Aumente a resiliência cibernética e proteja os dados contra ameaças de ransomware cibernético usando um cofre isolado, software de lógica analítica por ML com base em IA e muito mais

Com o Dell Technologies PowerProtect Cyber Recovery with CyberSense

À medida que a frequência das ameaças cibernéticas vai crescendo continuamente e que os métodos de ataque vão evoluindo, os planos de proteção de dados devem adotar uma abordagem que proteja e analise todos os componentes de TI, desde o mais superficial até os elementos mais profundos. O Dell PowerProtect Cyber Recovery pode ajudar a proteger os dados mais essenciais e confidenciais e, ao mesmo tempo, ajudar a garantir a recuperação adequada diante de um ataque cibernético ou de outro evento que cause transtornos.

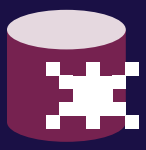
Dell PowerProtect Cyber Recovery é uma solução de gerenciamento, proteção e recuperação de dados que ajuda as organizações a proteger dados e aplicativos contra ransomware, ataques cibernéticos destrutivos e eventos inesperados. A solução usa uma abordagem de várias cópias; isso significa que, após a criação de backups, ela os copia em um armazenamento isolado para fins de proteção e análise. O PowerProtect Cyber Recovery é composto por vários componentes, inclusive um ou mais cofres de armazenamento, estabelecidos no local em um equipamento PowerProtect DD (anteriormente, conhecido como Data Domain) ou na nuvem por meio do Dell APEX Protection Storage for Public Cloud definido por software (anteriormente, conhecido como DD Virtual Edition). Em ambos os casos, o cofre conta com air gap operacional, ou seja, é isolado do ambiente de produção — e, possivelmente, conta com air gap físico no caso do ambiente local e com air gap lógico no caso do ambiente APEX. Isso torna extremamente difícil para os agentes mal-intencionados ou usuários não autorizados fazer log-in e comprometer as cópias de backup.

O PowerProtect Cyber Recovery também inclui o CyberSense, um mecanismo totalmente automatizado e integrado de lógica analítica de segurança inteligente que verifica dados, arquivos, bancos de dados e imagens no cofre automaticamente em busca de sinais de corrupção causados por um ataque de ransomware. O CyberSense oferece análise completa de conteúdo; usa as observações de arquivos como entradas para o modelo de aprendizado de máquina (ML) com base em inteligência artificial (AI); e detecta atividades mal-intencionadas, que incluem exclusões em massa, criptografia e outras alterações suspeitas na infraestrutura principal (inclusive do Active Directory e do DNS), nos arquivos de usuário e nos bancos de dados de produção essenciais que podem indicar ransomware ou um ataque destrutivo. Quando o CyberSense detecta padrões de corrupção, ele gera um alerta no painel de indicadores do PowerProtect Cyber Recovery que apresenta informações adicionais sobre a escala e o impacto do ataque.[1]

O PowerProtect Cyber Recovery ajuda as organizações a reduzir ataques cibernéticos, aumentar a resiliência dos dados com várias cópias de backups de dados provenientes de locais separados, diminuir o tempo de inatividade e manter a continuidade dos negócios. Este relatório usa dados publicamente disponíveis para destacar os principais recursos e funcionalidades de proteção de dados e apresenta as conclusões que tiramos após uma análise competitiva do CyberSense.

Proteja dados confidenciais

Criptografe dados em trânsito imutáveis durante a replicação de backup em cofres isolados física e logicamente



Detecte corrupção de páginas do SQL Server

O CyberSense encontrou uma infecção em que uma solução concorrente não conseguiu

Identificar cópias de backup não corrompidas

O CyberSense identificou a cópia de backup não infectada mais recente para recuperação

Segurança

O Dell PowerProtect Cyber Recovery oferece vários recursos de segurança para proteger dados essenciais contra ransomware e outras ameaças sofisticadas, impedir que usuários não autorizados obtenham acesso a informações confidenciais e acelerar a recuperação para que as organizações possam retomar as operações normais.

Os recursos e as funcionalidades dos equipamentos PowerProtect DD são essenciais para a segurança, a integridade e a recuperação que as soluções PowerProtect Cyber Recovery proporcionam. Eles incluem:

1. **Imutabilidade**
   Não é possível modificar nem excluir dados imutáveis; somente é possível gravá-los. Os sistemas DD podem gravar backups imutáveis nos sistemas de produção e no Cyber Vault. Isso significa que, se um agente mal-intencionado tiver algum tipo de acesso ao sistema de backup, ele não poderá modificar, excluir nem comprometer as cópias protegidas existentes.[2] Qualquer backup que o sistema DD criar no ambiente de produção é imediatamente imutável e disponível para que a TI o copie no cofre, a fim de oferecer maior segurança. A próxima seção deste relatório analisa a imutabilidade mais a fundo.

2. **Retention Lock**
   O recurso DD Retention Lock torna os dados imutáveis por um período predeterminado. Quando a solução coloca os dados sob um bloqueio de retenção, os usuários ou sistemas somente podem alterar, excluir ou modificar os dados quando o período de bloqueio expira.[3]

   O Retention Lock tem modos de governança e conformidade. O modo de conformidade pode permitir que os clientes atendam a muitos padrões normativos. Um terceiro independente certificou que o DD Retention Lock atende aos requisitos de armazenamento especificados nas Regras 17a-4(f)(2) e 240.18a-6(e)(2) da SEC e na Regra 4511(c) da FINRA.[4] Esse recurso também ajuda a apoiar os esforços de uma organização para cumprir as normas 21 CFR Part11 da FDA, a lei Sarbanes-Oxley Act, a norma IRS 98025 e 97-22, a norma ISO 15489-1 e o padrão MoREQ2010.[5]

   Como os invasores podem tentar contornar o Retention Lock alterando o relógio de um sistema, o que faria com que a solução excluísse arquivos antes do esperado, o DD tem um relógio de segurança interno. O sistema compara regularmente os horários dos relógios de segurança e do sistema. Se houver um desvio acumulado de duas semanas entre os dois em um só ano civil, o sistema desativará automaticamente o DD File System (DDFS) para impedir o acesso aos dados.[6]

3. **Criptografia de dados em trânsito com o DDBoost**
   Os dados em trânsito podem representar um risco significativo de segurança. O DDBoost limita a quantidade de dados em trânsito, permitindo que o servidor de backup ou o cliente de aplicativo envie apenas segmentos de dados exclusivos, e não todos os dados, pela rede para o equipamento DD. Além disso, as organizações podem usar o protocolo DDBoost com ou sem certificados para autenticação e criptografia de dados. Os certificados oferecem uma capacidade mais segura de transmissão de dados. A criptografia em trânsito permite que os aplicativos façam a criptografia de dados de backup ou restauração em trânsito do sistema pela LAN. O cliente pode usar Transport Layer Services (TLS) para criptografar a sessão entre o client e o sistema.[7]

