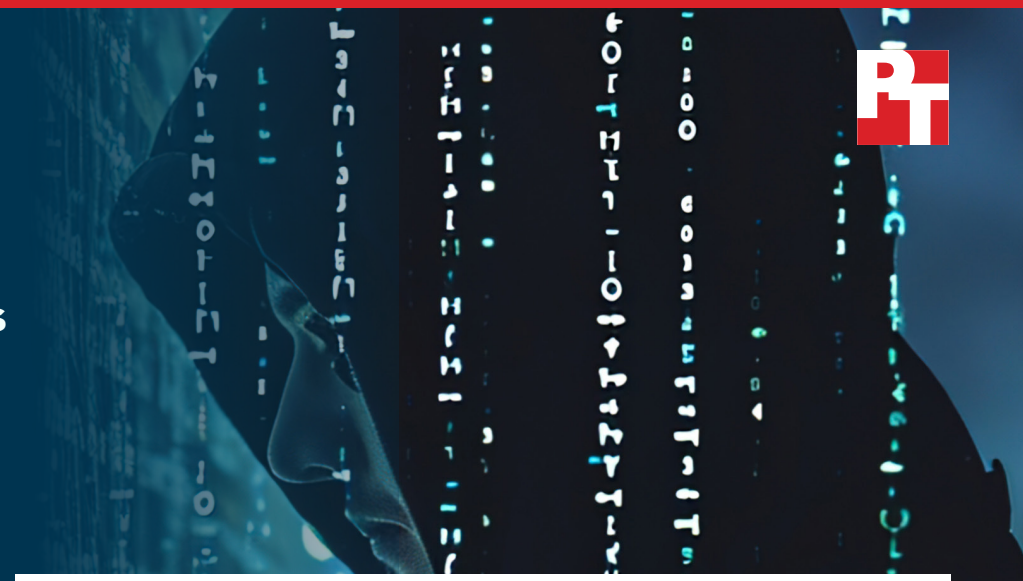


Reforce seu plano de proteção de dados com uma solução de recuperação cibernética mais sólida e rápida

Com base em nossa pesquisa, o Dell Technologies PowerProtect Cyber Recovery pode proporcionar isolamento físico de cofres de backup e verificação mais profunda de ransomware

Isolamento por air gap físico para cofres de backup

Crie uma barreira física que os dados não possam atravessar

Verificação mais profunda de ransomware

O CyberSense analisa o conteúdo dos arquivos e os bancos de dados, não apenas os metadados

Verifique 2 vezes mais cargas de trabalho com anomalias

Procure malware em mais lugares com uma só ferramenta

O custo médio de um ataque de ransomware aumentou quase 20% em 2 anos, chegando a US$ 5,23 milhões.[1] Soluções eficientes de recuperação cibernética podem reduzir ou, até mesmo, evitar esses possíveis custos, permitindo que as organizações se recuperem de incidentes imediatamente, reduzam a perda de dados, minimizem o tempo de inatividade e, no processo, preservem a integridade da marca. Essas soluções devem determinar e restaurar os dados conhecidamente íntegros após o ataque, garantindo que a organização possa recuperar dados e sistemas essenciais e, ao mesmo tempo, minimizando o risco aos negócios e o tempo de inatividade.

O Dell PowerProtect Cyber Recovery (Cyber Recovery) é uma solução desse tipo. Ele ajuda as organizações a proteger dados e aplicativos contra ransomware, ataques cibernéticos destrutivos e eventos inesperados. Este relatório usa dados publicamente disponíveis para contrastar os recursos e as funcionalidades fundamentais de proteção de dados do Cyber Recovery e de uma solução concorrente, o Rubrik Security Cloud (RSC). Nós analisamos especificamente os recursos e as funcionalidades que os clientes de soluções de recuperação cibernética podem achar importantes, inclusive o cofre de recuperação, a imutabilidade, o suporte a cargas de trabalho, a tecnologia de verificação, a capacidade de recuperação e o isolamento.

Ao contrário do RSC, o Cyber Recovery usa uma abordagem de várias cópias; isso significa que, após a criação de backups, ele copia esses backups (ou, normalmente, um subconjunto selecionado) em um armazenamento isolado para fins de proteção e análise. O Cyber Recovery engloba vários componentes, inclusive um ou mais cofres de armazenamento, estabelecidos no local em um equipamento PowerProtect Data Domain ou na nuvem por meio do Dell APEX Protection Storage for Public Cloud definido por software. Em comparação, o RSC não oferece opções locais de cofre. O 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 em busca de sinais de corrupção causados por um ataque de ransomware. A solução CyberSense pode verificar duas vezes mais cargas de trabalho de anomalias do que a solução Rubrik, o que pode permitir que o ML (machine learning, aprendizado de máquina) do CyberSense detecte o impacto do malware ou outras atividades de agentes de ameaças em um maior volume de dados. Nós examinaremos minuciosamente como o PowerProtect Cyber Recovery funciona de maneira diferente e pode ser mais vantajoso para sua organização.

Visão geral do produto

Visão geral do Dell PowerProtect Cyber Recovery

O Dell PowerProtect Cyber Recovery é composto por um equipamento de armazenamento que hospeda dados de produção e um equipamento de armazenamento de destino no cofre para fins de replicação. Ele também é composto pelo software Cyber Recovery, que coordena a sincronização, gerencia várias cópias de dados no sistema PowerProtect Data Domain (PPDD) do cofre do Cyber Recovery, supervisiona o processo de recuperação e supervisiona o processo de lógica analítica com o CyberSense.

A solução transfere dados exclusivos da MTree do PPDD de produção para o cofre por meio da replicação de MTrees viabiliza a imutabilidade dos dados* por um período definido. O cofre apresenta um servidor que contém o software Cyber Recovery e um componente onde a solução restaura aplicativos e dados de backup. Geralmente, cada cofre do Cyber Recovery hospeda muitos desses componentes. O cofre também contém um host de lógica analítica/indexação equipado com software de análise de dados, oferecendo integração direta entre o software Cyber Recovery e o CyberSense.

*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.

A Figura 1 apresenta uma visão geral da solução Dell Cyber Recovery.

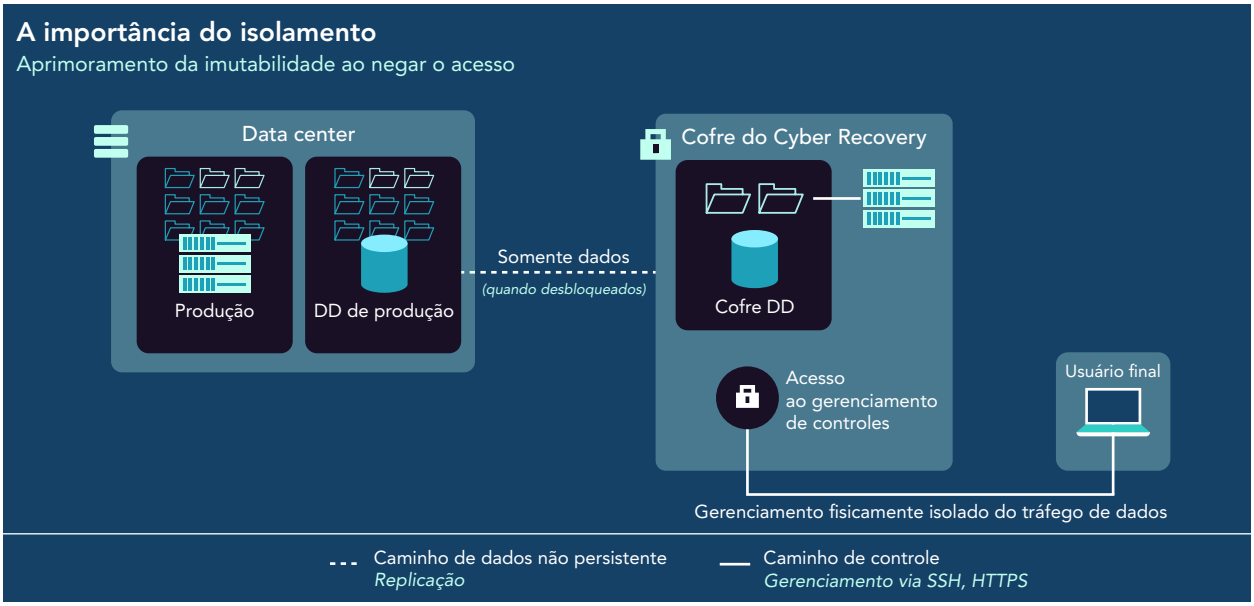


Figura 1: Dados de alto nível e arquitetura do caminho de controle do cofre do Cyber Recovery. Fonte: Principled Technologies.

