

Dell PowerProtect Cyber Recovery

Proteção moderna e resiliente contra ataques cibernéticos e de ransomware para dados essenciais.

POR QUE ESCOLHER O CYBER RECOVERY?

Os ataques cibernéticos são desenvolvidos para comprometer seus dados valiosos, inclusive seus backups. Proteger seus dados críticos e recuperá-los com a integridade assegurada é fundamental para retomar as operações de negócios normais após o ataque.

Estes são os componentes de uma solução com resiliência cibernética:

Imutabilidade dos dados

Crie cópias de dados imutáveis para preservar a integridade e a confidencialidade dos dados com camadas de segurança e controles.

Isolamento automatizado dos dados

Isole automaticamente cópias de dados inalteráveis do ambiente de backup de produção em um cofre digital seguro, com acesso restrito elevado.

Análises inteligentes

Verificações de integridade automatizadas usando aprendizado de máquina baseado em IA e indexação de conteúdo completo com análises eficazes dentro da segurança do cofre para determinar se os dados foram afetados por malware.

Recuperação e correção

Fluxos de trabalho e ferramentas para realizar a recuperação após um incidente usando processos de restauração dinâmicos e os procedimentos de DR existentes.

Planejamento e design da solução

Orientação especializada para selecionar conjuntos de dados essenciais, aplicativos e outros ativos vitais para determinar os RTOs e RPOs, e otimizar a recuperação.

O desafio: ataques cibernéticos são inimigos das empresas orientadas por dados.

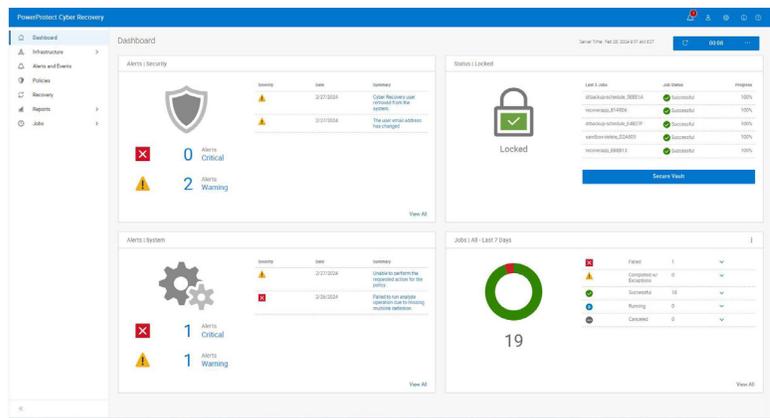
Os dados são a moeda da economia digital e um ativo vital que deve ser protegido, mantido confidencial e prontamente acessível. O mercado global moderno depende do fluxo contínuo de dados em redes interconectadas. As iniciativas de transformação digital e o uso crescente de IA generativa aumentam a exposição de informações confidenciais.

Isso faz com que os dados da sua organização sejam um alvo atraente e lucrativo para criminosos cibernéticos. Independentemente do setor ou do porte da organização, os ataques cibernéticos expõem continuamente os negócios e os governos a dados comprometidos, perda de receita devido ao tempo de inatividade, danos à reputação e multas regulatórias caras.

A implementação de estratégias de resiliência cibernética se tornou uma tarefa obrigatória para líderes empresariais e governamentais. Contudo, muitas organizações ainda confiam pouco em suas soluções de proteção de dados. O [Global Data Protection Index](#) relatou que 79% dos responsáveis pelas decisões de TI temem passar por um evento disruptivo nos próximos 12 meses. Enquanto isso, 75% temem que as medidas existentes de proteção de dados da empresa não consigam lidar com ameaças de malware e ransomware¹.

A solução: Dell PowerProtect Cyber Recovery

Para proteger seus negócios de ataques cibernéticos e criar uma abordagem de proteção de dados com mais resiliência cibernética, você pode modernizar e automatizar suas estratégias de recuperação e continuidade dos negócios. Ainda, você pode aproveitar as ferramentas inteligentes mais recentes para detectar e se defender de ameaças cibernéticas.



