COHESITY

RELATÓRIO DE RESILIÊNCIA CIBERNÉTICA

Organizações preparadas para os riscos ou vulneráveis: A disparidade em termos de resiliência cibernética nas organizações de médio porte

MAIO DE 2026

Todos falam sobre detectar e prevenir ataques cibernéticos, mas as manchetes contam uma história diferente. A prevenção e a detecção sozinhas não são mais suficientes. Mesmo as organizações mais avançadas estão sofrendo interrupções incapacitantes que se espalham das operações de TI para a sala de diretoria e muito mais.

Para entender por que e o que separa as organizações resilientes daquelas que ainda lutam, a Cohesity entrevistou 3.200 tomadores de decisão de operações de TI e operações de segurança em 11 países. Entre eles estavam quase 1.000 participantes de organizações de médio porte. As respostas revelam uma maior divisão de resiliência entre organizações prontas para o risco que podem se recuperar com rapidez e confiança, e seus pares expostos ao risco que permanecem vulneráveis a interrupções prolongadas e danos financeiros posteriores.

Nossa pesquisa examina os impactos reais de ataques cibernéticos materiais, como as organizações de médio porte avaliaram sua resiliência cibernética em relação às melhores práticas e as medidas que tomaram para detectar, responder e se recuperar desses incidentes. Ele também destaca o que eles aprenderam e como estão recorrendo à IA e à automação para acelerar a resiliência e fechar a divisão.

ATAQUES CIBERNÉTICOS MATERIAIS: **A NOVA REALIDADE DOS NEGÓCIOS MODERNOS**

Incidentes cibernéticos não são criados iguais. Muitas organizações gerenciam tentativas de phishing de rotina, investigações de malware ou interrupções de sistema quase diariamente. Mas os ataques cibernéticos materiais são diferentes. Nossa pesquisa definiu um ciberataque material como um incidente que causou impacto financeiro, de reputação, operacional ou de rotatividade de clientes mensurável.

ESSES ATAQUES DE ALTO IMPACTO NÃO SÃO MAIS CASOS ISOLADOS PARA ORGANIZAÇÕES DE MÉDIO PORTE.

75%

dos entrevistados sofreram pelo menos um ataque cibernético significativo.

55%

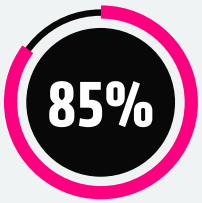
sofreram um nos últimos 12 meses.

25%

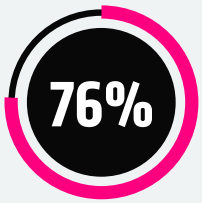
sofreram vários incidentes durante o período de 12 meses.

O CUSTO REAL DOS ATAQUES CIBERNÉTICOS MATERIAIS

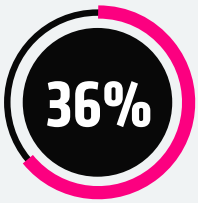
AS PRESSÕES FINANCEIRAS E REGULATÓRIAS TAMBÉM SE FIZERAM SENTIR NAS ORGANIZAÇÕES DE MÉDIO PORTE QUE PESQUISAMOS:



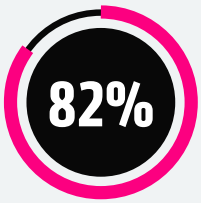
relataram perda de receita



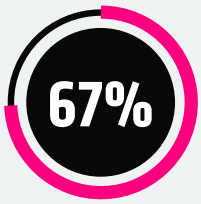
das organizações de capital aberto relataram ter revisado suas projeções financeiras[1]



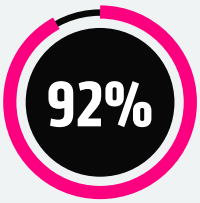
perderam clientes



pagaram um resgate – em média US$ 1,3 milhão por incidente



das organizações privadas realocaram o orçamento das iniciativas de crescimento



enfrentaram consequências legais ou regulatórias, incluindo multas regulatórias (46%) e ações judiciais ou ações coletivas (33%)

[1] Embora relativamente poucas empresas públicas tenham divulgado formalmente revisões de ganhos após um incidente cibernético, esses achados sugerem que os efeitos financeiros e operacionais vão muito além do que os registros públicos revelam.

