

# Uma plataforma completa de AppSec nativa na nuvem: conheça a Checkmarx One

## O Cenário

**O desenvolvimento de aplicações evoluiu.** Hoje, há mais softwares implantados em diversos ambientes, e o tempo para protegê-los é cada vez mais escasso. Deploys ocorrem várias vezes ao dia, o desenvolvimento é complexo e predominantemente nativo em nuvem.

A responsabilidade pela segurança não é mais exclusiva das equipes de segurança: agora é um esforço conjunto entre gerentes de AppSec e desenvolvedores. A colaboração e confiança entre CISOs, equipes de desenvolvimento e segurança são fundamentais para minimizar riscos e evitar aplicações vulneráveis.

**Construir #DevSecTrust exige uma abordagem holística.** Os CISOs precisam compreender os desafios enfrentados por suas equipes de AppSec e desenvolvimento, enquanto buscam maior visibilidade sobre a segurança de aplicações em toda a empresa. As ferramentas de AppSec devem atender às necessidades de diversos stakeholders, refletindo também a crescente influência dos desenvolvedores, cuja experiência se tornou um fator crítico na escolha de qualquer solução de AppSec.

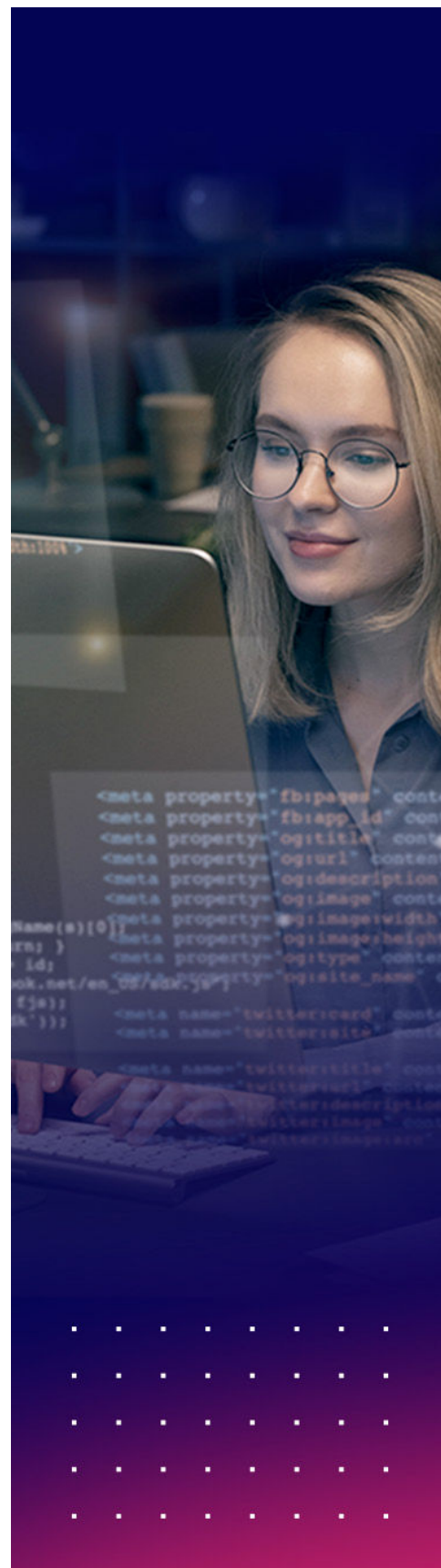
No entanto, muitos CISOs enfrentam dificuldades para obter o engajamento dos times de desenvolvimento, o que compromete a eficiência e a adesão às políticas de segurança de aplicações.

Além disso, em um cenário onde diferentes ferramentas de segurança – como uma colcha de retalhos – são utilizadas, a visibilidade se torna outro grande desafio. Com pontos de ameaça vindos de diversos componentes, como bibliotecas, códigos IaC,

ferramentas de IA e softwares open source, é comum que faltem indicadores claros. Muitos CISOs relatam dificuldades para monitorar quantas vulnerabilidades foram corrigidas desde o início do programa de AppSec e há quanto tempo elas estão rodando sem resolução, o que enfraquece o controle sobre a segurança.

Essas lacunas impactam diretamente os negócios: em uma pesquisa recente da Checkmarx com 200 CISOs, **77% dos entrevistados afirmaram que mais da metade da receita de suas organizações depende de aplicações sob sua responsabilidade de proteção.** Outro dado relevante é que **42% dos CISOs precisam divulgar publicamente seus relatórios de AppSec**, enquanto 44% compartilham essas informações mediante solicitação de compradores, como uma medida para tranquilizar clientes potenciais.

Em um cenário onde a confiança dos clientes e a continuidade dos negócios dependem das aplicações, investir em AppSec deixou de ser uma escolha e se tornou uma necessidade estratégica. Com a crescente complexidade do desenvolvimento de software e a pressão por maior transparência, garantir que a segurança esteja integrada em cada etapa do ciclo de vida do desenvolvimento (SDLC) é fundamental para a proteção e a longevidade das operações empresariais.



