COHESITY

RESILIENCE EVERYWHERE

RESILIÊNCIA CIBERNÉTICA NA ERA DO RANSOMWARE

Como a Cohesity ajuda as organizações a resistir e se recuperar de ataques cibernéticos, ao mesmo tempo em que se alinha ao Framework de Cibersegurança 2.0 do NIST.

CONTEÚDO

DA RESILIÊNCIA DE DADOS À RESILIÊNCIA CIBERNÉTICA

Desastres naturais representam uma enorme ameaça às operações da empresa. Uma queda de raio, furacão, tornado ou inundação pode causar sérios danos e paralisar os negócios. Nessas situações, as estratégias de resiliência de dados garantem que os dados permaneçam intactos e acessíveis mesmo em caso de falhas de hardware, exclusões acidentais ou desastres naturais.

Mas esses eventos não têm como alvo direto sua empresa com ataques intencionais contínuos.

Compare isso com uma ameaça cibernética. Os agentes de ameaça nunca param de trabalhar e empregar novas ferramentas para manter seus dados reféns e derrubar sua empresa. Os vetores de ataque são frequentemente multifacetados e evasivos. E o risco de reinjetar vulnerabilidades, contas comprometidas e outros artefatos de ataque de volta no seu ambiente é uma ameaça constante. Em comparação com os cenários tradicionais de continuidade de negócios e recuperação de desastres, onde a causa raiz é geralmente óbvia, responder a ameaças cibernéticas requer investigação para descobrir essas causas e promover correções para evitar sua recorrência.

Além disso, em um ataque de ransomware, a infraestrutura de segurança e as principais evidências podem ter sido afetadas pelo incidente, afetando a capacidade de fornecer produtos e serviços.

Ao desenvolver um negócio com resiliência cibernética, os líderes de TI e segurança precisam de processos mais robustos, dinâmicos e colaborativos em comparação com os processos usados para responder a uma interrupção padrão causada por desastres naturais ou interrupções técnicas. A resiliência cibernética se baseia em práticas de resiliência de dados e inclui elementos como preparação para segurança cibernética, planos de resposta a incidentes, treinamento de funcionários e a inteligência contra ameaças.

As ameaças cibernéticas de hoje precisam de soluções modernas que promovam a visibilidade global dos ativos de dados protegidos e simplifiquem a colaboração entre profissionais de TI e segurança.

Na Cohesity, nossas soluções modernas de segurança de dados com tecnologia de IA capacitam as organizações a fortalecer a prontidão cibernética, acelerar a resposta a incidentes e alcançar uma recuperação rápida e segura.

COM A COHESITY, VOCÊ PODE:

- Proteja todos os seus dados
- Garantir que seus dados sejam sempre recuperáveis
- Obter visibilidade das vulnerabilidades e ameaças em seus dados de backup
- Responder de forma rápida e eficaz a ataques e buscar ameaças que escapam das defesas tradicionais
- Recuperar sistemas e dados de forma rápida e segura

O resultado é um negócio mais resiliente, mais bem preparado para prevenir, resistir, responder e se recuperar de ataques cibernéticos.

UM PARADOXO ENTRE CONFIANÇA E CAPACIDADE

78% das organizações confiam na estratégia de resiliência cibernética de sua empresa[1]. Esse é geralmente um bom sinal, desde que essa confiança seja apoiada por capacidades concretas. Mas dados mostram uma desconexão entre a intenção estratégica e as capacidades reais.

98% visam recuperar dados e restaurar processos de negócios após um ataque em um dia[2].

Mas apenas **2%** conseguiram alcançar isso[3].

Felizmente, a Cohesity fornece um manual comprovado com processos e ferramentas para ajudar clientes em todo o mundo a retomar as operações rapidamente e mitigar os impactos de um ataque.

[1-3] Relatório global de resiliência cibernética da Cohesity 2024

SEIS SEGREDOS PARA CRIAR UM NEGÓCIO COM RESILIÊNCIA CIBERNÉTICA

Nossas soluções de segurança de dados na Cohesity ajudam as organizações a entender melhor, gerenciar e reduzir os riscos, além de fortalecer a resiliência cibernética em alinhamento com as principais funções da estrutura de segurança cibernética do NIST: Governar, Identificar, Proteger, Detectar, Responder e Recuperar.

GOVERNAR

- Classificar os dados de backup para entender os requisitos regulatórios
- Dar suporte à conformidade com estruturas de seguro cibernético e outras obrigações contratuais relacionadas a dados de terceiros

IDENTIFICAR

- Verificar sistemas frágeis em busca de vulnerabilidades sem impacto
- Identificar sistemas críticos que não têm backup
- Melhorar a resposta futura a incidentes e as atividades de BC/DR
- Identificar áreas de melhoria nos programas de resiliência cibernética das organizações

PROTEGER

- Proteger dados empresariais em escala
- Proteger backups contra ataques
- Testar backups e restaurações

DETECTAR

- Detecte criptografia de ransomware, ataques de wipers e insiders maliciosos.
- Busque proativamente indicadores de comprometimento para ficar imune a técnicas de evasão
- Envie detecções de segurança para ferramentas SOC para correlação
- Capture mais artefatos forenses e acione instantâneos incrementais com base em sinais de EDR/XDR
- Identifique malware em servidores NAS

RESPONDER

- Envolver a Cohesity CERT (Cyber Event Response Team) para acelerar a resposta e garantir uma recuperação segura
- Restaurar as ferramentas de resposta e o AD a um estado confiável e fornecer acesso rápido
- Estabelecer rapidamente uma sala limpa para resposta e recuperação
- Buscar passivamente artefatos para identificar sistemas impactados adicionais
- Análise forense de sistemas de arquivos históricos
- Entender as vulnerabilidades históricas que foram exploradas no ataque
- Auxiliar no cumprimento das obrigações regulatórias e de conformidade para notificar reguladores, parceiros e titulares de dados afetados

RECUPERAR

- Garanta que a recuperação de sistemas e dados permita a mitigação de ameaças.

