kyndryl

Resiliency Orchestration with Cyber Incident Recovery

Resiliência cibernética para recuperação rápida, confiável e escalonável em ambientes híbridos de multicloud

Índice

O momento atual requer rápidas mudanças

Quanto mais seus dados e aplicativos transitam em uma infraestrutura cada vez mais interconectada on-premises, nuvem pública e multicloud, maiores são as possibilidades para que os ataques cibernéticos interrompam a continuidade de seus negócios. A natureza complexa dos ambientes hibridos emulticloud expõe seus dados importantes e configurações de sistema, a níveis de risco mais altos do que antes, tanto que a probabilidade de um ataque cibernético tornou-se uma certeza inquestionável. Não importa o nível de vigilância de sua equipe de segurança de TI, um ataque cibernético acabará levando a uma interrupção dos negócios através de uma indisponibilidade, um roubo ou dados corrompidos, causando danos à reputação da empresa e perdas financeiras.

Em um passado não muito distante, as soluções tradicionais de recuperação de desastre conseguiam ajudar a mitigar os danos da maioria dos ataques cibernéticos convencionais. Mas isso foi muito antes de os ambientes multicloud híbridos se tornarem uma realidade. Embora as infraestruturas de TI tenham crescido em complexidade, os ataques cibernéticos também se tornaram mais sofisticados. A criptografia de dados e os ataques de malware agora estão sendo projetados de maneiras que antes eram inimagináveis, tendo também como alvo backups de dados. Como resultado, esses ataques estão obtendo acesso aos locais de backup e de recuperação de desastres, deixando os dados primários e os de backup inutilizáveis, além de atrasar significativamente a capacidade de restauração das operações essenciais de produção.

O Kyndryl Resiliency Orchestration with Cyber Incident Recovery minimiza o impacto de ataques cibernéticos nos negócios com uma recuperação rápida, confiável e escalonável em ambientes multicloud híbridos.

Cyber Recovery para um mundo de multicloud híbrida
O Kyndryl™ Resiliency Orchestration with Cyber Incident Recovery pode recuperar seus dados e suas configurações de plataforma, de forma rápidano caso de uma indisponibilidade cibernética. Ele fornece automação inteligente dos fluxos de trabalho de proteção de dados e de recuperação de desastres, além de permitir testes de recuperação, imutabilidade de dados, detecção de anomalias, monitoramento, gerenciamento e relatórios em ambientes multicloud híbridos A solução oferece recuperação de ataques cibernéticos automatizada, confiável e rápida de workloads físicos e virtuais, incluindo processos de negócios, aplicações, sistemas e bancos de dados.

A solução Cyber Incident Recovery fornece:
- Capacidade de teste fácil que não afeta os ambientes de produção
- Detecção mais rápida de corrupção de dados e resposta rápida para reduzir o tempo de inatividade
- Recuperação point-in-time eficiente que otimiza os objetivos do ponto de recuperação (RPOs)
- Escalabilidade para lidar com detecção e recuperação, no nível do site em minutos
- Visibilidade e relatórios simplificados para ajudar a atender aos requisitos de regulamentações

O Kyndryl Resiliency Orchestration with Cyber Incident Recovery oferece recuperação de ataques cibernéticos automatizado, confiável e rápida de workloads físicos e digitais.

Uma arquitetura que permite uma abordagem ágil voltada para resiliência cibernética

Os blocos de construção de tecnologia que compõem o recurso Cyber Incident Recovery fornecem uma plataforma que abrange as camadas de computação e dados de ambientes de produção e recuperação de desastres. Isso permite uma abordagem ágil para recuperação de workloads virtuais e físicas.

Armazenamento inalterável
O uso de tecnologia de armazenamento inalterável para dados de configuração ou armazenamento WORM (write-once-read-many) para dados de aplicativos ajuda a prevenir que não sejam corrompidos e permitam a capacidade de recuperação, não deixando que sejam feitas mudanças nos backups depois de salvos. Para dados de aplicações, essa abordagem também ajuda a reduzir seus custos de armazenamento, gravando apenas novas cópias point-in-time de mudanças incrementais.