4. **Segurança do DD Operating System (DD OS)**
   Os recursos de segurança do DD também se estendem ao sistema operacional. O DD OS implementa controles de acesso e restrições personalizados no shell Bash para fins de segurança. O modo shell Bash restrito permite que os usuários realizem apenas um conjunto de comandos predefinidos necessários para suas funções e tarefas. O DD OS melhora a integridade dos dados bloqueando comandos indefinidos que fazem modificações não autorizadas ou não intencionais no sistema.[8]

5. **Segurança do controle de acesso baseado em funções (RBAC) e do DD Filesystem (DDFS)**
   Os sistemas DD usam várias medidas para proteger arquivos e dados do file system. Primeiramente, os sistemas DD oferecem o RBAC, que permite que os administradores definam funções com privilégios específicos e atribuam usuários a essas funções. Somente usuários autorizados com privilégios apropriados podem acessar o equipamento e os dados que ele contém. Isso garante que os usuários tenham acesso apenas às funções e aos dados de que precisam para realizar suas tarefas, o que reduz o risco de acesso não autorizado ou de exposição acidental desses usuários aos dados.

   O DDFS também usa hash para verificação da integridade dos dados. O hash transforma determinada chave ou cadeia de caracteres em outro valor. O equipamento armazena fragmentos de dados exclusivos em contêineres de armazenamento lógico, e o file system realiza o hash dos fragmentos de dados e dos contêineres. Quando o sistema recupera dados, ele recalcula o valor de hash dos dados para corresponder ao valor de hash armazenado no DDFS, o que ajuda a garantir que não haja adulterações nem corrupções dos dados.[9]

6. **Autorização de função dupla**
   Quando uma organização ativa o modo de conformidade do DD Retention Lock, o sistema DD oferece segurança administrativa adicional na forma de log-in duplo. Isso significa que tanto o administrador do sistema quanto um segundo usuário autorizado (por exemplo, o diretor de segurança) devem fazer log-in juntos. O mecanismo de log-in duplo do modo de conformidade do DD Retention Lock funciona como uma proteção contra quaisquer ações que possam comprometer a integridade dos arquivos bloqueados antes da expiração do período de retenção.[10]

7. **Arquitetura de Invulnerabilidade de Dados**
   O DD OS proporciona verificação completa, prevenção e contenção de falhas, detecção e correção contínuas de falhas e capacidade de recuperação do file system para oferecer proteção contra problemas de integridade de dados causados por falhas de hardware e software. Quando o sistema DD recebe solicitações de gravação do software de backup, primeiramente, ele analisa um segmento de dados em termos de redundância, calculando a impressão digital do segmento de dados e a comparando com as impressões digitais existentes armazenadas no sistema. Ele armazena apenas segmentos de dados exclusivos e suas impressões digitais no disco. Em seguida, o DD lê continuamente os dados do disco, recalcula a impressão digital que lê e garante que ela corresponda à impressão digital existente no disco. O sistema DD conduz um processo de autocorreção para reconstruir dados corrompidos e restaurar os dados ao estado correto caso o sistema detecte corrupção durante esse processo (ou seja, se o que ele lê não corresponde ao que foi gravado). Além disso, o processo de autocorreção ajuda a proteger o sistema contra outras alterações que podem afetar a integridade da plataforma.

Imutabilidade*

Tornar os backups imutáveis e, portanto, somente leitura garante que uma organização possa confiar nesses backups para recuperação. Operacionalmente, a imutabilidade mantém a autenticidade e a confiabilidade dos dados.

*Os produtos Dell foram desenvolvidos para respaldar as iniciativas dos clientes para proteção de dados essenciais. Assim como acontece com qualquer produto eletrônico, os produtos de infraestrutura, proteção de dados e armazenamento podem apresentar vulnerabilidades de segurança. É importante que os clientes instalem atualizações de segurança assim que elas forem disponibilizadas pela Dell.

Como funciona

Os sistemas DD oferecem imutabilidade na forma como armazenam dados usando MTrees. MTrees são partições lógicas do file system. Quando um aplicativo grava dados em uma MTree, o sistema DD usa um recurso chamado Fast Copy para criar uma cópia point-in-time da MTree original em uma nova MTree. Na nova MTree, o DD aplica o Retention Lock para garantir que um usuário ou um processo não possa excluir a nova MTree por toda a duração definida pelo período de retenção. A nova MTree é uma cópia imutável dos dados e é independente da MTree original.[11]

As soluções PowerProtect Cyber Recovery também usam a replicação de MTrees para duplicar cópias de dados imutáveis de um DD de produção em outro DD no cofre por meio do protocolo DDBoost.[12] Na sincronização inicial entre os dois DDS, a solução copia todos os dados no DD do cofre. Todas as sincronizações subsequentes copiarão apenas segmentos de dados novos e alterados. O CyberSense, que nós discutiremos mais adiante neste relatório, verifica se há possíveis corrupções em todas as cópias imutáveis do cofre.

Abordagens de imutabilidade

A necessidade de excluir backups imutáveis é rara, mas acontece. As organizações podem acabar enfrentando problemas de capacidade e custos subsequentes depois de acumular backups imutáveis que não podem excluir. O armazenamento de backups pode exigir uma grande quantidade de capacidade. Por sua vez, isso requer custos contínuos de operação, gerenciamento e monitoramento, além do investimento inicial em hardware. A exclusão periódica de backups imutáveis pode ajudar a resolver esses problemas.

Como nós observamos, o Dell PowerProtect Cyber Recovery oferece imutabilidade utilizando o Retention Lock e outras ferramentas. O Retention Lock proporciona certa flexibilidade, já que os modos Compliance e Governance oferecem pequenas modificações na forma como os clientes podem implementar a imutabilidade. Imutabilidade significa que os usuários ou agentes mal-intencionados não podem excluir backups; mas, em certos casos, como problemas de capacidade de armazenamento, o PowerProtect Cyber Recovery permite que os clientes os excluam com o Retention Lock – modo Governance.

Em comparação com o PowerProtect Cyber Recovery, como se saem as ofertas semelhantes de outras empresas? Nós analisamos as informações disponíveis ao público do Cohesity Cyber Recovery, Veeam, Rubrik e Veritas NetBackup. Com exceção do Cohesity Cyber Recovery, as soluções podem residir no local ou externamente (Cohesity é uma solução em nuvem respaldada pela AWS). A documentação das quatro soluções alega oferecer imutabilidade; mas, notavelmente, Rubrik e NetBackup têm algumas diferenças em relação ao PowerProtect Cyber Recovery.

