IBM FlashSystem Cyber Vault

Destaques

- Detecte ciberataques mais cedo para minimizar os danos
- Acelere a recuperação de um ataque
- Reduza o tempo de recuperação de dias ou semanas para apenas algumas horas
- Promova a análise forense de ataques

O efeito comercial e financeiro dos ciberataques continua a aumentar. Os ciberataques podem ocorrer de várias formas: eles podem assumir muitas formas diferentes e continuar evoluindo. As empresas precisam ter uma estratégia de segurança cibernética geral em vigor para lidar com invasores que desejam roubar dados confidenciais de clientes ou informações valiosas para pedidos de resgate.

O armazenamento desempenha uma função essencial tanto na detecção de ataques quanto na recuperação rápida.

A Cópia Protegida da IBM® cria capturas instantâneas de dados imutáveis e isoladas para ajudar a proteger sua empresa contra ciberataques, malwares, atos de funcionários descontentes e outras violações de dados. Essas capturas estão no mesmo armazenamento do FlashSystem que os dados operacionais, por isso, a recuperação é mais rápida do que a restauração de cópias armazenadas separadamente.

A solução IBM FlashSystem® Cyber Vault complementa a Cópia Protegida da IBM. O FlashSystem Cyber Vault verifica automaticamente as cópias criadas regularmente pela Cópia Protegida em busca de sinais de violação de dados causadas por malware ou ransomware. Essa varredura serve a dois propósitos: ela ajuda a identificar rapidamente um ataque clássico de ransomware que tenha sido iniciado e foi desenvolvida para ajudar a identificar quais cópias de dados não foram afetadas por um ataque. Com essas informações, os clientes podem identificar mais rapidamente que um ataque está em andamento e identificar e recuperar com mais agilidade uma cópia limpa de seus dados.

Visão geral

O cibercrime continua sendo uma grande preocupação para as empresas. Quase todos os dias vemos relatos de novos ataques. O custo médio é de USD 4,24 milhões e a recuperação pode levar dias ou semanas.Os ciberataques tanto têm impacto imediato nos negócios quanto podem ter um impacto reputacional duradouro se a empresa ficar indisponível por um longo tempo.[1]

Infelizmente, é muito provável que os ciberataques continuem sendo uma ameaça significativa em 2022 e no futuro. Não é uma questão de *se* um dia você for violado, mas *quando será.*

Quando ocorre um ciberataque, a resposta de sua empresa faz a diferença entre danos financeiros e de reputação permanentes ou leves interrupções de curto prazo.

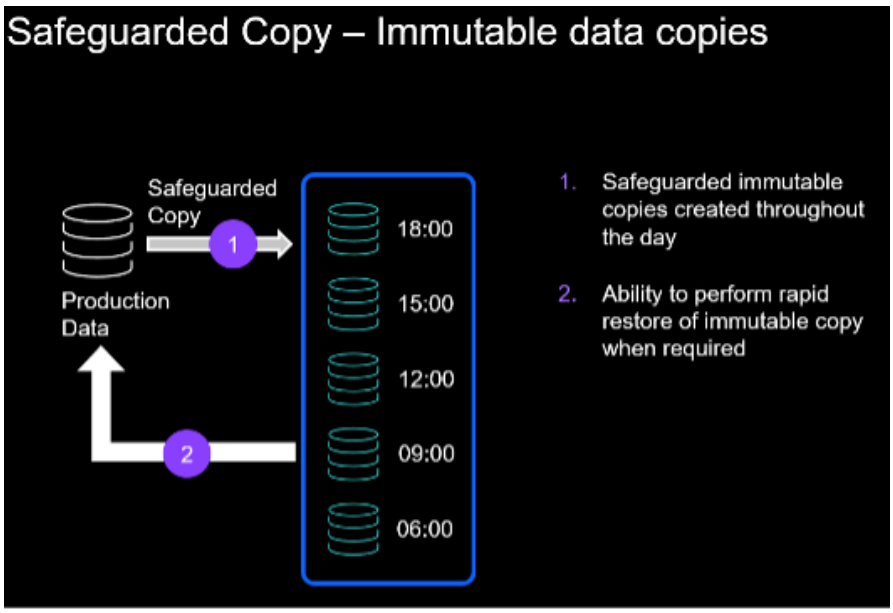
As soluções tradicionais de continuidade de negócios desenvolvidas e implementadas pela maioria das empresas têm alta disponibilidade (HA) e recuperação de desastres (DR) para proteger os dados contra ameaças convencionais (mas ainda relevantes). Infelizmente, elas não são capazes de proteger seus dados contra a gama cada vez maior de ciberataques.