Air-gapped protection
O isolamento de rede separa os ambientes de produção do armazenamento WORM, que contém os dados protegidos de backup em um local remoto ou de recuperação de desastre (DR). O acesso ao armazenamento WORM também é restrito apenas aos momentos em que os dados estão disponíveis para backup. Essa abordagem, combinada com armazenamento inalterável, ajuda a evitar que dados protegidos sejam corrompidos por malwares que pode transitar pela rede ou que sejam projetados especificamente para direcionar dados de backup.

Detecção de anomalia
O Kyndryl Resiliency Orchestration inclui um recurso de detecção de anomalias, que usa identificação heurística, suportada pela inteligência artificial (IA). Ele é treinado em diferentes padrões de mudança de malwares conhecidos - capturando e comparando os padrões de mudança nos dados de backup - para prever as anomalias de dados com alta precisão. Esse recurso de detecção de anomalias no site de recuperação (DR) ajuda a identificar capturas instantâneas de backup anômalos e restaurar a partir de cópias limpas.

Verificação de dados de configuração
Este componente usa o recurso integrado de detecção de anomalias baseado em IA para ajudar a garantir que a configuração ou os dados protegidos sejam limpos e recuperáveis. O processo, integrado ao Resiliency Orchestration, detecta automaticamente quando as configurações do sistema são modificadas. O Resiliency Orchestration também se integra com scripts para validação de aplicativos, fornecidos pelo cliente, para realizar testes em nível de aplicação e de dados.

Automação e orquestração
Ao automatizar o processo de recuperação completo para dados e aplicações, o Resiliency Orchestration permite a restauração rápida de seu ambiente de TI. O Resiliency Orchestration substitui os processos manuais tradicionais por fluxos de trabalho predeterminados, que foram testados e validados, permitindo recuperar completamente um processo de negócios, aplicação, banco de dados ou sistema discreto, com o clique de um botão. Esses fluxos de trabalho orquestram as várias etapas necessárias para recuperar sistemas e dados interconectados, reduzindo o erro humano. O Resiliency Orchestration ajuda a acelerar a implementação da solução, aproveitando uma extensa biblioteca de mais de 800 padrões predefinidos, que podem ser combinados para criar fluxos de trabalho.

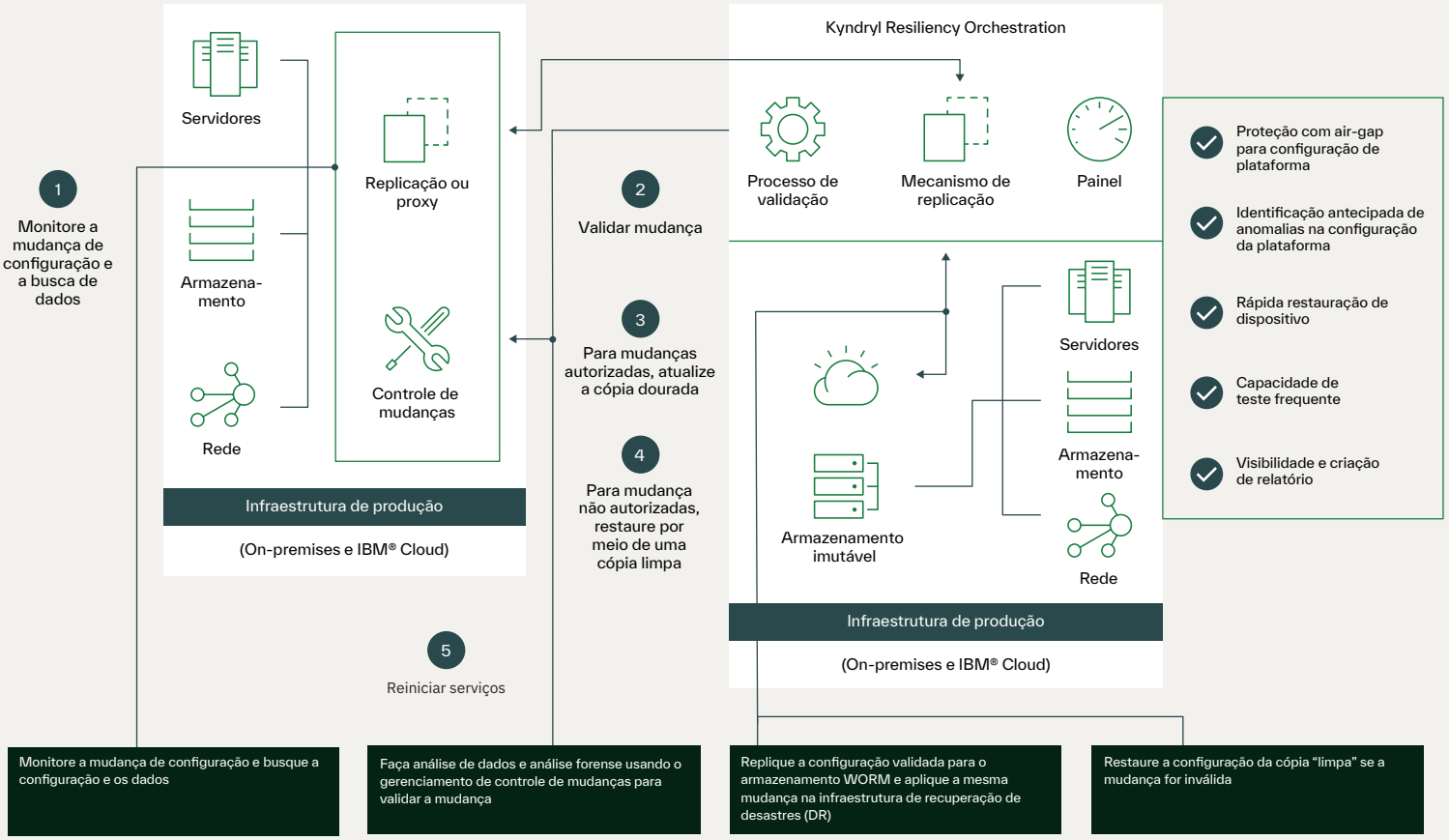
Cyber Incident Recovery for platform configuration