1.

Governar os dados de backup para entender os requisitos regulatórios e lidar com os riscos

O cenário de dados de hoje é amplo, como uma garagem abarrotada, tornando cada vez mais difícil localizar dados confidenciais e garantir que estejam protegidos adequadamente. Essa falta de visibilidade aumenta o risco de exposição de dados e não conformidade regulatória.

Para gerenciar esse risco, as organizações devem não apenas atender aos requisitos legais e regulatórios (como HIPAA, CCPA e GDPR), mas também demonstrar controles internos sólidos por meio de governança de cibersegurança eficaz. Cada vez mais, esses controles não se limitam à conformidade, eles estão se tornando essenciais para a obtenção de seguro de cibersegurança.

Com a frequência e a gravidade dos ataques cibernéticos em ascensão, o seguro cibernético se tornou uma estratégia crítica de transferência de risco. Ele ajuda a cobrir perdas financeiras, como recuperação de dados, honorários advocatícios e outras consequências após um incidente. Mas as seguradoras estão exigindo mais dos clientes, exigindo prova de proteção de dados e controles de segurança robustos antes de emitir ou renovar apólices.

Para superar esses requisitos, ajudamos as organizações a:

Descobrir e classificar dados confidenciais. Usar nossos instantâneos de backup ilimitados e imutáveis para descobrir e categorizar dados confidenciais em todo o seu ambiente. Nosso mecanismo de classificação de dados integrado usa centenas de classificadores e algoritmos baseados em IA para identificar e rotular informações regulamentadas e de alto risco, ajudando você a inventariar ativos digitais e aplicar políticas de segurança apropriadas.

Apoiar a conformidade com os requisitos de seguro cibernético e outras obrigações contratuais relacionadas a dados de terceiros. Nossa plataforma ajuda a atender às crescentes expectativas das seguradoras e reguladores, implementando controles de melhores práticas:

- Ambientes de backup isolados, separados da rede de produção
- Serviços dedicados de backup na nuvem
- Criptografia de dados em trânsito e em repouso
- Instantâneos de backup imutáveis
- Acesso baseado em função com credenciais separadas
- Aplicação de MFA tanto para acesso interno quanto externo
- Teste de integridade de backup antes da restauração para garantir que estejam livres de malware

2.

Identificar riscos de resiliência cibernética

O gerenciamento eficaz do risco de segurança cibernética requer uma compreensão clara das vulnerabilidades em todo o seu ambiente de TI, incluindo sistemas de backup. Isso também implica priorizar a proteção de ativos de dados de acordo com sua classificação e melhorar continuamente por meio de testes de segurança, simulações e lições aprendidas com esforços anteriores de resposta a incidentes e recuperação.

CyberScan
Powered by tenable

Verificar sistemas frágeis em busca de vulnerabilidades sem impacto.

Use o Cohesity CyberScan desenvolvido pela Tenable, para realizar varreduras de vulnerabilidade em instantâneos de backup e evitar impacto nos sistemas de produção.

Identificar sistemas críticos que não têm backup.

Integrar a Cohesity com seu fornecedor preferido de Gerenciamento de Postura de Segurança de Dados (Data Security Posture Management , DSPM) é uma maneira poderosa de descobrir riscos ocultos de resiliência cibernética. As soluções DSPM fornecem visibilidade sobre repositórios de dados conhecidos e esquecidos em várias plataformas de nuvem, classificam os dados para identificar informações confidenciais e determinam o risco de exposição.

Embora muitos dos seus dados confidenciais já possam estar protegidos pela Cohesity Data Cloud e pelas políticas de backup existentes, muitas vezes ainda existem lacunas significativas. É aí que entra a integração com DSPM.

Ao combinar insights do DSPM com a Cohesity, você pode identificar sistemas e dados críticos que não estão protegidos por backup e estender rapidamente as políticas de backup para incluí-los, aumentando a segurança e reduzindo os riscos.

Outros benefícios operacionais importantes incluem:

- Frequência otimizada de backups e retenções com base na criticidade dos dados nos datastores com backup da Cohesity
- Restauração priorizada de dados com base na criticidade dos dados para os negócios
- Resposta a incidentes simplificada por meio de análise “just-in-time” dos dados afetados (explorada mais adiante na função de resposta)

Juntos, o DSPM e a plataforma de segurança de dados com tecnologia de IA da Cohesity ajudam a melhorar sua postura de segurança em ambientes multinuvem.

2.

Identificar riscos de resiliência cibernética

Identificar melhorias para futuras atividades de resposta a incidentes e BC/DR.

Avalie as capacidades atuais de resposta e recuperação da sua organização e trace um caminho em direção às melhores práticas do setor com o **Modelo de maturidade de resiliência a ataques cibernéticos destrutivos (Destructive Cyberattack Resilience Maturity Model, DCARMM).**

Desenvolvido pela Cohesity, este modelo se alinha com as principais estruturas, como o SANS 6-Step Incident Response Process, RE&CT, MITRE D3FEND e NIST SP 800-61, permitindo que as empresas:

- Avaliar a preparação para ataques cibernéticos destrutivos
- Comparar a maturidade da resiliência com os colegas do setor ou padrões regionais
- Identificar lacunas e elaborar um roteiro para melhoria contínua

Sua organização pode usá-lo como uma ferramenta estratégica para fortalecer sua postura de resiliência cibernética e orientar o investimento em pessoas, processos e tecnologia.

Identifiquem áreas que precisam de melhoria em seu programa de resiliência cibernética investindo em avaliações de terceiros.