CONFIANÇA DIANTE DAS CONSEQUÊNCIAS

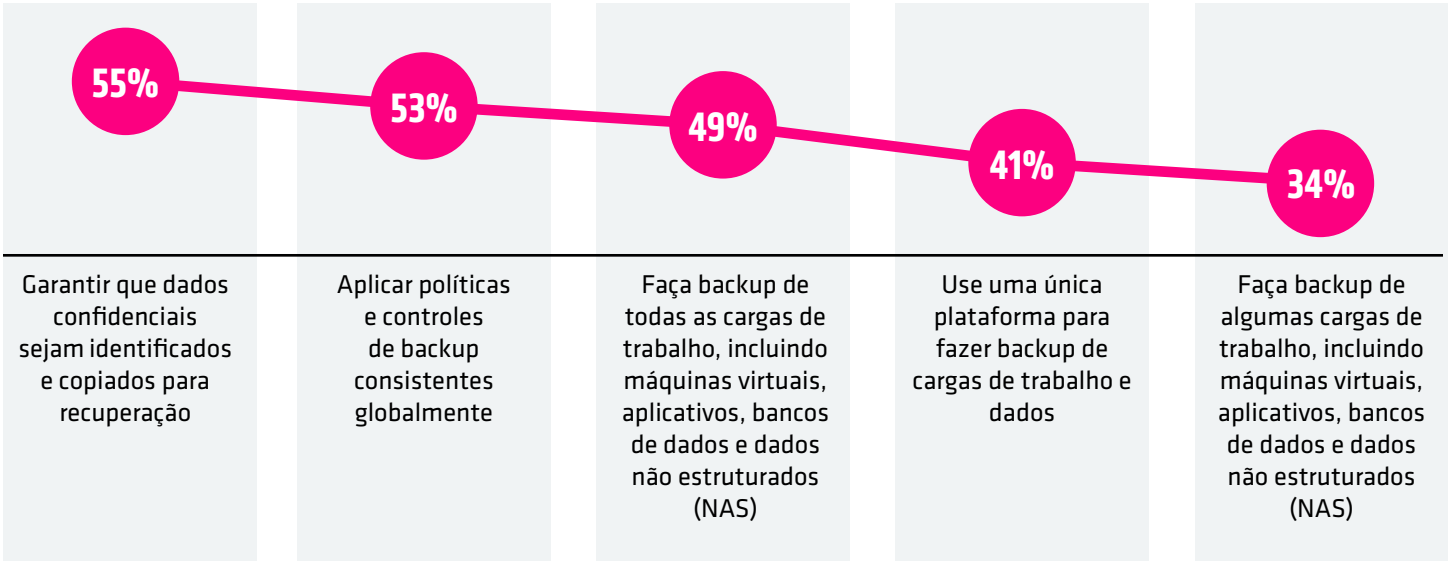
Dada a escala de consequências financeiras e operacionais revelada em nossa pesquisa, pode-se esperar uma preocupação generalizada com a resiliência organizacional. No entanto, muitos entrevistados (47%) expressaram total confiança de que sua estratégia de resiliência cibernética poderia suportar as ameaças de hoje. Esse nível de confiança está em forte contraste com os impactos significativos que muitas dessas mesmas organizações sofreram.

O QUE AS ORGANIZAÇÕES ESTÃO (OU NÃO ESTÃO) FAZENDO

Queríamos olhar abaixo da superfície e descobrir onde existem lacunas de resiliência. Para fazer isso, pedimos aos entrevistados que descrevessem sua abordagem a algumas das principais práticas e capacidades associadas a cinco dimensões principais da resiliência cibernética: **proteção de dados, recuperação de dados, detecção e investigação de ameaças, resiliência de aplicativos** e **otimização da postura de risco de dados.**

A PROTEÇÃO DE DADOS CONTINUA FRAGMENTADA EM AMBIENTES HÍBRIDOS E MULTINUVEM

O que sua organização faz para proteger todos os dados em ambientes híbridos e/ou multinuvem?



Pouco mais da metade das organizações de médio porte garante que os dados confidenciais sejam identificados e tenham cópias de segurança para recuperação. Aproximadamente a mesma porcentagem aplica políticas e controles de backup consistentes em todo o mundo. Menos da metade faz backup de todas as cargas de trabalho ou usa uma única plataforma para proteger cargas de trabalho e dados. Um terço faz backup apenas de cargas de trabalho selecionadas. Essa fragmentação limita a visibilidade e a consistência entre os ambientes. A resiliência cibernética madura depende da unificação de backup e recuperação em uma única plataforma inteligente protegida pelos princípios de confiança zero.