No Rubrik, os administradores podem excluir backups, mas não no lado do client e somente com determinados controles em vigor. Além disso, todas as gravações são "externas", o que significa que as novas gravações nunca têm contato com dados gravados anteriormente.[13]

Apesar de oferecer imutabilidade, os administradores ou agentes mal-intencionados podem excluir o bloqueio de backups em um armazenamento compatível com NetBackup WORM. Em seguida, eles podem excluir a imagem usando o comando bpexpdate.[14]

Isolamento

Isolamento de dados se refere à separação dos dados e ao acesso restrito a eles e é criado por barreiras ou limites para impedir o acesso não autorizado. O isolamento usa conexões temporárias de rede em vez de conexões persistentes.

O isolamento de dados ajuda os dados essenciais a permanecerem desconectados de uma rede infectada, em que um agente mal-intencionado pode tentar modificar configurações, excluir dados, alterar políticas ou interceptar o tráfego de rede para obter credenciais de usuário. Ele também reduz a superfície de ataque, diminuindo as oportunidades de os agentes mal-intencionados obterem acesso e controle. Além disso, as organizações podem restringir o acesso somente a pessoas autorizadas, o que impede que usuários não autorizados substituam dados.

Além dos recursos que nós observamos, o PowerProtect Cyber Recovery pode proporcionar isolamento físico e lógico, na forma de air gaps operacionais, a fim de proteger os dados. O PowerProtect Cyber Recovery pode usar um air gap físico, em que os dados de backup são fisicamente desconectados da rede de produção e armazenados em um local isolado, e um air gap lógico, que depende de controles de acesso à rede para separar as cópias de backup logicamente desconectadas do ambiente de produção. Ter ambos os tipos de air gaps é uma estratégia valiosa, já que um air gap por si só não pode impedir que um usuário interno com acesso de rede ao cofre acesse e comprometa os dados.

Um PowerProtect DD fisicamente isolado no local pode funcionar como o cofre, cujos componentes os usuários ou os sistemas do ambiente de produção não podem acessar e que é fisicamente desconectado da rede de produção.[15] Ao eliminar o acesso ao ambiente de recuperação a partir da rede de produção, uma organização pode reduzir a superfície de ataque. Conforme observado, o acesso aos dados isolados requer credenciais de segurança separadas, bem como autenticação baseada em vários fatores (MFA).[16]

Abordagens de isolamento

A Gartner afirma que "ambientes isolados de recuperação (IREs) com cofres de dados imutáveis (IDVs) oferecem o mais alto nível de segurança e recuperação contra ameaças internas, ransomware e outras formas de invasão".[17] Ela também observa que um "IRE com um IDV não substitui, mas complementa, os sistemas tradicionais de backup e recuperação de desastres (DR) entregando uma cópia de backup terciária imutável em um IRE equipado com todas as ferramentas, processos e recursos para recuperar os sistemas afetados".[18]

Ao analisar as informações disponíveis publicamente sobre as soluções Cohesity, Veeam, Rubrik e Veritas, nós descobrimos que cada uma tem pelo menos uma abordagem ligeiramente diferente de IRE em relação ao PowerProtect Cyber Recovery. Com a solução da Dell, os clientes podem isolar fisicamente ou logicamente os cofres do DD da produção para manter os planos de dados e de controle separados dos cofres. Além disso, o PowerProtect Cyber Recovery automatiza os air gaps, algo que nem todas as outras soluções fazem.

De acordo com a documentação:

- O Cohesity Cyber Recovery oferece apenas um air gap lógico automatizado e dinâmico para seu cofre FortKnox baseado em AWS.[19]
- A Veeam oferece suporte a um air gap lógico para provedores de nuvem pública e privada por meio do Veeam Cloud Connect, mas ele não é automatizado. A Veeam também oferece o Veeam Hardened Repository, que funciona como o cofre local da solução e que as organizações podem configurar para ter um air gap físico.[20]
- O Rubrik não oferece um air gap automatizado para o Rubrik Cloud Vault, mas os clientes podem adicionar um air gap lógico por meio de uma parceria com a Microsoft.[21]
- Os clientes da NetBackup devem ativar manualmente um air gap lógico e podem criar um air gap físico com uma solução externa.[22]

Como funciona

A Figura 1 mostra os caminhos de rede do cofre isolado do Cyber Recovery. Observe que o cofre não tem um caminho de gerenciamento ou controle ao ambiente de produção para reduzir o plano de ataque.

