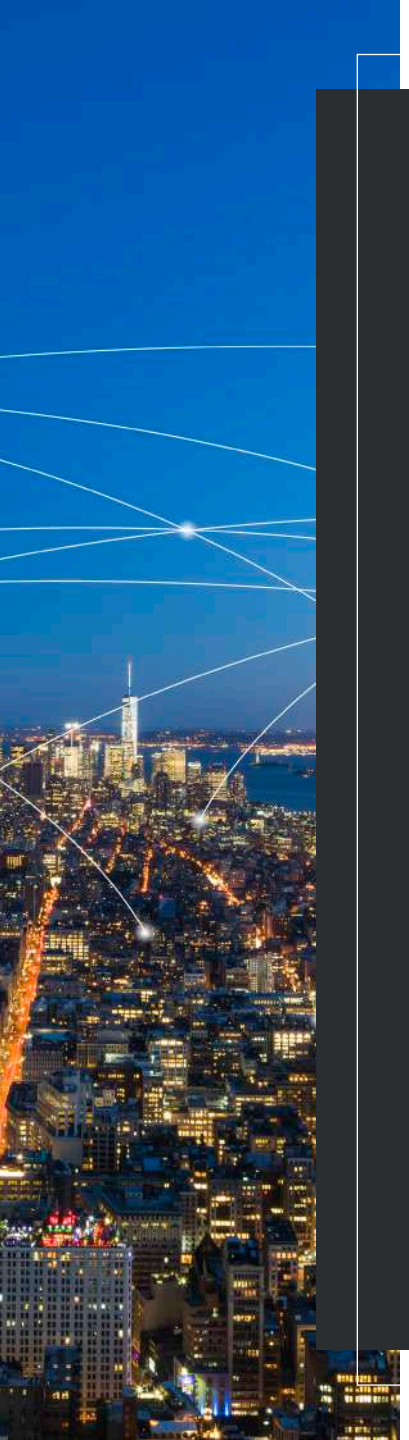
IBM **Global**
Technology Services

Resumo da solução

IBM Resiliency Orchestration com o Cyber Incident Recovery

Proteja os dados e as configurações da plataforma com um recurso criado com um objetivo específico que permite uma recuperação rápida, confiável e dimensionável após ciberataques

IBM®



Destaques

- Armazenamento imutável e com implementação air gap para dados e arquivos de configuração da plataforma
- Detecção rápida de anomalias nas configurações do sistema Windows ou Linux, incluindo o registro do Windows, as configurações de aplicativos e dispositivos
- A restauração rápida e orquestrada de dados e configurações da plataforma ajuda a reduzir o impacto da interrupção causada por um ciberataque ou por qualquer outra indisponibilidade
- A plataforma automatizada de testes e verificação permite a realização de testes frequentes sem afetar os sistemas da empresa
- A visibilidade do processo e os relatórios ajudam a atender aos requisitos de compliance

Os ciberataques continuam a incomodar organizações de todos os tamanhos. Embora as equipes de segurança de TI estejam melhorando a capacidade de prevenir a ocorrência de ciberataques, a questão continua sendo “quando” ocorrerá um ataque (caso ainda não tenha ocorrido) em vez de “se” ocorrerá um ataque. Uma interrupção nos negócios causada por ciberataques corrompendo configurações e dados críticos dos sistemas pode ser tão prejudicial para a reputação e o bem-estar financeiro da organização quanto o furto de dados ou uma indisponibilidade total de TI.

Isso se aplica principalmente quando os ciberataques envolvem a criptografia de dados ou malwares direcionados especificamente aos backups de dados. A exposição contínua da rede aos locais de backup e recuperação de desastre (RD) pode dar uma oportunidade para que o malware distorça ou criptografe esses dados, deixando os dados primários e os de backup inutilizáveis, atrasando significativamente a capacidade de retomar as operações no nível da produção.

Geralmente, o dano ocorre porque as soluções de recuperação de desastres existentes não são projetadas para a recuperação de ocorrências cibernéticas ou sofrem com problemas persistentes voltados aos recursos de recuperação de desastres: dependência excessiva de processos manuais, runbooks desatualizados e testes inadequados. O resultado é que a recuperação demora muito, os pontos de recuperação de dados são muito antigos ou a própria recuperação falha.