O PowerProtect Cyber Recovery oferece proteção comprovada, moderna, resiliente e inteligente para isolar dados essenciais, identificar atividades suspeitas e acelerar a recuperação de dados, permitindo facilitar uma recuperação mais inteligente de seus dados essenciais para retomar rapidamente as operações regulares de negócios. Com base em uma pesquisa da [Forrester Consulting](#), no caso de um ataque cibernético, o Dell PowerProtect Cyber Recovery ajuda a reduzir o tempo de inatividade em 75% e ajuda a reduzir as horas gastas na recuperação em 80%.²

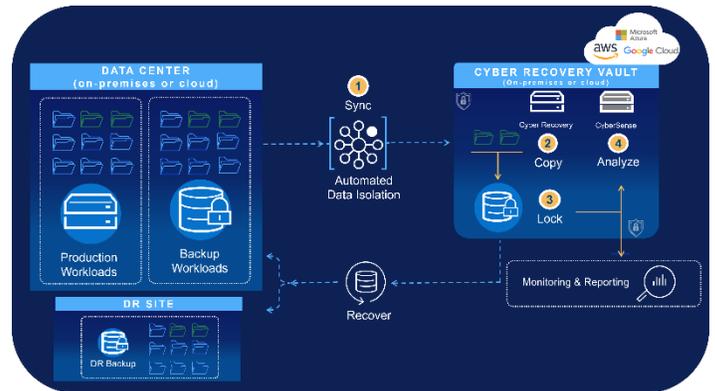
PowerProtect Cyber Recovery – Imutabilidade, Isolamento e Inteligência

Imutabilidade - PowerProtect Data Domain

O PowerProtect Data Domain é a base do Dell PowerProtect Cyber Recovery. Com várias camadas de segurança Zero Trust, ele fornece cópias de backup imutáveis para garantir a integridade e a confidencialidade dos dados. Recursos como raiz de confiança do hardware, inicialização segura, criptografia, bloqueio de retenção, acesso baseado em função e autenticação multifator ajudam a garantir a capacidade de recuperação de seus dados.

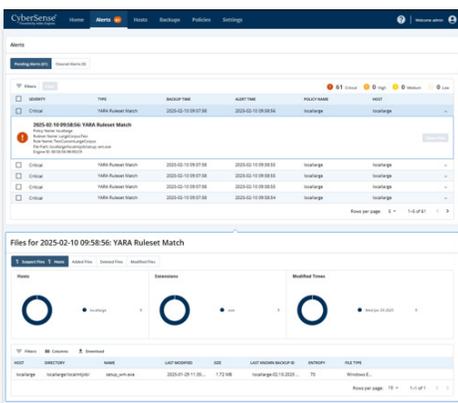
Isolamento - Cofre do Cyber Recovery

O cofre do PowerProtect Cyber Recovery é um ambiente isolado que oferece várias camadas de proteção para proporcionar resiliência contra ataques cibernéticos, até mesmo contra ameaças internas. O isolamento de dados automatizado do cofre copia com segurança (sincroniza) dados essenciais de backup (incluindo sistemas abertos e mainframe) para um cofre fisicamente isolado, longe da superfície de ataque da produção, nunca expondo o caminho de gerenciamento a um agente mal-intencionado. Em seguida, uma cópia imutável é criada automaticamente para impedir que os dados sejam modificados. Com gerenciamento, rede e serviços dedicados e independentes do ambiente de produção, são necessárias credenciais de segurança separadas e autenticação baseada em vários fatores para acessar os dados para operações de recuperação e testes.



Inteligência - CyberSense®

O PowerProtect Cyber Recovery é a primeira solução a integrar totalmente o CyberSense® para recuperações mais inteligentes contra ameaças cibernéticas, tudo isso na segurança do cofre do Cyber Recovery. O CyberSense vai além das soluções somente de metadados, com análise de conteúdo completo que detecta a corrupção de dados após um ataque com 99,99% de precisão³ e facilita a restauração inteligente e rápida. O CyberSense usa backups de dados imutáveis para observar como eles mudam ao longo do tempo e utiliza o aprendizado de máquina baseado em IA para detectar sinais de corrupção indicativos de um ataque de ransomware. O CyberSense detecta exclusões em massa, criptografia total e parcial e outras alterações suspeitas na infraestrutura de núcleo (incluindo Active Directory, DNS etc.), arquivos de usuários e bancos de dados resultantes de ataques sofisticados. Podem ser criados alertas de limite personalizados e, se forem detectados sinais de corrupção, o painel de alertas e os relatórios forenses pós-ataque facilitam o diagnóstico rápido da escala e do impacto do ataque, incluindo a identificação de uma cópia limpa dos dados para recuperar seus sistemas críticos. A pesquisa personalizada de assinatura de malware e regras YARA ajuda a personalizar e capacitar as organizações para que elas possam se defender proativamente contra ameaças cibernéticas.



PowerProtect Cyber Recovery - Opções de implementação

Cyber Recovery em ambientes híbridos e multinuvem

Os dados essenciais podem estar em muitos locais diferentes em uma empresa, seja no local, em diferentes data centers ou globalmente em várias nuvens e regiões. Independentemente do local, os dados precisam estar seguros e não compreendidos quando for necessária a recuperação de ataques cibernéticos.