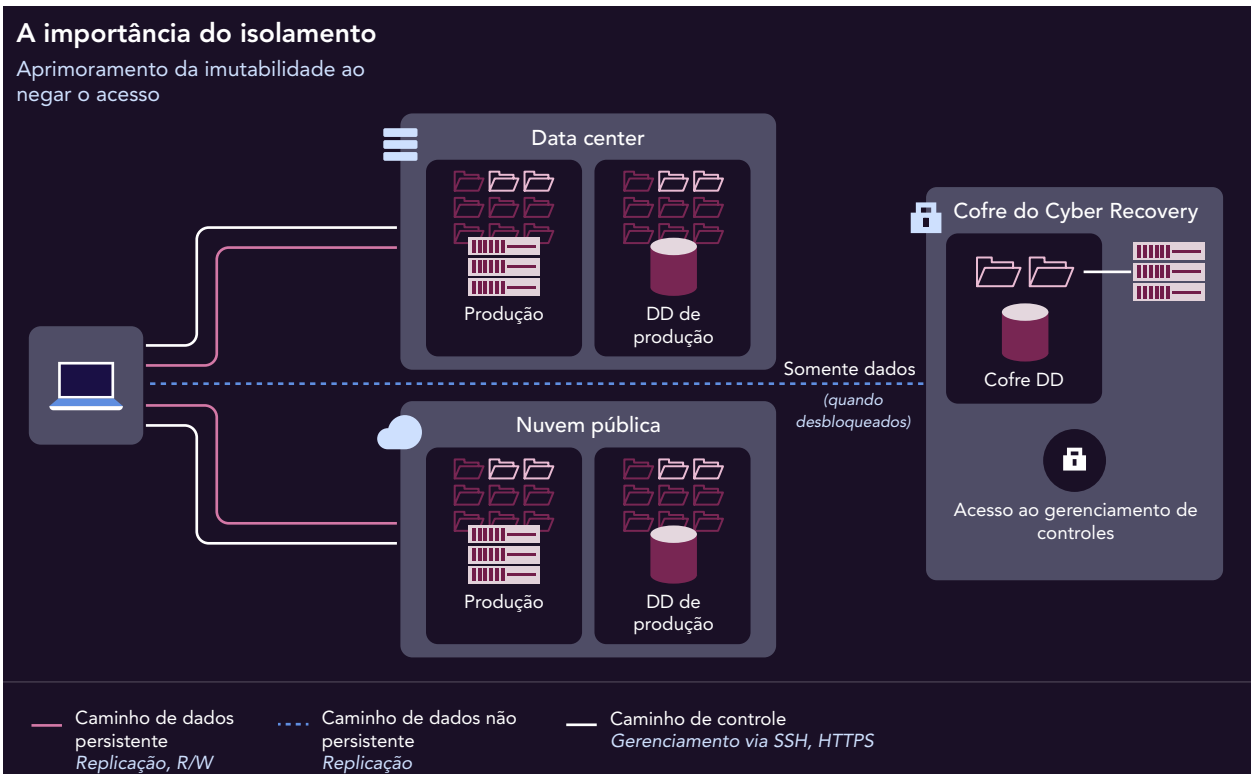


Figura 1: Dados de alto nível e arquitetura do caminho de controle do cofre do Cyber Recovery. Fonte: Principled Technologies.

A única conexão necessária do cofre do Cyber Recovery é um caminho de dados para a sincronização periódica de dados. A sincronização ocorre quando a solução Cyber Recovery inclui dados em intervalos curtos e orientados por políticas para fins de replicação.[23] O Guia da solução PowerProtect Cyber Recovery afirma que "a arquitetura básica da solução Cyber Recovery consiste em um par de sistemas PowerProtect DD e no host de gerenciamento do Cyber Recovery. Nessa configuração de nível básico, o software Cyber Recovery, que é executado no host de gerenciamento, ativa e desativa a interface Ethernet de replicação juntamente com contextos de replicação do sistema PowerProtect DD no cofre do Cyber Recovery para controlar o fluxo de dados do ambiente de produção ao ambiente do cofre".[24] A Dell sugere maneiras adicionais de as organizações protegerem e isolarem caminhos de dados. Em nossos testes, observamos que o Cyber Recovery desbloqueou e bloqueou o cofre durante e após a replicação.

Para a implementação física do cofre, a Dell recomenda "instalar o equipamento de cofre do Cyber Recovery em uma sala ou compartimento dedicado com controles de acesso físico. Essa sala protegida deve ter uma lista de acesso limitado com revogação de chave ou acesso por duas chaves. Também deve estar em vigor a videovigilância do equipamento e dos pontos de entrada ao compartimento ou à sala. Para obter segurança máxima, o software Cyber Recovery deve ser acessível apenas por acesso físico ao servidor de gerenciamento do Cyber Recovery e a um teclado e mouse associados".[25]

Com a separação dos caminhos de gerenciamento e controle, as opções de isolamento por air gap físico e lógico do Cyber Recovery o diferenciam das outras soluções. Algumas soluções permitem o acesso aos dados do cofre a partir de uma interface do ambiente de produção. Isso coloca os dados do cofre na mesma superfície de ataque que os dados de produção, o que pode permitir que agentes mal-intencionados acessem cópias de backup usando credenciais comprometidas.

CyberSense

A proteção eficaz dos dados requer uma estratégia abrangente que ofereça segurança em todos os níveis. Apesar de todos os recursos de autocorreção, segurança, imutabilidade e isolamento de uma solução Dell PowerProtect Cyber Recovery, ataques menos óbvios ainda podem se aprofundar em uma infraestrutura empresarial, como o nível de backup de dados, e eles podem acabar sendo detectados apenas depois do comprometimento dos dados de produção ou de um grupo inteiro de usuários. As soluções Dell PowerProtect Cyber Recovery oferecem uma última linha de defesa contra ataques cibernéticos e uma abordagem eficiente para acelerar a recuperação por meio do CyberSense. CyberSense é um mecanismo de lógica analítica que usa algoritmos de análise de ML baseados em IA para verificar e validar a integridade dos backups no cofre e o conteúdo de usuário nos arquivos dentro dos backups.

O CyberSense é executado dentro do cofre, isolado do ambiente de produção. Ele monitora arquivos, imagens de VM e bancos de dados do cofre, analisando a integridade dos dados para determinar se ocorreu um ataque cibernético. Quando a solução Cyber Recovery replica cópias de backup no cofre e aplica o recurso Retention Lock, o CyberSense verifica as cópias automaticamente, criando observações point-in-time dos arquivos, dos bancos de dados e da infraestrutura principal. O mecanismo de lógica analítica verifica o conteúdo completo dos arquivos e de cada página do banco de dados, não apenas os metadados. Enquanto outras soluções procuram por alterações nos metadados ou nos limites dos dados, o CyberSense verifica o conteúdo dos arquivos para validar a integridade dos dados. Com essas observações, o CyberSense consegue rastrear como os arquivos e bancos de dados mudam com o tempo e revelar muitos tipos avançados de ataques ocultos. Em seguida, o CyberSense gera uma lógica analítica que detecta padrões de corrupção que podem indicar atividades de agentes mal-intencionados, inclusive criptografia; exclusão, criação ou ofuscação de arquivos; e muito mais.[26] As outras soluções transferem a lógica analítica para a nuvem, o que possivelmente amplia a superfície de ataque, enquanto as organizações podem optar por executar o CyberSense no local ou em uma das muitas opções de nuvem compatíveis com o Cyber Recovery.

O CyberSense combina mais de 200 análises com observações de dados que se tornam mais úteis ao longo do tempo, à medida que as observações vão aumentando. O algoritmo de ML usa informações sobre milhares de infecções por malware para encontrar padrões incomuns de comportamento e distinguir entre atividades dos usuários e ransomware, ao mesmo tempo em que minimiza falsos positivos e negativos. Por meio de pesquisa contínua, o algoritmo recebe novas instruções sobre aspectos como variantes de ataque. Além disso, o algoritmo de ML recebe atualizações com base em dados reais de clientes existentes do CyberSense.[27]

Além disso, o CyberSense oferece suporte à indexação de dados em formatos comuns de backup em disco da Dell, IBM, CommVault e Veritas.[28] Ao oferecer suporte a formatos de backup de outros fornecedores, a Dell demonstra disposição para atender às diferentes realidades dos clientes no que se refere a backups de dados.