Para saber mais sobre os principais componentes da solução Dell PowerProtect Cyber Recovery, leia o Guia da solução Dell PowerProtect Cyber Recovery.

Visão geral do Rubrik Security Cloud

A Rubrik descreve o Rubrik Security Cloud como uma plataforma de software as a service (SaaS) que permite que os clientes "mantenham [seus] dados seguros, monitorem os riscos aos dados e recuperem rapidamente [seus] dados, onde quer que eles residam — na empresa, na nuvem e em aplicativos de SaaS".[4] Ela afirma que desenvolveu a solução em uma "arquitetura segura de microsserviços usando a infraestrutura e os serviços de alta disponibilidade em execução no Google Cloud Platform (GCP)".[5] A Figura 2 mostra a estrutura geral do Rubrik Security Cloud.

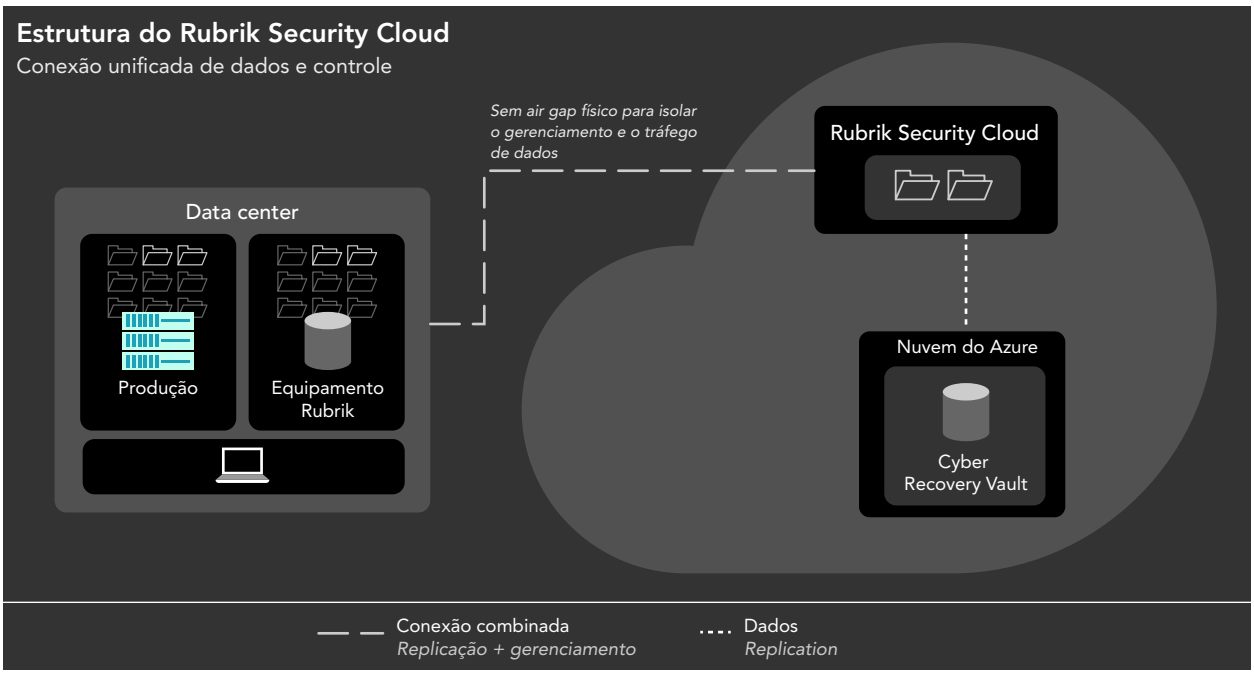


Figura 2: A estrutura geral do Rubrik Security Cloud. Fonte: Principled Technologies.

Suporte a recursos

Cofre de recuperação

Os cofres são o armazenamento dedicado que hospeda cópias criptografadas dos backups que a solução faz no ambiente de produção. Eles não fazem parte das soluções de backup de produção; em vez disso, cada um atua como um local isolado de "backup para o backup" a partir do qual os clientes podem recuperar backups validados.

A Dell oferece várias opções de cofre, inclusive no local, em um local remoto de colocação ou em uma nuvem pública. O cofre no local utiliza um PPDD com air gap operacional que reside no datacenter, possivelmente até mesmo no mesmo rack da solução de backup. Normalmente, uma solução com air gap é fisicamente isolada do ambiente de produção. Um cofre colocalizado externamente requer conexões de rede dedicadas a um cofre físico, como uma versão local, mas o cofre é geograficamente separado em um datacenter remoto. A Dell também oferece cofres na nuvem pública, fazendo parcerias com provedores de serviços em nuvem Amazon Web Services (AWS), Microsoft Azure e Google Cloud. Os cofres em nuvem pública podem proporcionar flexibilidade de configuração para atender às necessidades do cliente.[6, 7,8]

Rubrik Cyber Recovery é um componente do Rubrik Security Cloud. Oferecido por meio de um modelo de software "as a service", o cofre de recuperação usa armazenamento somente no Microsoft Azure. Muitos dos documentos disponíveis publicamente que nós encontramos em nossa pesquisa ligam o cofre do Rubrik Cyber Recovery ao Rubrik Cloud Vault, o nível de backup, que oferece imutabilidade.[9, 10] Esse cofre não requer hardware adicional e pode ser usado por qualquer versão da plataforma Rubrik Cloud Data Management (CDM) a partir da versão 6.02.

Imutabilidade

Imutabilidade se refere à condição de ser inalterável ou permanente. As cópias de backup e os backups imutáveis permitem que os administradores criem permanência para arquivos que os usuários ou os sistemas não podem modificar nem excluir antes de um intervalo de tempo designado. Em seguida, os arquivos são descartados; a solução os remove automaticamente. Geralmente, as soluções realizam esse processo por meio de políticas ou de definições que regem a forma como o sistema trata os arquivos.[11]

A imutabilidade do Dell PowerProtect Cyber Recovery depende de bloqueios de retenção, realizados por meio do recurso Retention Lock, para impedir a exclusão ou a modificação (por um período) ou a expiração antecipada forçada de cópias de backup. (O PPDD é um file system somente de anexação, independentemente de a organização ter ativado o Retention Lock ou não.[12]) Os clientes da Dell gerenciam backups usando MTrees do PPDD, que são partições lógicas definidas pelo usuário com configurações independentes de retenção que eles designam como destinos dos aplicativos de backup.[13] Os clientes podem escolher entre dois tipos de bloqueios de retenção: governança e conformidade. Os bloqueios de conformidade são os mais rigorosos e mais seguros dos dois. Os clientes ativam os bloqueios de retenção por MTree, o que significa que todos os arquivos dentro de uma MTree específica aderirão à definição de bloqueio de retenção dessa MTree, e definem o período de retenção por arquivo. Quando os clientes definem um bloqueio de retenção de conformidade, nenhum usuário ou sistema pode removê-lo. Um administrador pode reverter um bloqueio de retenção de governança, que é a opção menos rigorosa.[14]

A imutabilidade da solução Rubrik também depende de bloqueios de retenção para impedir a exclusão ou a expiração antecipada forçada de cópias de backup. Assim como o PowerProtect Cyber Recovery, a solução Rubrik anexa novos dados ao file system, em vez de substituir os dados existentes. A solução gera impressões digitais dos dados recebidos e as armazena com os dados. **A solução Rubrik não disponibiliza bloqueios de retenção por padrão**, e os clientes devem abrir um tíquete com o Suporte Rubrik ou ativar uma regra de duas pessoas para permitir bloqueios de retenção. (Antes da versão 7.0.1 do Rubrik Cloud Data Management, os clientes precisavam entrar em contato com o Suporte Rubrik para ativar os bloqueios de retenção; a documentação da Rubrik não deixa claro se os clientes ainda podem entrar em contato com o suporte para que isso funcione ou não.) Depois da ativação pelos clientes, os bloqueios de retenção impedem que os usuários ou os sistemas excluam dados fora dos parâmetros definidos. Os bloqueios de retenção do Rubrik exigem um servidor Network Time Protocol (NTP) externo para sincronização de horário, o que pode apresentar uma oportunidade para que agentes mal-intencionados manipulem a fonte do NTP de referência e, assim, expirem os bloqueios de retenção prematuramente.[15]

> *"A solução Rubrik não disponibiliza bloqueios de retenção por padrão, e os clientes devem abrir um tíquete com o Suporte Rubrik ou ativar uma regra de duas pessoas para permitir bloqueios de retenção."*

Licenciamento e assinaturas

Dell PowerProtect Cyber Recovery é uma solução licenciada. Durante a instalação, a Dell instala uma licença de avaliação de 90 dias por padrão. Após 90 dias, os clientes devem adquirir uma nova licença para continuar usando o produto. A Dell oferece licenciamento padrão (permanente) e licenciamento com base em assinatura.