O PowerProtect Cyber Recovery está disponível e pode ser transacionado por meio de marketplaces de nuvem pública para AWS, Microsoft Azure e Google Cloud para fornecer acesso rápido e proteger os dados em um cofre do Cyber Recovery na nuvem. O PowerProtect Cyber Recovery automatiza a sincronização de dados essenciais entre os sistemas de produção e o cofre do Cyber Recovery na nuvem pública. Ao contrário das soluções de backup padrão baseadas em nuvem, o acesso às interfaces de gerenciamento é bloqueado por controles de rede e exige credenciais de segurança separadas e autenticação multifator para acesso. A dispersão e a duplicação de dados em várias nuvens podem levar a riscos de segurança e conformidade, possíveis problemas de sincronização e aumento dos custos de recursos. Essa abordagem também pode reduzir a visibilidade em seus vários ambientes, levando a uma proteção insuficiente contra ameaças cibernéticas em constante evolução.

PowerProtect Data Domain All-Flash Ready Node

Enquanto os dados essenciais continuam a crescer, a capacidade de se recuperar de um evento cibernético de forma rápida e eficiente é fundamental para garantir a continuidade dos negócios e a resiliência cibernética. As organizações que estão expandindo o gerenciamento de dados essenciais devem se destacar na recuperação dos dados dos ambientes de recuperação isolados, como o cofre do Cyber Recovery. O Dell PowerProtect Data Domain All-Flash Ready Node oferece uma solução de recuperação cibernética simplificada, eficiente, econômica e com baixo consumo de energia, que apresenta recursos de restauração rápida e lógica analítica aprimorada do CyberSense para cumprir os SLAs da organização. Ao utilizar menos hardware, espaço e energia, as organizações podem melhorar as velocidades de acesso aos dados, aumentar a eficiência operacional e garantir a integridade dos dados, o que, em última análise, leva à redução do tempo de inatividade e dos custos gerais de manutenção.

PowerProtect Cyber Recovery – De volta às atividades

Recuperação e correção

O PowerProtect Cyber Recovery oferece procedimentos automatizados de restauração e recuperação para colocar os sistemas essenciais aos negócios novamente on-line com rapidez e confiança. A recuperação é integrada ao seu processo de resposta a incidentes. Depois que ocorre um evento, a equipe de resposta a incidentes analisa o ambiente de produção para determinar a causa raiz do evento. Após os ataques, o CyberSense oferece relatórios forenses para entender a profundidade e a amplitude do ataque e uma lista dos últimos conjuntos de backups bons antes da corrupção. Então, quando a produção está pronta para recuperação, o Cyber Recovery disponibiliza as ferramentas de gerenciamento e a tecnologia que executa a recuperação real de dados.

Planejamento e design da solução

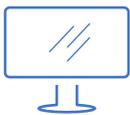
O Dell Professional Services for Cyber Recovery ajuda a determinar quais sistemas essenciais aos negócios devem ser protegidos e pode criar mapas de dependência para aplicativos e serviços associados, bem como a infraestrutura necessária para recuperá-los. O serviço também gera requisitos de recuperação e opções de design, além de identificar as tecnologias para analisar, hospedar e proteger seus dados, juntamente com um caso de negócios e implementação da linha do tempo.

Conclusão

Iniciativas do setor, como o Sheltered Harbor, têm utilizado o PowerProtect Cyber Recovery para proteger clientes, instituições financeiras e a confiança do público no sistema financeiro dos EUA, no caso de um ataque cibernético que cause falha em sistemas essenciais, incluindo backups. Com milhares de clientes, o Cyber Recovery com CyberSense oferece confiança aos líderes das empresas e provou acelerar a recuperação de dados no caso de uma ameaça cibernética.

O PowerProtect Cyber Recovery transmite a confiança de que você precisa, podendo identificar e restaurar rapidamente dados em boas condições e retomar as operações de negócios normais após um ataque cibernético.

É hora de voltar às atividades.



Saiba mais sobre o
Dell PowerProtect
Cyber Recovery



Entre em contato
com um especialista
da Dell Technologies



Veja mais recursos



Participe da
conversa com
#PowerProtect

¹ Com base na pesquisa da Vanson Bourne encomendada pela Dell Technologies: "Global Data Protection Index 2024 Snapshot". Outubro de 2023.

² Pesquisa da Forrester Consulting encomendada pela Dell Technologies: "The Total Economic Impact of Dell PowerProtect Cyber Recovery", agosto de 2023

³ Com base em um relatório de ESG encomendado pela Index Engines: "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption". Junho de 2024