CG // One

CHECK POINT CYBER SECURITY REPORT 2026:

INSIGHTS E ANÁLISE ESTRATÉGICA DA CG ONE

O QUE AS TENDÊNCIAS GLOBAIS DE AMEAÇAS SIGNIFICAM PARA CISOS E LÍDERES DE SEGURANÇA NO BRASIL.

ÍNDICE

INTRODUÇÃO

A CG One é a parceira mais antiga da Check Point no Brasil. Desde 1995, quando trouxemos ao país os primeiros firewalls da fabricante, acompanhamos de perto a evolução das ameaças digitais e das tecnologias de defesa.

Com mais de 40 anos de atuação, a CG One acompanha continuamente as tendências globais de ataques e defesa cibernética.

Este material apresenta uma análise executiva da CG One baseada no Cyber Security Report 2026, publicado pela Check Point Research. O objetivo é destacar os principais insights do relatório e traduzir suas implicações para CISOs e líderes de segurança.

INTRODUÇÃO

Boa leitura!

PRINCIPAIS TENDÊNCIAS DE CIBERSEGURANÇA

O Cyber Security Report 2026 mostra que o cenário de ameaças se tornou mais rápido, mais conectado e mais difícil de conter. Em vez de depender de técnicas isoladas, os atacantes passaram a combinar engenharia social, exploração de exposição, abuso de identidade e automação para ampliar escala e impacto. Na prática, isso significa que o risco deixou de estar concentrado apenas em malware ou vulnerabilidades específicas e passou a se distribuir por toda a superfície operacional da organização.

Confira as principais tendências:

Engenharia social além do e-mail

O relatório mostra que ataques de engenharia social evoluíram significativamente. O phishing tradicional deixou de ser o único vetor e deu lugar a **campanhas multicanal,** que utilizam chamadas telefônicas, aplicativos de mensagens, redes sociais e impersonação em tempo real.

Essas campanhas exploram a confiança do usuário e podem levar vítimas a executar ações que concedem acesso inicial aos atacantes.

O ecossistema de ransomware em 2025

O número de vítimas de ransomware atingiu **níveis recordes em 2025,** com mais de **7.960 organizações publicadas em sites de vazamento de dados,** representando crescimento de **53% em relação ao ano anterior.**

O relatório também destaca que o modelo **Ransomware-as-a-Service (RaaS)** continua impulsionando o crescimento do crime digital, permitindo que diferentes grupos e afiliados executem ataques em escala.

O impacto operacional do ciberespaço em conflitos

O relatório também analisa como operações cibernéticas passaram a integrar **conflitos geopolíticos e militares,** sendo utilizadas para apoiar operações militares, influenciar narrativas públicas e causar interrupções em infraestrutura crítica.

Nesse contexto, o ciberespaço atua não apenas como um domínio técnico, mas como um **instrumento estratégico em conflitos internacionais.**

A dominância de ameaças associadas à China

O relatório aponta a crescente atuação de grupos associados ao chamado **Chinese-nexus,** que se destacam pela persistência em campanhas de espionagem, comprometimento de infraestrutura crítica e infiltração prolongada em redes corporativas.

Esses grupos frequentemente operam com alto nível de sofisticação e objetivos estratégicos de longo prazo.

Dispositivos não monitorados como ponto de entrada

Outro ponto crítico identificado é o uso de **dispositivos não monitorados** como base inicial para ataques.

Equipamentos fora do escopo de monitoramento de segurança — como laptops pessoais, dispositivos BYOD ou sistemas mal gerenciados — tornam-se frequentemente o ponto inicial de comprometimentos que posteriormente evoluem para ataques maiores.

O PANORAMA DA IA NA CIBERSEGURANÇA

A inteligência artificial está transformando rapidamente o cenário de cibersegurança. O Cyber Security Report 2026 aponta que a IA deixou de ser apenas uma tecnologia auxiliar e passou a atuar como um **multiplicador de capacidades tanto para atacantes quanto para defensores.**

Ao reduzir o esforço necessário para analisar grandes volumes de dados, gerar conteúdo e automatizar tarefas, a IA permite que operações cibernéticas sejam conduzidas com maior velocidade, escala e eficiência. Como resultado, atividades que antes exigiam conhecimento técnico especializado passam a ser executadas de forma mais acessível e automatizada.