A Rubrik integra o Rubrik Cyber Recovery ao Rubrik Security Cloud (RSC). Os clientes devem ter uma assinatura do Rubrik Enterprise Edition para usar o Rubrik Cyber Recovery. Os termos de assinatura valem por três anos.[16,17] Em caso de falha do RSC, as cargas de trabalho do SAP HANA e DB2 exigem ferramentas de terceiros para recuperar dados, o que pode incorrer em custos adicionais de assinatura.[18]

Acesso ao gerenciamento

O gerenciamento do sistema Dell PowerProtect Cyber Recovery é local para qualquer topologia que os clientes escolherem para implementação. Como a solução inicia a recuperação a partir do cofre, os administradores fazem log-in na IU de gerenciamento, onde quer que o cofre resida. Os cofres no local oferecem aos administradores acesso local sem a necessidade de acesso à Internet (que os ataques cibernéticos podem prejudicar gravemente devido a ataques de negação de serviço)

ou protegem os dados ao romper a conexão com a Internet, conforme recomendado pelo National Institute of Standards and Technology (NIST). Os cofres colocalizados permitem o acesso físico ao equipamento a partir de um local remoto e usam conexões fora da Internet pública. Já os cofres em nuvem exigem acesso à Internet para recuperação, o que pode atrasar a recuperação no local até o encerramento do ataque cibernético e a retomada da conectividade normal da rede.

O gerenciamento do Rubrik Cyber Recovery requer acesso ao Rubrik Security Cloud, que exige acesso à Internet. Como nós observamos, esse tipo de conectividade pode atrasar a recuperação no local até que a funcionalidade da rede volte ao normal após um ataque cibernético.

Como os clientes devem ter acesso ao RSC para usar os recursos do Rubrik Cyber Recovery, o RSC se torna um ponto único de falha. Se esse serviço ficar indisponível, isso prejudicará a recuperação a partir do cofre para o cliente afetado. O Rubrik pode recuperar dez cargas de trabalho durante uma interrupção do serviço RSC, mas duas cargas de trabalho de banco de dados exigem ferramentas de terceiros e ajuda do Suporte Rubrik para recuperá-las.[19, 20] Além disso, as contas de administrador comprometidas ou os agentes mal-intencionados com acesso à plataforma RSC teriam acesso a toda a estrutura, e não a um só cofre.

Receba mais ajuda com o Managed Detection and Response da Dell

Algumas organizações podem não se sentir confortáveis para adotar uma abordagem "independente" de segurança cibernética. Para esses clientes, a Dell oferece o Managed Detection and Response (MDR), um serviço totalmente gerenciado que monitora e detecta ameaças e riscos e trabalha com os clientes para reduzi-los. De acordo com a Dell, o serviço oferece estes benefícios:[21]

- Suporte confiável, inclusive orientações especializadas para implementar e configurar as plataformas de lógica analítica de segurança para detecção e resposta estendidas (XDR) as quais a Dell oferece suporte
- Resposta a ameaças e configuração de segurança, com a inclusão de até 40 horas de configuração de segurança relacionada a serviços por trimestre
- Detecção e investigação 24/7, inclusive a busca proativa de ameaças específicas ao ambiente de cada cliente para descobrir novas ameaças ou variações de ameaças conhecidas que burlam os sistemas de segurança
- Início da resposta a incidentes cibernéticos, incluindo 40 horas de assistência anual na resposta a incidentes remotos, que permitem que as atividades investigativas comecem rapidamente

Quando combinado com o APEX Cyber Recovery Services, o MDR permite que os clientes escolham entre várias opções para monitorar, detectar e reduzir ameaças e riscos. A disponibilidade de opções pode significar uma cobertura expandida ou uma abordagem híbrida que atende às necessidades de sua organização.

Para obter mais informações sobre o MDR, acesse **https://www.dell.com/pt-br/lp/dt/managed-detection-response.**

Fluidez

Configuração

A configuração do Dell PowerProtect Cyber Recovery consiste na instalação de software em um sistema Linux ou na criação de um equipamento VMware® vSphere® a partir de um modelo Open Virtualization Format (OVF). A instalação do software requer 14 etapas,[22] enquanto a implementação alternativa do equipamento vSphere requer 8 etapas e leva 5 minutos.[23] Após a instalação, os administradores podem acessar a solução por meio de navegadores da Web a partir do ambiente isolado.

Os clientes precisam implementar separadamente o CyberSense, um mecanismo totalmente automatizado e integrado de lógica analítica de segurança inteligente.[24] As instruções para a instalação do CyberSense no Dell PowerProtect Cyber Recovery não estão disponíveis publicamente.[25]

A Dell tem várias métricas que os usuários podem ajustar, inclusive o objetivo de detecção de danos (DDO), o objetivo de avaliação de danos (DAO), o ponto do Cyber Recovery (CRP), a hora do Cyber Recovery (CRT), o intervalo de sincronização do Cyber Recovery e a contagem de cópias de dados do Cyber Recovery. A Dell também recomenda a caracterização dos dados que precisam de proteção. Esses dados podem ser essenciais, essenciais aos negócios, dependentes de serviços da infraestrutura principal ou outros aplicativos, ou gerais, como binários de aplicativos, imagens de inicialização e catálogos de backup. A variedade de opções proporciona aos clientes controle total sobre o ambiente de backup e a capacidade de personalizar a classificação dos dados. A Dell Consulting Services também pode oferecer mais assistência e sugestões.[26]

A configuração do Rubrik também consiste em várias etapas. Antes de criar um cluster, os serviços do Suporte Rubrik devem instalar e configurar o Rubrik CDM. Em seguida, um administrador faz download da versão mais recente ou desejada do CDM e a instala (15 etapas).[27] Depois, o administrador pode configurar um cluster do Rubrik usando a IU ou a CLI. Você pode configurar o cluster com a IU ou a CLI, e ambas as abordagens levam 24 etapas.[28, 29] Então, o administrador pode registrar os clusters do Rubrik usando um método on-line (12 etapas)[30] ou off-line (18 etapas).[31] Em seguida, o administrador ativa a autenticação baseada em vários fatores (MFA), que leva 13 etapas.[32] Por fim, o administrador adiciona a conta inicial (6 etapas) e quaisquer outras contas.[33] A Figura 3 mostra o número máximo de etapas possíveis para configurar cada solução de recuperação cibernética.

