

PANORAMA DA CIBERSEGURANÇA 2026:

O QUE VAI DEFINIR O ANO
NA SEGURANÇA DIGITAL



- 3** Apresentação
- 4** Introdução
- 6** Capítulo 1 – Segurança de IA e para IA
- 8** Capítulo 2 – API Security: quando automação, IA e lógica de negócio viram o novo alvo
- 10** Capítulo 3 – Application Security: o desafio de proteger código em alta velocidade
- 12** Capítulo 4 – Application Flow Governance: quando a segurança precisa entender o caminho da aplicação
- 13** Capítulo 5 – Cloud Security: a segurança precisa acompanhar a complexidade
- 15** Capítulo 6 – CPS Security: quando a superfície de ataque alcança o mundo físico
- 17** Capítulo 7 – OT Security: quando a segurança deixa o chão de fábrica e vai para o board
- 19** As ameaças aceleraram. A defesa precisa acelerar também. Por isso, conte com a CG One para a segurança do seu negócio em 2026
- 20** Somos parceiros dos maiores fabricantes de tecnologia
- 21** Fontes



APRESENTAÇÃO

Este relatório reúne a visão da CG One sobre o estado da cibersegurança em 2025 e as principais tendências que devem moldar 2026. A partir da análise dos estudos mais recentes publicados por nossos parceiros estratégicos, construímos uma leitura integrada que conecta dados globais às transformações já perceptíveis no mercado brasileiro.

Nos últimos anos, o cenário de ameaças evoluiu em velocidade inédita. A automação impulsionada por IA, a expansão dos bots, o aumento de abusos contra APIs e o crescimento do ecossistema criminoso tornaram os ataques mais rápidos, eficientes e difíceis de detectar. Paralelamente, a complexidade das arquiteturas modernas, envolvendo aplicações distribuídas, fluxos entre serviços, ambientes multicloud, dados sensíveis, OT e sistemas ciberfísicos, passou a exigir novos modelos de proteção, governança e visibilidade.

O objetivo deste relatório é apresentar um panorama claro e direto sobre como essas forças estão moldando o risco digital em 2025 e o que elas sinalizam para 2026, destacando os movimentos que mais impactam empresas que operam no Brasil.

Boa leitura!



INTRODUÇÃO

2025: O ANO EM QUE O ATAQUE ACELEROU

O ano de 2025 consolidou um dos cenários de ameaças mais agressivos já registrados. A leitura combinada dos principais relatórios globais de cibersegurança — como os estudos publicados por Check Point e Fortinet — indica que o ecossistema do cibercrime entrou em uma fase de escala industrial, impulsionada por automação, exploração acelerada de vulnerabilidades, mercados clandestinos mais estruturados e uma migração clara para modelos de ataque que maximizam impacto e retorno financeiro.

O primeiro sinal dessa transformação está na **velocidade do atacante**. Segundo a Fortinet, o volume de recon avançado — etapa em que criminosos rastreiam ativos expostos — cresceu **16,7%**, atingindo cerca de **36 mil varreduras por segundo** em serviços de internet, aplicações corporativas, OT e protocolos industriais como Modbus TCP. Em paralelo, foram registradas **97 bilhões de tentativas de exploração** de vulnerabilidades em apenas 12 meses, enquanto o tempo médio entre a divulgação de uma falha e sua exploração ativa caiu para **5,4 dias**, confirmando uma janela de exposição quase imediata.

Ao mesmo tempo, **o mercado clandestino se sofisticou**. A Fortinet detectou um aumento de **42%** no volume de credenciais comprometidas colocadas à venda, e os fóruns de darknet registraram um salto de **500%** em logs de credenciais circulando entre criminosos. Essa tendência é reforçada pela Check Point, que destaca um crescimento de **58% em ataques baseados em infostealers**, alimentando um ciclo em que invasões começam, cada vez mais, pela **compra de acessos prontos**, muitas vezes com privilégios elevados.



A superfície de ataque também se expandiu:

- ▶ Dispositivos móveis se tornaram ponto de entrada relevante, com campanhas de phishing multicanal e aplicativos falsos;
- ▶ Ambientes de nuvem e SaaS continuam entre os vetores mais explorados, sobretudo por erros de configuração;
- ▶ OT e IoT seguem expostos a protocolos inseguros e redes pouco segmentadas;
- ▶ E o e-mail permanece como o canal de ataque mais barato e mais lucrativo para grupos de crime organizado.