Nós testamos o software de lógica analítica inteligente orientada por ML de duas soluções prontas para uso de recuperação cibernética e proteção de dados empresariais: CyberSense for Dell PowerProtect Cyber Recovery em um Dell PowerStore™ 7000T e uma ferramenta da plataforma de gerenciamento de dados de um concorrente ("Fornecedor X"), com funcionamento parecido, em um equipamento de porte semelhante.

Como realizamos os testes

Nós executamos todos os testes remotamente e tivemos controle total e acesso irrestrito aos ambientes de teste. Tanto a solução Dell (inclusive CyberSense, o aplicativo de backup PowerProtect Data Manager, o APEX Protection Storage (anteriormente conhecido como DD Virtual Edition) e a solução PowerProtect Cyber Recovery) quanto a solução do Fornecedor X estavam localizadas em um laboratório de data center externo.

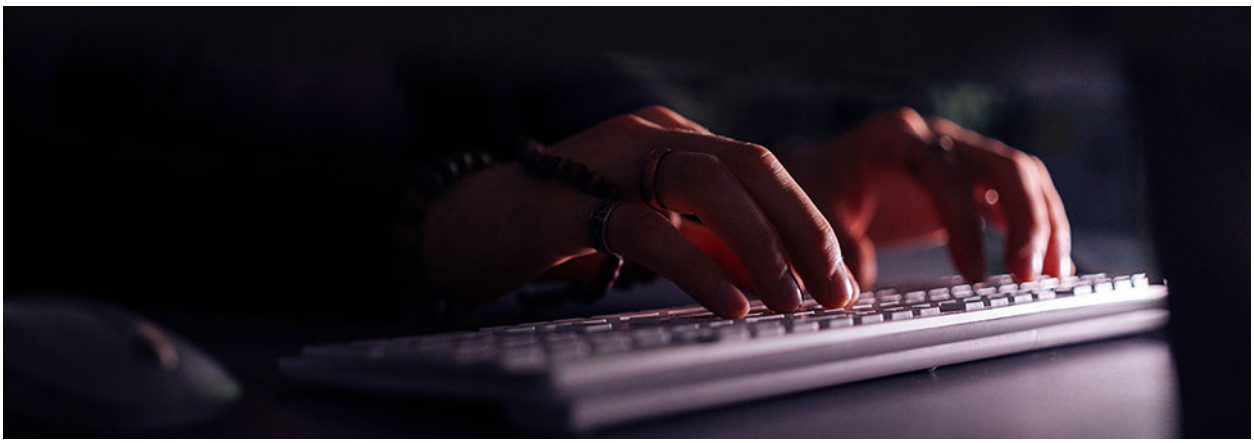
Em ambas as soluções, nós executamos três cenários de eventos mal-intencionados baseados em script que tinham como alvo os backups:

Figura 2: Nossos cenários de teste. Fonte: Principled Technologies.

Para ambas as soluções, os dois primeiros cenários seguiram o mesmo procedimento geral. Primeiro, nós criamos um backup completo de todas as VMs limpas nos equipamentos Dell PowerProtect Data Manager e do Fornecedor X, criamos backups incrementais para verificação e confirmamos que a solução de destino não detectou uma ameaça. Isso nos deu um conjunto de backups de linha de base no qual poderíamos executar os scripts de ataque.

Em seguida, executamos o script de simulação de ransomware em quatro VMs com diferentes sistemas operacionais e tipos de aplicativos, fizemos novos backups incrementais no equipamento de destino e verificamos se o software de lógica analítica de destino detectou a ameaça de criptografia.

Para o terceiro cenário (infectar uma página do SQL Server), nós seguimos um procedimento semelhante ao dos outros dois cenários, mas nos concentramos em VMs SQL e usamos um script de corrupção de página, em vez de um script de criptografia. Nós executamos o script em uma só VM.



O que descobrimos

Cenário 1: detectar arquivos criptografados com nomes de arquivo ofuscados

Esse cenário simulou um evento mal-intencionado que criptografou arquivos e ofuscou seus nomes, o que alterou os metadados do arquivo e o conteúdo deles. Esse tipo de ataque é normalmente conhecido como ransomware, um evento de segurança em que softwares mal-intencionados bloqueiam o acesso a um sistema de computador até que o proprietário ou usuário do sistema pague uma quantia previamente determinada. De acordo com a Cybersecurity and Infrastructure Security Agency (CISA) dos EUA, "os impactos econômicos e reputacionais do ransomware e da extorsão de dados provaram ser desafiadores e dispendiosos para organizações de todos os portes durante a interrupção inicial e, às vezes, a recuperação estendida".[29] O uso de um software de lógica analítica inteligente para detectar criptografia de backups pode fortalecer a estratégia de proteção de dados de qualquer organização, proteger informações confidenciais e valiosas e reduzir o potencial do dispendioso tempo de inatividade que os ataques cibernéticos causam.

Em nossos testes, ambos os aplicativos de lógica analítica inteligente detectaram os arquivos criptografados com nomes de arquivo alterados. A solução do Fornecedor X precisou de uma linha de base de 15 backups antes de detectar infecções (um backup completo e 14 backups incrementais), enquanto o CyberSense detectou infecções após apenas um backup completo, o que significa que a solução do Fornecedor X exigiu 14 backups adicionais em comparação com o CyberSense.

Quando a solução do Fornecedor X nos alertou sobre a atividade suspeita, ela apenas indicou que algo havia removido muitos arquivos e adicionado um número igual de arquivos, o que era uma atividade suspeita com base na classificação de entropia do backup.[30] A solução do Fornecedor X não indicou que os arquivos foram criptografados ou que os nomes dos arquivos foram alterados. Por outro lado, o Cyber Recovery with CyberSense nos alertou que algo tinha criptografado e ofuscado nomes de arquivo.

Os resultados do Fornecedor X poderiam indicar um falso positivo. Em outras palavras, se nós presumirmos que uma organização executa backups diários com a solução do Fornecedor X, ela poderia ter incluído 14 dias de arquivos infectados antes da deteção de anomalias. Por outro lado, o CyberSense precisou de apenas um backup de linha de base para alertar com inteligência sobre a infeção e os detalhes dela. A recuperação com o Cyber Recovery nessa fase de nosso exemplo ocorre a partir do cofre isolado, garantindo à organização que ele não expôs a rede de produção aos 14 backups infectados, como a solução do Fornecedor X.

Figura 3: O número de backups que cada solução exigiu para criar uma linha de base para detectar corrupção.
Fonte: Principled Technologies.