# A Solução

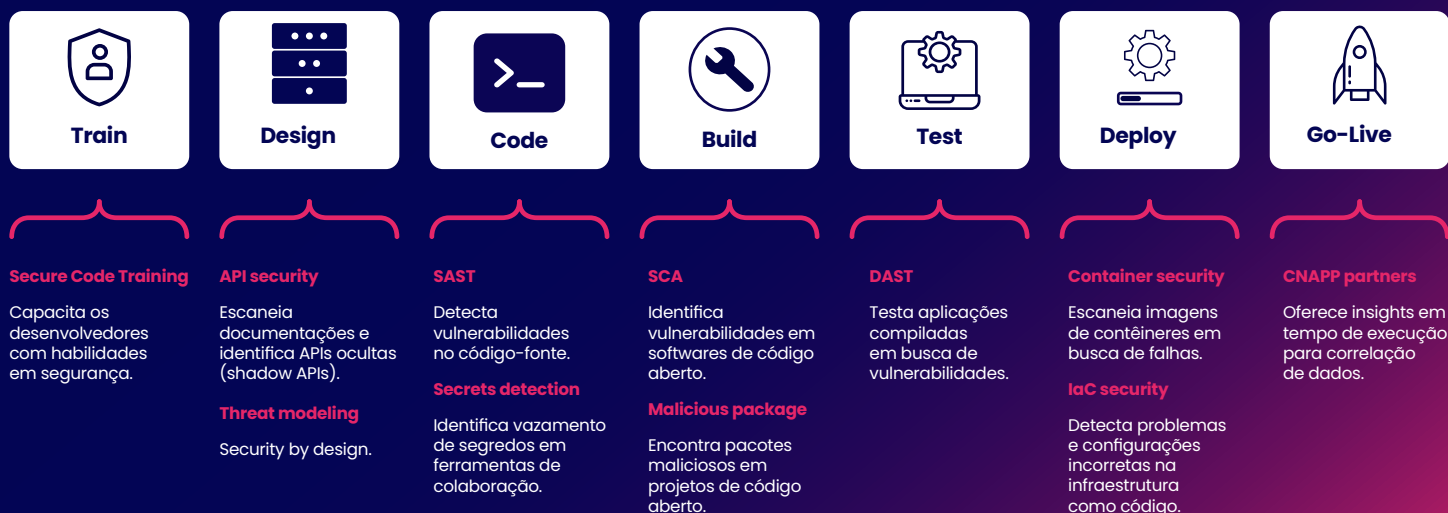
## Checkmarx One: uma plataforma de segurança de aplicações nativa na nuvem

**Tudo o que as empresas precisam para proteger o desenvolvimento de aplicações – do código à nuvem – em uma plataforma unificada.**

A plataforma Checkmarx One, fornecida pela CG One, oferece um conjunto completo de soluções de AppSec em uma plataforma unificada e nativa na nuvem. Com ela, você consolida seu conjunto de ferramentas de AppSec para reduzir o TCO (total cost of ownership – custo total de propriedade) **em até 50%.**

A plataforma fornece recursos para integrar e correlacionar dados de várias soluções, ajudando você a identificar quais vulnerabilidades são exploráveis. **Isso torna mais fácil analisar e priorizar vulnerabilidades em todo o escopo das suas aplicações.**

Tenha em um único lugar todas as soluções necessárias para a segurança de aplicações nativas em nuvem, incorporando AppSec em cada estágio do SDLC para um programa de segurança abrangente:



# Módulos



## ➤ Static Application Security Testing (SAST)

Realize varreduras rápidas e precisas para identificar riscos no seu código. Alterne facilmente entre análises profundas de aplicações críticas e varreduras rápidas e abrangentes, conforme sua necessidade.

## ➤ Software Composition Analysis (SCA)

Identifique riscos de segurança e de licenciamento em softwares de código aberto usados em suas aplicações. A funcionalidade Exploitable Path ajuda a determinar quais vulnerabilidades são realmente exploráveis, permitindo priorizar as correções e reduzir ruídos.

## ➤ Supply Chain Security (SCS)

Identifique proativamente ataques à cadeia de suprimentos e proteja ambientes de desenvolvimento com detecção de vulnerabilidades e pacotes maliciosos de código aberto, SBOMs (software bill of materials), Project Scorecard e detecção de segredos no código e nas fontes de desenvolvimento.

## ➤ API Security

Descubra todas as APIs em sua aplicação e compare o inventário completo com a documentação para eliminar APIs ocultas (shadow APIs) e APIs obsoletas (zombie APIs), mitigando riscos.

## ➤ Dynamic Application Security Testing (DAST)

Identifique vulnerabilidades visíveis apenas em produção e avalie seu comportamento ao testar contra uma ampla gama de ataques em aplicações web.

## > Container Security

---

Escaneie imagens de contêiner estáticas, verifique configurações e identifique pacotes de código aberto, detectando vulnerabilidades antes da produção.