Os serviços de consultoria em resiliência cibernética da Equipe de resposta a eventos cibernéticos (Cyber Event Response Team, CERT) da Cohesity oferecem iniciativas proativas, conduzidas por especialistas, projetadas para fortalecer sua resiliência cibernética antes que o próximo incidente ocorra. De avaliações de resiliência detalhadas baseadas no DCARMM a planos de ação personalizados, o CERT ajuda a identificar lacunas, reduzir riscos e criar defesas duradouras.

3.

Proteger dados empresariais em escala

À medida que os ambientes de dados se tornam mais complexos, impulsionados pelo tamanho e diversidade dos ativos de dados, o risco de impacto grave nos negócios de um ataque cibernético ou interrupção de dados também aumenta.

O uso de uma plataforma única e segura para fazer backup de todas as suas fontes de dados em ambientes locais, em nuvem e SaaS permite que você dimensione a proteção de dados enquanto minimiza significativamente o impacto de possíveis ataques.

Reduza sua superfície de ataque

Muitos ambientes são baseados em produtos pontuais fragmentados. Em contraste, a Cohesity consolida todos os componentes de backup e recuperação em uma única plataforma global. Ela inclui desduplicação global de comprimento variável em fontes de dados e compressão para reduzir ainda mais as superfícies de ataque.

Dimensione a proteção de dados em ambientes de dados

Como o Cohesity Data Cloud foi projetado com arquitetura de hiperescala, os administradores de TI podem expandir seus clusters Cohesity de forma ilimitada e armazenar instantâneos e clones ilimitados sem qualquer impacto no desempenho. A desduplicação de dados sem precedentes não apenas garante que você armazene mais dados a um custo muito menor, mas você também pode instanciar instantâneos a qualquer momento para dar suporte a investigações forenses.

3.

Proteger dados empresariais em escala

Proteger backups contra ataques

Usando os princípios de Zero Trust, a Cohesity adotou uma abordagem de segurança multicamadas que minimiza o risco de ransomware visando backups e o risco de exclusão inadvertida ou maliciosa de dados.

- **Instantâneos imutáveis de estado somente leitura**
  O Cohesity Data Cloud foi criado especificamente para impedir ataques cibernéticos armazenando instantâneos de backup em um estado imutável. Os instantâneos não são montados para aplicativos externos, e as modificações ou exclusões de instantâneos de backup imutáveis são desativadas sem aprovação.
- **Políticas de DataLock** – Nossos recursos de gravação única e leitura múltipla (WORM) para backup permitem que certas funções definam políticas de DataLock inalteráveis em trabalhos selecionados.
- **Autenticação multifatorial (Multifactor Authentication, MFA)**
  Qualquer pessoa que acesse um backup da Cohesity deve se autenticar usando duas formas de verificação. Oferecemos suporte a vários provedores de autenticação, para que sua organização possa manter uma autenticação forte mesmo se o servidor primário for afetado por um incidente cibernético.
- **Criptografia de dados** – A Cohesity oferece criptografia padrão AES-256, validada pelo FIPS e baseada em software, para dados em trânsito e em repouso.
- **Controle de acesso baseado em função e privilégio mínimo**
  A Cohesity reduz o risco de acesso não autorizado, permitindo que a equipe de TI conceda a cada pessoa um nível mínimo de acesso a dados necessários para realizar uma tarefa específica.
- **Separação de deveres** – Com o Cohesity Quorum, qualquer alteração no nível da raiz ou no sistema crítico deve ser autorizada por duas ou mais pessoas para proteger os dados contra ameaças internas e credenciais roubadas.

Isolar dados críticos de negócios

Você pode replicar dados automaticamente para outro cluster imutável da Cohesity no local ou na nuvem pública para garantir que uma cópia imutável adicional dos dados esteja sempre disponível.

Testar backups e restaurações

Usando a **orquestração de recuperação cibernética**, você pode gerar esquemas personalizáveis que automatizam os fluxos de trabalho de recuperação e permitem testes rigorosos em ambientes de não produção. Dessa forma, sua organização pode se preparar melhor para incidentes cibernéticos e otimizar a recuperação para reduzir o tempo de inatividade e a perda de dados.

4.

Detectar possíveis ataques cibernéticos e comprometimentos

Os cibercriminosos não param até encontrar e explorar qualquer vulnerabilidade em seu ambiente de dados. A detecção precoce de alterações anormais nos dados de backup ou no comportamento do usuário é essencial para minimizar o impacto de um ataque.

É aqui que a IA desempenha um papel fundamental: identificar padrões sutis de atividade de dados que podem passar despercebidos pelos humanos. E ao capturar automaticamente instantâneos de backup de dados críticos no início de um ataque de ransomware, detectado por ferramentas EDR/XDR, você pode reduzir a perda de dados e acelerar a recuperação.

Detecte criptografia de ransomware, ataques de wipers e insiders maliciosos.

Monitore, modele e otimize proativamente as operações usando análise preditiva para avaliar tendências. Nosso algoritmo baseado em IA estabelece padrões e verifica continuamente anomalias nos dados em instantâneos ao longo do tempo.

A detecção de anomalias acelera a remediação, enviando uma notificação aos administradores de TI e à equipe de suporte da Cohesity.

Isso fornece às equipes de segurança percepções sobre comportamentos que podem indicar um ataque de ransomware ou wiper, ou até mesmo a presença de um insider malicioso.

Esses alertas também podem ser compartilhados com seu Centro de Operações de Segurança usando suas ferramentas de correlação de eventos (por exemplo, SIEM).

Procure proativamente ameaças em dados de backup.