Um malware geralmente altera as configurações antes de corromper os próprios dados, portanto, é fundamental detectar qualquer alteração na configuração, antes que os dados atuais sejam infectados. O recurso de configuração de plataforma do Cyber Incident Recovery protege os dados de configuração de workloads virtuais e físicos, aplicações, sistemas de armazenamento e dispositivos de rede em ambientes on-premises, nuvem pública, nuvem híbrida e multicloud.

Manter os negócios disponíveis com uma "cópia dourada"
Este componente usa as tecnologias integradas para identificar qualquer mudança nas configurações do end-point de produção e alerta o usuário sobre qualquer mudança autorizada e não autorizada. Os alertas também podem fornecer chamados relevantes do software de gerenciamento de controle de mudanças. Para permitir a restauração rápida de serviços, o Cyber Incident Recovery replica uma "cópia dourada" dos dados de configuração do servidor e do dispositivo de armazenamento,protegido por air-gap.

Responder a mudanças de configuração inválidas e válidas
No caso de uma alteração válida, os dados de configuração são protegidos pela replicação de uma nova "cópia dourada" para um armazenamento inalterável. Se uma alteração inválida for identificada, a última cópia limpa das configurações do dispositivo é rapidamente restaurada para a infraestrutura de produção pelo Resiliency Orchestration, com base em políticas preestabelecidas e com o consentimento de gerenciamento apropriado. As configurações de máquina virtual e dedicada são restauradas em uma infraestrutura de produção limpa. No caso de alterações válidas, uma nova "cópia dourada" é criada em um armazenamento inalterável.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery for Platform Configuration