Cenário 2: detectar arquivos criptografados com nomes de arquivo originais

Esse cenário foi semelhante ao primeiro, mas o script manteve os nomes de arquivo originais dos arquivos criptografados. Essa alteração não afetou os metadados dos arquivos, apenas os próprios arquivos. Um ato como esse pode ser um ransomware bomba-relógio, no qual o ataque permanece inativo por um período antes da ativação. Esse tipo de ransomware pode escapar da detecção e ter como alvo os backups, tornando os backups infectados inúteis quando a organização precisar deles.[31] Sem alterações nos metadados, o arquivo pode parecer não estar infectado na superfície, o que ajuda a manter oculto o ataque inativo.

Em nossos testes, ambos os aplicativos de lógica analítica inteligente detectaram os arquivos criptografados. Novamente, a solução do Fornecedor X precisou de uma linha de base de 15 backups, incluindo 14 backups incrementais, antes de detectar uma anomalia. O CyberSense precisou de uma linha de base de apenas um backup completo antes de detectar uma anomalia.

Como no primeiro cenário, a solução do Fornecedor X apenas nos alertou que algo havia alterado muitos arquivos, o que era suspeito com base na classificação de entropia do backup. Ela não indicou que algo tinha criptografado os arquivos, enquanto o Cyber Recovery with CyberSense nos informou isso. A detecção de corrupção dessa maneira significa que o CyberSense está analisando o conteúdo dos arquivos, não apenas os metadados em nível de superfície. Esse tipo de verificação adiciona outra camada de segurança para seus backups e, portanto, sua infraestrutura digital ou seu patrimônio em geral. Pode-se sugerir que o CyberSense seja um "verdadeiro" aplicativo de lógica analítica inteligente. Além disso, as organizações podem detectar corrupção mais cedo com o CyberSense, pois a solução precisou de um número significativamente menor de backups para criar uma linha de base. Dependendo do agendamento de backups de uma organização, isso pode significar muitos dias antes.

Figura 4: O número de backups que cada solução exigiu para detectar corrupção. Fonte: Principled Technologies.

Cenário 3: detectar a corrupção da página do SQL Server

Esse cenário simulou um evento mal-intencionado que corrompe uma página do SQL Server. No SQL Server, a unidade fundamental do armazenamento de dados é a página, e o banco de dados lê ou grava páginas de dados inteiras.[32] Novamente, essa alteração não afetou os metadados, apenas os próprios arquivos. Esse tipo de ataque normalmente é conhecido como injeção de SQL, em que os invasores têm como alvo aplicativos baseados em dados SQL injetando código mal-intencionado em instruções SQL por meio de entradas em páginas da Web.[33] Mesmo infectados, os bancos de dados podem continuar em execução. Além do roubo de dados, a corrupção de páginas do SQL Server pode causar problemas de integridade de dados, perda de dados e interrupções na funcionalidade do banco de dados. Esses resultados podem prejudicar a reputação de uma organização, interromper os fluxos de trabalho operacionais, resultar em perda pecuniária e, até mesmo, incorrer em responsabilidades legais.

Embora as soluções CyberSense e do Fornecedor X tenham detectado a criptografia nos dois primeiros cenários, no terceiro cenário, somente o CyberSense conseguiu fazer uma verificação profunda o suficiente para detectar a corrupção na página do SQL Server. Isso mostra que, apesar de as duas soluções oferecerem capacidades semelhantes de detecção em alguns níveis, o CyberSense proporciona uma análise mais detalhada dos backups para aplicativos baseados em SQL Server, possivelmente essenciais para os negócios. Dessa forma, o CyberSense adiciona uma camada de resiliência de segurança com verificações mais profundas e proteção mais abrangente.

O SQL Server é usado em muitas aplicações dos setores financeiro, de varejo, de saúde e outros. Como o SQL Server pode atuar como o back-end da arquitetura de desenvolvimento, um ataque ao SQL Server pode resultar em tempo de inatividade, interromper operações e, possivelmente, ameaçar a receita gerada por esses aplicativos.

Restaurando e recuperando com o Dell PowerProtect Cyber Recovery

A estratégia de resiliência cibernética da Dell oferece uma ampla variedade de recursos de recuperação. Essas opções de recuperação incluem recursos comuns do setor, como recuperação tradicional ou com acesso instantâneo dos backups imutáveis mantidos na produção. Além disso, a Dell proporciona os recursos exclusivos de recuperação da solução PowerProtect Cyber Recovery. Como o PowerProtect Cyber Recovery mantém as cópias em isolamento e verifica a integridade delas com o CyberSense, as organizações podem acessar as cópias imediatamente após um ataque e usá-las para iniciar as etapas de recuperação ou fazer restaurações imediatas para plataformas alternativas de recuperação, como ambientes isolados seguros.

Compare esse caso de uso imediato em uma organização que só pode acessar dados em produção ou na nuvem pública. A organização só conseguirá acessar com segurança os dados armazenados na área comprometida depois de determinar e corrigir a causa raiz; encerrado a persistência do agente mal-intencionado; capturar imagens forenses para seguradoras e o departamento jurídico; verificar os dados novamente; e ter infraestrutura disponível suficiente (AD, DNS) para acessar a infraestrutura de backup. Esse processo pode levar dias ou semanas com base no escopo e na sofisticação do ataque.

Como funciona

Durante a produção normal, o PowerProtect Cyber Recovery cria pontos de restauração automaticamente para recuperação e lógica analítica de segurança. Em caso de um ataque cibernético, o Cyber Recovery usa procedimentos automatizados de restauração e recuperação e esses pontos de restauração para colocar on-line novamente os sistemas essenciais para os negócios. Os relatórios forenses e do CyberSense ajudam as equipes de recuperação e segurança cibernética a diagnosticar o impacto do ataque. Depois que o ambiente de produção está limpo e pronto para recuperação, o Cyber Recovery oferece as ferramentas e a tecnologia que realizam a verdadeira recuperação de dados.

Após um ataque cibernético, várias métricas de proteção de dados entram em ação para determinar a velocidade da recuperação (o tempo de recuperação cibernética, ou CRT) e o ponto no tempo ao qual os usuários podem retornar após um ataque destrutivo (o ponto de recuperação cibernética, ou CRP). Em uma solução Cyber Recovery, algumas dessas métricas são:

- **Objetivo de detecção de destruição (DDO):** é uma janela contínua com base no tempo entre um ataque e a detecção do ataque. Os mecanismos de lógica analítica e outros mecanismos do Cyber Recovery devem operar nesse período.
- **Objetivo de avaliação de destruição (DAO):** é o tempo alocado à equipe de segurança cibernética, após uma entrada não autorizada, para determinar o escopo dos danos e as possíveis respostas.
- **Intervalo de sincronização do Cyber Recovery:** é a frequência com que a solução Cyber Recovery copia dados do ambiente de produção para o cofre. O tempo se baseia em um Recovery Point Objective (RPO) estabelecido anteriormente para a solução. O período de retenção de cópias varia de acordo com a solução, mas normalmente varia de uma semana a um mês.
- **Contagem de cópias de dados do Cyber Recovery:** é o número de cópias de dados mantidas no cofre do Cyber Recovery. Quando alinhada com o intervalo de sincronização, essa métrica apresenta uma medida aproximada para o período cujos dados uma organização pode recuperar, por exemplo, 7 cópias associadas a um intervalo de 24 horas permitem que os usuários recuperem dados com até uma semana de idade.

