Construção da resiliência de negócios para proteção contra ataques cibernéticos destrutivos

Cyber Recovery com a Dell Technologies

DELL Technologies

Índice

3 O que é o Cyber Recovery? E por que ela é importante?	4 Os dados são da sua empresa… e as ameaças cibernéticas colocam sua empresa em risco	5 10 principais motivos para escolher a Dell EMC PowerProtect Cyber Recovery	6 A recuperação de desastres e a continuidade dos negócios não são suficientes para lidar com as ameaças cibernéticas modernas
7 Proteção contra ataques ransomware e destrutivos	8 Por que escolher o PowerProtect Cyber Recovery?	9 Por que o PowerProtect Cyber Recovery é a melhor opção	10 CyberSense para etectar, diagnosticar e recuperar-se rapidamente de ataques cibernéticos
11 8 maneiras com as quais o CyberSense Combate de maneira eficiente ataques ransomware e Outros ataques cibernéticos	12 O CyberSense permite Detecção precoce e Recuperação garantida	13 Dell EMC PowerProtect Cyber Recovery na Prática	14 Comprovado, com experiência Cyber Recovery Serviços de consultoria
15 Protegendo o cliente Dados e preservação Confiança pública nos Mercados financeiros dos Estados Unidos	17 Estudo de caso: Setor da área da saúde	18 Estudo de caso: Serviços financeiros	19 Comece agora!Sua Checklist para construir Resiliência cibernética

O que é o Cyber Recovery? E por que ela é importante?

Independentemente do setor, os dados impulsionam a empresa nos dias de hoje. O mercado global se baseia no fluxo constante de dados em redes interconectadas, e as iniciativas de transformação digital colocam ainda mais dados em risco.

O aumento no volume e no valor dos dados apresenta uma oportunidade para criminosos que usam ferramentas e táticas modernas — na verdade, 68% dos líderes de negócios afirmam que seus riscos de segurança cibernética estão aumentando (Accenture). A ameaça moderna de ataques cibernéticos e a importância de manter a confidencialidade, a disponibilidade e a integridade dos dados requerem soluções e estratégias modernas e comprovadas para proteger dados e sistemas vitais

Infelizmente, no ambiente de hoje voltado para dados, a recuperação de desastres (DR) tradicional e a continuidade dos negócios não são suficientes para lidar com as ameaças cibernéticas modernas. 69% dos entrevistados não têm a certeza de que poderiam recuperar todos os dados essenciais para os negócios no caso de um ataque cibernético.[1] Embora esses ataques sejam feitos de várias formas e os invasores tenham uma variedade de motivações, o objetivo dos esforços deles é consistente: destruir, roubar e resgatar dados digitais valiosos para fins financeiros, sociais ou políticos.

O Cyber Recovery, às vezes chamado de recuperação isolada, é um novo segmento de soluções de proteção de dados projetadas para lidar com a ameaça moderna de resgate e outras ameaças cibernéticas, para limitar a propagação de malware e reduzir a superfície do ataque em uma base global.

71%

de violações são motivadas por motivos financeiros

US$ 5,2 tri

dos riscos globais nos próximos 5 anos

Um ataque cibernético ocorre a cada

39 segundos

A estabilidade da receita e da existência de uma empresa depende da capacidade dela de isolar dados e garantir a disponibilidade para oferecer suporte a uma estratégia de continuidade dos negócios de ataques cibernéticos e operações de recuperação.