O **ransomware**, por sua vez, entrou em uma nova fase. A Check Point indica que o modelo operacional migrou da simples criptografia para **extorsão baseada em exfiltração de dados e ameaças de vazamento**, agora reforçadas por doxxing, pressão sobre executivos e divulgação pública progressiva. O setor de saúde é hoje o **segundo mais atacado no mundo**, reflexo não apenas do valor dos dados, mas também da impossibilidade de paralisação operacional. Grupos de Ransomware-as-a-Service amadureceram: poucos operadores controlam plataformas completas, oferecendo kits, suporte e programas de afiliação, trazendo ao crime digital a lógica de franquias.

Outro vetor que cresce de forma consistente é o **ataque à cadeia de suprimentos**. Ferramentas de terceiros, integrações API, acessos remotos, bibliotecas open-source e provedores de OT aparecem como portas de entrada frequentes. Tanto Fortinet quanto Check Point destacam que invasões bem-sucedidas começam, cada vez mais, por dependências externas.



E somado a tudo isso, 2025 foi o ano em que a **Inteligência Artificial entrou no ataque de forma explícita**. O relatório de IA da Check Point traz exemplos de modelos “dark” como HackerGPT, WormGPT e FraudGPT, além de plataformas falsas de IA, extensões maliciosas e uso de LLMs para criação automatizada de phishing, scripts, payloads e engenharia social personalizada. A automação deixou de ser diferencial do defensor — agora, é ferramenta madura também para o criminoso.

Esses dados mostram um cenário em que o atacante opera com **velocidade, escala e especialização inéditas**. Explorações acontecem dias após novas falhas serem divulgadas; credenciais comprometidas estão disponíveis para compra quase instantânea; e grupos criminosos têm acesso a ferramentas profissionais impulsionadas por IA.

Nos próximos capítulos, este relatório aprofunda como essa aceleração do ataque está impactando **domínios específicos da segurança**, analisando os principais movimentos em **Segurança de IA, APIs, aplicações, ambientes cloud, sistemas ciberfísicos (CPS) e OT**. A partir da leitura combinada dos relatórios globais e da visão prática da CG One, exploramos onde estão os riscos mais críticos hoje e o que deve ganhar prioridade em 2026.

CAPÍTULO 1

SEGURANÇA DE IA E PARA IA

A adoção corporativa de IA cresceu rapidamente, mas o cibercrime cresceu ainda mais. O relatório *The State of AI Cyber Security* da Check Point mostra que 2025 foi o ano em que a IA passou a atuar **ativamente a favor do atacante**, automatizando processos, ampliando escala e tornando ataques mais personalizados e difíceis de detectar.

LLMs públicos: o novo laboratório do cibercrime

Sempre que um novo LLM é lançado, ele vira imediatamente objeto de testes em fóruns underground. Criminosos usam esses modelos para:

- ↳ Gerar phishing convincente;
- ↳ Escrever scripts de exploração;
- ↳ Automatizar fraudes;
- ↳ Criar engenharia social hiperpersonalizada;
- ↳ Produzir payloads com baixa detecção.

Cada novo modelo público abre uma janela de oportunidade para o atacante, muitas vezes antes de as empresas entenderem como usá-lo de forma segura.

A ascensão dos “dark models”

Além dos LLMs abertos, surgiram modelos criados exclusivamente para fins criminosos, como:

- ↳ OnionGPT;
- ↳ HackerGPT;
- ↳ FraudGPT;
- ↳ WormGPT.

Esses modelos removem salvaguardas e permitem:

- ↳ Gerar malware;
- ↳ Montar campanhas de phishing completas;
- ↳ Criar ferramentas de fraude;
- ↳ Escrever scripts ofensivos sob demanda.

Não são versões modificadas, são **plataformas projetadas para abuso desde o início**.

Extensões e plataformas falsas de IA

Outro vetor em expansão envolve ferramentas que se disfarçam de IA legítima:

- ↳ **Extensões falsas** que imitam apps populares para roubar sessões e credenciais (incluindo casos envolvendo o nome “ChatGPT”);
- ↳ **Plataformas de IA forjadas**, criadas para distribuir malware ou capturar dados corporativos.

Esses ataques exploram a pressa das organizações em adotar IA sem validação adequada.

O risco não é apenas o modelo, é também o uso corporativo

Segurança de IA não se limita ao modelo: envolve proteger **como a IA é usada dentro da empresa**.