Recurso desenvolvido especificamente para resiliência cibernética

O Cyber Incident Recovery, desenvolvido com o IBM® Resiliency Orchestration, foi projetado para recuperar dados e configurações da plataforma com extrema rapidez em caso de indisponibilidade cibernética. Criado com um objetivo específico para recuperação cibernética, o Cyber Incident Recovery oferece:

- Recurso de testes fáceis que não afeta os ambientes de produção
- Detecção rápida de distorção de dados e resposta rápida para reduzir o tempo de inatividade
- Recuperação pontual eficiente que otimiza os objetivos de ponto de recuperação (RPO)
- Escalabilidade para lidar com a detecção e a recuperação em grande escala, em todas as instalações, em minutos
- Visibilidade e relatórios simplificados para ajudar a atender aos requisitos regulamentares

Os blocos de construção da tecnologia que compõem o recurso Cyber Incident Recovery oferecem uma plataforma que abrange as camadas de dados e de computação de ambientes de produção e de recuperação de desastres, permitindo uma abordagem Agile para recuperação de desastre cibernético. Essa arquitetura inclui:

Armazenamento imutável. O uso da tecnologia de armazenamento inalterável para dados de configuração ou para o armazenamento write-once-read-many (WORM) de dados de aplicativo ajuda a prevenir a distorção e propicia a capacidade de recuperação por não permitir que sejam feitas mudanças nos backups depois que eles são salvos. Para os

dados de aplicativo, essa abordagem também ajuda a reduzir os custos de armazenamento por gravar somente as novas cópias de mudanças incrementais em momentos específicos.

Proteção com implementação air gap. O isolamento de rede separa os ambientes de produção do armazenamento WORM que contém os dados de backup protegidos remotos ou em no local de recuperação de desastres. O acesso ao armazenamento WORM também é restrito somente aos momentos em que os dados estão disponíveis para backup. Essa abordagem, combinada com o armazenamento imutável, ajuda a prevenir que os dados protegidos sejam distorcidos por malwares que conseguem atravessar redes ou que são projetados especificamente para atacar dados de backup.

Verificação de dados de configuração. Esse componente ajuda a possibilita que a configuração ou os dados que estão sendo protegidos estejam limpos e recuperáveis. Esse processo, integrado ao Resiliency Orchestration, detectará automaticamente quando as configurações do sistema forem modificadas e não correspondem às versões "reais". O Resiliency Orchestration também será integrado aos scripts de validade de aplicativo fornecidos pelo cliente para oferecer testes no nível do aplicativo e dos dados.

Automação e orquestração. Com a automatização do processo completo de recuperação de dados, de aplicativos, de comutadores e da infraestrutura de computação, o Resiliency Orchestration permite a restauração rápida do ambiente de TI. O Resiliency Orchestration substitui os processos manuais tradicionais por fluxos de trabalho pré-determinados que já foram testados e validados, para que baste clicar em um botão para recuperar um processo de negócios, um aplicativo, um banco de dados ou um sistema discreto inteiro. Esses fluxos de trabalho orquestram as diversas etapas necessárias para recuperar sistemas e dados interconectados, limitando o erro humano. O Resiliency Orchestration ajuda a acelerar a implementação da solução por utilizar uma ampla biblioteca com mais de 450 padrões predefinidos que podem ser combinados para criar fluxos de trabalho.