Ransomware e outros ataques usam táticas enganosas para ocultar malware. A caça a ameaças da Cohesity ajuda você a encontrar ameaças evasivas usando detecção de ameaças orientada por IA que identifica as variantes mais recentes de ransomware e outros ataques cibernéticos.

Nossa extensa biblioteca de padrões comportamentais é atualizada frequentemente com as ameaças mais recentes.

Também oferecemos suporte a feeds de inteligência de ameaças comerciais, como o CrowdStrike Falcon Adversary Intelligence, e ingerimos quaisquer IOCs no formato YARA de outras fontes de terceiros.

4.

Detectar possíveis ataques cibernéticos e comprometimentos

Envie detecções de segurança para ferramentas SOC para correlação

Envie detecções críticas de segurança, como IOCs, anomalias em alterações em dados de backup e alertas de dados confidenciais, para suas ferramentas SOC (por exemplo, SIEM, SOAR) para dar suporte à rápida detecção e resposta a ameaças.

A Cohesity se integra a plataformas líderes, como CrowdStrike, Splunk e Microsoft, para compartilhar telemetria sem problemas, para que o SOC possa agregar, analisar e correlacionar insights da Cohesity com dados de registro de alto volume de toda a sua infraestrutura.

O resultado: uma visão unificada e em tempo real que aumenta a visibilidade e acelera a detecção de possíveis ransomwares ou outras ameaças cibernéticas.

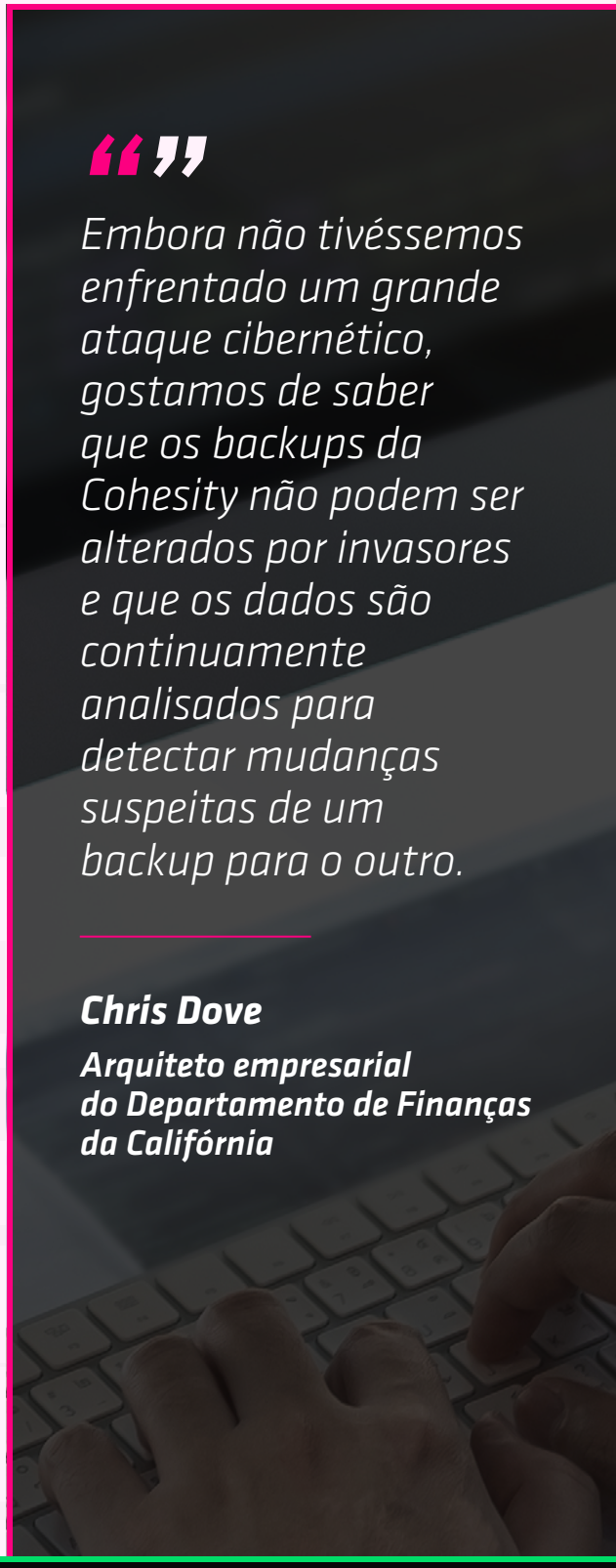
Capture mais artefatos forenses e dispare instantâneos incrementais com base no sinal de EDR/XDR.

A integração entre o Cohesity Data Cloud e o Cisco XDR permite automatizar o backup de dados críticos quando o Cisco XDR detecta um ataque de ransomware, reduzindo os objetivos de ponto de recuperação (RPO) e minimizando a interrupção dos negócios.

Esses instantâneos de backup também fornecem aos responsáveis pela resposta a incidentes um contexto mais granular de alterações no sistema de arquivos, tornando as investigações forenses mais rápidas e eficazes.

Identificar malware em servidores NAS.

Além de monitorar as taxas de alteração dos dados de backup para detectar possíveis ataques de ransomware, a Cohesity detecta e alerta de forma exclusiva sobre anomalias em nível de arquivo em arquivos não estruturados e dados de objetos.



> *"Embora não tivéssemos enfrentado um grande ataque cibernético, gostamos de saber que os backups da Cohesity não podem ser alterados por invasores e que os dados são continuamente analisados para detectar mudanças suspeitas de um backup para o outro.*

Chris Dove
Arquiteto empresarial do Departamento de Finanças da Califórnia

5.

Responder rapidamente a incidentes cibernéticos

Depois que um incidente cibernético é detectado, a organização deve agir rapidamente para conter o incidente, investigar seu escopo e mitigar riscos para permitir uma recuperação segura.