1. Índice global de proteção de dados da Dell Technologies

Os dados são a sua empresa…
e as ameaças cibernéticas colocam sua empresa em risco

Riscos técnicos

- Todos os dados estão suscetíveis a um ataque cibernético
- A replicação do armazenamento principal pode replicar dados corrompidos
- Catálogo de backup não replicado
- A recuperação da fita é lenta e propensa a falhas
- Cópias de backup não isoladas da rede

Riscos de pessoas e dos processos

- A TI e as operações acessam a maioria dos ativos de backup, se não todos
- Equipes de segurança não atribuídas aos ativos
- Os maus atores dentro do firewall podem excluir backups primários
- Dados essenciais ou não para os negócios não são separados
- As imagens de backup podem ser expiradas sem aprovação

área da saúde

varejo

petróleo e gás

ciências da vida

serviços financeiros

instituições governamentais

indústria

firmas de advocacia / setores jurídicos de corporações

Os 10 principais motivos para escolher Dell EMC PowerProtect Cyber Recovery

1. Cofre digital reforçado dedicado com lacuna de ar física e operacional
2. Protege contra ataques internos, exigindo vários logins separados para acessar o cofre
3. Os dados gravados no cofre são inalterados e invariáveis
4. O malware pode entrar no cofre, mas não tem capacidade de executar ou infectar dados fora do cofre
5. Primeira a integrar a indexação de conteúdo total, a lógica analítica inteligente, o aprendizado de máquina e as ferramentas forenses
6. Identifica e restaura rapidamente o último arquivo ou conjunto de dados válido para recuperação rápida
7. Automação de fluxo de trabalho de recuperação total para retomar rapidamente operações comerciais
8. Primeiro Solution Provider de tecnologia no programa de parceria Sheltered Harbor Alliance
9. Primeira fornecedora de tecnologia desenvolvendo uma solução de armazenamento em cofre de dados turnkey do Sheltered Harbor
10. Fonte única para arquitetura de solução, implementação e suporte para as soluções Cyber Recovery, CyberSense e Sheltered Harbor

A recuperação de desastres e a continuidade dos negócios não são suficientes para lidar com as ameaças cibernéticas modernas

Os invasores estão atacando sistemas, dados e backups. Eles estão criptografando o catálogo de backup, além dos sistemas e dos dados. A recuperação de desastres está on-line e não é isolada até o nível de um cofre cibernético, o que torna a DR vulnerável a esses ataques. Uma solução de cofre cibernético com lacuna de ar assegura que uma cópia protegida dos dados essenciais seja mantida em formato original.

A verdadeira resiliência cibernética requer uma recuperação cibernética.

A solução PowerProtect Cyber Recovery inclui um cofre digital seguro que é isolado física e logicamente da rede de produtos e backups com uma lacuna de ar operacional. Os dados essenciais são protegidos dentro do cofre em um formato imutável com períodos de retenção bloqueados. Isso oferece a melhor chance possível de recuperação caso seus backups primários tiverem sido comprometidos ou seu local de DR tiver sido violado ou infectado. Sem uma solução Cyber Recovery, uma empresa gasta um tempo significativo recuperando os últimos backups sem saber se são bons ou não. Este é um trabalho longo, intenso, iterativo e dispendioso.

categoria	recuperação de desastres	resiliência cibernética
Tempo de recuperação	Quase instantâneo	Confiável e rápido
Ponto de recuperação	Idealmente contínuo	Média de 1
Natureza do desastre	Inundação, queda de energia, condições meteorológicas	Ataque cibernético, direcionado
Impacto do desastre	Regional, geralmente contido	Global, espalha-se rapidamente
Topologia	Conectada, vários destinos	Isolada, além da DR
Volume de dados	Abrangente, todos os dados	Seletiva, inclui serviços básicos
Recuperação	DR padrão (por exemplo, failback)	Recuperação seletiva, iterativa; parte da CR

Proteção contra ataques cibernéticos e ransomware

Os reguladores globais em diversos setores concordam em como proteger melhor os dados essenciais e os ativos digitais contra ameaças cibernéticas. Eles determinaram que a proteção de uma cópia de dados essenciais de maneira isolada é a maneira mais conhecida de fornecer recuperação de ataques de destruição e ransomware.

“Uma arquitetura de backup de dados com lacuna de ar…”

"Confidencialidade, integridade, disponibilidade e resiliência"

"Considere manter os backups off-line e indisponíveis"

"Certifique-se de que os backups não estejam conectados às redes que estão fazendo backup."