## > Infrastructure-as-Code (IaC) Security

---

Escaneie seus arquivos IaC para encontrar vulnerabilidades de segurança, problemas de conformidade e configurações incorretas de infraestrutura, utilizando milhares de consultas predefinidas.

## > Cloud and Runtime Insights

---

Estenda a segurança de aplicações (AppSec) até a produção por meio de tecnologias e parcerias da Checkmarx. Receba insights em tempo de execução diretamente de provedores de serviços em nuvem ou por meio de parcerias tecnológicas, correlacionando esses insights com vulnerabilidades de código aberto para proteger contêineres durante a execução das aplicações.

## > Codebashing

---

Treine desenvolvedores em práticas de codificação segura com trilhas de aprendizado personalizadas, reduzindo o risco de segurança desde a primeira linha de código.



# Características

---

## Application Security Posture Management (ASPM): o poder da plataforma

O ASPM ajuda as equipes de AppSec a aproveitarem melhor seu conjunto de ferramentas para gerenciar de forma eficaz seus papéis cada vez mais desafiadores. À medida que mais empresas adotam uma mentalidade de integração total, passam a adquirir mais ferramentas de AppSec e acabam lidando com um número excessivo de produtos, ferramentas e controles de segurança distintos que precisam ser implementados e gerenciados – tudo isso sem contar com recursos e pessoas suficientes para gerenciar de maneira eficaz.

O ASPM possibilita a correlação de resultados entre as ferramentas de AppSec individuais, permitindo que você priorize facilmente a remediação das vulnerabilidades mais críticas e maximize o uso dos recursos da sua equipe.

## Otimize a experiência dos desenvolvedores em seu programa de AppSec

A AppSec não se resume apenas à identificação de vulnerabilidades, mas também à sua correção. Para garantir a segurança total das aplicações, a colaboração entre as equipes de AppSec, que identificam as fraquezas de segurança, e os desenvolvedores, que as corrigem, é fundamental. Abordar a segurança de aplicações requer uma abordagem holística que preencha a lacuna entre esses dois jogadores essenciais, e o caminho para o sucesso passa pelos próprios desenvolvedores.

Por isso, líderes bem-sucedidos em AppSec reconhecem a importância de colocar a experiência do desenvolvedor no centro de seus programas – **e a plataforma foi projetada com isso em mente.**

## Potencializada por Inteligência Artificial

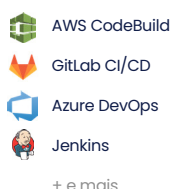
A rápida ascensão da IA Generativa (GenAI) trouxe um conjunto interconectado de desafios e oportunidades para as equipes de Segurança de Aplicações. Para aproveitar ao máximo essa tecnologia, plataforma é potencializada por IA para proporcionar uma experiência ágil e eficaz para os desenvolvedores e profissionais de segurança. Utilize ferramentas de IA generativa nas etapas de remediação de vulnerabilidades e reduza o tempo para detectar e corrigir falhas de segurança.

## Personalize a plataforma para se ajustar ao seu SDLC

Embora as etapas do SDLC sejam similares em todas as empresas, a forma como cada organização as aborda, em termos de tecnologia e processos, é única. No final, você precisa de uma plataforma de AppSec que funcione do jeito que você trabalha. Por isso, com a nossa plataforma você integra-se a todas as ferramentas, sejam elas novas ou legadas:

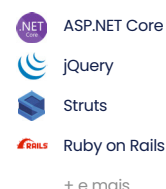
### CI/CD

Automatize a varredura como parte do seu pipeline CI/CD.



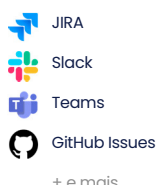
### Development Frameworks

Dê suporte às equipes de desenvolvimento em suas metodologias, com compatibilidade para mais de 100 frameworks.



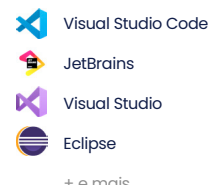
### Feedback Tools

Coloque as vulnerabilidades no contexto e no fluxo de trabalho dos próprios desenvolvedores.



### IDE

Permita que os desenvolvedores revisem e corrijam vulnerabilidades diretamente em seu IDE preferido.



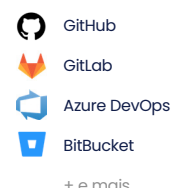
### Programming Languages

Mantenha-se atualizado com as linguagens de programação mais recentes, com suporte nativo para mais de 50 linguagens.



### SCM Integrations

Automatize a varredura no momento em que o código é enviado, possibilitando que sua equipe avance ainda mais na abordagem shift left.



# CG//One

Comece a  
revolução de  
**AppSec** no  
seu negócio  
hoje.



**Clique aqui e solicite uma demo**

## Somos parceiros oficiais da Checkmarx no Brasil

Somos a CG One, a evolução da marca Compugraf. Há mais de 40 anos no mercado de tecnologia, oferecemos soluções de cibersegurança escaláveis para detectar e bloquear ataques antes mesmo que aconteçam. Desenvolvemos e gerenciamos soluções de última geração para Segurança da Informação, Proteção de Redes e Gerenciamento Integrado de Riscos.