A única solução é investir em tecnologias atualizadas e processos automatizados que ajudem a proteger sua empresa contra um evento cibernético e recuperar rapidamente as operações de negócios críticas. Durante um evento cibernético, a rápida recuperação é a maior prioridade para qualquer empresa. Toda empresa, independentemente do tamanho ou setor, precisa de uma estratégia de resiliência de dados bem definida, incluindo resiliência cibernética, para recuperar-se rapidamente de uma violação de dados e de ataques semelhantes.

Cópia protegida da IBM

A Cópia Protegida da IBM cria regularmente capturas instantâneas de dados isoladas (separados dos servidores) e imutáveis (sem possibilidade de alteração) para ajudar a proteger sua empresa contra ciberataques, malware, atos de funcionários descontentes e outras violações de dados. Como as capturas instantâneas da Cópia Protegida estão no mesmo armazenamento do FlashSystem que os dados operacionais, a recuperação é mais rápida do que a restauração de cópias armazenadas separadamente.

Neste exemplo, uma política da Cópia Protegida realiza automaticamente cópias de capturas instantâneas imutáveis a cada três horas.



Operação da Cópia Protegida da IBM

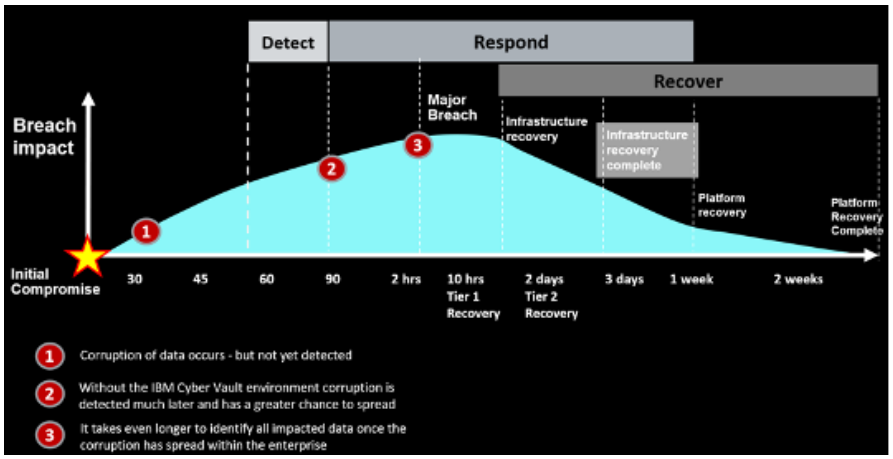
IBM FlashSystem Cyber Vault

Para ter uma resiliência cibernética completa, é necessário realizar a detecção de intrusão e o monitoramento de comportamentos incomuns em todos os níveis da infraestrutura, incluindo pessoas, programas e sistemas interconectados, como fornecedores externos e recursos de cloud. A criação de relatórios e painéis oportunos para alertar as equipes sobre atividades e comportamentos incomuns é parte fundamental de uma detecção bem-sucedida.

Todos os funcionários, contratados e outras pessoas que trabalham com ferramentas ou sistemas de TI precisam atualizar regularmente seus conhecimentos e treinamentos sobre como evitar pontos de ataque comuns, como phishing, smishing, vishing ou engenharia social. Eles também precisam se sentir engajados e reconhecer os eventos que devem ser relatados como comportamentos incomuns, pois isso é realmente um esforço em equipe.

Simplificando, se a primeira detecção de um ataque de ransomware ocorre depois que ele aconteceu, já é tarde demais. É essencial investir, usar e se dedicar a tecnologias, ferramentas, processos, monitoramentos, treinamentos e comunicações adequados para lidar com incidentes antes que eles ocorram. Isso é fundamental para obter segurança cibernética e resiliência de classificação corporativa.

O diagrama a seguir mostra o tempo médio que as empresas do setor levam para recuperar suas operações de negócios. Você notará que o tempo comum é algo em torno de duas a três semanas.