AS MEDIDAS DE RECUPERABILIDADE DE DADOS SÃO COMUNS, MAS A MATURIDADE VARIA

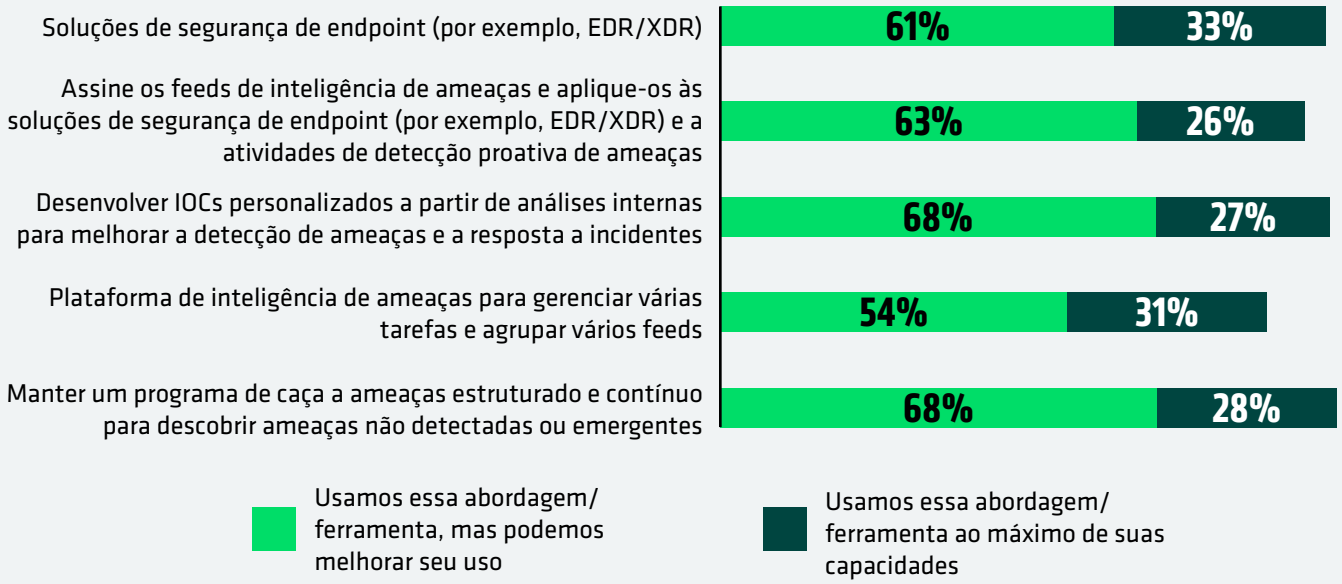
O que sua organização faz para garantir que seus dados sejam sempre recuperáveis?

60%	Requer autorização adicional para tarefas administrativas de alto risco associadas a soluções de backup e recuperação
53%	Autenticação multifator em nossa solução de backup
47%	Siga a “regra de backup 3-2-1” (três cópias dos dados, armazenadas em dois tipos diferentes de mídia, com uma cópia mantida fora do local)
42%	Proteja dados críticos com imutabilidade
38%	Direitos de acesso de privilégio mínimo em cargas de trabalho de backup

Muitas organizações de médio porte reforçaram os controles de acesso aos ambientes de backup, sendo que mais da metade exige autorização adicional do administrador para tarefas de alto risco. Cerca de metade exige a autenticação multifatorial e quase metade segue a regra de backup 3-2-1. São poucos os que protegem dados críticos por meio da imutabilidade ou aplicam direitos de acesso com o mínimo de privilégios. Essas lacunas tornam a recuperação total menos certa. A resiliência cibernética madura depende de cópias de recuperação verificadas, isoladas e à prova de adulteração.

AS FERRAMENTAS DE DETECÇÃO E INVESTIGAÇÃO DE AMEAÇAS SÃO SUBAUTILIZADAS

Até que ponto sua organização usa cada um dos seguintes métodos ou ferramentas para detectar e investigar ameaças?