Além dos requisitos de recuperação, o tipo de dados que a solução protege pode ajudar a determinar o intervalo de sincronização e o tempo de retenção de dados. De acordo com o Guia da solução Cyber Recovery, para obter a maior flexibilidade de recuperação, os usuários podem categorizar os dados que a solução protege em um dos seguintes fluxos de backup:[34]

- Backups de binários e executáveis, inclusive compilações de aplicativos e distribuições de nível básico do sistema operacional
- Backups completos de aplicativos e file systems, inclusive imagens e dados específicos de aplicativos

Esses fluxos separados de backup levam a duas estratégias de recuperação diferentes:

1. **Restauração de dados e binários de aplicativos no cofre do Cyber Recovery:**
   A solução identifica pontos de restauração utilizáveis, além do malware e locais de persistência dele, e decide se deve limpar o malware da imagem de backup ou recriá-la usando cópias do cofre do Cyber Recovery. Depois de aplicar patches de segurança, a solução restaura os dados para um host de recuperação usando o runbook de DR do aplicativo e, em seguida, determina se o processo de recuperação eliminou os efeitos do malware. Em seguida, ela realiza uma execução de teste no aplicativo usando a computação do cofre e limpa ou recria a imagem do ambiente de produção. Por fim, o Cyber Recovery conecta o host de recuperação à produção e copia o aplicativo e os dados de volta para o ambiente de produção. A Figura 5 ilustra esse processo.

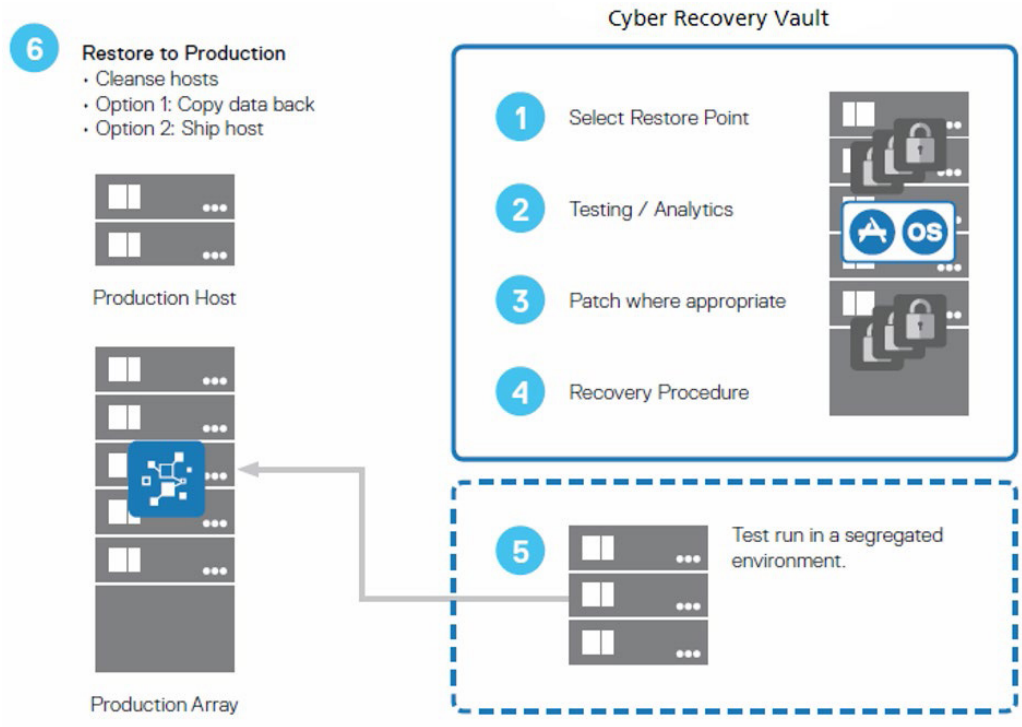


Figura 5: O processo de restauração de dados e binários de aplicativo. Fonte: Dell Technologies.[35]

2. **Recriação completa a partir do cofre do Cyber Recovery:**
   Nessa abordagem, a solução Cyber Recovery reformata os sistemas de produção com base no nível de danos determinado pela avaliação forense durante a resposta a incidentes. Em seguida, a solução recria binários por meio de cópias do cofre do Cyber Recovery e aplica os patches de segurança disponíveis. Por fim, ela restaura cópias apropriadas de aplicativos, dados e arquivos de configuração para o ambiente de produção usando os runbooks de DR associados do aplicativo. A Figura 6 ilustra esse processo.

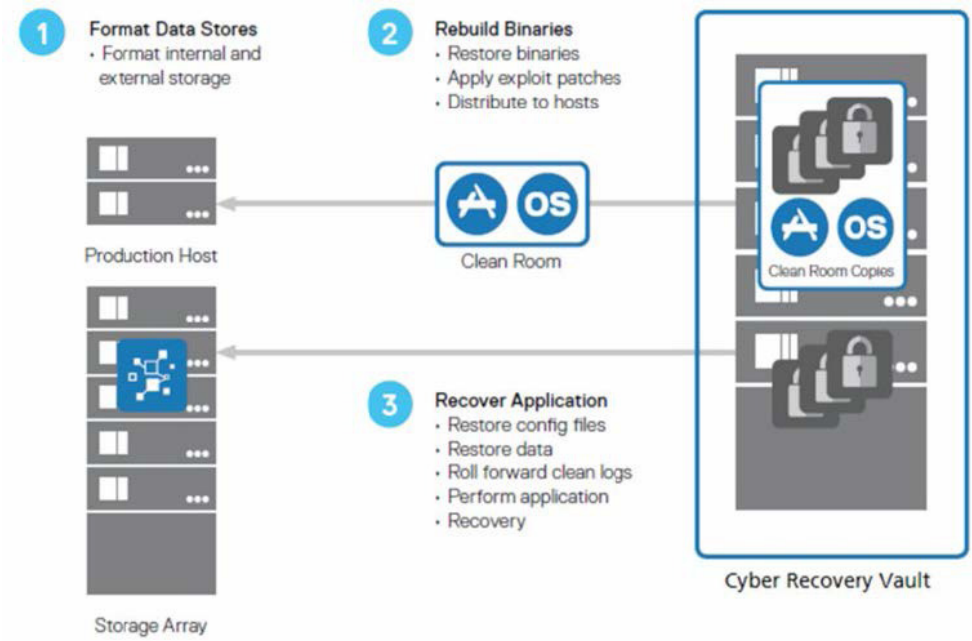


Figura 6: O processo de recriação completa a partir do cofre do Cyber Recovery. Fonte: Dell Technologies.[36]