Incidentes de alto impacto, como ataques de ransomware e wiper, podem interromper os sistemas necessários para fornecer produtos e serviços aos clientes, bem como os sistemas internos de TI essenciais para gerenciá-los. Esses cenários exigem um fluxo de trabalho diferente e mais estruturado que vai além dos protocolos padrão de violação de dados.

Apressar-se para se recuperar sem investigar e mitigar a ameaça pode deixar vulnerabilidades subjacentes ativas, arriscando a reinfecção e o tempo de inatividade prolongado.

A recuperação segura de tais ataques requer a compreensão de como o incidente ocorreu e como remediar suas causas raiz. Esta abordagem disciplinada é a essência de cada estrutura de melhores práticas para resposta a incidentes de segurança cibernética.

1. **Envolva a CERT da Cohesity** no início do processo de resposta a incidentes para obter assistência rápida e especializada. Nossa equipe ajuda a conter a ameaça, minimizar o tempo de inatividade, auxiliar na análise forense da infraestrutura de backup, apoiar a conformidade regulatória e os requisitos de notificação de violação e facilitar a recuperação segura para a produção.

2. **Restaure as ferramentas de resposta para um estado confiável e forneça acesso rápido.** Quando um ataque cibernético ocorre, e sua empresa está inoperante, não há tempo a perder. A resposta rápida é fundamental, e uma **digital jump bag**™ ajuda você a agir imediatamente.

   Idealmente preparado antes de um incidente, a mochila digital de emergência é um repositório protegido e confiável que fornece acesso rápido às ferramentas, software, arquivos de configuração e documentação necessários para lançar uma resposta eficaz. Armazenado em um local protegido e imutável além do alcance dos adversários, é a base para toda a solução Cohesity Clean Room, apoiando as etapas críticas da resposta a incidentes e permitindo uma recuperação segura e confiante.

3. **Restaure a infraestrutura limpa do Active Directory (AD).** Poucos sistemas são mais críticos para os negócios, ou mais fortemente direcionados, do que o AD. No começo de uma resposta a um incidente, é indispensável investigar minuciosamente e limpar completamente seu ambiente AD antes de colocar outras ferramentas de resposta de volta on-line e, certamente, antes de restaurar o AD para produção. Pular esta etapa deixa a porta aberta para que os invasores entrem novamente, prejudicando os esforços de recuperação e prolongando a interrupção dos negócios.

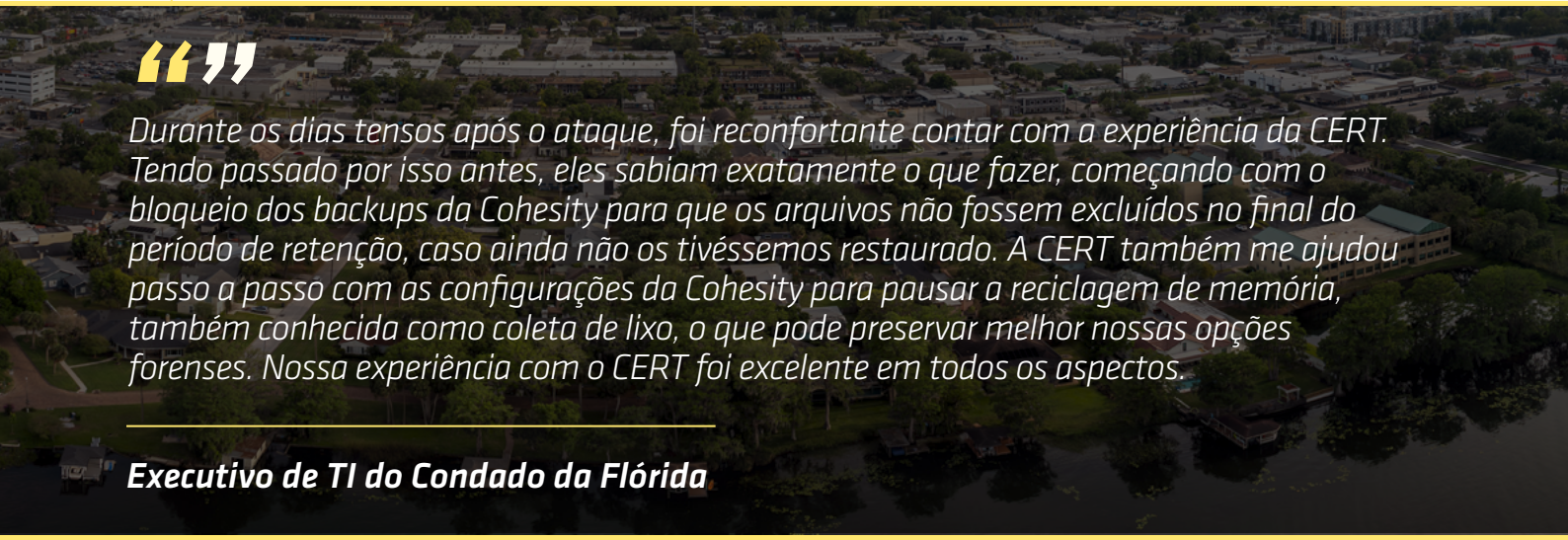
   Com o **Cohesity Identity Resilience, com tecnologia Semperis**, você pode restaurar o AD para um estado confiável até 90% mais rápido.

5.

Responder rapidamente a incidentes cibernéticos

4. **Estabelecer rapidamente uma sala limpa para resposta e recuperação.** Uma sala limpa deve ser implementada como um ambiente confiável onde analistas e investigadores conduzem investigações forenses, entendem as vulnerabilidades exploradas no ataque e garantem que os dados infectados não sejam reintroduzidos nos ambientes de produção.