Ao mesmo tempo, a adoção crescente de serviços baseados em inteligência artificial nas organizações cria novas superfícies de exposição, introduzindo desafios adicionais relacionados à proteção de dados, governança de informação e segurança de aplicações.

Nesse contexto, o relatório destaca algumas das principais formas pelas quais a IA está impactando o cenário de ameaças:

Da integração à autonomia: a evolução do uso de IA

O relatório aponta que o uso de inteligência artificial na cibersegurança está evoluindo de uma fase inicial de **integração em ferramentas existentes** para um cenário em que sistemas passam a operar com níveis crescentes de autonomia.

Inicialmente, a IA foi utilizada para apoiar tarefas específicas, como análise de dados e automação de processos. No entanto, a tendência observada é o desenvolvimento de sistemas capazes de executar sequências mais complexas de atividades, incluindo reconhecimento, análise de ambientes e tomada de decisão.

Esse movimento aponta para um cenário em que operações cibernéticas — tanto ofensivas quanto defensivas — passam a depender cada vez mais de **processos automatizados e adaptativos.**

Serviços de IA como nova superfície de ataque

À medida que organizações incorporam plataformas e serviços baseados em inteligência artificial, essas tecnologias passam também a representar **novas superfícies de ataque.** Interfaces de acesso a modelos de IA, APIs e ambientes de processamento de dados podem introduzir novos pontos de exposição, ampliando o escopo de segurança que precisa ser monitorado.

Nesse contexto, sistemas de IA devem ser considerados parte integrante da superfície de ataque corporativa, exigindo controles de segurança específicos.

LLMs como vetor de vazamento de dados sensíveis

Modelos de linguagem de grande escala (LLMs) introduzem um novo tipo de risco relacionado à **exposição involuntária de informações sensíveis.** Usuários podem inserir dados confidenciais em ferramentas baseadas em IA durante atividades cotidianas, como geração de textos, análise de documentos ou automação de tarefas.

Esse comportamento pode levar ao processamento ou armazenamento de informações estratégicas fora do controle da organização, criando desafios adicionais para governança de dados e proteção de informações críticas.

Uso de serviços de IA por atores maliciosos

O relatório também destaca que atores maliciosos estão utilizando cada vez mais serviços públicos de inteligência artificial para apoiar suas operações. Essas plataformas podem ser utilizadas para diversas atividades dentro do ciclo de ataque, incluindo geração de conteúdos fraudulentos, automação de interações com vítimas e criação de scripts ou códigos maliciosos.

O acesso relativamente aberto a essas ferramentas reduz barreiras técnicas e amplia o número de atores capazes de conduzir campanhas sofisticadas.