Principais riscos:

- **Shadow AI:** colaboradores usando ferramentas públicas com dados sensíveis;
- **Plugins e extensões sem validação:** coleta indevida de informações e sessões;
- **Fluxos de dados sem governança:** conteúdo corporativo indo para modelos externos sem controle;
- **Código gerado por IA:** aumento da velocidade, mas também da superfície de vulnerabilidades.

Proteção de modelos LLMs: quando a IA corporativa vira ativo crítico

Além do uso indevido de ferramentas públicas e da proliferação de modelos “dark”, 2025 também marcou o avanço da **IA proprietária dentro das empresas**. Cada vez mais organizações treinam ou utilizam LLMs próprios, conectados a bases internas, dados sensíveis, sistemas corporativos e fluxos críticos de negócio.

Nesse contexto, surge uma nova categoria de risco: **a segurança do próprio modelo**. Os relatórios da Check Point mostram que atacantes já exploram falhas específicas de IA, como:

- Prompt injection;
- Jailbreaks;
- Vazamento de dados via respostas do modelo;
- Manipulação de comportamento do LLM;
- Abuso de integrações com sistemas internos.

Quando um LLM corporativo é comprometido, o impacto vai além de um incidente tradicional: o modelo pode passar a **expor dados sensíveis, tomar decisões incorretas, executar ações indevidas ou servir como vetor de acesso a outros sistemas**.



O QUE ISSO SIGNIFICA PARA AS EMPRESAS

A IA mudou o perfil do atacante: agora, **máquinas escrevem, testam e iteram ataques** em uma velocidade difícil de acompanhar. Para a CG One, isso exigirá para 2026:

- Tratar Segurança de IA como um **novo domínio de risco corporativo**;
- Ter **visibilidade total** sobre ferramentas, usos e dados expostos;
- Conectar o tema a **Data Security** (evitar vazamento via ferramentas públicas);
- Integrar com **AppSec** (revisão do código gerado por IA);
- Trabalhar na proteção de **modelos LLMs corporativos**;
- E reforçar **governança e educação** para uso seguro de IA.

A IA acelerou a ofensiva. A defesa precisa evoluir com a mesma velocidade, protegendo não apenas modelos, mas **tudo o ecossistema de uso de IA** dentro das organizações.

CAPÍTULO 2

API SECURITY: QUANDO AUTOMAÇÃO, IA E LÓGICA DE NEGÓCIO VIRAM O NOVO ALVO

APIs se tornaram o motor da inovação digital: suportam integrações, experiências de cliente, automações e aplicações modernas. Mas, em 2025, também se consolidaram como um dos alvos mais explorados por atacantes e bots impulsionados por IA.

APIs deixaram de ser apenas um elemento técnico e passaram a ser um componente central do risco cibernético. Em 2026, proteger APIs será tão estratégico quanto proteger dados, identidade e aplicações.

O ataque automatizado às APIs ganhou escala com IA

O relatório da Akamai *Fraud and Abuse Report 2025* mostra que bots impulsionados por IA cresceram **300% em um ano**, automatizando ataques que antes dependiam de habilidade humana. Esses bots:

- ↘ Exploram **fluxos de sessão**;
- ↘ Abusam de **autenticação e autorização**;
- ↘ Detectam padrões de negócio;
- ↘ Testam e iteram ataques em escala.

A Akamai destaca que vários desses bots conseguem intensificar riscos em aplicações e **APIs**, explorando lógica de negócio e mecanismos de autenticação de forma automatizada.

Enquanto isso, atividades como scraping avançado, abuso de endpoints e automação de fraudes se tornaram mais difíceis de detectar porque muitos desses bots passaram a imitar comportamento humano.

APIs se tornaram porta de entrada para comprometimento de identidade e movimento lateral

A Fortinet reforça que APIs desempenham um papel crítico no comprometimento de ambientes cloud. Em sua telemetria global, a empresa observou:

- ↘ **Novas APIs sendo invocadas por contas comprometidas** (20% dos casos);
- ↘ Uso de APIs como vetor para **escalar privilégios**;
- ↘ Exploração de APIs de metadados (T1556.004) para assumir identidades em nuvem;
- ↘ Uso de APIs para manter persistência e realizar exfiltração silenciosa.

O recado é claro: APIs deixaram de ser apenas um meio de integração e tornaram-se um mecanismo central para ataques baseados em identidade.