As ferramentas de detecção e investigação de ameaças são amplamente implantadas, mas muitas vezes subutilizadas. A maioria das organizações de médio porte utiliza segurança de endpoints, feeds de inteligência contra ameaças, IOCs personalizados, plataformas de inteligência contra ameaças e programas estruturados de detecção proativa de ameaças; no entanto, apenas uma minoria aproveita essas ferramentas em todo o seu potencial. A resiliência cibernética madura depende da integração dessas ferramentas em um loop de inteligência contínua que melhora a visibilidade, detecção e resposta.

MEDIDAS DE RESILIÊNCIA INCOMPLETAS AUMENTAM O RISCO DE REINFECÇÃO

O que a sua organização faz/faria para garantir a resiliência dos aplicativos contra ataques cibernéticos?

57% Identificar e remediar lacunas de controle de segurança antes de restaurar sistemas para produção

60% Realizar ensaios simulados anuais de ponta a ponta, envolvendo uma equipe multifuncional composta por representantes das áreas técnica, jurídica, estratégica, executiva e de comunicação

56% Utilizar um repositório online e protegido de sistemas e informações críticas para apoiar a resposta a incidentes e a recuperação

47% Usar um ambiente isolado para investigação de incidentes, remediação e recuperação segura

33% Imutabilidade para todos os dados de backup

As organizações de médio porte estão aprimorando sua abordagem em relação à resiliência das aplicações, mas ainda há lacunas. A maioria identifica falhas nos controles de segurança antes de restaurar os sistemas. Uma proporção semelhante mantém repositórios on-line protegidos. Mais da metade também realiza ensaios anuais de recuperação. São cada vez menos os que utilizam ambientes isolados para investigação e recuperação seguras. Uma porcentagem ainda menor aplica a imutabilidade a todos os dados de backup. Essas lacunas deixam os processos de recuperação vulneráveis à reinfecção ou perda de dados. A resiliência cibernética madura combina a preparação com zonas de recuperação seguras e verificáveis.

A CLASSIFICAÇÃO DE DADOS GANHA FORÇA À MEDIDA QUE O USO PARA GESTÃO DE RISCOS SE EXPANDE

Como sua organização usa abordagens/ferramentas de descoberta e classificação de dados para minimizar a exposição ao risco de dados em toda a sua propriedade de dados?

Identificar e resolver violações de segurança e privacidade de backup para conformidade

Utilize a classificação de dados de backup para determinar as obrigações de conformidade relativas aos dados afetados

Definir e entender a materialidade do ataque cibernético antes que ocorra um incidente

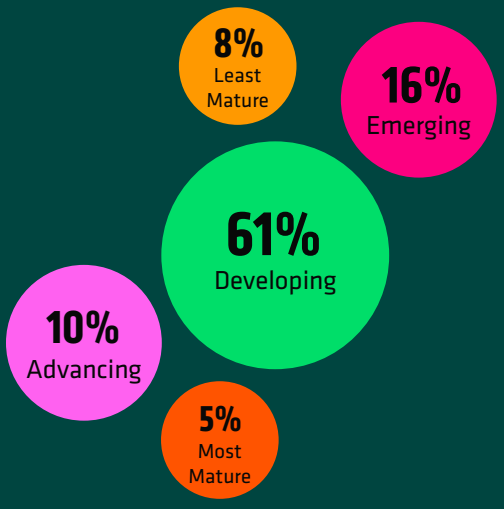
Identificar e priorizar sistemas para backup

As organizações de médio porte estão utilizando a descoberta e a classificação de dados de forma mais estratégica nas áreas de conformidade, resposta e recuperação. Quase dois terços tratam de violações de privacidade e segurança, enquanto mais da metade utiliza a classificação para orientar a conformidade durante um ataque. Mais da metade também define a relevância antes de um incidente e prioriza os backups com base nos riscos. A resiliência cibernética madura transforma a classificação em uma abordagem sistemática que otimiza a postura de risco dos dados e informa proteção, resposta e recuperação.

UMA IMAGEM MAIS CLARA DA MATURIDADE DA RESILIÊNCIA

Quando pontuadas coletivamente, as respostas dos entrevistados serviram como um barômetro de alto nível da maturidade da resiliência cibernética, revelando padrões claros sobre como as organizações de médio porte estão desenvolvendo, ou enfrentando dificuldades para desenvolver, a resiliência na prática. Embora a maioria se enquadre no estágio de desenvolvimento, apenas 5% demonstram as capacidades mais maduras e integradas que definem organizações prontas para o risco.