*Air-gap não suportado para armazenamento inalterável hospedado na nuvem

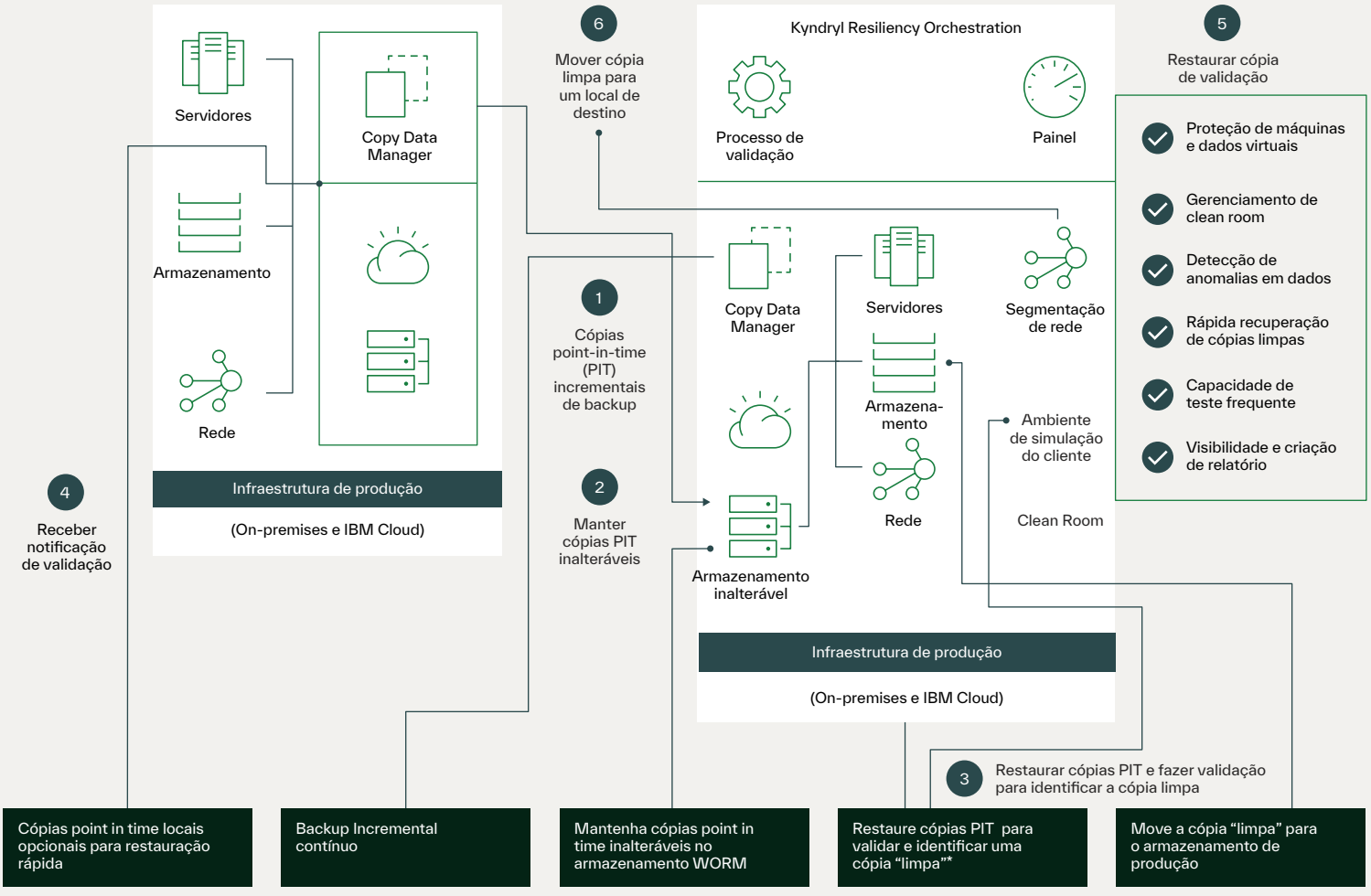
Cyber Incident Recovery for data

O recurso de dados do Cyber Incident Recovery permite uma recuperação rápida, e altamente confiável, contra ataques cibernéticos que corrompem os próprios dados. Ele protege os dados por meio do uso de proteção de air-gap e armazenamento inalter[ável enquanto orquestra a recuperação rápida no local de recuperação de desastres.

Protegendo grandes volumes de dados em todos os ambientes
O Cyber Incident Recovery é projetado para lidar com grandes volumes de dados de aplicativos, não importa onde esses dados estejam. Ele emprega tecnologia de gerenciamento de dados de cópia para criar e manter cópias incrementais de dados point-in-time (PIT). Como essas cópias são mantidas em um armazenamento inalterável, como armazenamento de objeto em nuvem ou armazenamento com recurso WORM, elas são cópias "eternas" que não podem ser alteradas. O software de gerenciamento de dados de cópia replica os dados para uma recuperação de desastre ou local alternativo, criando as cópias PIT. As cópias PIT também podem ser feitas e armazenadas no local de produção, dessa forma, se tornam um recurso de restauração rápida.