APIs são agora um dos riscos mais esperados pelos times de AppSec

O relatório *The Future of Application Security in the Era of AI* da Checkmarx confirma uma tendência: a superfície de ataque de APIs cresceu mais rápido do que a capacidade de defendê-la.

Os estudos mostram que:

- **32% das organizações acreditam que um API breach será um dos incidentes mais prováveis nos próximos 12–18 meses;**
- APIs concentram riscos relacionados a **business logic abuse**;
- Falhas de autenticação e autorização permanecem entre os vetores mais explorados;
- APIs mal documentadas ou desconhecidas (shadow/zombie APIs) continuam sendo um dos maiores pontos cegos.

Com o uso crescente de microserviços, open-source e pipelines acelerados por IA, APIs passaram a ser criadas, expostas e modificadas em ciclos muito mais rápidos, muitas vezes sem segurança acoplada desde o design.



O QUE ISSO SIGNIFICA PARA AS EMPRESAS

API Security deixou de ser uma preocupação apenas de AppSec para se tornar uma disciplina transversal que impacta:

- **Cloud security** (identidade, governança, postura);
- **Fraude e abuso** (bots, automação, scraping, lógica de negócio);
- **AppSec** (shift-left de APIs, código gerado por IA);
- **Dados** (exposição via APIs públicas, SaaS e integrações).

Para empresas, isso significará em 2026:

- Acelerar **API discovery** para eliminar shadow/zombie APIs;
- Adotar plataformas integradas de **proteção de APIs e aplicações**;
- Incluir APIs na governança de identidade e acesso;
- Aplicar princípios de **zero trust** a cada requisição;
- Monitorar tráfego com foco em comportamento, não apenas em assinatura;
- Validar segurança desde o design até o runtime com **shift-left + observabilidade**.

2026 será o ano em que as APIs deixarão de ser apenas um risco técnico e passarão a ser um risco estratégico.

CAPÍTULO 3

APPLICATION SECURITY: O DESAFIO DE PROTEGER CÓDIGO EM ALTA VELOCIDADE

O relatório da Checkmarx mostra que o ciclo de desenvolvimento moderno — impulsionado por IA, pipelines automatizados e pressões de entrega — criou uma nova dinâmica: o software evolui rápido demais para que a segurança acompanhe com modelos tradicionais. O resultado é um aumento do risco no próprio processo de desenvolvimento.

A IA já participa da construção do software

A velocidade aumentou porque a IA passou a atuar como copiloto dos desenvolvedores. O estudo revela:

- ↘ Uso amplo de **assistentes de código baseados em IA**;
- ↘ Em muitos times, **mais de 60% do código** já é gerado automaticamente.

Isso acelera entregas, mas também multiplica a chance de introduzir vulnerabilidades logo no primeiro commit.

Segurança ainda não acompanha o ritmo

Mesmo com automação crescente, a maturidade de AppSec continua abaixo do necessário:

- ↘ Ferramentas como SAST, SCA e DAST ainda são usadas de forma **fragmentada**;
- ↘ Menos da metade das empresas integra segurança diretamente no pipeline.

O resultado é um ciclo em que vulnerabilidades entram cedo e são descobertas tarde demais.



Código vulnerável indo para produção

A pressão por velocidade cria uma cultura perigosa:

▼ **81%** das organizações admitem liberar código vulnerável para produção em alguns momentos.

Não por falta de ferramentas, mas por falta de tempo, prioridade ou automação de correção.

Incidentes de segurança continuam crescendo

A consequência é clara:

▼ **98%** das organizações registraram ao menos um incidente relacionado a código inseguro nos últimos anos.

À medida que mais software depende de integrações, APIs e componentes open-source, o impacto das vulnerabilidades se multiplica.



O QUE ISSO SIGNIFICA PARA AS EMPRESAS

Para a CG One, AppSec em 2026 exigirá abandonar modelos reativos e adotar uma abordagem **code-to-cloud**, cobrindo todo o ciclo de desenvolvimento:

- ▼ Integrar segurança diretamente no pipeline;
- ▼ Automatizar triagem, correção e priorização;
- ▼ Incorporar inteligência artificial na defesa, não apenas no desenvolvimento;
- ▼ Reforçar governança de bibliotecas open-source e IaC;
- ▼ E conectar AppSec à segurança de dados e de IA.

Se a velocidade do desenvolvimento aumentou, a segurança precisa acompanhar, protegendo o código desde o primeiro commit até a produção.