5. **Buscar passivamente artefatos para identificar sistemas impactados adicionais.** Nossa capacidade de caça a ameaças detecta IOCs em toda a infraestrutura da sua organização, mesmo quando os sistemas estão isolados para contenção. Essa capacidade é resiliente às técnicas comuns de evasão de defesa que podem cegar ou atrasar a detecção por ferramentas tradicionais de segurança de endpoint.



> *"Durante os dias tensos após o ataque, foi reconfortante contar com a experiência da CERT. Tendo passado por isso antes, eles sabiam exatamente o que fazer, começando com o bloqueio dos backups da Cohesity para que os arquivos não fossem excluídos no final do período de retenção, caso ainda não os tivéssemos restaurado. A CERT também me ajudou passo a passo com as configurações da Cohesity para pausar a reciclagem de memória, também conhecida como coleta de lixo, o que pode preservar melhor nossas opções forenses. Nossa experiência com o CERT foi excelente em todos os aspectos.*

Executivo de TI do Condado da Flórida

6. **Examinar de maneira forense sistemas de arquivos históricos.** Nossa proteção de dados permite o acesso a uma série temporal completa de instantâneos imutáveis via interface do usuário e API, para que as equipes de resposta possam realizar investigações forenses detalhadas em nível de arquivo em dados de backup retidos.

7. **Entender as vulnerabilidades históricas que foram exploradas no ataque.** Com a solução CyberScan da Cohesity, você pode verificar instantâneos de backup em busca de vulnerabilidades conhecidas. Isso permite que as equipes de segurança identifiquem vulnerabilidades durante um ataque, mesmo que um sistema esteja inacessível devido à contenção, tenha sido apagado ou corrigido por um criminoso após uma intrusão.

8. **Auxiliar no cumprimento das obrigações regulatórias e de conformidade para notificar reguladores, parceiros e titulares de dados afetados.** Nossa classificação de dados orientada por IA verifica backups para identificar dados confidenciais e regulamentados, ajudando as organizações a atender aos requisitos regulatórios, mesmo em ataques cibernéticos destrutivos em que armazenamentos de dados críticos são criptografados ou apagados. Também ajudamos a restaurar os recursos de comunicação necessários para o gerenciamento de incidentes como parte da solução Cohesity Clean Room. Modelos de comunicação para notificar as partes interessadas podem ser mantidos na mochila digital de emergência para acesso rápido.

6.

Recuperar sistemas e dados com segurança

A fase de recuperação da resposta a um incidente deve apoiar a erradicação completa das ameaças, prevenção de reinfecção e redução da probabilidade de ataques futuros semelhantes.

A solução Cohesity Clean Room oferece a flexibilidade de escolher sua estratégia de recuperação preferida, seja recuperando e limpando sistemas existentes ou reconstruindo do zero.

Ela oferece suporte à recuperação rápida de volumes, permitindo que todo o sistema de arquivos seja recuperado antes da aplicação de medidas de mitigação para erradicar ameaças. Ela também permite reconstruções rápidas a partir de imagens de software confiáveis e configurações conhecidas como boas.

“Nossa organização sofreu um ataque crítico de ransomware que praticamente paralisou toda a nossa infraestrutura. Com a Cohesity, conseguimos recuperar máquinas e compartilhamentos de arquivos, verificar a integridade, limpar e colocar os aplicativos novamente no ar.

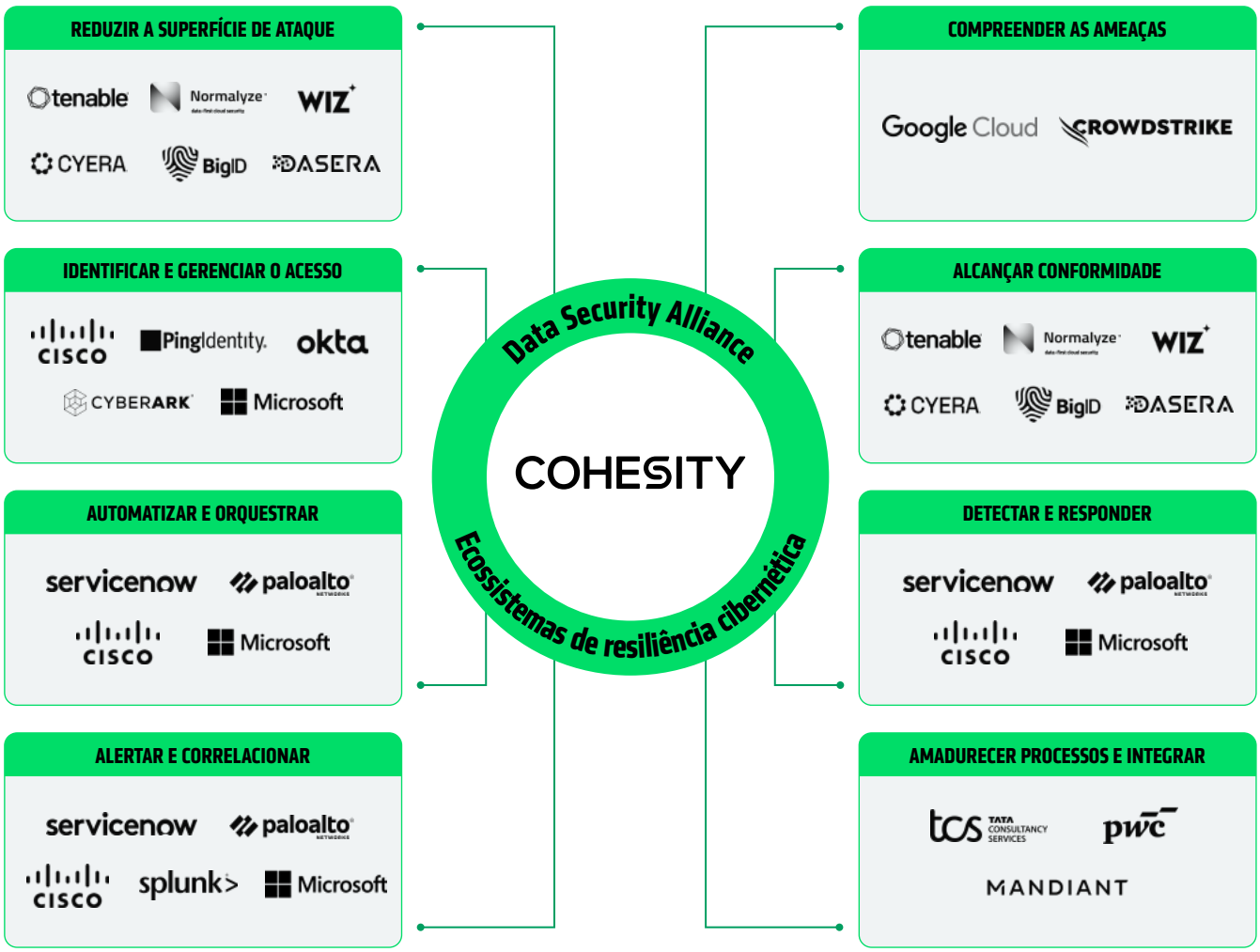
A Cohesity literalmente nos poupou centenas de horas de trabalho e, eu diria, evitou que tivéssemos de pagar o valor de resgate. Ainda temos nossos empregos e a comunidade continua com um hospital funcional porque tivemos muito sucesso com a Cohesity.”

