incomuns fora do horário de trabalho, e identifica ameaças e falhas de segurança em bancos de dados que podem ser exploradas por hackers. E para ajudar os gestores de segurança a entender onde estão as ameaças, o Guardium Data Risk Manager mantém um painel executivo para ajudar a visualizar os riscos relacionados aos dados, para que executivos e lideranças possam tomar ações imediatas.

O IBM Storage Insights e o IBM Spectrum Control monitoram o armazenamento flash da IBM. Eles permitem visualizar uma carga de trabalho de E/S atual em relação a uma linha de base anterior, e ajudam a detectar um ataque em andamento.

Os alertas podem ser configurados para acionar se um sistema de armazenamento estiver sob alguns tipos de estresse. Por exemplo, se a taxa de redução de dados mudar radical e subitamente, isso pode indicar que um ataque cibernético está criptografando seus dados. Um ataque também pode causar uma mudança significativa no desempenho. Da mesma forma, desvios ou anomalias na taxa de gravação podem indicar um ataque cibernético.

Teste e Validação de Cópias de Dados

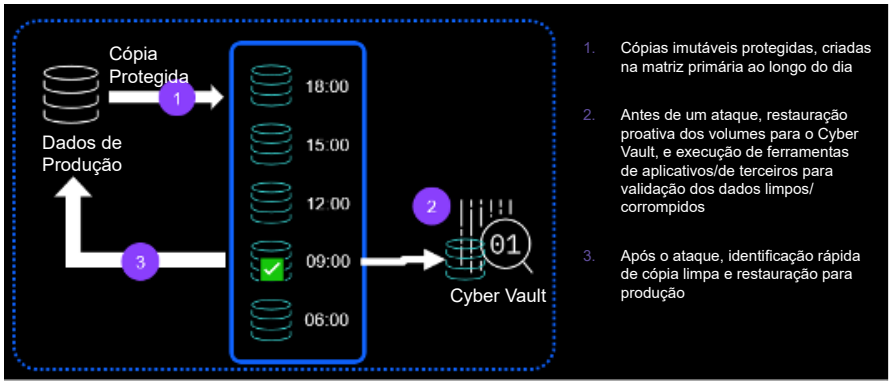
A solução IBM FlashSystem Cyber Vault oferece os seguintes recursos de resiliência cibernética:

- **Validação de dados: Validação operacional regular das cópias pontuais do Safeguarded Copy, para detecção proativa de corrupção de dados, ou garantia que a cópia é valida antes de qualquer outra ação.**
- **Análise forense:** Execução de uma cópia do sistema de produção para investigar um problema e determinar a ação de recuperação. Planejamento sobre quais ferramentas e procedimentos seriam aplicáveis para identificar a causa e o escopo de um ataque.
- **Recuperação cirúrgica:** Extração de dados da Cópia Protegida e restauração no ambiente de produção. Essa operação é fundamental para a restauração de dados, arquivos ou sistemas de volta à produção, em caso de perda de dados, intencional ou não intencional.
- **Recuperação catastrófica:** Essa opção é a última alternativa, a qual todos esperam que nunca seja usada. A solução IBM FlashSystem Cyber Vault oferece esse recurso, sendo recomendado realizar regularmente um exercício completo de recuperação catastrófica em um sistema de teste ou desenvolvimento, para aquisição de confiança na recuperação em caso de um ataque.
- **Backup off-line:** Execute um novo backup com sua solução de backup tradicional do ambiente validado, para uma camada de proteção adicional e retenção de dados de longo prazo.

Recuperação Rápida

O IBM FlashSystem Cyber Vault foi desenvolvido para permitir uma recuperação rápida e confiável dos aplicativos críticos, em poucos minutos a algumas horas, para proteção da reputação e da marca de sua organização. Após um ataque cibernético, o velho ditado é ainda mais verdadeiro: tempo é dinheiro!

Como vimos, a combinação de snapshots do IBM Safeguarded Copy, validação do Cyber Vault e automação permite restaurar rapidamente um ambiente de produção após um ataque.



