

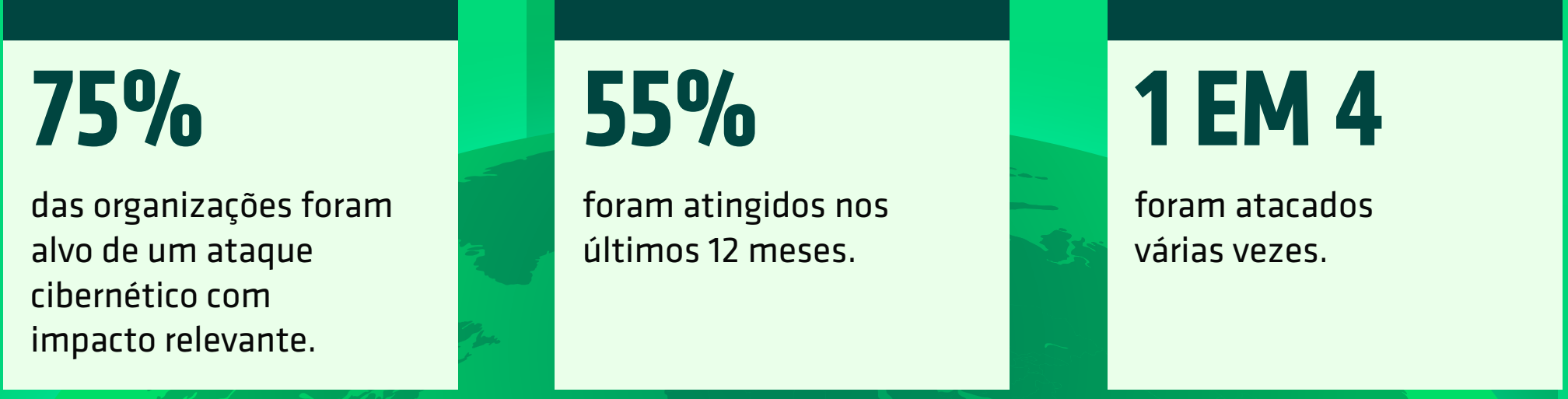
PREPARADO PARA O RISCO OU EXPOSTO AO RISCO

A disparidade em termos de resiliência cibernética nas organizações de médio porte



Os ataques cibernéticos não são mais eventos isolados, eles passaram a ser parte do mundo digital. Cada dia traz um novo lembrete de que as empresas de médio porte em todo o mundo estão cada vez mais na mira dos criminosos. Nenhum negócio está imune. A frequência e a sofisticação cada vez maiores das ameaças resultaram em um aumento nos ataques cibernéticos com impacto material, causando prejuízos financeiros, operacionais e de credibilidade mensuráveis.

UMA PESQUISA GLOBAL COM QUASE 1.000 TOMADORES DE DECISÃO NAS ÁREAS DE TI E OPERAÇÕES DE SEGURANÇA DE ORGANIZAÇÕES COM 1.000 A 1.999 FUNCIONÁRIOS REVELA A REALIDADE.



OS PREJUÍZOS SÃO GRANDES E OS CUSTOS SE MULTIPLICAM COM RAPIDEZ.

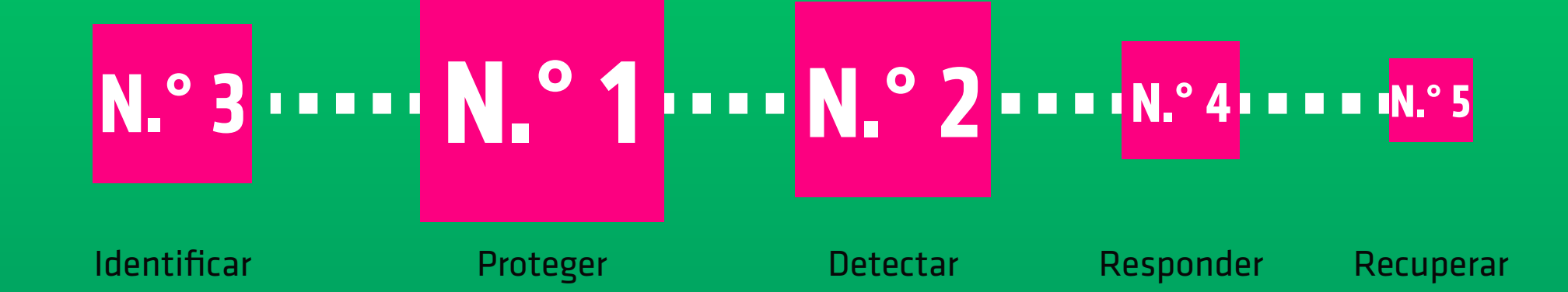


MESMO QUE AS EVIDÊNCIAS SEJAM INEQUÍVOCAS, MUITAS ORGANIZAÇÕES SUPERESTIMAM SUA RESILIÊNCIA.