Por que escolher o PowerProtect Cyber Recovery?

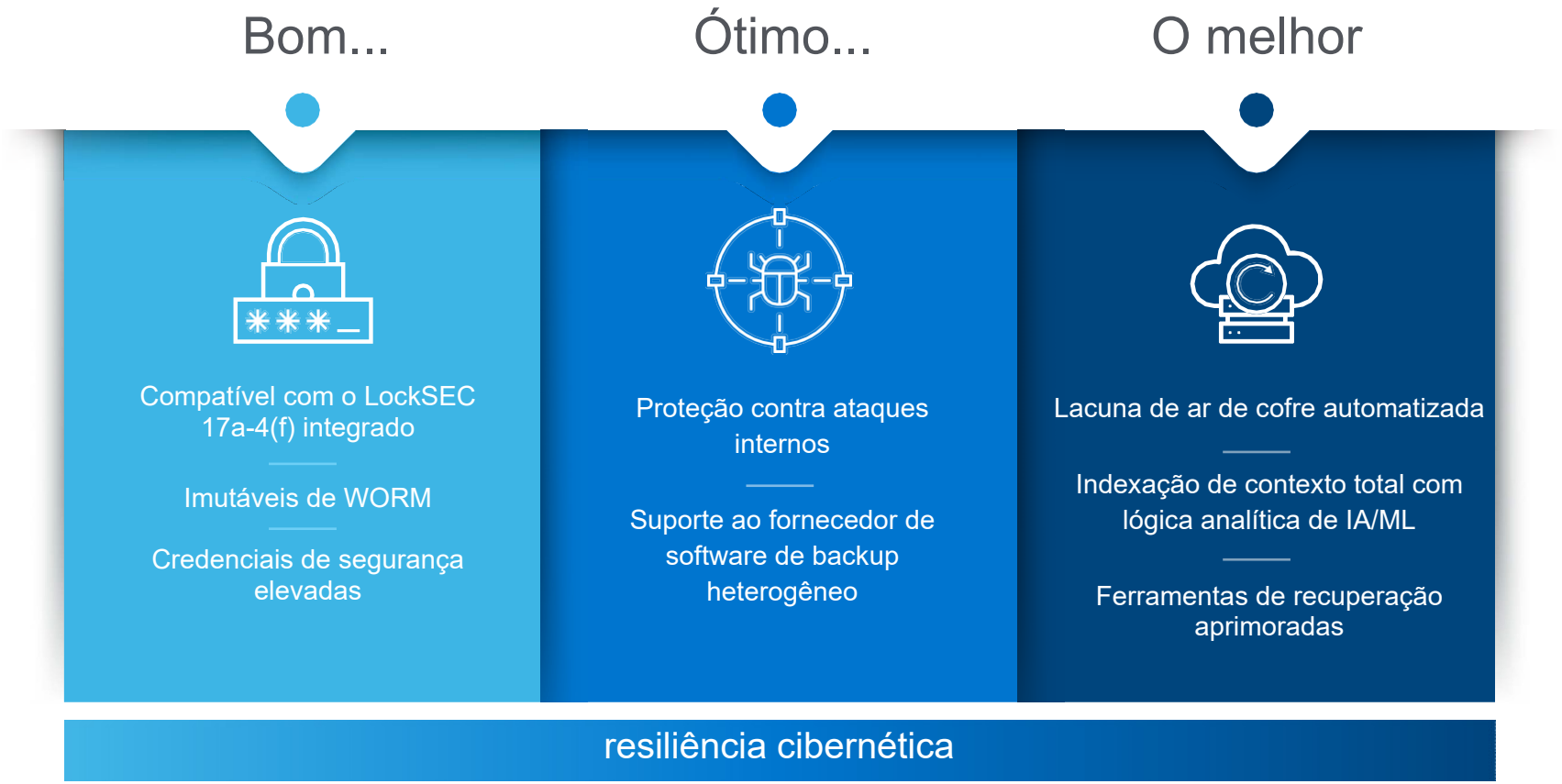
A última linha de defesa da proteção de dados contra ataques cibernéticos