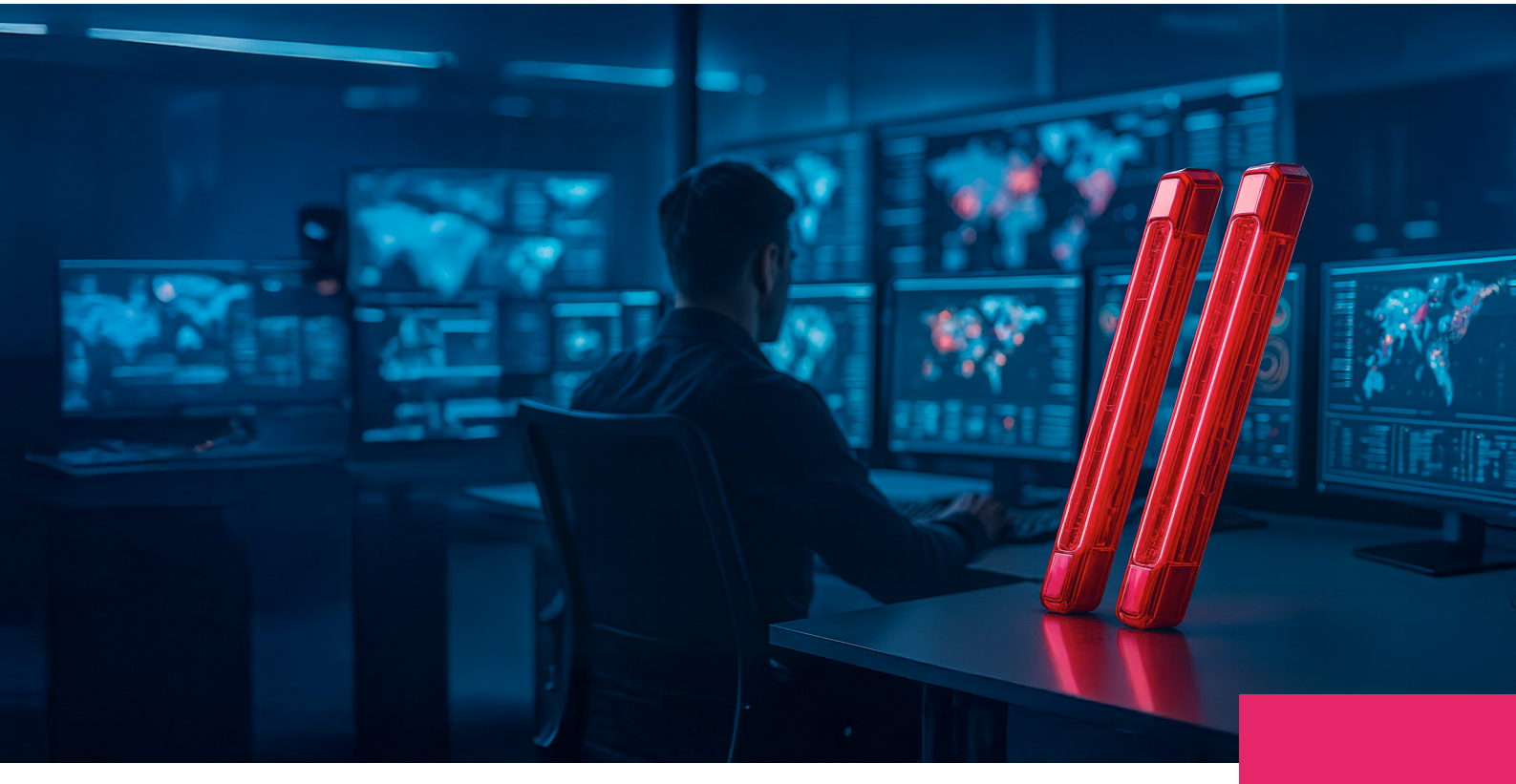
IA aplicada à engenharia social e roubo de identidade

A evolução da inteligência artificial também está ampliando o impacto da engenharia social. Ferramentas de IA generativa permitem criar mensagens altamente convincentes e adaptadas a contextos específicos, aumentando a eficácia de ataques que exploram identidade e confiança. Esse tipo de capacidade facilita a execução de campanhas de phishing personalizadas, fraudes baseadas em impersonificação e outros ataques que dependem da manipulação do comportamento humano.

IA no desenvolvimento de malware e operações autônomas

Outro impacto relevante observado no relatório é o uso crescente de IA no desenvolvimento e adaptação de malware. Ferramentas baseadas em inteligência artificial podem auxiliar na criação, modificação e otimização de códigos maliciosos, além de contribuir para a automação de diferentes etapas do ciclo de ataque.

Esse avanço aponta para o surgimento de operações cibernéticas cada vez mais autônomas, nas quais parte significativa das atividades ofensivas pode ser conduzida com mínima intervenção humana.



PREVISÕES PARA 2026: O FUTURO DA CIBERSEGURANÇA

O Cyber Security Report 2026 indica que o cenário de ameaças continuará evoluindo rapidamente nos próximos anos, impulsionado principalmente pela expansão da superfície digital, pelo uso crescente de inteligência artificial e pela profissionalização do crime cibernético.