Duração comum de uma recuperação cibernética

Mesmo assim, de acordo com um estudo, embora 41% dos negócios atingidos por um ataque de ransomware tenham conseguido retomar as operações em cerca de 30 dias, mais da metade (58%) disse que levou mais de um mês para isso, 29% disseram ter levado mais de três meses e *9% relataram mais de cinco a seis meses.*[2]

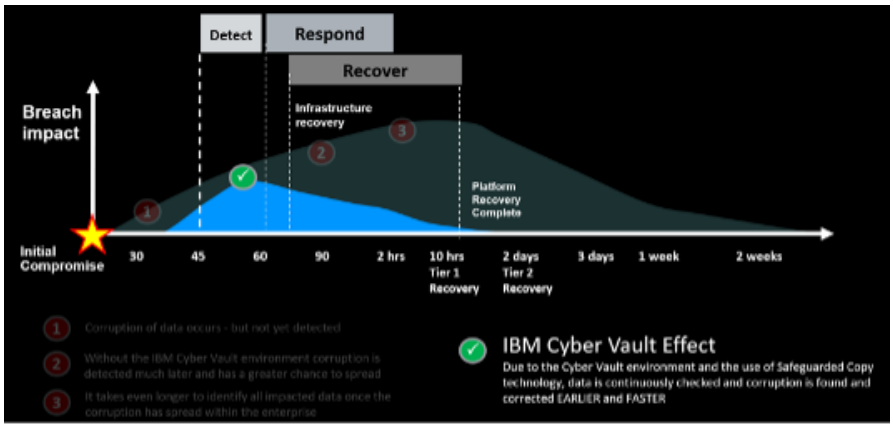
Uma solução de armazenamento de resiliência cibernética precisa fornecer recursos para a proteção contra os desafios específicos de um ciberataque. O primeiro recurso absolutamente necessário é o isolamento lógico ou físico: cópias de dados imutáveis que não podem ser corrompidas ou apagadas por um invasor cibernético.

Em segundo lugar, são necessárias ferramentas para validar continuamente esses dados a fim de ajudar a detectar um ataque e criar confiança na qualidade e na validade de um backup para recuperação após a ocorrência de um ciberataque. Essas ferramentas também ajudarão a equipe de TI na realização da análise forense necessária para avaliar o incidente, na formulação de estratégias e opções de recuperação ideais e na determinação do escopo da recuperação, dos arquivos, dos bancos de dados ou de sistemas inteiros.

A solução IBM FlashSystem Cyber Vault é um blueprint implementado pelo IBM Lab Services ou por Parceiros de Negócios IBM que foi desenvolvido para ajudar a acelerar a detecção e a recuperação de ciberataques. A solução Cyber Vault é executada continuamente e monitora as capturas instantâneas criadas pela Cópia Protegida. Com ferramentas de banco de dados padrão e softwares de automação, o FlashSystem Cyber Vault verifica se há alguma violação nas

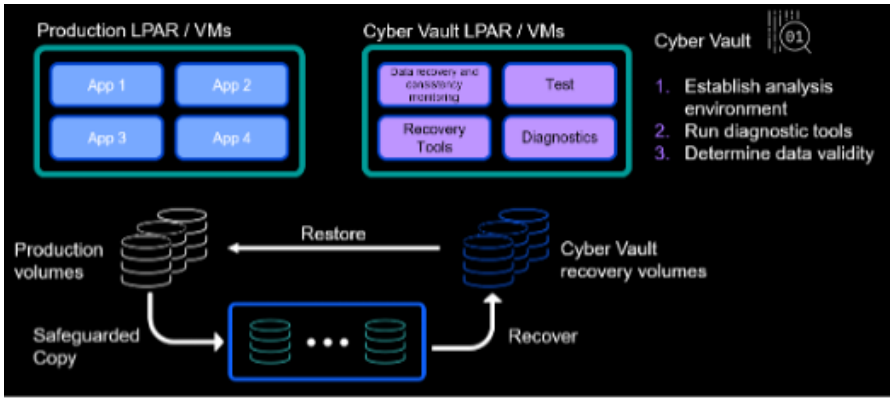
capturas instantâneas da Cópia Protegida.