A Dell EMC PowerProtect Cyber Recovery automatiza os fluxos de trabalho de maneira completa para proteger dados essenciais, identificar atividades suspeitas e realizar a recuperação de dados, quando necessário. O cofre do Cyber Recovery é desconectado da rede por meio de uma lacuna de ar automatizada e armazena todos os dados essenciais fora da rede para isolá-lo do ataque. Isso promove a resiliência de negócios, fornece garantia após a extrema perda ou destruição de dados e inclui dados de configuração de negócios e tecnologia para permitir a rápida recuperação do ambiente e a retomada de operações de negócios normais.

- Os dados essenciais residem fora da rede e isolados de ataques cibernéticos
- O cofre do Cyber Recovery tem uma lacuna de ar da rede para impedir o acesso
- Atualização por meio do processo de replicação com base em limites aceitáveis de exposição a riscos da conectividade de tempo de funcionamento e dos parâmetros de perda de dados
- Corrigido contra ameaças enquanto estiver off-line e capaz de reter cópias iterativas para versões n atuais (com base nas necessidades dos negócios)
- Permite a visibilidade completa da integridade de todos os dados e metadados protegidos
- Aumenta a eficiência de prevenção/detecção da segurança cibernética quando executado em ambiente protegido
- O diagnóstico de vetores de ataque pode ocorrer em um ambiente de cofre isolado
- A lógica analítica monitora a integridade dos dados que são armazenados em backup e do catálogo de backup

Por que o PowerProtect Cyber Recovery é a melhor opção

Somente o PowerProtect Cyber Recovery combina várias camadas de proteção e segurança em uma solução turnkey para fornecer o máximo de proteção para dados essenciais.



CyberSense para detectar, diagnosticar e recuperar rapidamente de ataques cibernéticos

Totalmente integrado à Dell EMC PowerProtect Cyber Recovery, o CyberSense audita seus dados e detecta indicadores de comprometimento e ataques:

- Compreende proativamente quando um ataque está em andamento com mais de 99% de precisão
- Permite identificar e diagnosticar ameaças em potencial e recuperar dados "confiáveis" rapidamente
- Reduz o tempo de inatividade e as interrupções dos negócios para que você possa retomar operações normais com confiança

Quando um ataque passa por defesas em tempo real e corrompe arquivos ou bancos de dados, você tem a confiança de que os dados limpos são isolados no cofre do Cyber Recovery e foram analisados pelo CyberSense. O CyberSense está constantemente monitorando a integridade dos dados dentro do cofre e detecta exclusões em massa, criptografia e mais de 100 tipos de alterações em arquivos e bancos de dados que resultam de ataques comuns. Se o CyberSense detectar sinais de corrupção, um alerta é gerado, com o vetor de ataque e a listagem de arquivos afetados. Isso permite que as operações de negócios continuem com o mínimo ou nenhuma interrupção e rapidamente, em vez de em muitas semanas ou meses.