Cyber Incident Recovery para configuração de plataforma

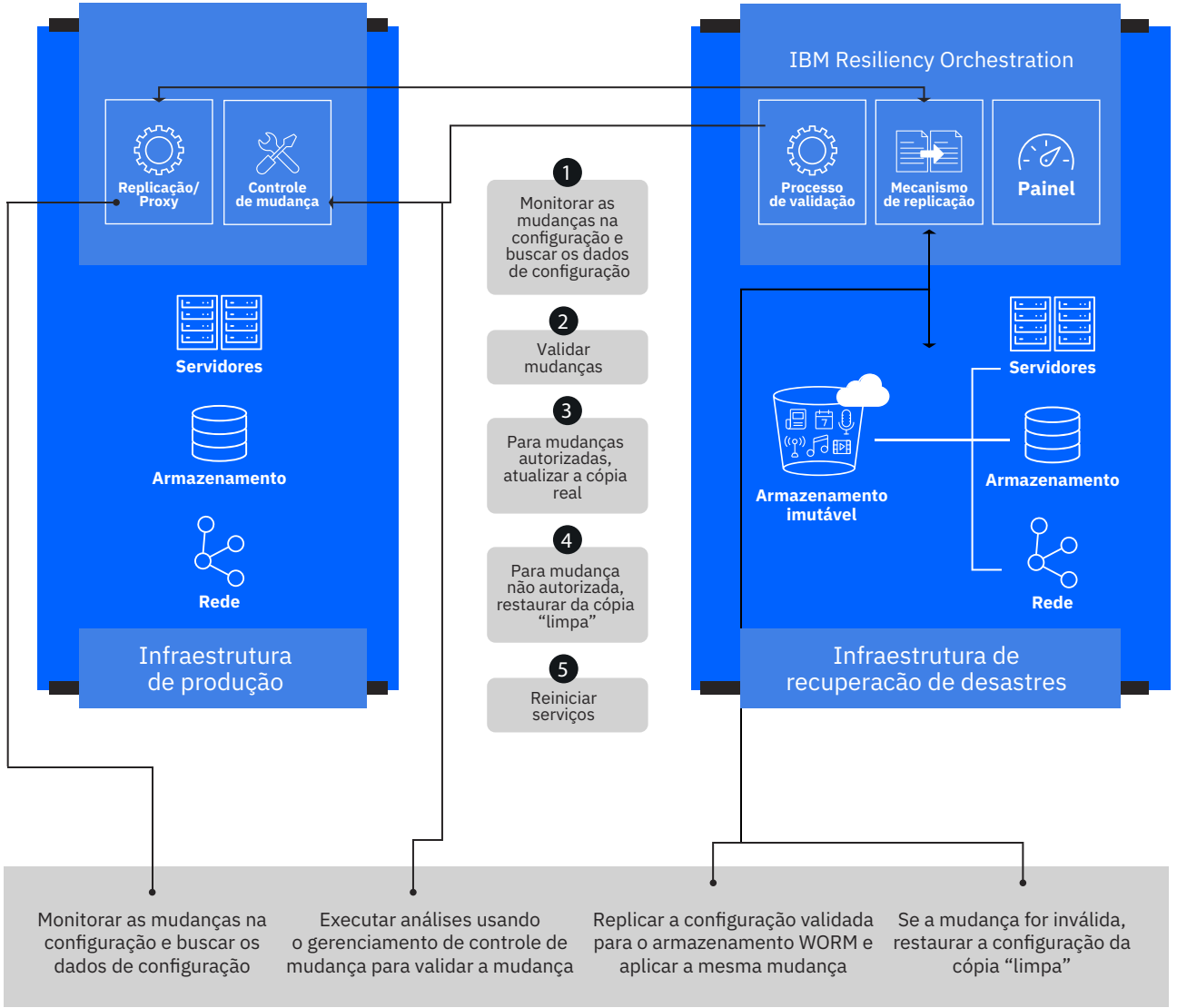
Para fazer negócios de forma ininterrupta é necessário contar com a disponibilidade contínua da infraestrutura de TI de base dos aplicativos críticos para os negócios: os servidores físicos, as instâncias de VM, os sistemas de armazenamento e os dispositivos de rede. Os ciberataques podem paralisar os negócios distorcendo os dados de configuração dessas plataformas.

O recurso de configuração de plataforma do Cyber Incident Recovery (veja Figura 1) permite a recuperação rápida dos serviços replicando uma “cópia real” dos dados de configuração do servidor e do dispositivo para o armazenamento imutável protegido com implementação air gap em um armazenamento de objetos em nuvem ou no data center da IBM. Os dispositivos de produção são examinados para detectar mudanças nos dados de configuração. O sistema analisa a mudança para determinar se ela é válida e fornece alertas quando detecta uma mudança suspeita nos dados de configuração. Os alertas também podem fornecer chamados relevantes do software de gerenciamento de controle de mudança.

No caso de uma mudança válida, os dados de configuração são protegidos pela replicação de uma nova “cópia real” para o armazenamento imutável. Se uma mudança inválida for identificada, a cópia limpa mais recente das configurações do dispositivo será restaurada rapidamente para a infraestrutura de produção pelo Resiliency Orchestration, com base nas políticas pré-estabelecidas e com o consentimento adequado do gerenciamento. As configurações dedicadas e de máquina virtual são restauradas para uma infraestrutura de produção limpa.

Cyber Incident Recovery para configuração de plataforma

Figura 1: O Cyber Incident Recovery para configuração de plataforma ajuda a proteger os dados de configuração de servidores físicos e virtuais, além de dispositivos de armazenamento e de rede.