Quando ele encontra essas mudanças, isso é um sinal imediato de que um ataque pode estar ocorrendo. Ao preparar uma resposta, saber quais são as capturas instantâneas mais recentes sem evidência de um ataque acelera a determinação de qual captura instantânea usar. Como as capturas instantâneas da Cópia Protegida estão no mesmo armazenamento do FlashSystem que os dados operacionais, a recuperação é mais rápida do que a restauração de cópias armazenadas separadamente. Com essas vantagens, o Cyber Vault do FlashSystem foi desenvolvido para ajudar a reduzir o tempo de recuperação de ciberataque de dias para apenas horas.



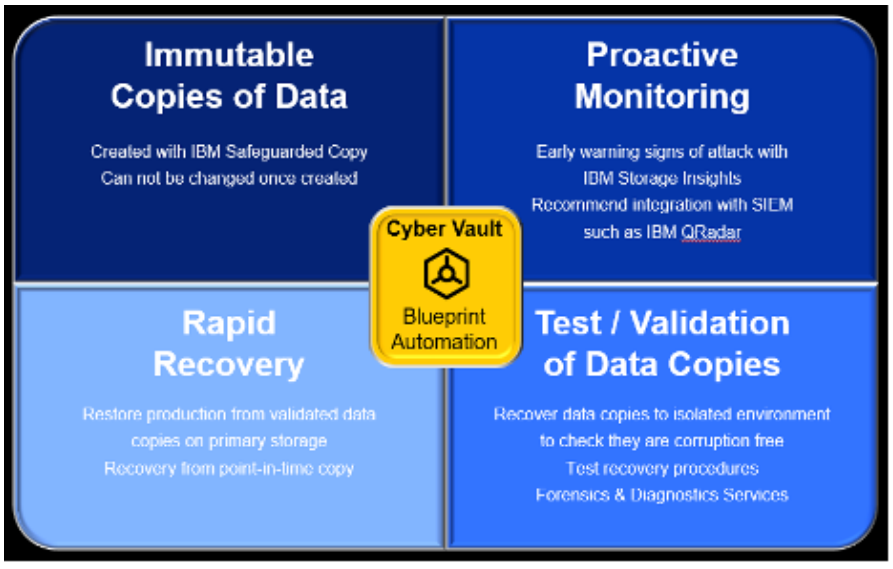
Efeito do IBM Cyber Vault

A solução IBM FlashSystem Cyber Vault fornece um ambiente seguro e isolado no qual uma réplica do ambiente de produção é mantida. O ambiente do IBM FlashSystem Cyber Vault não afeta o ambiente de produção, pois ele utiliza um ambiente de simulação/sala limpa (partições lógicas ou VMs) para executar processos de validação de dados sem afetar as cargas de trabalho de produção. Esse ambiente de simulação também é o local para treinar suas equipes, realizar análises forenses após a detecção de violações de dados e, com base na análise, realizar procedimentos de recuperação cirúrgica com a tranquilidade de que, se algo der errado em qualquer etapa da recuperação, suas equipes sempre poderão voltar para a cópia pontual original da Cópia Protegida.



Ambiente do IBM Cyber Vault

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



Operações do IBM Cyber Vault

Veja alguns detalhes de cada um desses elementos

Cópias imutáveis de dados

A Cópia Protegida da IBM é o mecanismo de proteção mais recente para dados na família IBM FlashSystem e nos sistemas de armazenamento IBM SAN Volume Controller. Como nos sistemas IBM DS8000®, a Cópia Protegida ajuda a proteger seus dados para evitar que eles sejam comprometidos acidentalmente ou deliberadamente. Ela também permite uma recuperação rápida de cópias protegidas pontuais quando ocorre um ciberataque.

A Cópia Protegida fornece cópias ou capturas instantâneas seguras e pontuais de dados de produção ativos que não podem ser alteradas ou excluídas (conhecidas como cópias imutáveis). Essas Cópias Protegidas geralmente são criadas em um ambiente de armazenamento separado da produção e são acessadas apenas pelo sistema de recuperação do IBM FlashSystem Cyber Vault.

Monitoramento proativo

Detectar uma ameaça antes que ela aconteça é fundamental para acelerar o tempo de recuperação e a disponibilidade operacional.

O IBM Security® QRadar® é uma solução de SIEM (gerenciamento de eventos e informações de segurança) que pode monitorar, inspecionar, detectar e derivar insights para identificar ameaças potenciais aos dados armazenados no IBM FlashSystem e no IBM Spectrum® Virtualize. Ela fornece recursos avançados de resiliência cibernética e detecção de ameaças, como visibilidade centralizada, implementação flexível, inteligência automatizada, machine learning, investigação proativa de ameaças e muito mais.