Sam Stewart
Analista de sistemas de rede do Sky Lakes Medical Center

FORTALECENDO A RESILIÊNCIA CIBERNÉTICA POR MEIO DE PARCERIAS

A resiliência cibernética é um esporte de equipe. Nenhuma solução de um único fornecedor pode investigar e corrigir um incidente em sua totalidade.

É por isso que criamos o Data Security Alliance, um ecossistema de empresas líderes em segurança e recuperação cibernética que ajuda você a reduzir os riscos de recuperação cibernética, aumentar a eficiência do seu Centro de Operações de Segurança e proteger mais do seu patrimônio de dados usando ferramentas que você já tem.



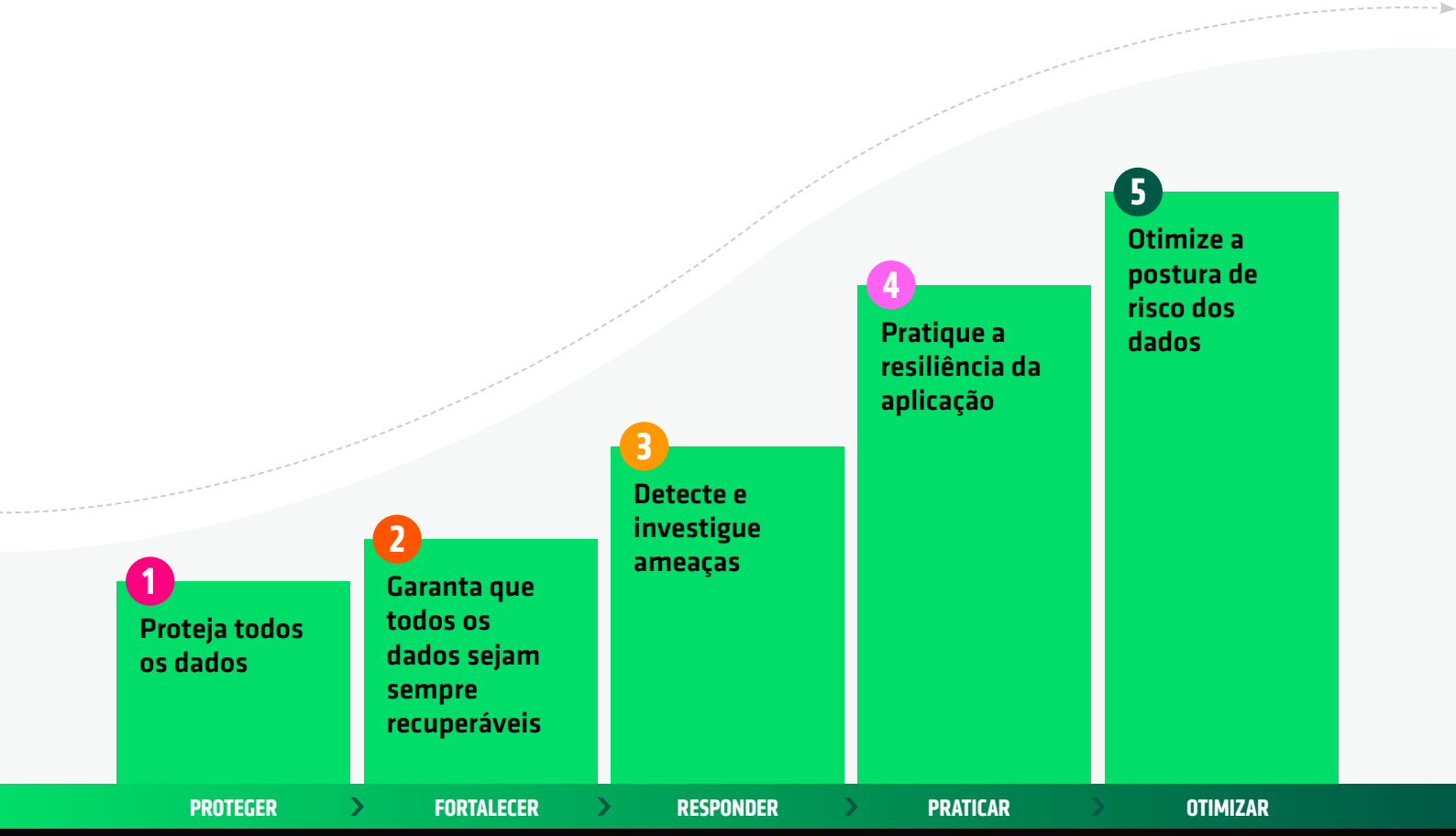
O QUE ACONTECE DEPOIS

PARA SUA ORGANIZAÇÃO...

