Sumário executivo

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.

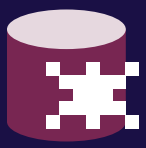
Dell PowerProtect Cyber Recovery é uma solução de gerenciamento, proteção e recuperação de dados que ajuda as organizações a proteger dados e aplicativos contra ransomware, ataques cibernéticos destrutivos e eventos inesperados. A solução usa uma abordagem de várias cópias; isso significa que, após a 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 podem ser essenciais para a segurança, a integridade e a recuperação que as soluções PowerProtect Cyber Recovery proporcionam. Esses recursos incluem Retention Lock, DDBoost, Controle de acesso baseado em função (RBAC), dupla autorização e muito mais.

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. Muitas vezes, 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, a fim de proteger 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.[2] Ao eliminar o acesso ao ambiente de recuperação a partir da rede de produção, uma organização pode reduzir a superfície de ataque.

Imutabilidade*

Tornar os backups imutáveis e, portanto, somente leitura ajuda a garantir que uma organização possa confiar nesses backups para recuperação. Operacionalmente, a imutabilidade mantém a autenticidade e a confiabilidade dos dados. Os sistemas DD, inclusive os contidos nas soluções PowerProtect Cyber Recovery, podem oferecer imutabilidade na maneira como armazenam dados usando partições lógicas do file system chamadas de MTrees. As soluções também usam a replicação de MTrees para duplicar cópias de dados imutáveis de um DD de produção para outro DD do cofre por meio do protocolo DDBoost.[3]

*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.

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.

Nós testamos o CyberSense e uma ferramenta da plataforma de gerenciamento de dados de um concorrente (que chamamos de "Fornecedor X") com funcionamento parecido em um equipamento de tamanho semelhante. Nos testes, constatamos que o PowerProtect Cyber Recovery detectou infecção nas páginas do banco de dados SQL, algo que a solução do Fornecedor X não conseguiu fazer. O PowerProtect Cyber Recovery também exigiu menos backups do que a solução do Fornecedor X para determinar a corrupção dos dados.

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, "MTree Replication", acessado em 11 de setembro de 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.
3. 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.

▶ Consulte a versão original em inglês deste resumo

Leia o relatório ▶

Principled Technologies®

Facts matter.®