A CURVA DE MATURIDADE DA RESILIÊNCIA CIBERNÉTICA



Menos maduro (8%): Backups, políticas e medidas de segurança estão, em grande parte, ausentes ou são inconsistentes. Os controles de MFA e administrativos raramente são aplicados, a recuperação muitas vezes carece de isolamento e as avaliações de conformidade ou de materialidade costumam ser negligenciadas.

Emergente (16%): Algumas práticas de resiliência estão em vigor, mas de forma inconsistente. Organizações podem fazer backup de dados confidenciais, aplicar políticas globais ou usar MFA, mas raramente em combinação. As iniciativas de inteligência contra ameaças e de conformidade já existem, mas ainda são imaturas e fragmentadas.

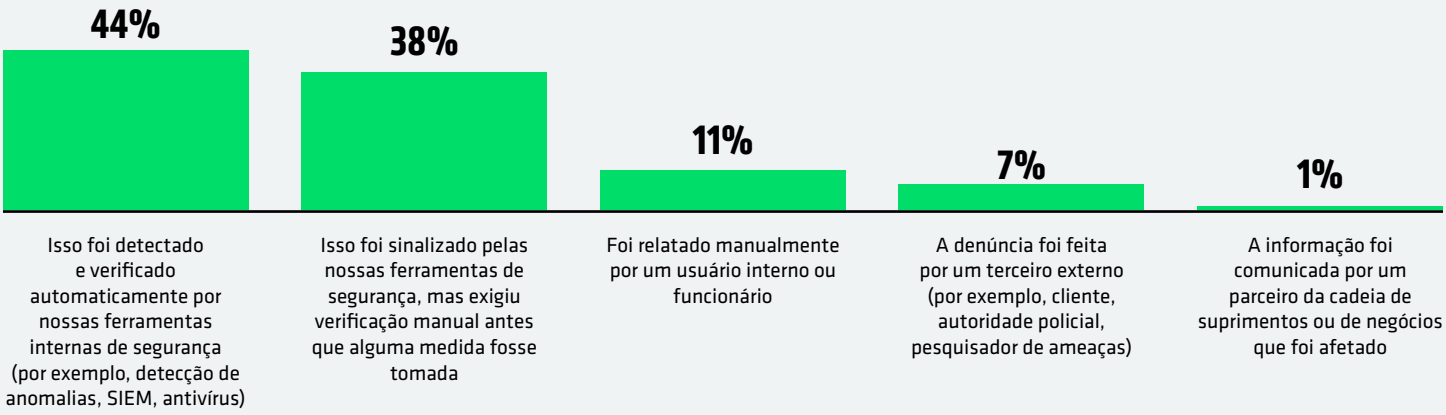
Em desenvolvimento (61%): Práticas essenciais, como backups, controles administrativos e inteligência de ameaças, são mais comuns, embora ainda desiguais. Ambientes de recuperação, verificações de conformidade e correção de falhas de segurança são aplicados de forma esporádica, o que faz com que os esforços de resiliência tenham eficácia parcial.

Avançando (10%): A maioria das práticas essenciais é aplicada de forma consistente, incluindo políticas globais de backup, aprovações administrativas e correção de problemas antes da recuperação. As informações sobre ameaças são utilizadas, mas não estão totalmente otimizadas, e ainda existem algumas lacunas no que diz respeito à recuperação isolada e à cobertura completa da conformidade.

Mais maduro (5%): A resiliência é sistêmica e abrangente. Os dados confidenciais são copiados para backup globalmente, a autenticação multifatorial (MFA) e os controles administrativos são padrão, a inteligência contra ameaças é maximizada, a recuperação é garantida por meio de medidas corretivas e as salvaguardas de conformidade são cumpridas de forma consistente.