O IBM QRadar pode detectar padrões maliciosos utilizando várias origens de dados e ferramentas e técnicas de análise, como logs de acesso, heurística, correlação com logs de outros sistemas, incluindo logs de rede ou de servidor, fluxos de rede, dados de pacote e até mesmo a detecção de vetores de ameaça desconhecidos com recursos do IBM Watson® for Security. O IBM QRadar tem integração com a Cópia Protegida da IBM para realizar uma captura instantânea protegida de dados ao primeiro sinal de um possível ataque.

O IBM Security Guardium® Data Protection descobre e classifica automaticamente dados confidenciais de toda a empresa, fornecendo monitoramento de atividades de dados em tempo real. Ele é aprimorado pelo Guardium Vulnerability Assessment, que detecta vulnerabilidades comportamentais, como compartilhamento de contas, logins administrativos em excesso e atividades incomuns após o horário comercial, e identifica ameaças e falhas de segurança em bancos de dados que podem ser exploradas por hackers. A fim de ajudar os diretores de segurança a entender onde estão as ameaças aos negócios, o Guardium Data Risk Manager conta com um painel executivo que ajuda a visualizar os riscos de negócios relacionados aos

dados para que os executivos e a gerência possam tomar ações imediatas e proteger os negócios.

O IBM Storage Insights e o IBM Spectrum Control monitoram o armazenamento flash da IBM. Eles fornecem a capacidade de visualizar uma carga de trabalho de E/S atual em relação a uma referência anterior e ajudam a fornecer uma indicação de um ataque em andamento.

Os alertas podem ser definidos para serem acionados se um sistema de armazenamento estiver sob muitos tipos de estresse. Por exemplo, se a taxa de redução de dados mudar radicalmente de maneira repentina, isso pode indicar que um ciberataque está criptografando dados no momento. Um ataque também pode causar uma mudança significativa no desempenho. Da mesma forma, desvios ou anomalias na taxa de mudanças de gravação podem ser um indicador de que um ciberataque está ocorrendo.

Teste e validação de cópias de dados

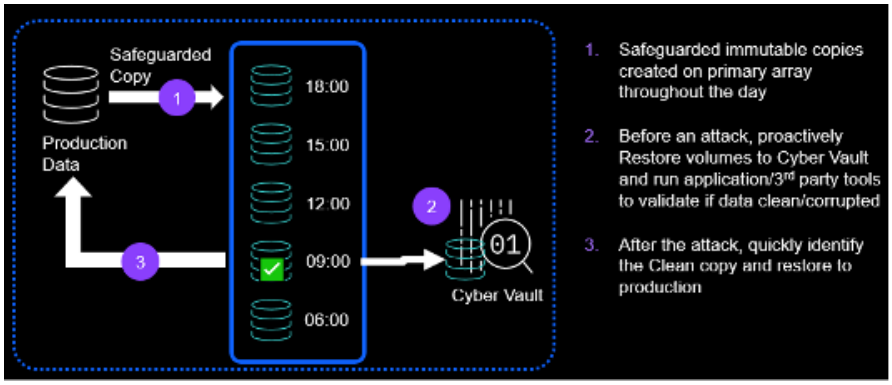
A solução IBM FlashSystem Cyber Vault fornece os diferentes recursos a seguir de resiliência cibernética:

- **Validação de dados:** obtenha uma validação operacional regular das cópias pontuais da Cópia Protegida para fornecer detecção proativa de violação de dados ou garantia de que a Cópia está validada e limpa antes de quaisquer ações adicionais.
- **Análise forense:** realize uma cópia do sistema de produção e use-a para investigar um problema e determinar a ação de recuperação. Planeje quais ferramentas e procedimentos podem ser usados para identificar a causa e o escopo de um ataque.
- **Recuperação cirúrgica:** extraia dados da Cópia Protegida e restaure-os logicamente no ambiente de produção. Se houver uma perda de dados intencional ou não intencional, essa operação será fundamental para restaurar dados, arquivos ou sistemas de volta ao uso na produção.
- **Recuperação catastrófica:** esta é a última opção que todos esperam precisar usar. A solução IBM FlashSystem Cyber Vault fornece esse recurso e, como uma melhor prática, deve-se realizar regularmente um exercício completo de recuperação catastrófica em um sistema de teste ou desenvolvimento para que seja possível adquirir confiança na recuperação em caso de um ataque.
- **Backup off-line:** faça um novo backup com sua solução de backup tradicional do ambiente validado com sucesso para incluir uma camada de proteção adicional e retenção de dados a longo prazo.