Os clientes do Rubrik não conseguem ajustar outras métricas, o que pode reduzir a flexibilidade para atender às suas necessidades. Um revisor afirmou: "A maioria da interface do usuário é bem simples e fácil, mas algumas áreas não descrevem para que se usa uma opção ou há opções ausentes. Embora isso facilite a experiência do usuário, muitos itens ajustáveis não estão presentes e exigem a abertura de um túnel de suporte para que um funcionário do suporte faça uma alteração no ambiente do cliente".[34]

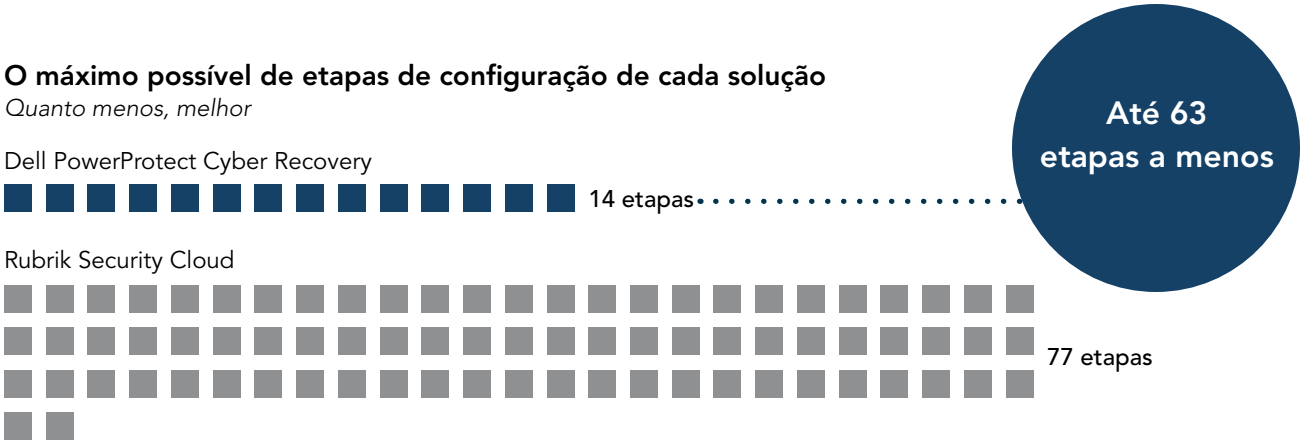


Figura 3: O número máximo de etapas possíveis para configurar o Dell PowerProtect Cyber Recovery e o Rubrik Security Cloud. Quanto menos, melhor. Fonte: Principled Technologies.

Manutenção

Nós observamos que, após a configuração, as IUs da Dell e da Rubrik para a realização de operações de manutenção diária são semelhantes. Após a configuração, os clientes podem configurar o Dell PowerProtect Cyber Recovery para estas tarefas:[35, 36]

- Gerar automaticamente relatórios de trabalhos do Cyber Recovery de acordo com um agendamento e em resposta a uma solicitação manual do usuário
  - Um usuário ou um agendamento cria trabalhos quando inicia uma política, uma operação de recuperação, um backup do sistema ou uma operação de limpeza
- Monitorar automaticamente o status do cofre, a capacidade de armazenamento, as operações do Cyber Recovery, os alertas quando a cópia/sincronização falha ou se o cofre do Cyber Recovery fica inativo e os trabalhos do Cyber Recovery
- Verificar a presença de ataques de maneira automática e contínua e, em seguida, exibir alertas do CyberSense em ordem de gravidade, informando o número de arquivos, hosts, políticas afetadas, ameaças específicas detectadas, o momento do ataque para que você possa encontrar um backup limpo e uma lista de arquivos corrompidos para usar na análise do ataque

Da mesma forma, os clientes podem configurar o Rubrik para fazer estas tarefas:[37]

- Usar automaticamente o Rubrik Security Cloud para rastrear, monitorar e exibir todos os eventos de todos os clusters do Rubrik conectados. Ele oferece três tipos de eventos:[38]
  - "Critical" — eventos que exigem atenção, como backup, arquivamento ou replicação com falha
  - "Warning" — houve a conclusão de um backup, um arquivamento ou uma recuperação
  - "Informational" — somente para fins informativos
- Verificar os snapshots de maneira automática e contínua em busca de indicadores novos e existentes de comprometimento usando o Threat Monitor, que informa a hora em que a solução criou o último snapshot, a linha do tempo dos eventos, a hora de detecção, o número de arquivos alterados, o número de arquivos suspeitos, o nome do cluster e o tipo e o nome do objeto

Suporte a cargas de trabalho com anomalias

Tanto o Rubrik Security Cloud Data Threat Analytics quanto o CyberSense verificam vários tipos de carga de trabalho. Mas, de acordo com as fontes encontradas, o CyberSense oferece suporte a duas vezes mais cargas de trabalho com detecção de anomalias. Isso inclui a verificação dos seguintes tipos de cargas de trabalho:

- VMs
- Infraestrutura principal
- Arquivos de usuário que podem conter documentos, contratos e propriedade intelectual
- Bancos de dados
- Backups feitos por outros clients

"Ao contar o número de cargas de trabalho compatíveis que encontramos nos dados publicamente disponíveis, verificamos que o CyberSense oferece suporte a 21 cargas de trabalho de detecção de anomalias e, o Rubrik, a 7."

Ao contar o número de cargas de trabalho compatíveis que encontramos nos dados publicamente disponíveis, verificamos que o CyberSense oferece suporte a 21 cargas de trabalho com detecção de anomalias e, o Rubrik, a 7. Portanto, de acordo com os dados publicamente disponíveis compartilhados por cada um deles, o CyberSense oferece suporte a duas vezes mais cargas de trabalho do que o Rubrik Security Cloud Data Threat Analytics. Quanto mais dados uma solução de recuperação cibernética puder verificar, melhor será a chance de encontrar malware furtivo ou outra corrupção.

Suporte a cargas de trabalho de VM

As cargas de trabalho de VM se referem aos aplicativos, aos serviços ou às tarefas que as VMs executam em um servidor de host físico ou um ambiente de nuvem. Como essas cargas de trabalho podem variar de função e há muitas outras maneiras que podem aumentar sua exposição a malware, a verificação de VMs é essencial. O Rubrik Security Cloud Data Threat Analytics, que "compreende os serviços Anomaly Detection, Threat Monitoring, Threat Hunting e de recuperação de dados em recursos protegidos",[39] oferece suporte à verificação das seguintes cargas de trabalho de VM:[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

O CyberSense oferece suporte à verificação das seguintes cargas de trabalho de VM:[41, 42,43]

- VMware
- Amazon Web Services (AWS)
- Hyper-V, com backups do Dell Avamar ou do Dell NetWorker

A VMware afirma que "80% das cargas de trabalho virtualizadas são executadas na tecnologia VMware".[44] No 1° trimestre de 2024, o fornecedor mais popular do mercado de serviços de infraestrutura em nuvem, a Amazon Web Services (AWS), controlava 31% de todo o mercado. O Microsoft Azure ocupa o 2º lugar, com 25% de participação no mercado.[45]

Infraestrutura principal

A infraestrutura principal são os componentes e serviços básicos que viabilizam a operação de um ambiente de tecnologia. A detecção de malware nesse nível pode reduzir a gravidade de um ataque, pois a funcionalidade da infraestrutura principal pode afetar muitos sistemas e usuários. A documentação do Rubrik Security Cloud não menciona suporte à verificação de qualquer infraestrutura principal.[46]

Por outro lado, o CyberSense oferece suporte à verificação da seguinte infraestrutura principal:[47]

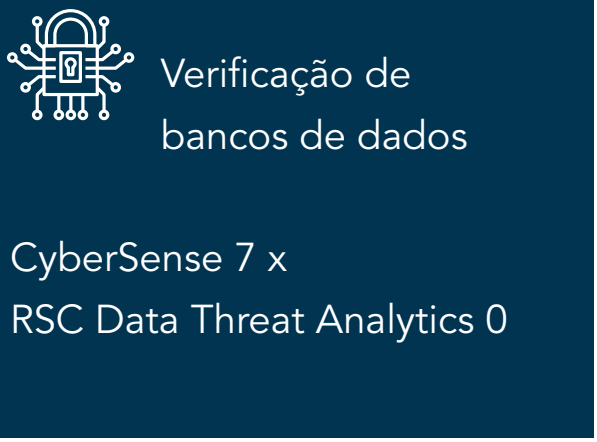
- Active Directory
- DNS
- LDAP

Arquivos de usuário que podem conter documentos, contratos e propriedade intelectual

O Rubrik Security Cloud Data Threat Analytics oferece suporte à verificação dos seguintes arquivos de usuário:[48]

- Conjuntos de arquivos e dados de NAS
- Grupos de volumes do Windows
- Linux e Windows

O CyberSense pode verificar arquivos de usuário do Linux e do Windows.[49]



Bancos de dados

Os aplicativos podem usar diferentes tipos de bancos de dados por muitos motivos. Sendo assim, conseguir detectar a presença de malware em vários bancos de dados pode ser fundamental para uma resposta rápida. O Rubrik Security Cloud Data Threat Analytics pode fazer backup de bancos de dados, mas nós não encontramos documentação pública que informe se ele pode verificar esses backups de banco de dados.