Responder rapidamente a ataques cibernéticos para manter a continuidade dos negócios
Quando um gerente de recuperação de desastre recebe uma notificação de que uma violação de dados ou uma infecção por malware de criptografia foi descoberta, o teste automatizado de cópias PIT é executado no site de recuperação de desastre para verificar a capacidade de recuperação dos dados. A última cópia "limpa" identificada pelo processo de teste e verificação é então recuperada na infraestrutura de recuperação de desastre pelo software Resiliency Orchestration. Os testes também podem ser realizados com frequência no site de recuperação de desastre, ajudando a garantir a capacidade de recuperação dos dados sem afetar as operações de negócios.
O Resiliency Orchestration ajuda a garantir que as plataformas possam ser recuperadas rapidamente, em paralelo.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery for Data



Painéis e relatórios que simplificam o gerenciamento

O Cyber Incident Recovery inclui um painel que simplifica o gerenciamento de recuperação cibernética e o monitoramento de mudanças na configuração da plataforma e mudanças de dados. Ele fornece visibilidade em tempo real de RPO e desvios de objetivo de tempo de recuperação (RTO), status de validação de captura instantânea e atualizações críticas de recuperação cibernética.

Enquanto isso, a alta administração ou o conselho de administração podem receber atualizações críticas de recuperação cibernética, em tempo real, para uma tomada de decisão mais rápida e informada.

Melhor rastreamento de vulnerabilidades e maior visibilidade
O painel do Cyber Incident Recovery informa o número de vulnerabilidades em seus ambientes, junto com o nível de gravidade de cada uma.
É possível rastrear vulnerabilidades abertas e tomar decisões informadas pela visibilidade de desvio de RPO cibernético, desvio de RTO cibernético, status de validação de captura instantânea e prontidão cibernética atual.

Robusta funcionalidade de relatório
O módulo de relatório integrado oferece um rico conjunto de relatórios, incluindo resiliência cibernética ou postura de recuperação de desastres, que podem ser exportados e compartilhados com os reguladores para fins de conformidade, junto com gráficos capturados durante as operações normais de negócios.

O Cyber Incident Recovery fornece visibilidade em tempo real de desvios de RPO e RTO, status de validação de captura instantânea e atualizações críticas

A solução de Business Resilience Services da Kyndryl conta com décadas de experiência ajudando clientes em todo o mundo com suas necessidades de backup e recuperação.

Diferenciais da Kyndryl
- Conhecimento de todo o ciclo de vida de resiliência
- Recuperação automatizada de workloads físicos, virtuais e em nuvem
- Mais de 800 padrões predefinidos para implementação mais rápidas, eficientes e escalabilidade
- Escolha de nuvens, incluindo AWS, Azure e IBM Cloud, para escalabilidade corporativa

Confiabilidade
- Mais de 9.000 clientes estão protegidos com os serviços de recuperação de desastre e gerenciamento de dados da Kyndryl
- A Kyndryl conta com mais de 3,5 exabytes em backups anuais e sob gerenciamento

Uma pesquisa global
- Há mais de 300 Kyndryl Resiliency Centers em mais de 50 países ao redor do mundo
- A Kyndryl dedica mais de 6.000 profissionais em todo o mundo à resiliência

Por que escolher a Kyndryl?

A Kyndryl tem grande experiência em desenhar, implementar e gerenciar infraestruturas tecnológicas complexas, agregando o que há de mais moderno, eficiente e seguro às operações de nossos clientes. Estamos empenhados em desenvolver a infraestrutura essencial, capaz de impulsionar o progresso humano. Estamos construindo nossa base de excelência, criando sistemas com soluções atuais: trazendo as alianças estratégicas , investindo em nosso negócio e trabalhando junto com nossos clientes para ampliar seu potencial.

Pronto para saber mais?

Para saber mais sobre o que o Kyndryl Resiliency Orchestration with Cyber Incident Recovery pode fazer por você, entre em contato com seu representante Kyndryl ou acesse www.kyndryl.com

kyndryl

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP Brasil

Produzido nos Estados Unidos da América
Julho de 2021