Recuperação Rápida de Dados do IBM Cyber Vault

Estruturas para Resiliência Cibernética de TI

As regulamentações e estruturas específicas variam de acordo com o país ou região. Uma estrutura comumente citada foi lançada em 2013 e atualizada em 2018 pelo *National Institute for Standards and Technology* (Instituto Nacional de Padrões e Tecnologia - NIST).

A Estrutura de Segurança Cibernética do NIST apresenta uma política de orientação de segurança cibernética sobre como as organizações podem avaliar e melhorar sua capacidade de prevenção, detecção e reação contra ataques. Essa estrutura básica envolve uma metodologia aceita pelo setor, para criar um plano de desenvolvimento e proteção e garantir a entrega de serviços críticos. O diagrama abaixo descreve as cinco categorias da Estrutura NIST:

Estrutura NIST

Identificar – elaboração de um plano para que, em caso de ataque, estar preparado e confiante na capacidade de restauração dos sistemas de TI de volta ao estado anterior, o que exige um conhecimento detalhado do escopo de seus ativos críticos necessários para continuar as operações, além de uma estratégia de recuperação rápida.

Proteger – foco na identificação de pontos fracos antes de um possível ataque, garantindo que os dados sejam armazenados em uma infraestrutura imune a qualquer atividade maliciosa. Isso envolve questões de gerenciamento de ID, controle de acesso, conscientização e segurança e proteção de dados, bem como tecnologia de proteção proativa.

Detectar – busca de ameaças desconhecidas através de monitoramento e análises avançadas, para descobrir rapidamente quaisquer ameaças.

Responder – Inclui a coordenação da reação, análise, contenção, mitigação e comunicação

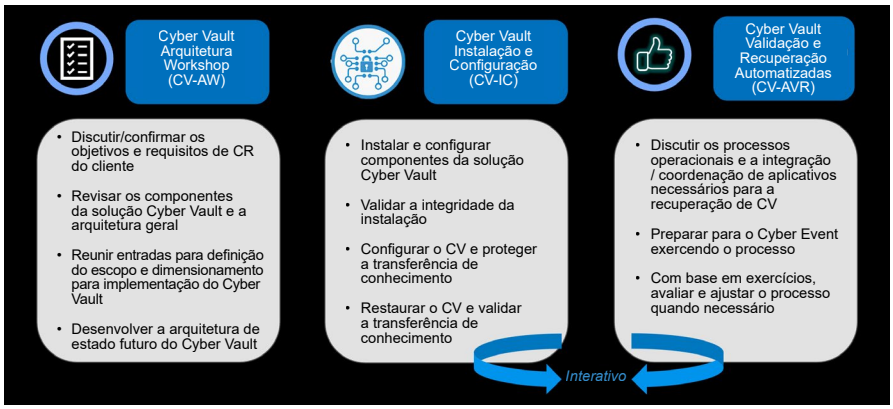
Recuperar – Retorno à operação de forma rápida e eficiente. Envolve coordenar diferentes aspectos e, uma vez analisadas as ações necessárias, automatizar a recuperação o máximo possível.

A solução IBM FlashSystem Cyber Vault aborda os principais componentes da Estrutura NIST Cybersecurity.

IBM Lab Services

O IBM Systems Lab Services oferece serviços de infraestrutura para a criação de soluções corporativas de TI e nuvem híbrida. Os consultores Lab Services colaboram com as organizações através de profundo conhecimento técnico, excelentes ferramentas e metodologias comprovadas. Esses especialistas ajudam seus clientes a resolver desafios de negócios, treinam áreas de TI com novas habilidades e sobre como aplicar as melhores práticas. O IBM Lab Services oferece profundo conhecimento técnico para uma ampla variedade de serviços de infraestrutura de TI, incluindo armazenamento.

O IBM Lab Services oferece um conjunto completo de serviços para ajudar seus clientes a implementar e utilizar a solução Cyber Vault. Esses serviços Cyber Vault podem incluir preparação, planejamento e implementação da solução Cyber Vault e, se necessário, prestar assistência na recuperação de incidentes cibernéticos.