O CyberSense oferece suporte à verificação dos seguintes bancos de dados, com verificações em nível de página:[50]

- SQL
- Oracle®
- SAP HANA
- Db2
- PostgreSQL
- Epic® Caché
- MariaDB/MySQL

Backups feitos por outros clients

Algumas organizações podem ter backups de dados de vários fornecedores para proporcionar redundância, cumprir normas ou algum outro motivo significativo. A documentação do Rubrik Security Cloud não menciona o suporte à verificação de backups feitos por outros clients de backup.[51]

Com uma clara vantagem nessa categoria, o CyberSense oferece suporte à verificação de backups feitos pelos seguintes clients de backup:[52, 53,54]

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- Exchange
- Avamar
- Commvault

Tecnologia de verificação

O Rubrik Security Cloud inclui muitas ferramentas de verificação e para auxiliar a verificação do Data Threat Analytics:

- O Rubrik Anomaly Detection mostra arquivos suspeitos, alterações de snapshots[55] e detalhes de anomalias na forma de incidentes de anomalia para que os clientes os estudem e usem na investigação de snapshots.[56] O software também oferece opções para recuperação.[57]
- O Rubrik VM Encryption Detection detecta ataques em arquivos de disco virtual do VMware vSphere.[58]
- O Rubrik Threat Monitoring mostra informações sobre ameaças e correspondências detectadas.[59]
- O Rubrik Threat Hunt é uma verificação iniciada pelo usuário em busca de indicadores de comprometimento.[60]
- O Rubrik Quarantine isola objetos que aparecem em uma busca de ameaças.[61]

O Rubrik RSC também tem conectores do Rubrik Backup Service para cada cluster do Rubrik.

Os clientes do Rubrik devem selecionar a ferramenta correta para sua tarefa e podem ter que iniciar verificações manualmente ou usar várias ferramentas para realizar a tarefa. Por outro lado, a Dell tem uma só opção para verificação do CyberSense, que os clientes podem achar mais fácil de gerenciar e administrar.

A verificação do CyberSense vai mais fundo do que a verificação "somente superficial" do Rubrik RSC Data Threat Analytics. O CyberSense realiza verificações completas de conteúdo dos arquivos e verificações de bancos de dados em nível de página, além de detectar criptografia parcial de arquivos.[62] A ferramenta usa um banco de dados de aprendizado de máquina (ML) treinado pela Index Engines em milhares de ameaças aos dados e contém mais de 200 pontos de lógica analítica para detectar corrupção de dados.[63] Ao contrário do Rubrik Threat Monitoring e do Threat Hunt, o CyberSense não depende de agências externas de Threat Intelligence para oferecer assinaturas de malware. Em vez disso, ele detecta novas ameaças.[64]

O CyberSense também não depende de limites arbitrários de alterações aceitáveis de arquivos nem de níveis de entropia entre os snapshots, o que pode gerar falsos negativos. Ele também não treina o ML para uma linha de base de comportamentos anteriores do cliente.[65, 66, 67]

"O CyberSense também não depende de limites arbitrários de alterações aceitáveis de arquivos nem de níveis de entropia entre os snapshots, o que pode gerar falsos negativos...."

O software Rubrik Anomaly Detection depende exclusivamente de metadados para determinar se um snapshot está corrompido antes de fazer qualquer análise de conteúdo. Em comparação com o ML contínuo do CyberSense, o software Rubrik descobre corrupção após a obtenção de assinaturas. O Rubrik Anomaly Detection precisa criar um modelo comportamental para definir a linha de base normal de um cliente. Pode ser necessário fazer vários backups para estabelecer isso. O modelo comportamental do Rubrik requer pelo menos dois backups para criar uma

linha de base de alterações típicas em um file system quando não há ataques. No entanto, um só conjunto de estatísticas de alterações pode não ser suficiente para estabelecer o que é típico. Os eventos de negócios podem desencadear mais ou menos atividades ou mais tipos suspeitos de atividades que não ocorreram entre o primeiro e o segundo snapshot do Rubrik. Quanto mais backups a solução Rubrik analisar, mais precisamente ela poderá treinar o modelo comportamental para uma linha de base.[68, 69]

O CyberSense contém toda a sua lógica analítica no cofre. No pipeline de análise comportamental do file system, o Rubrik envia metadados sobre as alterações do file system do cliente à plataforma em nuvem Polaris para fazer a análise comportamental, o que abre uma superfície de ataque.[70]

Os clientes somente podem usar o Rubrik Threat Monitoring e o Threat Hunt como parte da edição Rubrik Enterprise.[71] Os clientes devem realizar verificações do Threat Hunt com privilégios de controle de acesso baseado em função (RBAC), e os usuários devem indicar quais indicadores específicos de comprometimento (IOC) desejam procurar.[72] Essa não é uma prática recomendada do setor.[73] Como o CyberSense, o Threat Hunt oferece suporte a conjuntos de arquivos de NAS, VMware, AHV e Hyper-V e aos servidores Linux e Windows.[74]

As seções abaixo apresentam mais detalhes sobre como a solução Rubrik oferece detecção de ameaças.

Metadados e estatísticas do file system

O modelo comportamental de ML do Rubrik Anomaly Detection registra as alterações no file system desde o último snapshot — como o número de arquivos adicionados, excluídos ou movidos — na forma de metadados.[75] Em seguida, há o treinamento de um modelo de ML com base nessas alterações para criar uma "linha de base" de modelo comportamental do file system. O Rubrik sinalizará um snapshot como anômalo se detectar muitas alterações. Depois que a análise comportamental sinalizar um snapshot, a solução iniciará uma análise do conteúdo de arquivos.[76] O monitoramento de metadados pode adicionar uma camada de segurança, mas pode não oferecer a proteção necessária para evitar ou reduzir o tempo de inatividade de um evento.

> *"O CyberSense não precisa de uma linha de base; ele monitora e analisa alterações de conteúdo de arquivos e bancos de dados a partir das primeiras cópias de backup."*

Por outro lado, **o CyberSense não precisa de uma linha de base; ele monitora e analisa alterações de conteúdo de arquivos e bancos de dados a partir das primeiras cópias de backup.** A abordagem do CyberSense oferece mais especificidade, pois o software analisa até mesmo partes de um arquivo ou páginas individuais de um banco de dados. Semelhante à solução Rubrik, as verificações do CyberSense incluem propriedades de metadados e alimentam os resultados no mecanismo de ML. Mas, ao contrário da solução Rubrik, o CyberSense não se limita à verificação de metadados, e a Index Engines treina o mecanismo de ML em ataques documentados pela Index Engines, não em assinaturas ou comportamentos anteriores do cliente.[77, 78]

Thresholds (Limites)

Durante a análise comportamental, o ML do Rubrik determina a probabilidade de ocorrer uma anomalia em um file system. Se a solução Rubrik achar provável, ela realizará a análise de conteúdo. Isso pode ser um limite de "comportamento anômalo" determinado pelo modelo comportamental. Por exemplo, a solução Rubrik pode sinalizar um comportamento anômalo quando vê muitos arquivos novos ou modificados, ou um aumento da aleatoriedade ou de indicadores de criptografia.[79] Durante a análise de conteúdo, o Rubrik Anomaly Detection exibe alterações no conteúdo de arquivos e calcula a probabilidade de criptografia, computando a entropia do file system. A entropia de um file system mostra a probabilidade de um ataque de ransomware ter arquivos criptografados. Se a entropia exceder um limite de anomalia, a solução alertará o usuário.[80, 81] A eficácia na detecção da corrupção dos dados depende do rigor do limite. A tolerância excessiva pode causar falsos negativos e, portanto, uma falsa percepção de segurança.[82] Os clientes devem definir os limites corretamente.

Por outro lado, o CyberSense verifica se há criptografia parcial de um arquivo, verificando o conteúdo do arquivo para proporcionar uma confiança de 99,99% (de acordo com a Dell e a Index Engines) na detecção de corrupção de dados.[83]

Assinaturas e extensões de arquivo

O Rubrik Threat Monitoring e o Threat Hunt verificam snapshots em busca de IOCs. Quando uma das várias fontes de Threat Intelligence que o Rubrik monitora detecta um novo IOC, o Threat Monitoring envia o feed de ameaças que contém regras de Yet Another Ridiculous Acronym (YARA) para identificação do novo malware, também conhecido como assinatura de malware, a todos os clusters do Rubrik. Em seguida, os clusters iniciam a verificação.[84] Um relatório recente da WatchGuard sugere que 57,8% dos malwares evitam a detecção de assinaturas. Malwares avançados, como BianLian, podem empregar métodos para escapar do reconhecimento de assinaturas, e as novas variantes de malware podem ter assinaturas ligeiramente diferentes das originais. Dessa forma, pode ser mais difícil manter a Threat Intelligence atualizada.[85]

Em comparação, o CyberSense usa mais de 200 mecanismos de lógica analítica e oferece um modelo de ML treinado em milhares de variantes de ransomware. A Index Engines provou que o método do CyberSense pode detectar variantes sofisticadas que, antes, não eram identificadas sem fazer download de assinaturas,[86] o que é outra vantagem de não depender da Internet durante um evento.