CAPÍTULO 4

APPLICATION FLOW GOVERNANCE: QUANDO A SEGURANÇA PRECISA ENTENDER O CAMINHO DA APLICAÇÃO

O relatório *AlgoSec State of Network Security Report 2025* evidencia um ponto crítico que afeta diretamente a resiliência das empresas: **a falta de visibilidade sobre como as aplicações realmente se conectam.**

Ambientes híbridos, multicloud e arquiteturas distribuídas criaram dependências complexas — entre APIs, bancos de dados, microserviços, firewalls, gateways, SD-WAN e SASE — que tornam a conectividade tão importante quanto o próprio código.

Segundo o estudo, **71% das equipes de segurança relatam dificuldades de visibilidade sobre conectividade de aplicações, políticas de segurança e dependências**, o que atrasa a detecção de ameaças, aumenta a probabilidade de falhas de configuração e expõe aplicações a caminhos laterais não intencionais.

Essa lacuna operacional, mais do que vulnerabilidades técnicas, é hoje um dos maiores fatores de risco. Regras permissivas, segmentação incompleta, mudanças feitas sem validação e permissões excessivas entre ambientes criam brechas que atacantes exploram com facilidade, especialmente em infraestruturas distribuídas.

A abordagem orientada pela AlgoSec, centrada na aplicação, reforça a necessidade de mapear fluxos, automatizar análise de impacto e aplicar o princípio de menor privilégio na conectividade. Em outras palavras: **não basta proteger a aplicação; é preciso proteger o caminho que ela percorre.**



O QUE ISSO SIGNIFICA PARA 2026

Com a expansão contínua de cloud, SD-WAN, SASE e automação, as empresas precisarão:

- ▶ Garantir visibilidade completa dos fluxos entre aplicações;
- ▶ Fortalecer segmentação baseada em necessidade real;
- ▶ Automatizar validação de políticas antes de mudanças;
- ▶ Reduzir caminhos laterais que facilitam intrusões;
- ▶ Integrar segurança de aplicações, nuvem e rede em um único fluxo de governança.

Em um cenário cada vez mais distribuído, **governar conectividade é tão essencial quanto proteger código ou infraestrutura.**

CAPÍTULO 5

CLOUD SECURITY: A SEGURANÇA PRECISA ACOMPANHAR A COMPLEXIDADE

A nuvem se tornou a espinha dorsal da arquitetura moderna, mas a complexidade cresceu mais rápido que os controles. O *2025 Cloud Security Report* da Fortinet revela que grande parte das brechas atuais nasce menos em ataques sofisticados e mais em **erros de configuração, falta de visibilidade e ambientes multi-cloud difíceis de orquestrar**.

A realidade hoje é híbrida e multi-cloud

Segundo a Fortinet, a maioria das empresas já opera em um ambiente fragmentado:

- ↘ **54%** usam modelos híbridos (on-prem + cloud).
- ↘ **78%** utilizam **dois ou mais provedores de nuvem**.

Essa diversidade aumenta flexibilidade, mas cria superfícies de ataque mais amplas e inconsistências de política entre plataformas.

Segurança e compliance são as maiores barreiras

Mesmo com adoção avançada, as principais preocupações continuam sendo:

- ↘ **61%** veem segurança como o maior desafio na nuvem.
- ↘ Lacunas de **compliance**, exposição de dados e falta de padronização aparecem como riscos críticos.

Não é falta de tecnologia, é falta de **uniformidade e governança**.



Falta de profissionais especializados

A escassez de competências em cloud security continua um obstáculo:

- ↘ **76%** das organizações relatam dificuldade para contratar ou formar times com conhecimentos avançados de segurança em nuvem.

A consequência: ambientes ficam configurados de forma inconsistente, aumentando risco e dependência de terceiros.

Visibilidade e detecção continuam incompletas

Mesmo empresas maduras admitem limitações ao monitorar ambientes cloud:

- ↘ **64%** não se sentem plenamente confiantes na detecção de ameaças em tempo real.

A fragmentação entre provedores, workloads efêmeros e SaaS sem integração tornam a detecção mais complexa do que no data center tradicional.

O movimento do mercado: convergência e automação

O estudo aponta uma direção clara:

- ↘ **97%** preferem **plataformas unificadas** de segurança em nuvem.
- ↘ Adoção de **CSPM** (Cloud Security Posture Management) e **CNAPP** cresce de forma acelerada.