Os dados analisados no relatório mostram que ataques estão se tornando **mais rápidos, mais automatizados e mais orientados por dados,** enquanto organizações enfrentam um ambiente cada vez mais complexo, com múltiplos vetores de exposição.

Nesse contexto, as previsões para 2026 apontam para um cenário em que automação, inteligência artificial, identidade digital e gestão de exposição se tornam elementos centrais tanto para atacantes quanto para defensores. A seguir, estão os principais movimentos destacados no relatório.

A engenharia social continuará evoluindo com apoio da IA

O relatório indica que ataques de engenharia social devem continuar crescendo em sofisticação e escala. Ferramentas de inteligência artificial permitem criar mensagens cada vez mais convincentes e personalizadas, facilitando campanhas de fraude, phishing e manipulação psicológica.

Essa evolução reduz as barreiras técnicas para execução de ataques e aumenta significativamente a taxa de sucesso dessas campanhas.

O modelo de ransomware continuará se expandindo

O modelo **Ransomware-as-a-Service (RaaS)** continuará sendo um dos principais motores do crime cibernético. Esse modelo permite que diferentes atores participem do ecossistema de ataques, oferecendo infraestrutura, ferramentas e serviços especializados para afiliados.
Como resultado, o ransomware tende a continuar evoluindo como um modelo de **negócio estruturado,** com divisão de funções e profissionalização crescente das operações.

Identidade digital seguirá como um dos principais alvos

Credenciais e identidades digitais continuam sendo um dos pontos mais explorados pelos atacantes.

O relatório destaca que comprometer contas privilegiadas, sistemas de autenticação ou identidades corporativas permite aos atacantes obter acesso inicial e movimentar-se dentro das redes com maior facilidade.

Por esse motivo, a proteção de identidade tende a se consolidar como um dos pilares da segurança corporativa.

A superfície de ataque continuará se expandindo

A adoção acelerada de tecnologias digitais, serviços em nuvem e plataformas baseadas em inteligência artificial está ampliando significativamente a superfície de ataque das organizações. Novos serviços, dispositivos conectados e aplicações corporativas criam ambientes cada vez mais complexos, dificultando a identificação e priorização de riscos.

Nesse cenário, a capacidade de **mapear e gerenciar continuamente a exposição digital** torna-se essencial para reduzir o risco de ataques.

Ataques se tornarão mais automatizados

A automação continuará desempenhando um papel crescente nas operações ofensivas. Ferramentas baseadas em inteligência artificial e automação permitem que atacantes executem etapas inteiras do ciclo de ataque de forma mais rápida e com menor intervenção humana.

A disputa entre ataque e defesa será cada vez mais baseada em dados

O relatório aponta que a capacidade de coletar, analisar e interpretar grandes volumes de dados será um fator decisivo na evolução da cibersegurança. Atacantes utilizam dados para identificar alvos e vulnerabilidades, enquanto defensores dependem da análise de telemetria e eventos para detectar atividades maliciosas.

Nesse contexto, a segurança tende a se tornar cada vez mais orientada por **análise de dados e inteligência operacional.**

O papel estratégico da cibersegurança continuará crescendo

Por fim, o relatório destaca que a cibersegurança continuará ganhando relevância estratégica dentro das organizações.

Ataques cibernéticos têm impacto direto sobre operações, reputação e continuidade de negócios, tornando a segurança digital um tema cada vez mais relevante para a liderança executiva.

Como resultado, o papel do CISO tende a se expandir, com maior envolvimento em decisões estratégicas relacionadas a risco, governança e resiliência digital.

RECOMENDAÇÕES PARA CISOS EM 2026

A evolução do cenário de ameaças exige uma abordagem mais estratégica por parte dos líderes de segurança. Com ataques cada vez mais rápidos, automatizados e distribuídos por diferentes vetores, as organizações precisam ir além da proteção tradicional baseada apenas em perímetro ou vulnerabilidades isoladas.

Nesse contexto, o papel do CISO passa a envolver não apenas a implementação de controles técnicos, mas também a construção de visibilidade operacional, governança de risco e capacidade de resposta a incidentes.