Eventos de criptografia em massa

A solução Rubrik monitora eventos de criptografia em massa calculando a entropia de todo o file system.[87] O CyberSense é muito mais específico. Além de verificar o file system em geral, ou até mesmo cada arquivo individual, ele também verifica partes do conteúdo interno dos arquivos. De acordo com a Index Engines, calcular a entropia em apenas um arquivo inteiro em vez de partes dele somente "detectará a criptografia extrema de todo o arquivo" ou eventos de criptografia em massa.[88]

Capacidade de recuperação

Com base na documentação, nós consideramos que a recuperação com o Dell PowerProtect Cyber Recovery é um processo mais objetivo e simplificado do que a recuperação com o Rubrik. Esta seção do relatório, inclusive suas subseções, contrastam os recursos de recuperação das duas soluções e como elas os implementam.

A documentação do Rubrik observa quais de seus recursos de recuperação funcionam para quais tipos de VM. Isso pode parecer oferecer um nível útil de especificidade, mas as muitas estipulações e variações tornam a recuperação complexa. Por exemplo, quando os clientes do Rubrik precisam recuperar dados, arquivos e sistemas, eles devem selecionar quais objetos de snapshot desejam incluir no plano de recuperação. Depois de criar um ou mais planos de recuperação, o Rubrik oferece muitas opções de capacidade de recuperação, como as seguintes:[89, 90, 91, 92, 93]

- Recuperar arquivos por meio de download ou substituição e recuperá-los em uma pasta separada, exportá-los para um host diferente ou exportá-los para um serviço em cluster
- Recuperar arquivos de VMs por meio de download ou substituição e recuperá-los em uma pasta separada ou exportá-los para outra máquina virtual
- Recuperação total de um snapshot de VM ou disco por meio das seguintes opções:
  - "Live Mount", que cria uma VM a partir do snapshot
  - "Mount virtual disks", que cria discos virtuais a partir do snapshot
  - "Instant recovery", que substitui a VM atual por uma nova VM criada pelo snapshot
  - "Export", que cria uma VM a partir do snapshot em um datastore selecionado
  - Recuperação de VMs em lote
- Recuperação cibernética em massa de planos de recuperação via "Live Mount" e "Export"
- Recuperação do Rubrik Security Cloud Orchestrated Application para fazer a recuperação de desastres de VM localmente, a um local remoto ou a um ambiente de teste isolado

A recuperação em lote do Rubrik demonstra ainda mais complexidade. A Tabela 1 mostra os recursos de recuperação em lote que o Rubrik oferece com base no hypervisor.[94]

Tabela 1: Recursos de recuperação em lote que o Rubrik oferece para diferentes hypervisors. Fonte: Rubrik.

Opções de criação de VM				
	Live Mount	**Live Mount com migração opcional**	**Exportar**	**Instant recovery**
VMs vSphere	Disponível, usa o cluster do Rubrik como datastore	Não disponível	Disponível, usa o datastore do hypervisor recuperado	Disponível, usa o cluster do Rubrik como datastore
VMs AHV	Disponível, usa o cluster do Rubrik como datastore	Disponível, usa o cluster do Rubrik como datastore e usa o contêiner Nutanix para todas as gravações subsequentes	Disponível, usa o contêiner Nutanix como datastore	Não disponível
Máquinas virtuais Hyper-V	Disponível, usa o cluster do Rubrik como datastore	Não disponível	Disponível, usa o datastore do hypervisor recuperado	Disponível, substitui a VM atual por uma nova do snapshot. Usa o cluster do Rubrik como datastore.

Na solução Rubrik, geralmente, o repositório de dados recuperados é o cluster do Rubrik, e não o ambiente de produção, o que pode causar problemas. Nós apresentamos esses problemas na próxima seção, "Rubrik limitations". Por outro lado, o PowerProtect pode colocar os dados recuperados em ambientes de produção ou de recuperação para proporcionar uma recuperação mais rápida e suave que pode minimizar o tempo de inatividade.

A Tabela 2 mostra informações adicionais da Rubrik sobre a recuperação de VMs vSphere.[95] Como mostra a tabela, a maioria dos datastores de recuperação do vSphere está no cluster do Rubrik.

Tabela 2: Recursos de recuperação que o Rubrik oferece para VMs vSphere. Fonte: Rubrik.

Recursos de recuperação que o Rubrik oferece para vSphere				
Ação	**Datastore**	**Estado de energia**	**Rede**	**VM de origem**
Recuperar arquivos	Não aplicável	Não aplicável	Não aplicável	Sem impacto
Live mount	Cluster local do Rubrik	Ativado ou desativado	Desconectado	Sem impacto
Mount virtual disks	Cluster local do Rubrik	Aceso	Desconectado	Sem impacto
Instant recovery	Cluster local do Rubrik	Aceso	Conectada (opcional)	Desligada e renomeada
Exportar	Datastore do hypervisor	Apagado	Desconectado	Sem impacto
In-place recovery	Datastore do hypervisor	Aceso	Igual à VM de origem	A opção "In-place recovery", que significa recuperação no local, substitui os arquivos de disco virtual da VM de origem pelos dados de disco virtual do snapshot, sem alterar as propriedades da VM

A solução Rubrik não implementa amplamente a recuperação em massa, cujas opções são limitadas e complexas. Como explica a seção "Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"" deste relatório, o Dell PowerProtect é simplificado e mais objetivo.

Desmascarando a restauração em massa

A Rubrik anuncia a recuperação em massa, que ela define como a restauração rápida das operações de negócios ao recuperar aplicativos, arquivos ou usuários em escala.[96] Ela oferece muitas opções para recuperação em massa. No entanto, a solução Rubrik geralmente armazena os dados recuperados no cluster do Rubrik, e não no ambiente de produção.[97] Até que a solução conclua a migração, as cargas de trabalho dependem da disponibilidade do sistema. O cluster local do Rubrik é um armazenamento de nível 3; assim, os clientes teriam que fazer uma migração adicional ao ambiente de produção para retornar aos níveis de desempenho planejados. Com esse ponto único de falha e com o desempenho reduzido enquanto o sistema conclui a migração, nós só poderemos considerar que houve a conclusão da recuperação quando a solução Rubrik restaurar as cargas de trabalho para o ambiente de produção.

O Dell PowerProtect também oferece recuperação em massa, permitindo que os usuários selecionem várias VMs para recuperação na IU correspondente.

O Dell PowerProtect Data Manager oferece o equivalente à "restauração em massa" da Rubrik

Em comparação com a solução Rubrik, a solução Dell também oferece várias opções equivalentes para recuperação de VMs vSphere. O Dell PowerProtect pode colocar os dados da VM em ambientes de produção ou de recuperação. A maioria das opções da Rubrik coloca os dados somente no cluster do Rubrik. A Tabela 3 mostra as opções para recuperação da Dell.[98, 99, 100,101]

Tabela 3: Opções para recuperação da Dell. Fonte: Principled Technologies.