A prioridade agora não é “mais ferramentas”, mas **menos silos**.



O QUE ISSO SIGNIFICA PARA AS EMPRESAS

Para a CG One, Cloud Security em 2026 significará:

- ↘ Reduzir superfícies de ataque criadas por ambientes multi-cloud;
- ↘ Adotar plataformas unificadas com visão de postura e risco;
- ↘ Integrar identidade, rede, dados e configuração em um mesmo ecossistema;
- ↘ E operar com **visibilidade contínua**, não apenas auditorias pontuais.

A nuvem já é padrão. Agora, a segurança precisa atingir o mesmo nível de velocidade, integração e automação.

CAPÍTULO 6

CPS SECURITY: QUANDO A SUPERFÍCIE DE ATAQUE ALCANÇA O MUNDO FÍSICO

Sistemas ciberfísicos (CPS) — que integram TI, OT, IoT, sistemas industriais e dispositivos conectados — ampliaram drasticamente a superfície de ataque das organizações. O relatório *The Global State of CPS Security 2025* da Claroty mostra que 2025 foi o ano em que riscos digitais passaram a gerar impactos reais no mundo físico, pressionando empresas a repensarem governança, fornecedores e continuidade operacional.

Cadeia de suprimentos virou vetor crítico

Mudanças globais e dependência crescente de terceiros elevaram o risco estrutural:

- ▼ **49%** das organizações afirmam que tensões econômicas e geopolíticas aumentaram o risco em CPS;
- ▼ **67%** estão reavaliando a **geografia da cadeia de suprimentos** por preocupações de segurança;
- ▼ **73%** estão revisando **acesso remoto de terceiros** aos sistemas operacionais.

A fragilidade não está apenas no ambiente interno — está também nos parceiros conectados.

Acesso de terceiros está por trás de muitos incidentes

O estudo evidencia que fornecedores muitas vezes introduzem risco sem que a empresa perceba:

- ▼ **46%** registraram incidentes originados em acessos de terceiros;
- ▼ **54%** descobriram lacunas de segurança ou compliance **somente após o incidente ocorrer**.

Ou seja: em CPS, o atacante muitas vezes entra pela porta de alguém que já tem acesso autorizado.



Reguladores estão aumentando a pressão

Com incidentes crescendo, setores regulados enfrentam exigências mais rígidas:

- **76%** acreditam que novas regulações exigirão revisões profundas na estratégia de segurança de CPS.
- Normas internacionais (NIST, IEC, ENISA) estão sendo cada vez mais incorporadas pelos programas corporativos.

Com OT, CPS e TI convergindo, a cobrança sobre governança e resiliência tende a aumentar.

Operações críticas exigem visibilidade total

Ambientes CPS reúnem:

- Dispositivos IoT com pouca segurança;
- Sistemas industriais legados;
- Redes OT pouco segmentadas;
- Aplicações modernas conectadas via API.

Sem inventário, sem monitoramento contínuo e sem segmentação, o risco de interrupção operacional cresce exponencialmente.



O QUE ISSO SIGNIFICA PARA AS EMPRESAS

Proteger CPS em 2026 vai demandar:

- Tratar cadeia de suprimentos como parte do perímetro;
- Estabelecer controles fortes de acesso remoto de fornecedores;
- Integrar OT, IoT e TI em um mesmo modelo de visibilidade;
- Reforçar governança e alinhamento a normas internacionais;
- Preparar operações para impacto físico e indisponibilidade, não apenas vazamento de dados.

Quando o digital encontra o físico, o risco se amplifica. CPS é hoje um dos pontos mais sensíveis da segurança corporativa e um dos que mais exigem evolução imediata.

CAPÍTULO 7

OT SECURITY: QUANDO A SEGURANÇA DEIXA O CHÃO DE FÁBRICA E VAI PARA O BOARD

O relatório *State of Operational Technology 2025* da Fortinet mostra que 2025 foi um ano de virada para OT Security. O tema deixou de ser responsabilidade exclusiva das operações industriais e passou a ser tratado como **assunto estratégico**, com impacto direto em continuidade, risco corporativo e regulamentação. A convergência entre TI e OT trouxe benefícios, mas também ampliou a superfície de ataque dos ambientes industriais — historicamente isolados e agora cada vez mais conectados.