As soluções Cyber Recovery incluem hosts de recuperação físicos ou virtuais (ou ambos) que o software Cyber Recovery pode usar para recuperação. Esses hosts incluem um servidor de recuperação de aplicativos de backup, que é um servidor designado para o qual o aplicativo de backup e o catálogo de aplicativos de backup se recuperam, e um servidor de recuperação de aplicativos. As organizações podem implementar vários servidores dependendo dos requisitos de recuperação da solução. O software Cyber Recovery pode expor cópias de dados de área restrita (um ambiente de teste para executar software novo ou não testado com segurança) a qualquer host para realizar recuperações de dados dentro do cofre, como dados de file system; dados de backup da IBM, CommVault e Veritas; ou dados protegidos pelo Dell NetWorker, pelo Dell Avamar, por um Dell PowerProtect DP Appliance ou pelo software Dell PowerProtect Data Manager. Depois de recuperar um aplicativo de backup dentro do cofre, a solução pode restaurar esses dados para hosts adicionais de recuperação no cofre.

As organizações dimensionam o servidor de recuperação de aplicativos de backup antecipadamente para que os usuários possam recuperar todos os aplicativos de backup protegidos pela solução Cyber Recovery. Da mesma forma, o servidor de recuperação de aplicativos é um servidor designado ao qual a solução recupera aplicativos. Alguns aplicativos podem exigir que os clientes recuperem primeiro outros aplicativos dependentes. A infraestrutura do cofre pode oferecer suporte à recuperação do maior aplicativo de produção que a solução protege.

Conclusão

Ao construir um plano de proteção de dados, as organizações devem considerar muitos vetores de ataque. Isso inclui a proteção de todos os dados; mas, ainda mais importante, dos dados essenciais imprescindíveis para as operações. O PowerProtect Cyber Recovery isola os dados essenciais e ajuda a garantir a recuperação adequada dos dados em caso de um ataque cibernético. O Cyber Recovery usa a lógica analítica do CyberSense, que se baseia em ML, para determinar a integridade dos dados do cofre e identificar dados limpos de backup para recuperação. Em nossos testes, constatamos que o PowerProtect Cyber Recovery detectou infecção nas páginas do banco de dados SQL (algo que uma solução concorrente não conseguiu fazer). O PowerProtect Cyber Recovery também exigiu menos backups do que uma solução concorrente para determinar a corrupção dos dados. Além de tudo isso e muito mais, a solução Cyber Recovery oferece muitas opções de recuperação, recorrendo aos dados não comprometidos do cofre para proporcionar um retorno eficiente e suave às operações.

1. Dell, "CyberSense® para PowerProtect Cyber Recovery", acessado em 8 de setembro de 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", acessado em 23 de agosto de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
4. Cohasset Associates, Inc, "Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)", acessado em 27 de outubro de 2023, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, "Data Domain: Perguntas frequentes sobre o Retention Lock", acessado em 12 de setembro de 2023, https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.
6. Dell, "Data Domain: Perguntas frequentes sobre o Retention Lock".
7. Dell, "Encryption types offered by DD series encryption appliance", acessado em 8 de setembro de 2023, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, "Dell EMC Data Domain – Security Configuration Guide", acessado em 11 de setembro de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, "Role Based Access Control (RBAC) in Data Domain", acessado em 11 de setembro de 2023, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, "Dell EMC Data Domain — Guia de configuração de segurança" (em inglês).
11. Dell, "MTree Replication", acessado em 11 de setembro de 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, "Dell EMC Data Domain - DataDomain MTree overview and limits", acessado em 11 de setembro de 2023, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", acessado em 13 de dezembro de 2023, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, "NetBackup™ Security and Encryption Guide", acessado em 13 de dezembro de 2023, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.
15. Principled Technologies, "Dell EMC Cyber Recovery protected our test data from a cyber attack", acessado em 21 de agosto de 2023, http://facts.pt/rkew01n.
16. Dell, "Dell PowerProtect Cyber Recovery", acessado em 12 de setembro de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.
17. Jerry Rozeman e Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware", acessado em 14 de dezembro de 2023, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman e Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware".
19. Nikitha Okmar, "Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era", acessado em 13 de dezembro de 2023, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, "How to protect your data from ransomware and encryption Trojans", acessado em 13 de dezembro de 2023, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, "Rest easy with immutable, off-site data storage", acessado em 13 de dezembro de 2023, https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, "NetBackup Isolated Recovery Environment", acessado em 13 de dezembro de 2023, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.
23. CSI Group, "Dell Cyber Recovery Vault (overview by CSI)", acessado em 23 de agosto de 2023, https://youtu.be/ej5nZzWNRM0.
24. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
25. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
26. Dell, "CyberSense® para PowerProtect Cyber Recovery".
27. Dell, "CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines", acessado em 13 de setembro de 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, "CyberSense for Dell Cyber Recovery", acessado em 25 de setembro de 2023, https://indexengines.com/csmatrix.
29. CISA, "#StopRansomware Guide", acessado em 1 de agosto de 2023, https://www.cisa.gov/stopransomware/ransomware-guide.
30. "Em segurança, a maioria das pessoas usa a Entropia de Shannon, um algoritmo específico que retorna um valor entre 0 e 8. Quanto maior o número, mais aleatórios serão os dados e, muitas vezes, um valor maior significa que os dados estão compactados ou criptografados". Mueller, Clint, "How to Use Entropy Analysis in Penetration Testing", 28 de agosto de 2023, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, "How to Protect Your backups from Ransomware in 2023", 1 de agosto de 2023, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, "Guia de arquitetura de página e extensões", acessado em 3 de agosto de 2023, https://learn.microsoft.com/pt-br/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, "SQL Injection", acessado em 3 de agosto de 2023, https://www.w3schools.com/sql/sql_injection.asp.
34. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
35. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
36. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).

Veja a ciência que respalda este relatório ▶

▶ Consulte a versão original deste relatório, em inglês, em https://facts.pt/64FU3b2

Principled Technologies®

Facts matter.®

Este projeto foi encomendado por Dell Technologies.