Opções para recuperação da Dell	
Tipo	**Sobre o recurso**
Restauração em nível de arquivo	Restaura somente arquivos infectados no local ou por reversão
Live VM	Restaura uma VM para o cluster, com migração posterior para a produção
Restore to new	Restaura para o ambiente original ou um novo ambiente (por exemplo, um ambiente "limpo" ou uma infraestrutura de recuperação); durante a restauração, os usuários podem selecionar várias VMs de uma vez para uma restauração em massa ou em escala
Access/Live VM	Cria uma cópia isolada dos dados de produção
Orquestração de recuperação	Permite que os administradores agendem a recuperação ou a disponibilizem sob demanda; prioriza a recuperação automática de VMs para o ambiente de produção ou recuperação

Limitações do Rubrik

A solução Rubrik coloca em quarentena os snapshots infectados com malware para análise futura. No entanto, a solução Rubrik não coloca os snapshots em quarentena por padrão. Então, os clientes podem fazer download e realizar análises forenses manualmente ou com ferramentas de terceiros nos próprios arquivos em quarentena, o que possivelmente os expõe a malware.[102, 103]

> *O CyberSense realiza análises sem exigir que o usuário realize sua própria perícia, e o software automatiza a criação de pontos de restauração.*

Por padrão, o CyberSense analisa arquivos e bancos de dados. Os usuários não precisam colocar os snapshots em quarentena manualmente. **O CyberSense realiza análises sem exigir que o usuário realize sua própria perícia, e o software automatiza a criação de pontos de restauração.**[104]

O Rubrik RSC no modo de gerenciamento somente RSC é um ponto único de falha para muitos recursos. Algo mais preocupante ainda é que um ataque pode causar uma interrupção do serviço RSC e afetar a conectividade do usuário com a Internet ou a conectividade entre o local do usuário e o RSC. Após esses ataques, a solução oferecerá um conjunto limitado de recursos aos usuários, disponíveis por meio da IU do Rubrik CDM ou de automação baseada em API, mas apenas se os usuários criarem uma conta de serviço RSC antes do ataque.[105, 106] Uma organização pode recuperar as seguintes cargas de trabalho e dados sem o RSC: MongoDB, Microsoft Exchange, arquivos, snapshots do Hyper-V, Live Mount de volumes gerenciados, arquivos de host de NAS, Oracle, SQL Server, VCD e VMware.[107] A recuperação do SAP HANA sem o RSC requer ferramentas de terceiros, como Studio e Cockpit Cross, e o Suporte Rubrik por meio do túnel de suporte. A recuperação do IBM Db2 sem o RSC requer ferramentas de terceiros da IBM e o Suporte Rubrik também por meio do túnel de suporte.[108]

Air gap/isolamento

O NIST define air gap como "uma interface entre dois sistemas em que (a) eles não estão conectados fisicamente e (b) qualquer conexão lógica não é automatizada (ou seja, os dados são transferidos pela interface apenas manualmente, sob controle humano)".[109]

Os air gaps podem ajudar a controlar o fluxo de dados de uma origem para um destino e podem ser um componente importante de qualquer estratégia de recuperação cibernética e proteção contra ransomware. Se um ataque ou um evento comprometer os sistemas de backup de produção, a capacidade de impedir o tráfego dos sistemas de produção aos backups protegidos em seus cofres de recuperação cibernética pode atuar como um mecanismo de segurança.

Isolamento físico

Você pode ter visto um exemplo de uma solução fisicamente isolada no filme "Missão Impossível", em que o personagem principal tinha que contornar todos os outros recursos de segurança da instalação para acessar dados confidenciais em um sistema de computador que não estava conectado a uma rede externa. O isolamento físico também pode usar segmentos normalmente desconectados da rede física dedicada para transmitir cópias de backup dos sistemas de produção para o cofre. Quando desconectados, esses air gaps criam uma barreira física que os dados não podem cruzar automaticamente, o que dificulta o acesso por agentes mal-intencionados.

As organizações podem isolar fisicamente o Dell PowerProtect Cyber Recovery para ativar uma estratégia de air gap operacional. A solução usa uma conexão física dedicada e realiza a replicação de dados como uma operação de extração do cofre, e não como uma operação de envio a partir da solução de backup. Durante a cópia/replicação, a solução ativa a conexão, criptografa os dados e os migra pela linha dedicada.[110] Depois de concluir a replicação, a solução desativa a conexão novamente no lado do cofre. A solução torna as cópias do cofre imutáveis com políticas de retenção bloqueadas; assim, mesmo que um usuário ou um sistema obtenha acesso, ele não poderá modificar nem excluir as cópias do cofre. Nenhum tráfego de gerenciamento atravessa o caminho de replicação; portanto, **mesmo que os agentes mal-intencionados obtenham controle da solução de backup local, o cofre iniciará e desconectará o caminho de replicação e usará extrações unidirecionais somente de dados a partir da fonte de dados, limitando assim o acesso direto ao cofre.**[111]

Isolamento lógico

O isolamento lógico, por outro lado, usa sistemas que podem residir na mesma rede física, mas cria separação e controle lógicos de rede para garantir que os sistemas não possam enviar dados entre si. A solução usa implementações de segurança adicionais, como criptografia e hash, além de RBAC e autenticação baseada em vários fatores, para garantir que um sistema ou um usuário não autorizado não possa ler os dados que residem em outro sistema.

A Rubrik descreve seu recurso de recuperação cibernética como o aproveitamento de uma estratégia de air gap lógico.[112, 113] Muitas das declarações públicas disponíveis da Rubrik lançam dúvidas sobre a necessidade de air gaps. Uma apresentação da Rubrik intitulada "Rubrik Security – Air Gap and immutability" (Segurança da Rubrik: air gap e imutabilidade, em tradução livre) afirma que a solução nativa da empresa conta com air gap porque não há como acessar nem editar os backups depois que a solução os cria, mesmo que o equipamento Rubrik permaneça na rede física.[114] No entanto, um agente mal-intencionado e autenticado ainda poderia obter acesso à GUI do equipamento, o que poderia gerar ramificações para a recuperação. Para diminuir esse risco, a Rubrik tem bloqueios de retenção que impedem a expiração dos backups, o que os torna imutáveis. Após a ativação, os bloqueios de retenção também impedem que um cluster do Rubrik seja apagado e redefinido às configurações de fábrica. De acordo com o Guia de segurança do Rubrik CDM, a solução desativa globalmente os bloqueios de retenção do cluster por padrão e exige que os clientes entrem em contato com o Suporte Rubrik para ativá-los.[115] As fontes disponíveis publicamente não esclarecem se o Suporte Rubrik também pode desativar bloqueios de retenção, o que desperta o medo de que um agente mal-intencionado e autorizado ainda possa contornar as camadas de segurança.

> *"Nenhum tráfego de gerenciamento atravessa o caminho de replicação; portanto, mesmo que os agentes mal-intencionados obtenham controle da solução de backup local, o cofre iniciará e desconectará o caminho de replicação e usará extrações unidirecionais somente de dados a partir da fonte de dados, limitando assim o acesso direto ao cofre."*

Conclusão

As organizações devem considerar ativamente os diversos vetores de ataque em seus datacenters. Um bom plano de proteção de dados busca proteger todos os dados, especialmente os dados críticos e essenciais às operações. Nós analisamos as informações publicamente disponíveis sobre o Dell PowerProtect Cyber Recovery e o Rubrik Secure Cloud para ver como ambas as soluções abordam o gerenciamento, a proteção e a recuperação de dados.

O PowerProtect Cyber Recovery isola fisicamente as cópias de backup de dados essenciais em um cofre e garante a capacidade de recuperação delas em caso de um ataque cibernético. A solução emprega uma estratégia de air gap operacional com isolamento físico, algo que o Rubrik Secure Cloud não pode alegar que faz, pois a solução recorre ao isolamento lógico.

O Cyber Recovery usa a lógica analítica do CyberSense, que se baseia em ML, para avaliar a integridade dos dados no cofre e identificar dados limpos de backup para recuperação. O Rubrik Secure Cloud, por outro lado, oferece uma ferramenta de lógica analítica treinada em ML que procura anomalias, em vez de realizar verificações profundas nos arquivos.

Além disso, a solução Cyber Recovery oferece várias opções para recuperação, aproveitando os dados não comprometidos do cofre para promover um retorno eficiente e contínuo às operações. Em muitos casos, o PowerProtect Cyber Recovery pode oferecer recursos e vantagens que o Rubrik Secure Cloud não tem. Isso o torna uma solução possivelmente mais segura que pode fazer análises mais profundas para minimizar o tempo de inatividade e acelerar a recuperação.