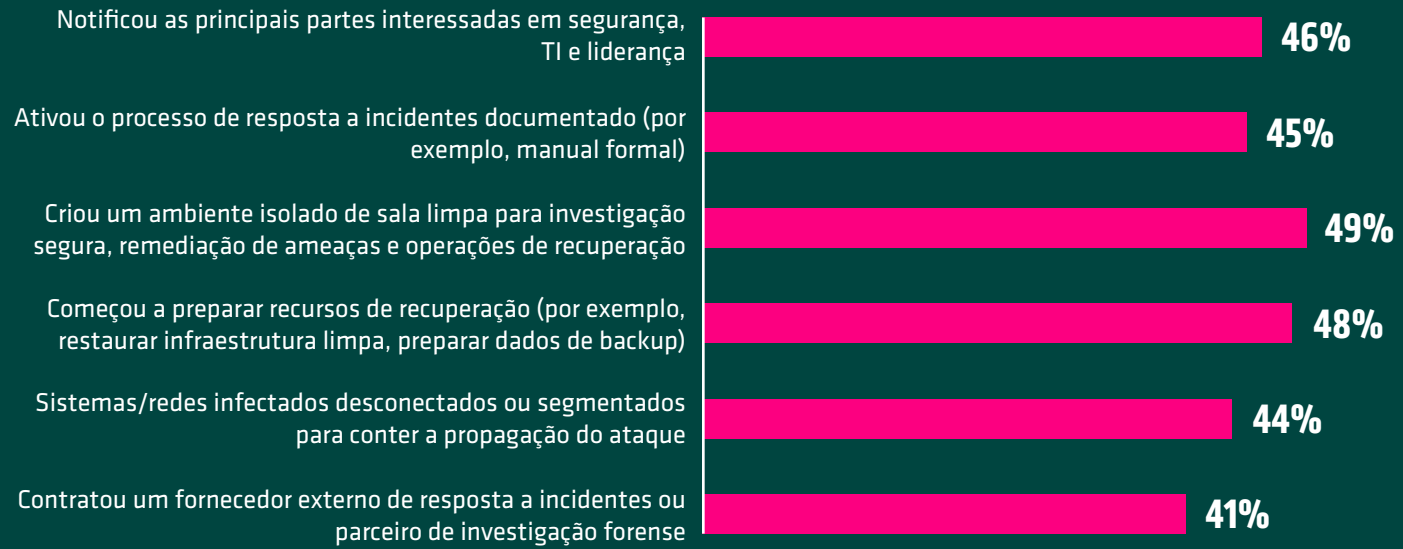
RESILIÊNCIA SOB FOGO

COMO AS EQUIPES IDENTIFICARAM O ATAQUE



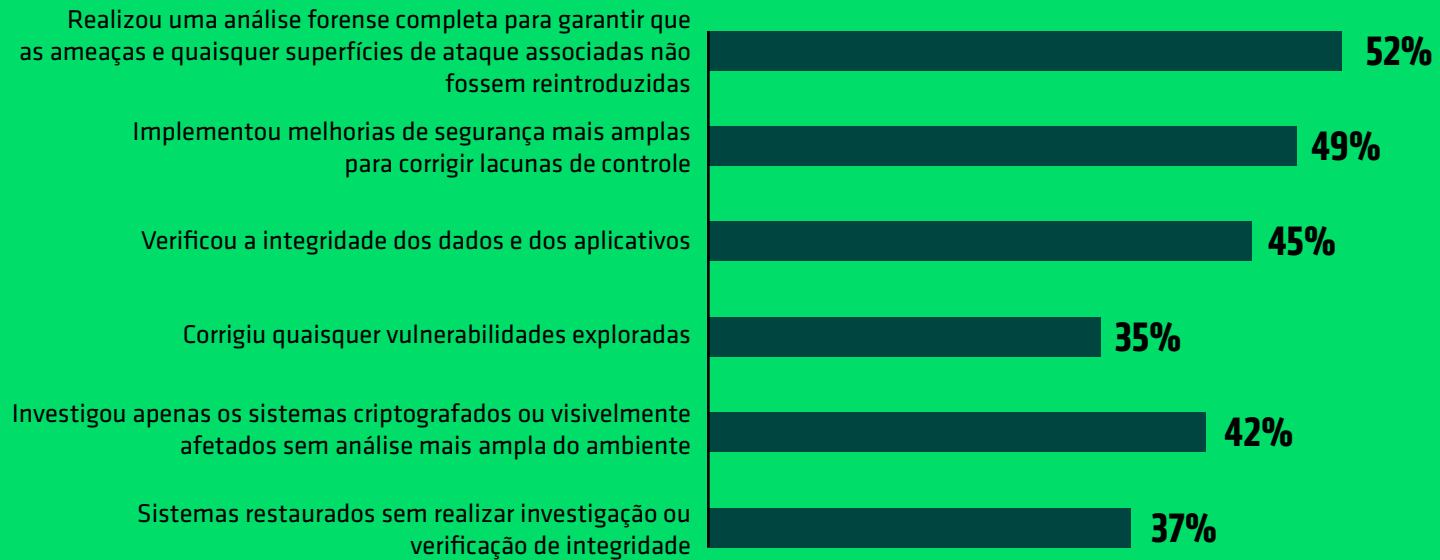
Em caso de um ataque cibernético, a maioria das organizações de médio porte detecta os incidentes internamente, sendo que a maior parte deles é identificada automaticamente e verificada por ferramentas de segurança. Muitos outros são sinalizados pelas ferramentas, mas exigem verificação manual antes que alguma medida seja tomada. São relatados muito menos incidentes por funcionários ou por terceiros. A detecção é, em grande parte, realizada por meio de ferramentas, embora a validação humana ainda desempenhe um papel importante.