Lógica analítica

Aprendizado de máquina

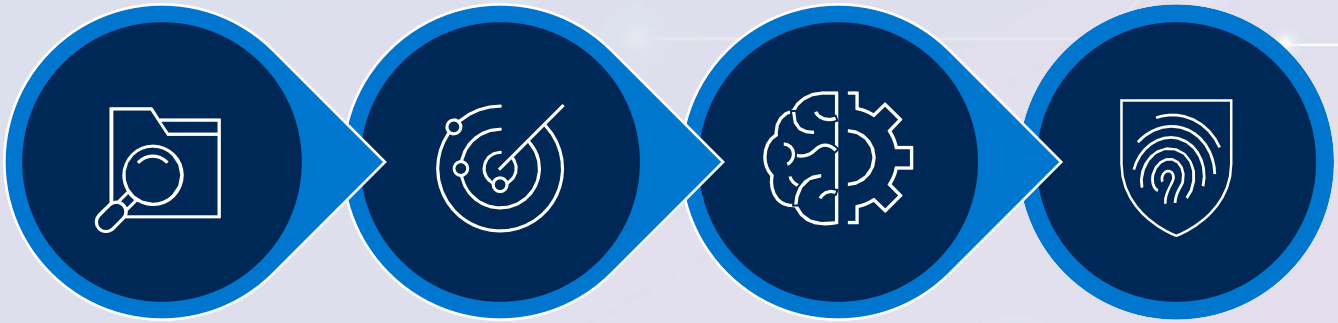
Ferramentas forenses

8 maneiras com as quais o CyberSense combate de maneira eficiente ataques ransomware e outros ataques cibernéticos

1. Detecta riscos de ataques cibernéticos que os concorrentes não podem identificar
2. Aprendizado de máquina e análise de nível de conteúdo total exclusiva
3. Fornece mais de 100 heurística para identificar atividades suspeitas
4. Integração profunda com o Cyber Recovery para automação e alertas de fluxo de trabalho
5. Ferramentas forenses após o ataque para determinar rapidamente o vetor de ataque e a lista de dados afetados
6. Identifica o último conjunto de dados bom conhecido para recuperação
7. Resiliência incomparável para recuperar e restaurar rapidamente dados de um ataque
8. Tudo isso realizado na segurança do cofre do Cyber Recovery

O CyberSense permite detecção precoce e recuperação garantida

O CyberSense realiza a indexação de conteúdo total de todos os dados que entram no cofre e gera estatísticas que são comparadas às verificações anteriores. A lógica analítica é, então, inserida no modelo de aprendizado de máquina, e os resultados são utilizados para determinar a integridade dos dados e se eles foram corrompidos. Além disso, o CyberSense fornece relatórios e detalhes para auxiliar no diagnóstico e recuperação do ataque e fornece o vetor de ataque utilizado para manipular os dados.



índice abrangente

Alterações no conteúdo ao longo do tempo

lógica analítica de segurança

+100 estatísticas indicativas de ataques cibernéticos

aprendizado de máquina

Treinado em milhares de troianos e mais de 20 vetores de ataque

Cyber Recovery com CyberSense

- Indexação de conteúdo completa
- Notificação de vetor de ataque
- Identificação de arquivo corrompido
- Alterações/exclusões de dados
- Contas de usuário violadas
- Arquivos executáveis violados
- Identificação da última cópia boa

Dell EMC PowerProtect Cyber Recovery na prática

"Os ataques cibernéticos estão amadurecendo a cada minuto, em todos os cantos do mundo. Para ter sucesso nesse ambiente, tivemos que mudar a forma como pensamos sobre os dados, como os utilizamos e protegemos. Queremos mantê-lo limpo e, em seguida, garantir que seja feito o backup. Depois, temos que testar essa proteção, confirmar se ela está em um bunker de dados, de modo que, no caso de qualquer plano de ataque de malware contra nós no futuro, tenhamos 100% de proteção da cópia de ouro e possamos retirá-la do cofre, da área protegida, e colocá-la de volta, para que as vidas das pessoas voltem ao normal, e elas não tenham uma disrupção da experiência."

bob bender
diretor de tecnologia,
cooperativa de crédito federal dos fundadores
Leia mais

Caso de uso: Sheltered Harbor

Preservar a confiança pública no caso de um evento devastador, como um ataque cibernético, causa falhas nos sistemas essenciais de uma instituição

Estudo de caso: área da saúde

Protege os dados confidenciais essenciais e as operações de negócios

Estudo de caso: serviços financeiros

Protege a plataforma de negociação de títulos e os dados essenciais

Serviços de consultoria de recuperação cibernética experientes e comprovados

Com uma equipe de consultores que traz uma experiência aprofundada no projeto e na implementação de soluções Cyber Recovery, bem como décadas de recuperação de desastres e conhecimento de negócios, a Dell pode ajudar sua empresa a operacionalizar um cofre do Cyber Recovery. Isso pode incluir a identificação de requisitos do cofre, conjuntos de dados, aplicativos, sequenciamento de carga de trabalho e muito mais para o cofre.