---

1. Anastasia Dergacheva e Jesse R. Taylor, "Study Finds Average Cost of Data Breaches Continued to Rise in 2023", acessado em 25 de julho de 2024, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", acessado em 18 de abril de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
4. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation", acessado em 18 de abril de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
5. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation", acessado em 18 de abril de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
6. Rob Emsley, "Public Cloud Vault to Secure, Isolate and Recover Data", acessado em 20 de março de 2024, https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, "Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure", acessado em 20 de março de 2024, https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, "Cyber Recovery on Google Cloud Platform", acessado em 20 de março de 2024, https://infohub.delltechnologies.com/pt-br/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, "Up to $5m compensation if Rubrik Cloud Vault recovery busted", acessado em 20 de março de 2024, https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, "Frequently Asked Questions about Rubrik Cloud Vault", acessado em 20 de março de 2024, https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", acessado em 22 de março de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, "Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability", acessado em 7 de junho de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, "Consolidate Governance and Compliance Archive Data", acessado em 4 de abril de 2024, https://infohub.delltechnologies.com/pt-br/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", acessado em 24 de março de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, "Retention-locked SLA Domain attributes", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, "Rubrik Cyber Recovery", acessado em 20 de março de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, "Rubrik Licensing: Subscribe to Simplicity", acessado em 20 de março de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, "Workloads require third-party tools for recovery", acessado em 6 de maio de 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, "Recoverable workloads during RSC service disruption", acessado em 6 de maio de 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, "Workloads require third-party tools for recovery".
21. Dell, "Fortaleça sua postura de segurança com o Managed Detection and Response", acessado em 2 de abril de 2024, https://www.delltechnologies.com/asset/pt-br/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, "Guia de instalação do Dell PowerProtect Cyber Recovery 19.13" (em inglês), acessado em 20 de março de 2024, https://www.dell.com/support/manuals/pt-br/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=pt-br&lwp=rt.
23. Dell, "Guia de instalação do Dell PowerProtect Cyber Recovery 19.13" (em inglês).
24. Dell, "Guia de instalação do Dell PowerProtect Cyber Recovery 19.13" (em inglês).
25. Dell, "Installing CyberSense in Dell PowerProtect Cyber Recovery", acessado em 20 de março de 2024, https://infohub.delltechnologies.com/pt-br/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
27. Rubrik, "Downloading and installing Rubrik CDM", acessado em 20 de março de 2024, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, "Setting up a Rubrik cluster using the UI", acessado em 20 de março de 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, "Setting up a Rubrik cluster using the CLI", acessado em 20 de março de 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, "Registering Rubrik clusters using the online method", acessado em 20 de março de 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, "Registering Rubrik clusters using the offline method", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, "Enabling MFA", acessado em 21 de março de 2024, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.

33. Rubrik, "Adding the initial account", 21 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.
34. TrustRadius, "Learning Rubrik by putting the pieces together Brik by Brik", acessado em 21 de março de 2024, https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).
36. Index Engines, "CyberSense®: How it Works", acessado em 21 de março de 2024, https://www.indexengines.com/how-it-works.
37. Rubrik, "Anomaly event details", acessado em 21 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, "Events page", acessado em 21 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, "RSC Data Threat Analytics", acessado em 21 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, "RSC Data Threat Analytics".
41. Dell Technologies, "Dell PowerProtect Cyber Recovery: Reference Architecture", acessado em 6 de maio de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, "Dell EMC Avamar for Hyper-V", acessado em 16 de maio de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V", acessado em 16 de maio de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/technical-support/docu92011.pdf.
44. VMware, "Accelerate IT. Innovate with your cloud", 9 de maio de 2024, https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, "Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024", 17 de julho de 2024, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik, "RSC Data Threat Analytics".
47. Dell Technologies, " CyberSense® para PowerProtect Cyber Recovery ", acessado em 27 de junho de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik, "RSC Data Threat Analytics".
49. Index Engines, "CyberSense® Support Matrix", acessado em 21 de março de 2024, https://www.indexengines.com/csmatrix.
50. Dell Technologies, "CyberSense® para PowerProtect Cyber Recovery".
51. Rubrik, "Keep Your Databases Running in the Face of Any Threat".
52. Index Engines, "CyberSense® Support Matrix".
53. Dell Technologies, "Dell EMC Avamar for Hyper-V".
54. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V".
55. Rubrik, "Anomaly incidents", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, "Data Threat Analytics events", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, "Viewing Anomaly Detection", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, "VM Encryption Detection", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, "Viewing the Threat Monitoring page", 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, "Initiating a threat hunt", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, "Quarantining matched files or objects", acessado em 2 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, "CyberSense® para PowerProtect Cyber Recovery".
63. Dell, "CyberSense® para PowerProtect Cyber Recovery".
64. Index Engines, "The Power of CyberSense's Machine Learning", acessado em 2 de abril de 2024, https://go.indexengines.com/csmachinelearning.
65. Index Engines, "The Power of CyberSense's Machine Learning".
66. Index Engines, "The Power of CyberSense's Machine Learning".
67. Dell, "CyberSense® para PowerProtect Cyber Recovery".
68. Rubrik, "Anomaly Detection behavioral model", acessado em 20 de maio de 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.

69. Amazon, "Modelos de ML de treinamento", acessado em 2 de abril de 2024,https://docs.aws.amazon.com/pt_br/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, "Defense in Depth with Polaris Radar", acessado em 21 de março de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, "Data Threat Analytics Dashboard", acessado em 21 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, "Initiating a threat hunt", acessado em 21 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, "What Is A Malware File Signature (And How Does It Work)?", acessado em 4 de abril de 2024, https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.
74. Rubrik, "Threat hunts", acessado em 21 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, "Anomaly Detection Features", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, "Behavioral model".
77. Index Engines, "The Power of CyberSense's Machine Learning".
78. Dell, "CyberSense® para PowerProtect Cyber Recovery".
79. Rubrik, "Behavioral model".
80. Rubrik, "Anomaly Detection features".
81. Rubrik, "Behavioral model".
82. Dell, "CyberSense® para PowerProtect Cyber Recovery".
83. Morningstar, "Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery", acessado em 17 de julho de 2024, https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.
84. Rubrik, "Threat Monitoring", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, "The Power of CyberSense's Machine Learning".
86. Index Engines, "The Power of CyberSense's Machine Learning".
87. Rubrik, "Anomaly Detection Features", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, "The Power of CyberSense's Machine Learning".
89. Rubrik, "Investigating and recovering anomalous files for filesets", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, "Investigating and recovering anomalous files for virtual machines", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, "Full snapshot recovery of a virtual machine", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, "Recovery of a batch of virtual machines", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, "Performing bulk recovery for Recovery Plans", acessado em 22 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html.
94. Rubrik, "Recovery of a batch of virtual machines", acessado em 4 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, "Recovery of virtual machines", acessado em 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. O repositório de dados recuperados é geralmente o cluster do Rubrik, e não o ambiente de produção.
97. Rubrik, "Recovery of a batch of virtual machines", acessado em 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, "Restore plan", acessado em 16 de abril de 2024, https://infohub.delltechnologies.com/pt-br/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.
99. Dell, "PowerProtect Data Manager overview", acessado em 16 de abril de 2024, https://infohub.delltechnologies.com/pt-br/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.
100. Dell, "Guia do usuário e de administração do PowerProtect Data Manager 19.9" (em inglês), acessado em 16 de abril de 2024, https://www.dell.com/support/manuals/pt-br/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, "Recovery Orchestration with PowerProtect Data Manager Overview", acessado em 16 de abril de 2024, https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, "Quarantine files or objects", 24 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/quarantine.html.
103. Rubrik, "Downloading quarantined files for forensic analysis", 24 de março de 2024, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.

104. Forrester, "The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery", acessado em 16 de abril de 2024, https://www.delltechnologies.com/asset/pt-br/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.

105. Rubrik, "Workload recovery during an RSC service disruption", acessado em 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.

106. Rubrik, "Rubrik CDM APIs and service account workflows", acessado em 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.

107. Rubrik, "Recoverable workloads during RSC service disruption", acessado em 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.

108. Rubrik, "Workloads require third-party tools for recovery", acessado em 16 de abril de 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, "Computer Security Resource Center Glossary: air gap", acessado em 29 de julho de 2024, https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, "Guia da solução Dell PowerProtect Cyber Recovery" (em inglês).

111. Dell, "Dell PowerProtect Cyber Recovery: Reference Architecture".

112. Adam Eckerle, "Debunking the Myths about Air Gaps", acessado em 14 de março de 2024, https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, "Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value", acessado em 14 de março de 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, "Rubrik Air Gap and Immutability", acessado em 14 de março de 2024, https://vimeo.com/561870246.

115. Rubrik, "Retention locks in the Rubrik cluster", acessado em 18 de março de 2024, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

▶ Consulte a versão original em inglês deste relatório

Este projeto foi encomendado por Dell Technologies.

Principled Technologies®

Facts matter.®