Apresentamos algumas recomendações prioritárias para líderes de segurança enfrentarem os desafios do novo cenário digital:

Tratar identidade como um dos principais perímetros de segurança

Com a crescente adoção de ambientes distribuídos, nuvem e trabalho remoto, a identidade digital tornou-se um dos principais vetores de ataque. Credenciais comprometidas, privilégios excessivos ou controles de autenticação inadequados podem permitir que atacantes obtenham acesso inicial a ambientes corporativos e se movimentem dentro da rede.

Nesse contexto, fortalecer mecanismos de autenticação, controle de privilégios e monitoramento de identidade torna-se essencial para reduzir o risco de comprometimento.

Por que isso importa para o CISO: Ataques baseados em identidade estão entre os vetores mais comuns de acesso inicial. A proteção de identidades e privilégios torna-se um elemento central para impedir que atacantes obtenham controle sobre ambientes corporativos.

Reduzir continuamente a superfície de exposição

Organizações modernas operam em ambientes cada vez mais complexos, com aplicações distribuídas, serviços em nuvem e dispositivos conectados. Essa expansão aumenta significativamente a superfície de ataque e dificulta a identificação de pontos de exposição que possam ser explorados por atacantes. Por isso, o relatório enfatiza a importância de monitorar continuamente a infraestrutura digital e identificar exposições que possam representar risco real de comprometimento.

Por que isso importa para o CISO: A capacidade de identificar e priorizar exposições reais permite que equipes de segurança concentrem esforços nos riscos com maior probabilidade de gerar impacto operacional.

Ampliar visibilidade sobre ambientes digitais

A visibilidade continua sendo um dos principais desafios para equipes de segurança. Ambientes híbridos, dispositivos não monitorados e sistemas distribuídos podem criar lacunas de monitoramento que permitem que atacantes operem sem serem detectados.

Garantir coleta de telemetria adequada, monitoramento contínuo e análise de eventos é fundamental para detectar atividades suspeitas em estágios iniciais de um ataque.

Por que isso importa para o CISO: Sem visibilidade adequada, organizações podem permanecer comprometidas por longos períodos sem perceber a presença de atacantes em seus ambientes.

Preparar a organização para resposta a incidentes

O relatório também destaca que, diante do aumento da sofisticação dos ataques, as organizações devem assumir que incidentes ocorrerão. Por isso, a capacidade de responder rapidamente a eventos de segurança torna-se um elemento crítico para limitar impactos operacionais e financeiros.
Isso inclui preparação de processos, definição clara de responsabilidades e desenvolvimento de planos de resposta a incidentes.

Por que isso importa para o CISO: Uma resposta rápida e estruturada pode reduzir significativamente o impacto de ataques cibernéticos e acelerar a recuperação operacional.

Incorporar inteligência e análise de dados na defesa

A crescente complexidade do cenário de ameaças exige que decisões de segurança sejam cada vez mais orientadas por dados. Ferramentas capazes de analisar grandes volumes de telemetria, identificar padrões e priorizar riscos tornam-se essenciais para apoiar as equipes de segurança.
Nesse contexto, inteligência de ameaças e análise avançada de dados passam a desempenhar um papel central na proteção de ambientes digitais.

Por que isso importa para o CISO: A capacidade de transformar dados em inteligência operacional permite detectar ataques mais cedo e responder com maior eficácia.