Entrega básica do Cyber Recovery

Instale e inicialize rapidamente a operação do cofre de recuperação cibernética

Implementação avançada do Cyber Recovery

Fornece uma capacidade limitada de oferecer algumas opções, gera uma amostra de runbook e trabalha com alguns softwares de terceiros

Consultores do Cyber Recovery

Os serviços de consultoria do Cyber Recovery fornecem níveis variados de opções estratégicas, arquiteturas de destino e até mesmo um roteiro acionável para adoção do Cyber Recovery

Cyber Recovery personalizado

Os serviços personalizados do Cyber Recovery implementam opções avançadas, planos de recuperação personalizados, runbooks adicionais e muito mais

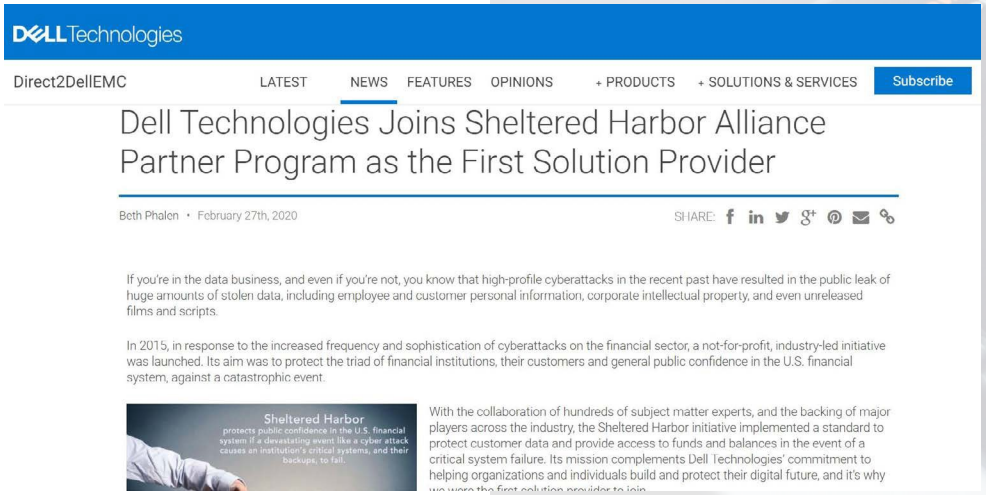
Proteção e preservação dos dados do cliente Confiança pública nos mercados financeiros dos Estados Unidos

Líder no modo de preparação do Sheltered Harbor

O Sheltered Harbor foi criado para proteger os clientes, as instituições financeiras e a confiança pública no sistema financeiro se um evento catastrófico como um ataque cibernético que causa falhas em sistemas essenciais, incluindo backups. Com a implementação do Sheltered Harbor padrão, as instituições podem estar preparadas para fornecer aos clientes acesso em tempo hábil a saldos e fundos nesses piores cenários.

A Dell Technologies é o primeiro Solution Provider no Sheltered Harbor Alliance Programa de parceria e prevê o endosso da solução dele em junho de 2020.

saiba mais


DELL Technologies

Direct2DellEMC LATEST NEWS FEATURES OPINIONS + PRODUCTS + SOLUTIONS & SERVICES Subscribe

Dell Technologies Joins Sheltered Harbor Alliance Partner Program as the First Solution Provider

Beth Phalen • February 27th, 2020 SHARE:

If you're in the data business, and even if you're not, you know that high-profile cyberattacks in the recent past have resulted in the public leak of huge amounts of stolen data, including employee and customer personal information, corporate intellectual property, and even unreleased films and scripts.