AÇÕES QUE AS EQUIPES TOMARAM APÓS CONFIRMAR O ATAQUE



Após confirmarem um ataque, as organizações de médio porte adotaram uma série de medidas para conter a ameaça e iniciar a recuperação. Equipes semelhantes começaram a preparar recursos de recuperação, criaram ambientes isolados de sala limpa, notificaram as principais partes interessadas, desconectaram os sistemas infectados e ativaram os planos de resposta. Um número ligeiramente menor contratou parceiros externos de resposta a incidentes. Esses padrões sugerem que as medidas de resposta são amplamente adotadas, mas ainda não estão totalmente padronizadas em todas as ações críticas.

MEDIDAS TOMADAS ANTES DE COLOCAR SISTEMAS E DADOS DE VOLTA ON-LINE



Antes de restabelecer o funcionamento dos sistemas e dos dados, as organizações de médio porte adotaram uma combinação de medidas forenses e de correção. Cerca de metade realizou análises forenses completas, implementou melhorias mais abrangentes de segurança ou verificou a integridade dos dados e dos aplicativos, enquanto um número semelhante se concentrou apenas nos sistemas visivelmente afetados. Uma parcela menor corrigiu vulnerabilidades exploradas ou restaurou sistemas sem investigação ou verificação. Essas lacunas podem aumentar o risco de reinfecção ou de exposição residual.

DESAFIOS QUE AS EQUIPES ENFRENTARAM DURANTE O ATAQUE

51%

Impossibilidade de nos comunicarmos ou nos coordenarmos dentro da nossa equipe devido à indisponibilidade de sistemas essenciais (por exemplo, e-mail, aplicativos colaborativos, sistema de tickets)

47%

Pressão da liderança para restaurar os sistemas antes que o ataque fosse remediado

41%

As ferramentas de segurança foram contornadas e os backups foram atacados

40%

Nós nos recuperamos, mas depois fomos reinfectados porque as ameaças não foram totalmente erradicadas

37%

Falta de acesso a pontos de recuperação limpos e validados

As equipes enfrentaram uma série de desafios operacionais e técnicos durante o ataque. Cerca de metade teve dificuldade para se comunicar enquanto os sistemas estavam fora do ar ou sentiu pressão para restaurar os sistemas antes que a correção estivesse concluída. As equipes também relataram casos de contorno de ferramentas de segurança, ataques a backups, reinfecção após a recuperação ou falta de acesso a pontos de recuperação não infectados. Esses desafios destacam lacunas na preparação que podem complicar a resposta e prolongar os transtornos.

ONDE O INVESTIMENTO EM RESILIÊNCIA NÃO É SUFICIENTE

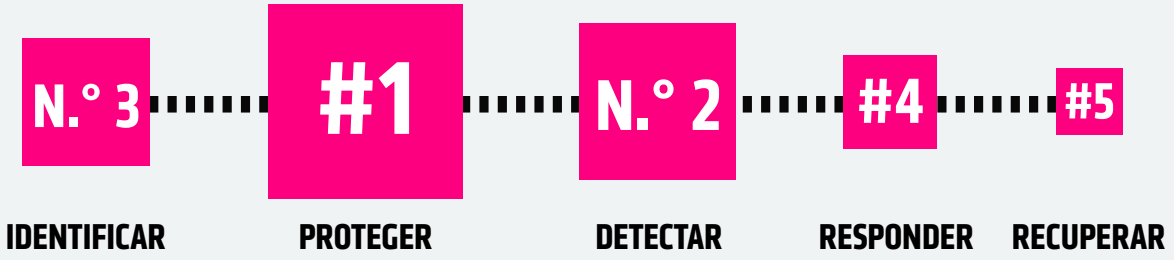
Até mesmo organizações bem preparadas lutam para sustentar a resiliência quando um ataque acontece. À medida que a pressão operacional aumenta, lacunas de coordenação, remediação incompleta e riscos de reinfecção expõem como a recuperação frágil pode ser sem processos unificados e garantia contínua.