A MAIORIA AINDA PRIORIZA A PREVENÇÃO E A DETECÇÃO EM DETRIMENTO DAS FUNÇÕES, IGUALMENTE CRÍTICAS, DE RESPOSTA E RECUPERAÇÃO.

Ordem baseada na estrutura de segurança cibernética do NIST. O tamanho da caixa representa, em ordem decrescente, a proporção dos investimentos em resiliência cibernética.



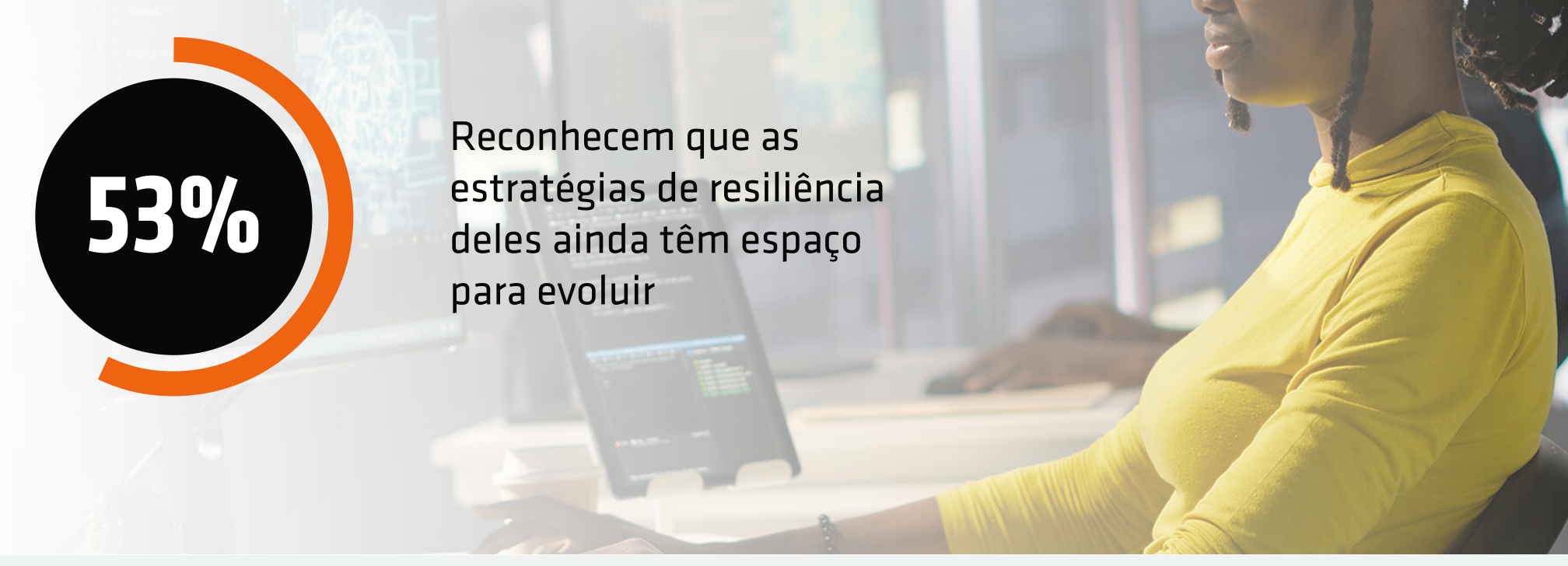
A CONFIANÇA E OS PADRÕES DE GASTOS REVELAM APENAS UMA PARTE DA HISTÓRIA

A verdadeira resiliência depende das práticas e dos recursos que a respaldam. Avaliadas em relação a critérios concretos de desempenho, apenas 5% das organizações demonstram maturidade nas cinco áreas essenciais: **proteção de dados, recuperação de dados, detecção e investigação de ameaças, resiliência de aplicativos e otimização do risco relacionado a dados.**



Para as organizações com maior resiliência cibernética, a resiliência é sistemática e abrangente. Entre outras práticas recomendadas, elas garantem que os dados confidenciais tenham backup em nível global, que a autenticação multifatorial e os controles administrativos sejam aplicados, que a inteligência contra ameaças seja maximizada, que a recuperação seja assegurada por meio de medidas corretivas e que as salvaguardas de conformidade sejam cumpridas de forma consistente.

MAS A MATURIDADE NÃO É ESTATICA.



A consciência da necessidade de aumentar a resiliência está impulsionando a próxima evolução, viabilizada pela automação e IA. À medida que as ameaças se tornam mais rápidas e mais complexas, a automação é fundamental para acelerar a detecção, simplificar a resposta e fortalecer a recuperação.



VOCÊ ESTÁ PREPARADO PARA OS RISCOS?

- 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

A Vanson Bourne realizou uma pesquisa com 3.200 líderes de TI e segurança das regiões da América do Norte, Ásia-Pacífico, Europa e América Latina, representando organizações com 1.000 ou mais funcionários em 2025. Entre os entrevistados, estavam 977 participantes de organizações de médio porte com 1.000 a 1.999 funcionários.