In 2015, in response to the increased frequency and sophistication of cyberattacks on the financial sector, a not-for-profit, industry-led initiative was launched. Its aim was to protect the triad of financial institutions, their customers and general public confidence in the U.S. financial system, against a catastrophic event.

With the collaboration of hundreds of subject matter experts, and the backing of major players across the industry, the Sheltered Harbor initiative implemented a standard to protect customer data and provide access to funds and balances in the event of a critical system failure. Its mission complements Dell Technologies' commitment to helping organizations and individuals build and protect their digital future, and it's why

SHELTERED HARBOR

Elementos essenciais do Sheltered Harbor

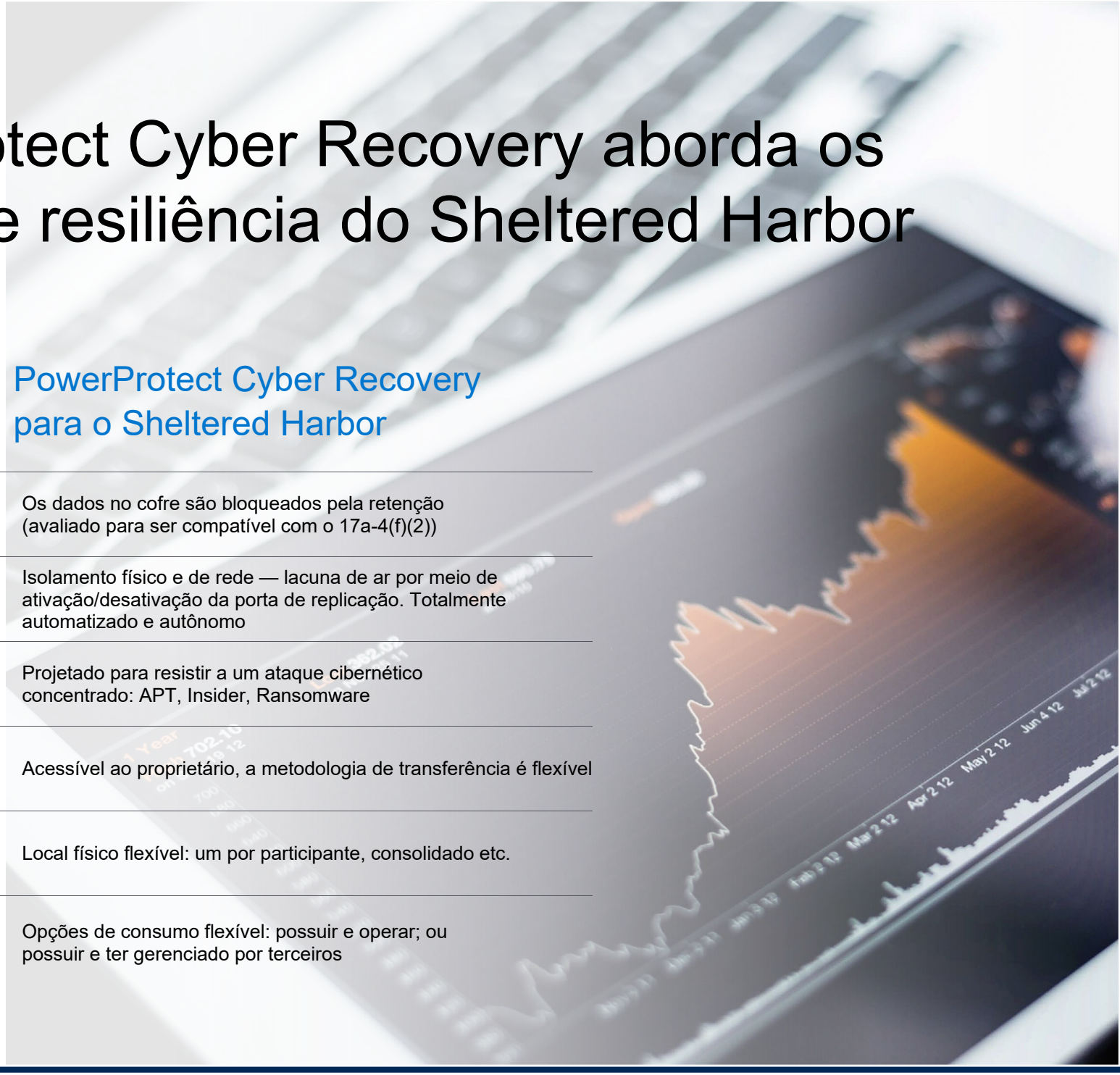
Armazenamento em cofre de dados

Planejamento de resiliência

Certificação

O PowerProtect Cyber Recovery aborda os requisitos de resiliência do Sheltered Harbor

SHELTERED HARBOR COFRE DE DADOS	PowerProtect Cyber Recovery para o Sheltered Harbor
Imutável	Os dados no cofre são bloqueados pela retenção (avaliado para ser compatível com o 17a-4(f)(2))
Separado	Isolamento físico e de rede — lacuna de ar por meio de ativação/desativação da porta de replicação. Totalmente automatizado e autônomo
Sobrevivência	Projetado para resistir a um ataque cibernético concentrado: APT, Insider, Ransomware
Acessível	Acessível ao proprietário, a metodologia de transferência é flexível
Descentralizado	Local físico flexível: um por participante, consolidado etc.
Propriedade do participante	Opções de consumo flexível: possuir e operar; ou possuir e ter gerenciado por terceiros



Setor da área da saúde

Protege os dados confidenciais essenciais e as operações de negócios

Desafios

- Direcionamento das instituições da área da saúde, impacto de grandes ataques
- Restrições de orçamento
- Pressões regulamentares

PowerProtect Cyber Recovery

- Implementação rápida de cofre e lacuna de ar operacional de turnkey