As 5 etapas da Cohesity para a resiliência cibernética

Você conheceu os seis segredos para construir um negócio com resiliência cibernética e como apoiamos cada estágio da Estrutura de Segurança Cibernética (Cybersecurity Framework, CSF) do NIST. Agora é hora de colocar esses insights em ação.

Para ajudá-lo a começar, desenvolvemos um **manual de cinco etapas** sobre resiliência cibernética alinhado com as melhores práticas do setor para resposta e recuperação cibernética. É um guia prático que mostra como implementar ações concretas e repetíveis usando a Cohesity Data Cloud e os serviços. Cada etapa ajuda você a alcançar os resultados das funções centrais do NIST.



As ***5 etapas*** da Cohesity para a resiliência cibernética

1. PROTEGER TODOS OS DADOS

Alinhamento com a CSF do NIST: ***Proteger***

Desenvolva resiliência protegendo os dados em todos os lugares onde eles residem, em escala empresarial. A Cohesity Data Cloud suporta **mais de 1.000 fontes de dados**, incluindo VMs, aplicativos SaaS, bancos de dados e ambientes NAS, reduzindo custos e riscos por meio de desduplicação e compressão globais.

Essa abordagem reduz os custos de armazenamento para TI e reduz a superfície de ataque para equipes de segurança, dois fatores críticos para uma função de proteção mais forte.

2. GARANTIR QUE OS DADOS SEJAM RECUPERÁVEIS

Alinhamento com o NIST CSF: ***Proteger e recuperar***

A proteção é tão forte quanto sua capacidade de recuperação.

- **Fortaleça sua plataforma:** Ative defesas como MFA, controle de acesso baseado em função e o Quorum para aplicar a separação de tarefas e minimizar o risco interno.
- **Isole dados críticos:** crie cópias seguras e recuperáveis com o cofre cibernético da Cohesity, disponível como um cofre em nuvem gerenciado pela Cohesity ou uma solução autogerenciada.

Essas etapas garantem que você possa restaurar cópias confiáveis quando isso for mais importante.

3. DETECTAR E INVESTIGAR AMEAÇAS

Alinhamento com a CSF do NIST: ***Identificar e detectar***

A resiliência depende da detecção precoce. Com a Cohesity, você pode:

- **Identificar vulnerabilidades**, incluindo lacunas na proteção de dados.
- **Verificar continuamente os backups** em busca de indicadores de ransomware e malware.
- **Procurar ameaças específicas** em dados de backup para que você esteja imune a técnicas de evasão.
- **Enviar as descobertas** para suas ferramentas SIEM/SOAR para rápida correlação e resposta do SOC.

Os resultados: as ameaças são detectadas mais cedo e as equipes de resposta agem mais rapidamente.

4. PRATIQUE A RESILIÊNCIA DA APLICAÇÃO

Alinhamento com a CSF do NIST: ***Responder e recuperar***

Descubra a etapa final >

Não espere um ataque para testar seu plano de recuperação.

- **Teste regularmente:** Pratique seus planos de recuperação como se estivesse sob ataque para validar seus processos de recuperação e prontidão.
- **Recuperação automatizada:** Use a orquestração de recuperação da nossa plataforma para otimizar fluxos de trabalho e acelerar a restauração do sistema após um incidente.

Esta etapa transforma a recuperação de um processo manual e estressante em um manual repetível e bem praticado

As ***5 etapas*** da Cohesity para a resiliência cibernética

5. OTIMIZAR A POSTURA DE RISCO DOS DADOS

Alinhamento com o CSF do NIST: ***Governar, identificar e responder***

- **Fortalecer a governança de segurança de dados:** use seus dados da Cohesity e nossos recursos de classificação de dados para entender quais dados você tem, avaliar seu nível de risco e aplicar os controles de segurança corretos
- **Identificar sistemas críticos que não têm backup:** identifique dados sensíveis em todo o seu ambiente, incluindo backups, e garanta que estejam adequadamente protegidos. Você pode simplificar esse processo combinando os recursos da sua ferramenta de gerenciamento de postura de segurança de dados (DSPM) preferida e de nossa plataforma.
- **Avaliar o impacto do incidente:** Se ocorrer uma violação, e especialmente se seus armazenamentos de dados críticos forem criptografados ou apagados, você pode usar seus backups para avaliar rapidamente quais dados confidenciais e regulamentados podem ter sido expostos, para que você possa cumprir as obrigações regulatórias e de conformidade para notificar reguladores, parceiros e titulares de dados afetados.

Veja a resiliência cibernética em ação

Descubra como 7 organizações de diferentes setores se recuperaram de forma rápida e segura de ataques de ransomware.

OBTENHA O E-BOOK

REUNINDO TUDO

Juntos, nosso manual de resiliência cibernética em cinco etapas oferece um caminho claro e acionável para operacionalizar o NIST CSF.

Com a moderna plataforma de segurança de dados da Cohesity, você pode não apenas proteger e recuperar, mas também otimizar continuamente sua postura de resiliência cibernética.

SAIBA MAIS SOBRE NOSSAS SOLUÇÕES DE RESILIÊNCIA CIBERNÉTICA

COHESITY
RESILIENCE EVERYWHERE

6100008-006-EN 11-2025