

## Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect

### Serviço Cyber Recovery com capacidade multi-cloud

#### Confiável e seguro

- Ambiente de cofre isolado de forma física e lógica, desconectado de redes corporativas por meio de air gap operacional
- Cópias de dados imutáveis em um cofre seguro fora do local, mantendo a integridade dos dados
- A lógica analítica inteligente fornece o M/L e a indexação total de conteúdo dentro do cofre

#### Econômico

- Infraestrutura principal do cofre fornecida “as a service”
- Conexão direta de grande largura de banda e baixa latência com provedores de serviços em nuvem pública
- Taxas de saída de R\$ 0 do Microsoft Azure e da Oracle Cloud

#### Conveniência sem perdas

- Proteja os dados críticos que residem na nuvem ou no local
- Restaure os dados em qualquer provedor de serviços em nuvem pública de forma contínua
- Obtenha a flexibilidade e a conveniência da nuvem sem comprometer a segurança

#### Proteção cibernética para implementações no local e na nuvem

Toda hora, todos os dias, ransomware e outros ataques cibernéticos sofisticados ameaçam roubar ou comprometer o ativo mais essencial de uma empresa, os dados. Isso pode levar à perda de receita, danos à reputação e multas regulatórias caras. Proteger seus dados críticos e recuperá-los com a integridade dos dados validada é fundamental para retomar as operações de negócios normais após o ataque.

Ambientes híbridos e multi-cloud oferecem flexibilidade operacional, capacidade de dimensionamento rápido e acesso a serviços e hardware inovadores. No entanto, a abordagem de espalhar e duplicar dados em várias nuvens pode levar a novos 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 à proteção insuficiente contra as atuais ameaças cibernéticas em constante evolução. É necessária uma forma melhor de tornar seus dados simultaneamente acessíveis a provedores de serviços em nuvem pública sem comprometer a segurança, manter sua liberdade de escolher qualquer provedor e evitar a limitação a um único fornecedor.

Com um número maior de cargas de trabalho e dados migrados para a nuvem, é fundamental investir em uma solução de proteção cibernética para dados críticos, onde quer que estejam. A Dell Technologies oferece um cofre de dados seguro e lógica analítica inteligente que protegem seus dados críticos de ataques cibernéticos, ransomware e ameaças internas.

#### Cyber Recovery com capacidade multi-cloud

Configurar um cofre do Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect, desenvolvido pela Faction, é simples. Esse serviço de armazenamento em cofre de dados seguro é um cofre com espaço vazio criado em uma infraestrutura segura e com capacidade multi-cloud que protege seus dados críticos de ataques cibernéticos. Quando a recuperação de dados é necessária, você pode optar por restaurar os dados de seu cofre para a AWS, o Microsoft Azure, o Google Cloud e a Oracle Cloud ou voltar ao seu ambiente no local.

A lógica analítica inteligente do CyberSense é totalmente integrada a esse serviço do Cyber Recovery e tem uma abordagem única na descoberta de ataques cibernéticos, observando as alterações nos dados com o passar do tempo e usando lógica analítica para detectar sinais de corrupção devido a ransomware. Isso valida a integridade dos dados protegidos externamente e dentro do cofre do Cyber Recovery, fornecendo uma camada adicional de garantia.

#### Arquitetura segura do Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect

O ambiente de cofre seguro inclui um sistema Multi-Cloud Data Services for Dell EMC PowerProtect que funciona como destino de replicação para seus sistemas principais Dell EMC PowerProtect DD ou Dell EMC PowerProtect DD Virtual Edition (DDVE). Os recursos de computação dedicados executam as ferramentas de gerenciamento do Cyber Recovery e todas as ferramentas de lógica analítica do CyberSense. Combinada com a segurança física e o isolamento do cofre, essa solução inclui um air gap operacional que permite o acesso ao cofre pelo tempo suficiente para replicar os dados do sistema principal, mas o acesso é extremamente limitado. Em todas as outras ocasiões, o cofre é desconectado do ambiente de produção do cliente. Cópias imutáveis de dados selecionados pelo usuário são criadas no cofre do Cyber Recovery hospedado em um data center da Faction. Depois que a cópia dos dados selecionados está em segurança dentro do cofre seguro e isolado, não

é possível alterar nem excluir os dados de nenhuma forma por um período determinado. A lógica analítica do CyberSense, com o aprendizado de máquina e os recursos de indexação total de conteúdo, pode analisar cada conjunto de dados dentro da segurança do cofre.