- CyberSense para análise/alertas de ameaças cibernéticas ativas

Resultados

- "Ninguém mais tem uma lacuna de ar como a Dell Technologies"
- Preparado para resposta com o mínimo de investimento em comparação ao risco de incidente catastrófico de US$10 milhões

Serviços financeiros

Proteja a plataforma de negociação de títulos e os dados essenciais

Desafios

- Risco de interrupção de US$10 milhões/dia
- Conselho preocupado com a conformidade com as normas do FFIEC e da Federal Reserve

PowerProtect Cyber Recovery

- Processo automatizado e orquestrado para minimizar impactos operacionais
- Runbooks de recuperação para todos os ambientes de armazenamento e backup

Resultados

- Mandato do Conselho de reunião para recuperação eficiente e confiável da destruição cibernética
- Forneceu um ambiente fundamental para proteger aplicativos adicionais ao longo do tempo

Comece agora! Sua checklist para construir a resiliência cibernética

Dê o próximo passo

Autenticação, identidade e segurança

- Active Directory/LDAP
- Dumps DNS
- Certificados
- Registros de eventos (incluindo dados de SIEM)

Sistema de rede

- Configuração de switch/roteador
- Configurações de firewall/balanceamento de carga
- Design de serviços IP
- Configuração de controle de acesso
- Firmware/microcódigo/patches

Armazenamento

- Configuração de hardware de backup
- Configurações de SAN/array
- Configurações de abstração de armazenamento
- Firmware/microcódigo/patches

Documentação

- Runbooks e checklists de CMDB, Cyber Recovery e D/R de ativos
- Extração do gerenciamento
- Listas de contatos e recursos de HR

Ferramentas de host e criação

- Compilações de plataformas físicas/virtuais
- Ferramentas de operações de desenvolvimento e scripts de automação
- Firmware/microcódigo/patches
- Software do fornecedor
  - > Binários (imagens douradas)
  - > Configurações e ajustes

Propriedade intelectual

- Código-fonte
- Algoritmos patenteados
- Bibliotecas de desenvolvedores

A proteção da sua empresa começa com a proteção dos seus dados.

Saiba mais em www.DellTechnologies.com/CyberRecovery