Cyber Incident Recovery para dados

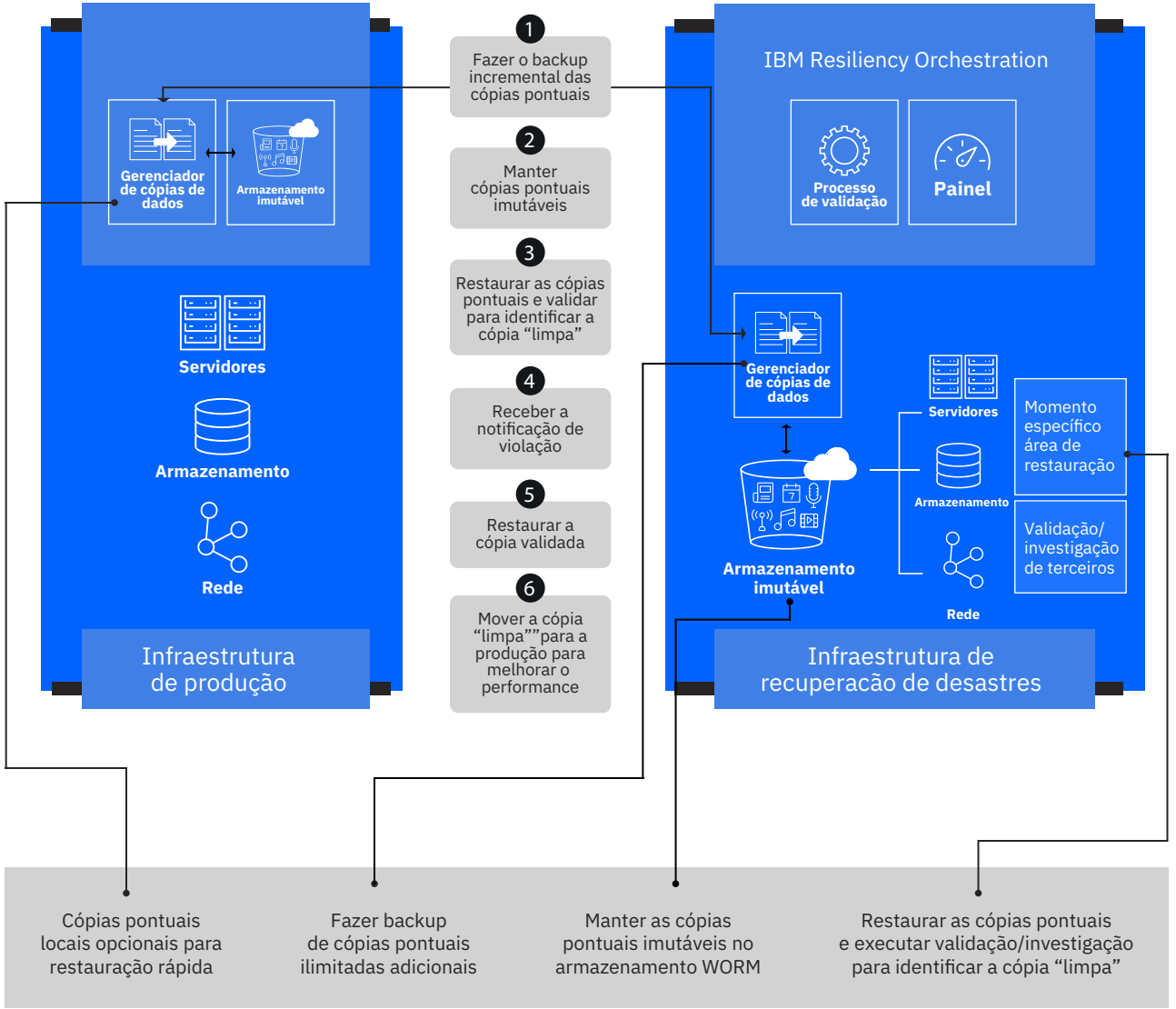
O recurso de dados do Cyber Incident Recovery permite uma recuperação rápida e altamente confiável após ciberataques que distorcem dados. Ele protege os dados usando a proteção com implementação air gap e o armazenamento imutável, além de orquestrar a recuperação rápida nas instalações de recuperação de desastres do cliente.

O Cyber Incident Recovery para dados oferece o backup eficiente de grandes volumes de dados com testes sem interrupção e restauração rápida. O Cyber Incident Recovery foi projetado para lidar com grandes volumes de dados de aplicativo. Ele emprega a tecnologia de gerenciamento de cópia de dados para criar e manter cópias de dados incrementais de momentos específicos. Como essas cópias são mantidas em um armazenamento imutável, como o armazenamento de objetos em nuvem ou o armazenamento com o recurso WORM, elas são cópias “perenes” que não podem ser alteradas. Como é mostrado na Figura 2, o software de gerenciamento de cópia de dados replica dados para instalações de Recuperação de Desastre ou para outras instalações, criando cópias pontuais. Opcionalmente, as cópias pontuais também podem ser feitas e armazenadas nas instalações de produção para permitir a restauração rápida.