Recuperação rápida

O IBM FlashSystem Cyber Vault foi desenvolvido para fornecer recuperação rápida e confiável, em minutos ou horas, de seus aplicativos críticos para proteger a reputação e o valor da marca de sua empresa. Após um ciberataque, o velho ditado é ainda mais verdadeiro: *tempo é dinheiro!*

Como vimos, a combinação das capturas instantâneas da Cópia Protegida da IBM, da validação do Cyber Vault e da automação oferece a capacidade de restaurar rapidamente um ambiente de produção após um ataque.



Recuperação rápida de dados do IBM Cyber Vault

Estruturas para a resiliência cibernética de TI

As regulamentações e estruturas específicas variam de acordo com o país ou região do mundo. Uma estrutura comumente citada foi lançada em 2013 e atualizada em 2018 pelo Instituto Nacional de Padrões e Tecnologia (NIST).

A Estrutura de Segurança Cibernética do NIST fornece uma política de orientação de segurança de computador sobre como as empresas podem avaliar e melhorar sua capacidade de prevenir, detectar e responder a ciberataques. Essa estrutura básica é uma metodologia aceita pelo setor para a criação de um plano de desenvolvimento e implementação de proteções que garantam a entrega de serviços críticos aos negócios. O diagrama a seguir descreve as cinco categorias da estrutura do NIST:

Estrutura NIST

Identificar: trata-se de preparar uma estratégia de recuperação rápida e um plano para que, quando você for atacado, esteja preparado e confiante em sua capacidade de restaurar os sistemas de TI de negócios para o estado anterior, o que requer um conhecimento detalhado do escopo de seus ativos críticos aos negócios, o que é necessário para continuar as operações.

Proteger: trata-se de descobrir antes dos invasores seus pontos fracos e garantir que seus dados sejam armazenados em uma infraestrutura que não possa ser violada por nenhuma atividade maliciosa. Isso envolve tópicos como gerenciamento de IDs, controle de acesso, capacitação, segurança de dados e proteção de dados, bem como tecnologia de proteção proativa.

Detectar: descubra rapidamente ameaças desconhecidas com monitoramentos e análises avançadas.

Responder: trata da coordenação de sua resposta, ou seja, análises, contenção, redução e comunicação

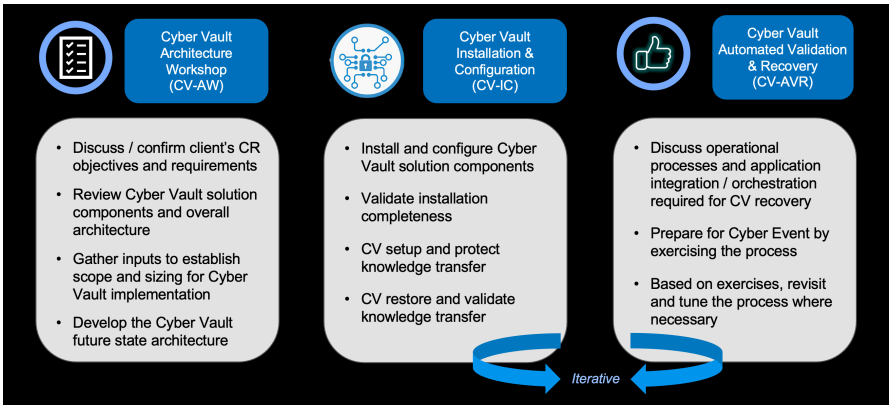
Recuperação: volte a operar de forma rápida e eficiente. Isso envolve orquestrar muitas partes móveis e, uma vez analisadas as ações necessárias, automatizar o máximo possível da recuperação.

A solução IBM FlashSystem Cyber Vault aborda os principais componentes da estrutura de segurança cibernética do NIST.