Essas tendências refletem a forma como as organizações de médio porte estão alocando seus orçamentos para resiliência cibernética atualmente. Perguntamos aos entrevistados como eles distribuem seus gastos entre as cinco funções principais da Estrutura de segurança cibernética do NIST: identificar, proteger, detectar, responder e recuperar.

A maioria continua a investir fortemente em prevenção, proteção e detecção, enquanto os recursos destinados à resposta e à recuperação comprovada são comparativamente menores. O resultado é uma curva de maturidade que ainda se inclina mais para a defesa do que para a restauração, destacando uma oportunidade ainda inexplorada de fortalecer a resiliência onde ela é mais importante: após o ataque.

ESTRUTURA DE SEGURANÇA CIBERNÉTICA DO NIST.

O tamanho da caixa representa, em ordem decrescente, a proporção dos investimentos em resiliência cibernética



A IA E A AUTOMAÇÃO SURGEM COMO MULTIPLICADORES DE RESILIÊNCIA

Os resultados também mostram que as organizações de médio porte consideram a IA um poderoso facilitador da resiliência cibernética, particularmente na melhoria da velocidade de detecção e precisão de resposta. Quase todos os entrevistados classificaram ferramentas como detecção de anomalias, análise de comportamento do usuário e investigação e resposta a ameaças orientadas por IA como eficazes no fortalecimento de sua postura de segurança.

Assistentes mais novos baseados em IA generativa, capazes de consultas de ameaças de linguagem natural e análise contextual, estão ganhando força como uma maneira de simplificar e acelerar a tomada de decisões. Cinquenta e seis por cento das organizações de médio porte afirmaram que uma das principais lições aprendidas após um ataque cibernético foi a necessidade de maior automação nas etapas de detecção, resposta e recuperação. Isso reflete a crescente demanda por plataformas integradas de automação e orquestração, onde a IA atua como um multiplicador de força, impulsionando maior eficiência, consistência e eficácia nesses processos.

Ao olhar para o futuro, a maioria espera que a IA desempenhe um papel cada vez mais estratégico na defesa cibernética até o final de 2026. Cinquenta e seis por cento acreditam que a IA apoiará a tomada de decisão humana, aprimorando a análise e as recomendações, com os humanos permanecendo no controle das ações finais. Trinta e sete por cento esperam que a IA se torne central para a detecção e resposta, mesmo tomando algumas decisões autônomas. Isso sinaliza uma trajetória clara: A IA está evoluindo de um assistente para uma base operacional de resiliência cibernética, pronta para aumentar a velocidade, a precisão e a confiança na detecção, resposta e recuperação.

O FUTURO DA RESILIÊNCIA COMEÇA AGORA

Embora as organizações de médio porte estejam fazendo progressos mensuráveis na resiliência cibernética, muitas ainda têm espaço para melhorar sua resposta, recuperação e validação da prontidão após um ataque. A resiliência cibernética representa uma enorme vantagem competitiva. O futuro pertence a organizações que investem em pessoas, produtos e processos para se recuperar mais rapidamente, manter a confiança do cliente e manter os negócios em movimento quando outros não conseguem. Quando a interrupção é praticamente inevitável, a resiliência não é apenas proteção, é desempenho.

Desenvolva resiliência antes que ocorra uma crise:

- Conheça as soluções de resiliência cibernética da Cohesity para empresas de médio porte
- Avalie o nível de maturidade da sua resiliência cibernética com este quadro de indicadores de resiliência
- Aumente o nível com um plano de ação de resiliência cibernética de cinco etapas

METODOLOGIA

COHESITY

A Cohesity contratou a Vanson Bourne para pesquisar 3.200 tomadores de decisão de TI e segurança em setembro de 2025, formando a base dessas descobertas. Os entrevistados representam organizações nos EUA (500), Brasil (200), Reino Unido (400), Alemanha (400), França (400), Emirados Árabes Unidos/Arábia Saudita (100), Austrália (200), Coreia do Sul (200), Japão (400), Índia (200) e Singapura (200). As organizações tinham 1.000 ou mais funcionários e vieram de uma variedade de setores públicos e privados, com foco em serviços financeiros, setor público e saúde.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000049-001-PT-BR 7-2026