Quando um gerenciador de Recuperação de Desastre recebe uma notificação de que foi descoberta uma violação de dados ou uma infecção por malware de criptografia, são realizados testes automatizados das cópias pontuais nas instalações de Recuperação de Desastres (RD) para verificar a capacidade de recuperação dos dados. Em seguida, a cópia “limpa” mais recente identificada pelo processo de teste e verificação é recuperada na infraestrutura de RD pelo processo rápido de

recuperação do software do gerenciador de cópia de dados. Os testes também podem ser realizados com frequência nas instalações de RD, ajudando a assegurar a capacidade de recuperação de dados sem afetar as operações de negócios. O Resiliency Orchestration ajuda a possibilitar que as plataformas possam ser recuperadas rapidamente, em paralelo.

Figura 2: O Cyber Incident Recovery para dados oferece o backup eficiente de grandes volumes de dados com testes sem interrupção e restauração rápida.



Os painéis e relatórios simplificam o gerenciamento

O Cyber Incident Recovery inclui um recurso de painel (veja Figura 3) que ajuda no monitoramento de mudanças na configuração da plataforma e de mudanças nos dados. Ele também pode fornecer atualizações de recuperação cibernética críticas em tempo real à gerência sênior ou aos diretores, permitindo que eles tomem decisões conscientes rapidamente.

Um painel de incidente cibernético oferece detalhes como o número de vulnerabilidades e o nível de gravidade e permite o rastreamento de vulnerabilidades abertas. Um painel de dados cibernéticos oferece visibilidade do desvio de RPO cibernético, do desvio de RTO cibernético, do status de validação de captura instantânea e da preparação cibernética atual.

O módulo de relatório integrado oferece um rico conjunto de relatórios, incluindo a situação de resiliência cibernética ou de RD, que podem ser exportados e compartilhados com os órgãos regulamentares para questões de conformidade, juntamente com gráficos capturados durante as operações de negócios normais.

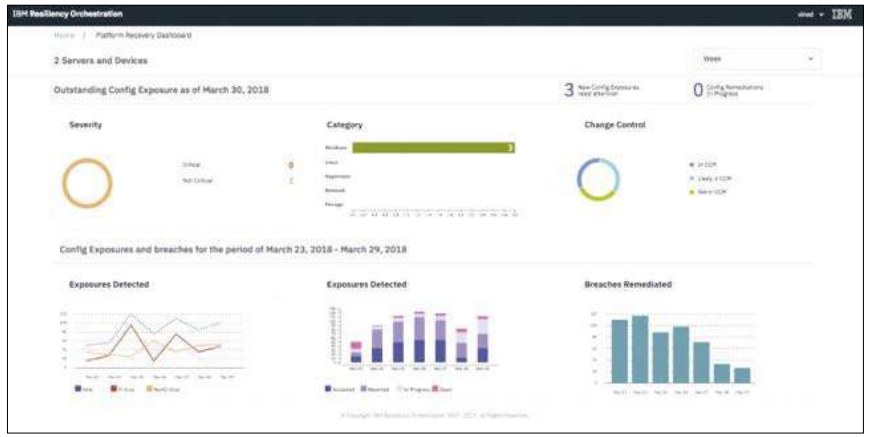


Figura 3: Painel central

Por que a IBM?

O IBM Business Resiliency Services tem quase 60 anos de experiência ajudando clientes no mundo todo com suas necessidades de backup e recuperação. Atualmente, mais de 9 mil clientes estão protegidos com nossos serviços de gerenciamento de dados e recuperação de desastre. Além disso, temos mais de 3,5 exabytes de dados submetidos a backup anualmente e sob nosso gerenciamento. Mais de 300 IBM Resiliency Centers em mais de 60 países no mundo todo fornecem recuperação de desastre gerenciada e proteção de dados, com mais de 6 mil profissionais globais da IBM dedicados à resiliência.

Quer conhecer mais sobre o Cyber Incident Recovery e saber como a IBM pode ajudar a sua empresa?

Fale com o especialista

IBM **Global**
Technology Services

IBM Business Resiliency Services
3039 Cornwallis Rd., Bldg. 201
Research Triangle Park, NC 27709

Produzido nos Estados Unidos da América, agosto de 2018