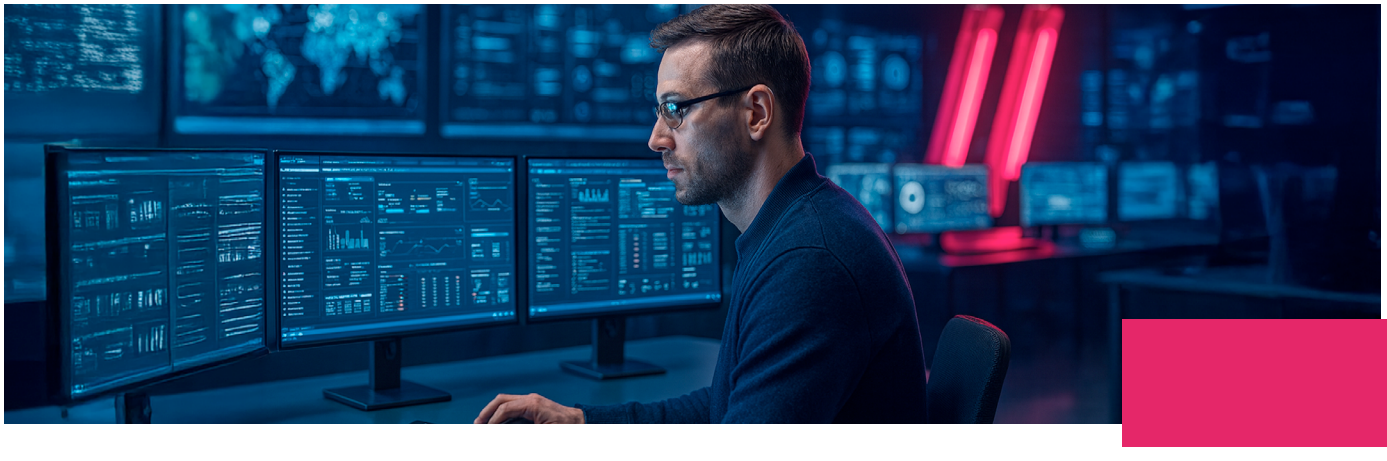
Trabalhar a perspectiva de Exposure Management

O Cyber Security Report 2026 destaca que o crescimento da superfície digital das organizações torna cada vez mais difícil identificar quais vulnerabilidades ou exposições realmente representam risco relevante.

Em vez de tratar apenas vulnerabilidades isoladas, a abordagem de Exposure Management busca identificar, priorizar e reduzir as exposições que efetivamente podem ser exploradas por atacantes.

Essa abordagem considera fatores como contexto, acessibilidade e impacto potencial, permitindo que equipes de segurança priorizem esforços de forma mais eficiente. Ao focar nas exposições que realmente podem levar a comprometimentos, organizações conseguem reduzir riscos de forma mais estratégica, direcionando recursos para os pontos de maior impacto dentro de sua superfície digital.

Por que isso importa para o CISO: Em um cenário de ataques cada vez mais rápidos e automatizados, a capacidade de identificar e priorizar exposições críticas torna-se essencial para reduzir o risco real de comprometimento.



AS AMEAÇAS ACELERARAM.
A DEFESA PRECISA ACELERAR TAMBÉM.

A análise do Cyber Security Report 2026, da Check Point Research, reforça uma tendência clara: os atacantes estão operando com níveis cada vez maiores de **velocidade, automação e inteligência.** A combinação de engenharia social avançada, inteligência artificial, expansão da superfície digital e novos modelos de ataque está redefinindo o cenário de risco para organizações em todo o mundo.

Em 2026, as empresas precisarão fortalecer sua capacidade de **reduzir exposição, proteger identidades, ampliar visibilidade e responder rapidamente a incidentes**. Mais do que implementar novas tecnologias, será essencial adotar modelos de segurança contínua, integrar diferentes camadas de proteção e transformar dados em inteligência operacional.

A CG One segue comprometida em apoiar organizações brasileiras nessa jornada. Como a parceira mais antiga da Check Point no Brasil, acompanhamos de perto a evolução das ameaças e das tecnologias de defesa, combinando **expertise, soluções líderes de mercado e serviços especializados** para ajudar empresas a transformar complexidade em resiliência digital. Com mais de **43 anos de experiência no mercado de tecnologia,** apoiamos nossos clientes na construção de estratégias de cibersegurança capazes de antecipar riscos e proteger operações críticas.

Atuamos em todo o ecossistema de proteção com:

Infrastructure Security

Identity & User Security

AppSec & DevOps

Managed Security Services (MSS)

Aceleramos a defesa para que sua empresa avance com segurança, hoje e no futuro.

CG//One