### Proteção para implementações do Multi-Cloud Data Services for Dell EMC PowerProtect

Quando combinados com o Multi-Cloud Data Services for Dell EMC PowerProtect, os clientes obtêm proteção de dados soberana em todas as nuvens (AWS, Google Cloud, Oracle e Azure) e podem proteger seus dados críticos em um cofre seguro do Cyber Recovery. O Multi-Cloud Data Services for Dell EMC PowerProtect pode ser usado como um sistema multifuncional, um destino de backup para dados de aplicativos nativos na nuvem ou um destino de replicação para sistemas PowerProtect existentes. O cofre do Cyber Recovery é uma opção extra que pode ser facilmente adicionada para fornecer isolamento de dados críticos contra ataques cibernéticos e validação da integridade dos dados.

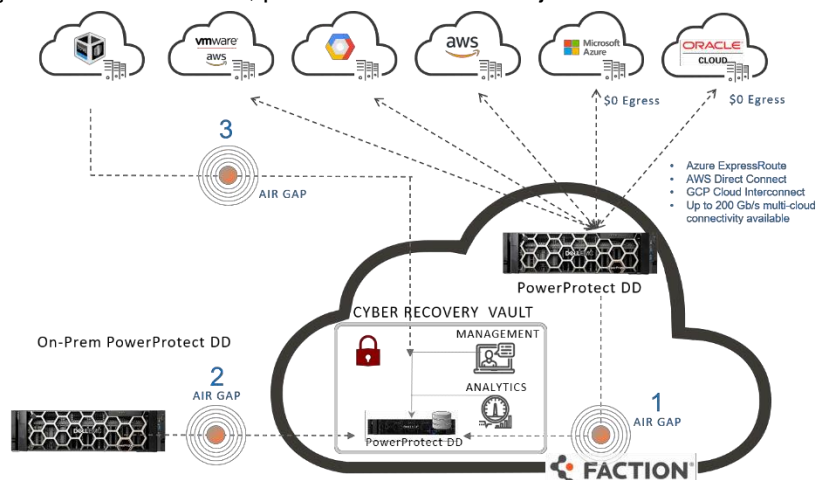


Figura 1: Casos de uso do Multi-Cloud Data Services for Dell EMC PowerProtect

1. Proteção para implementações do Multi-Cloud Data Services for Dell EMC PowerProtect
2. Proteção de dados no local do cliente
3. Proteção de dados na nuvem pública

### Proteção de dados no local do cliente

Os clientes podem replicar dados de um local PowerProtect DD para um cofre do Cyber Recovery em um dos data centers da Faction. Isso oferece às organizações a recuperação a quando os backups principais ou de produção são comprometidos ou o local de DR é violado ou infectado. Se ocorre um ataque cibernético, eles podem identificar rapidamente a cópia mais recente dos dados no cofre remoto do Cyber Recovery e recuperar seus sistemas essenciais no local ou optar por recuperar na nuvem se o serviço tiver sido arquitetado com essa opção de recuperação.

### Proteção de dados na nuvem pública

Para aplicativos nativos na nuvem que já usam o PowerProtect DDVE (um destino de backup virtual na nuvem compatível com AWS, Google Cloud e Azure), o cofre do Cyber Recovery é um serviço opcional que permite que os clientes repliquem dados críticos em um cofre seguro.

### Dell EMC PowerProtect Cyber Recovery com CyberSense

O PowerProtect Cyber Recovery é a primeira solução a integrar totalmente o CyberSense, que adiciona uma camada de proteção inteligente para ajudar a encontrar dados corrompidos quando um ataque entra no data center. Essa abordagem inovadora fornece indexação total de conteúdo e usa aprendizado de máquina para analisar mais de cem estatísticas baseadas em conteúdo e detectar sinais de corrupção devido a ransomware. O CyberSense localiza corrupção com até 99,5% de confiança, ajudando na identificação de ameaças e no diagnóstico de vetores de ataque, além de proteger o conteúdo essencial aos negócios, tudo isso na segurança do cofre.

### Soluções de proteção de dados da Dell Technologies: mostrando o seu caminho para a nuvem

Você pode proteger dados essenciais na nuvem sem comprometer a integridade, a confidencialidade ou a disponibilidade. O Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect protege seus dados críticos, independentemente de estarem hospedados na nuvem ou no local de um único destino com confiança. Para obter mais informações, clique aqui.



[Saiba mais](#) sobre o Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect



[Entre em contato](#) com um especialista da Dell Technologies



[Saiba](#) mais sobre soluções de proteção de dados na nuvem e backup