Serviços de Implementação para o IBM FlashSystem Cyber Vault

Resumo

Os efeitos comerciais e financeiros dos ataques cibernéticos continuam a aumentar. Os ataques cibernéticos podem ocorrer de várias maneiras. Eles podem assumir formas diferentes e continuar a evoluir. Quer o objetivo do invasor seja roubar dados confidenciais de clientes ou reter informações para fins de resgate, as organizações devem manter uma estratégia geral de Segurança Cibernética.

As abordagens tradicionais de HA/DR para proteção de dados funcionam para os fins pretendidos, mas são inadequadas para proteção contra ataques cibernéticos. A replicação remota baseada em armazenamento para alta disponibilidade ou a recuperação de desastres reproduz todas as alterações (maliciosas ou não) na cópia remota.

Os dados armazenados em mídia offline ou na nuvem podem levar muito tempo para recuperar um ataque generalizado. A recuperação em larga escala pode levar de dias a semanas, o que pode resultar em um tempo de inatividade substancial para a empresa.

O recurso Safeguarded Copy no IBM FlashSystem e no IBM SAN Volume Controller foi desenvolvido para criar automaticamente snapshots imutáveis e eficientes de acordo com o planejamento. Esses snapshots são armazenados especificamente pelo sistema, e não podem ser conectados aos servidores, o que cria um ambiente de isolamento virtual de malware ou outras ameaças. Eles também não podem ser alterados e/ou excluídos, exceto de acordo com um planejamento, para proteção contra erros ou ações cometidas pela equipe.

A solução IBM FlashSystem Cyber Vault se baseia em Cópias Protegidas para acelerar a detecção e a recuperação de ataques cibernéticos. Através das ferramentas de banco de dados padrão e software de automação, o FlashSystem Cyber Vault verifica os snapshots do Safeguarded Copy quanto a violações.

Se o FlashSystem Cyber Vault detectar essas alterações, isso indica imediatamente que um ataque pode estar ocorrendo, de modo que a recuperação através de snapshots sem evidência de um ataque pode ser iniciada. E como esses snapshots do Safeguarded Copy ficam no mesmo local de armazenamento do FlashSystem e dados operacionais, sua recuperação é mais rápida do que a restauração de cópias armazenadas separadamente. Com essas vantagens, o FlashSystem Cyber Vault foi criado para reduzir o tempo de recuperação de ataques cibernéticos de dias para apenas algumas horas.

1. Fonte: IBM Institute for Business Value 2021 Cost of a Data Breach report, https://www.ibm.com/security/data-breach

2. IT World Canada, “Average ransomware payment for Canadian firms hits $450,000”, https://www.itworldcanada.com/article/average-ransomware-payment-for-canadian-firms-hits-450000/467792

Por que a IBM?

A IBM oferece um vasto portfólio de hardware, software e serviços, para ajudar as organizações a atender suas necessidades de infraestrutura de TI de forma econômica. Isso inclui soluções robustas de armazenamento de dados, para um armazenamento confiável e sempre ativo, além da recuperação de desastres. Como as necessidades de negócios mudam, as soluções da IBM enfatizam a interoperabilidade e a integração de novos casos de uso ou abordagens, de análises a backup em diferentes locais e recuperação quase instantânea. Com a IBM, as organizações podem criar uma infraestrutura de armazenamento flexível, robusta e resiliente, para suporte a operações críticas e conformidade regulatória.

Os recursos IBM Storage e IBM Security foram desenvolvidos para oferecer uma solução abrangente para prevenção, detecção e recuperação de ataques cibernéticos.

Para mais informações

Visite nossa página de soluções para saber mais sobre a família FlashSystem, ou entre em contato com seu representante IBM ou Parceiro de Negócios IBM. Caso necessite de um contato, preencha este formulário para agendar uma consulta com um especialista da IBM.

Além disso, o IBM Global Financing oferece várias opções de pagamento para ajudá-lo a adquirir a tecnologia necessária para expandir seus negócios. Oferecemos gerenciamento completo do ciclo de vida para produtos e serviços de TI, desde a aquisição até a substituição. Acesse: https://www.ibm.com/financing/flash