OT finalmente chega à liderança executiva

A governança de OT evoluiu, refletindo a criticidade das operações:

- ▶ **52%** das organizações já têm CISO/CSO como responsável direto pela segurança de OT.
- ▶ A tendência segue acelerada: intenção de mover OT para o CISO chega a 80% nos próximos 12 meses.

Isso mostra que OT deixou de ser “coisa do chão de fábrica” e se tornou parte do **framework corporativo de risco**.

Maturidade operacional em avanço

A Fortinet aponta uma elevação clara na maturidade dos programas de OT Security:

- ▶ **49%** das organizações afirmam estar em **Nível 4** de maturidade (processos estruturados, uso de threat intelligence, monitoramento contínuo).

Esse avanço reduz impacto de intrusões, mas ainda não elimina os riscos trazidos pela conectividade crescente.



Ambientes industriais continuam vulneráveis

Mesmo com maior governança, desafios técnicos persistem:

- Sistemas **legados** difíceis de atualizar;
- Protocolos **não projetados para segurança** (Modbus, DNP3, outros);
- Falta de segmentação entre TI e OT;
- Dispositivos críticos operando sem visibilidade contínua.

A combinação de legado + conectividade cria cenários em que um ataque simples pode gerar impacto operacional severo.

TI e OT: uma convergência inevitável

A integração entre ambientes trouxe ganhos, mas também tensões:

- TI exige segurança, padronização e telemetria;
- OT exige estabilidade, disponibilidade e mínima intervenção.

O ponto crítico: qualquer mudança em OT pode parar produção, o que reforça a necessidade de **processos seguros de atualização, visibilidade granular e segmentação adequada**.



O QUE ISSO SIGNIFICA PARA AS EMPRESAS

Para a CG One, OT Security em 2026 exigirá equilíbrio entre **continuidade operacional e segurança avançada**, incluindo:

- Governança de OT integrada ao CISO e às estruturas corporativas;
- Inventário contínuo de ativos industriais;
- Segmentação forte entre TI e OT, com integração controlada e monitorada;
- Monitoramento 24x7 com contexto operacional;
- Processos formais de gestão de mudanças (GMUD) específicos para ambientes industriais;
- Alinhamento a normas globais (NIST, IEC, ENISA) e requisitos regulatórios.

OT entrou definitivamente na pauta executiva e a segurança das operações físicas se tornou parte essencial da resiliência do negócio.

AS AMEAÇAS ACELERARAM. A DEFESA PRECISA ACELERAR TAMBÉM. POR ISSO, CONTE COM A CG ONE PARA A SEGURANÇA DO SEU NEGÓCIO EM 2026.

A análise integrada dos relatórios dos nossos parceiros mostra um ponto comum: **o atacante opera com mais velocidade, escala e inteligência do que nunca**. Em 2025, IA, multi-cloud, dados, aplicações modernas, OT e CPS ampliaram a superfície de risco, e 2026 exigirá que a defesa evolua com a mesma rapidez.

As organizações brasileiras precisarão adotar **modelos de segurança contínua**, fortalecer governança, integrar áreas antes isoladas e modernizar operações de detecção e resposta. Não se trata apenas de tecnologia, mas de **visibilidade, integração e disciplina operacional**.

A CG One segue comprometida em apoiar empresas nessa transição, unindo expertise, tecnologia e serviços gerenciados para transformar complexidade em resiliência.

Com mais de **43 anos de experiência no mercado de tecnologia**, oferecemos soluções de cibersegurança escaláveis para **detectar e bloquear ataques antes mesmo que aconteçam**. 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.



ENTRE EM CONTATO **COM UM
ESPECIALISTA**

SOMOS PARCEIROS DOS MAIORES FABRICANTES DE TECNOLOGIA

A CG One trabalha lado a lado com os **principais fabricantes globais de tecnologia**, oferecendo soluções líderes de mercado para os desafios atuais de cibersegurança:



FONTES

Check Point Software Technologies

- 2025 Cyber Security Report
- The State of AI Cyber Security Report

Fortinet

- 2025 Fortinet Threat Landscape Report
- 2025 Data Security Report
- 2025 Cloud Security Report
- 2025 State of Operational Technology and Cybersecurity Report

Akamai

- State of the Internet / Security — Fraud and Abuse Report 2025: Charting a Course Through AI's Murky Waters

AlgoSec

- AlgoSec State of Network Security Report 2025

Clarity

- The Global State of CPS Security – 2025

Checkmarx

- The Future of Application Security in the Era of AI – 2026 Outlook



CG//One