IBM Lab Services

O IBM Systems Lab Services oferece serviços de infraestrutura para ajudá-lo a criar soluções corporativas de TI e cloud híbrida. Os consultores do Lab Services colaboram com as empresas, oferecendo profundo conhecimento técnico, ferramentas valiosas e metodologias de sucesso. Os especialistas ajudam os clientes a resolver desafios de negócios e treinam departamentos de TI em novas habilidades e em como aplicar melhores práticas. O IBM Lab Services oferece conhecimento técnico profundo com relação a uma ampla variedade de serviços de infraestrutura de TI, incluindo armazenamento.

O IBM Lab Services oferece um conjunto completo de serviços para ajudar os clientes a acelerar a adoção e o uso da solução Cyber Vault. Esses serviços para o Cyber Vault podem incluir preparação, planejamento e implementação da solução Cyber Vault e, se necessário, assistência na recuperação de incidentes cibernéticos.



Serviços de implementação do IBM FlashSystem Cyber Vault

Resumo

Os efeitos comerciais e financeiros dos ciberataques continuam a aumentar. Os ciberataques podem ocorrer de várias formas. Eles podem assumir muitas formas diferentes e continuar evoluindo. As empresas precisam ter uma estratégia de segurança cibernética geral em vigor para lidar com invasores que desejam roubar dados confidenciais de clientes ou informações valiosas para pedidos de resgate.

As abordagens de HA/DR tradicionais para a proteção de dados funcionam bem para os propósitos pretendidos, mas são inadequadas para a proteção contra ciberataques. A replicação remota baseada em armazenamento para alta disponibilidade ou recuperação de desastres replica todas as mudanças (maliciosas ou não) na cópia remota.

Os dados armazenados em mídias off-line ou na cloud podem levar muito tempo para serem recuperados de um ataque generalizado. A recuperação em larga escala pode levar de dias a semanas, o que pode causar um tempo de inatividade substancial para as empresas.

O recurso Cópia Protegida no IBM FlashSystem e no IBM SAN Volume Controller foi desenvolvido para criar automaticamente capturas instantâneas imutáveis e eficientes de acordo com um planejamento. Essas capturas instantâneas são armazenadas especificamente pelo sistema e não podem ser conectadas a servidores, o que cria um ambiente de isolamento virtual contra malware ou outras ameaças. Elas também não podem ser alteradas ou excluídas, exceto de acordo com um cronograma planejado, o que ajuda na proteção contra erros ou ações da equipe.

A solução IBM FlashSystem Cyber Vault se baseia na Cópia Protegida e ajuda a acelerar a detecção e a recuperação de ciberataques. Com ferramentas de banco de dados padrão e softwares de automação, o FlashSystem Cyber Vault verifica se há alguma violação nas capturas instantâneas da Cópia Protegida.

Quando o FlashSystem Cyber Vault encontra essas mudanças, isso é um sinal imediato de que um ataque pode estar ocorrendo, portanto, é possível começar rapidamente a recuperação com as capturas instantâneas mais recentes sem evidência de um ataque. Como as capturas instantâneas da Cópia Protegida estão no mesmo armazenamento do FlashSystem que os dados operacionais, a recuperação é mais rápida do que a restauração de cópias armazenadas separadamente. Com essas vantagens, o Cyber Vault do FlashSystem foi desenvolvido para ajudar a reduzir o tempo de recuperação de ciberataque de dias para apenas horas.

1.Fonte: relatório de 2021 do IBM Institute for Business Value sobre o custo de uma violação de dados, 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 escolher a IBM?

A IBM oferece um grande portfólio de hardwares, softwares e serviços para ajudar as empresas a atender necessidades de infraestrutura de TI de forma econômica. Esse portfólio inclui soluções robustas de armazenamento de dados para permitir um armazenamento confiável e sempre ativo, além de 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, desde análises até backup multissite e recuperação praticamente instantânea. Com a IBM, as empresas podem criar uma infraestrutura de armazenamento flexível, robusta e resiliente para suportar operações críticas a fim de evitar interrupções e manter a conformidade regulamentar.

As ofertas IBM Storage e IBM Security são desenvolvidas para trabalhar juntas e fornecer uma solução abrangente para a prevenção, a detecção e a recuperação de ciberataques.

Saiba mais

Visite nossa página de soluções para saber mais sobre a família FlashSystem de sistemas de dados ou entre em contato com seu representante ou Parceiro de Negócios IBM. Para se conectar, preencha este formulário e agende uma consulta com um especialista em armazenamento da IBM.

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

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.