E-BOOK

Top 10

considerações ao escolher uma solução **CNAPP**

CG//One

ÍNDICE

Qual é o elo mais fraco na segurança do seu aplicativo?

Você sabe qual é o elo mais fraco no seu processo de desenvolvimento de software?

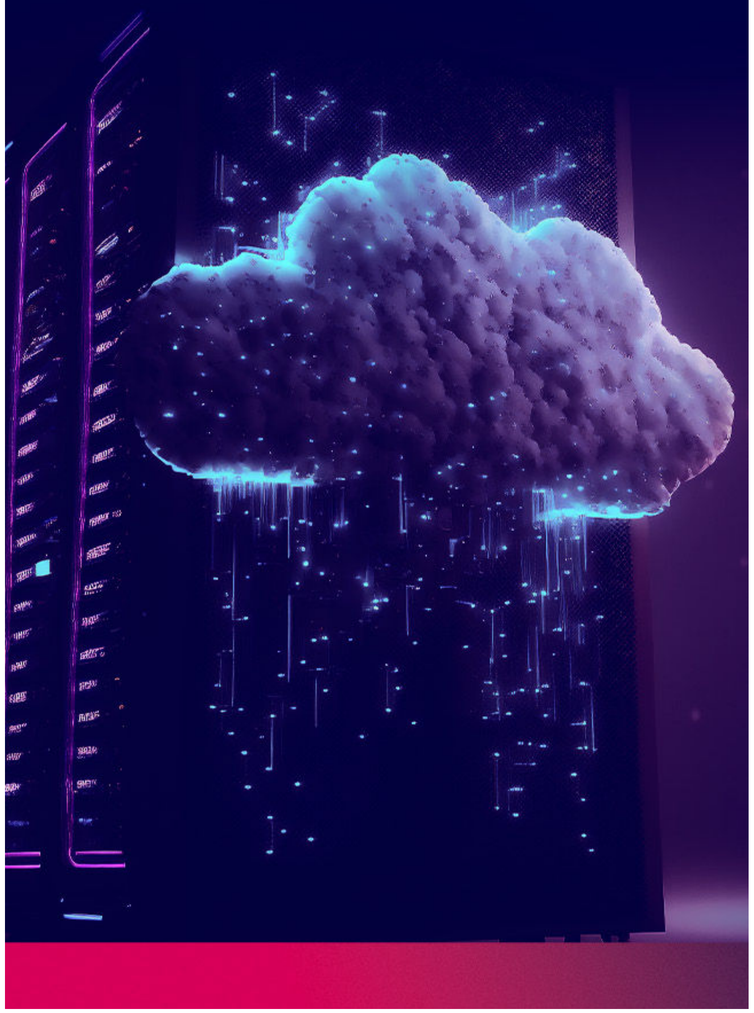
A preocupação com a segurança dos aplicativos está crescendo com o aumento do software de código aberto, APIs e outros componentes de terceiros – todas práticas comuns no desenvolvimento de aplicativos atualmente.

Em meio ao pânico crescente sobre as vulnerabilidades de um software, as agências de segurança do governo dos EUA emitiram orientações conjuntas para os desenvolvedores em setembro de 2022 para reprimir o problema, dizendo: “O comprometimento da cadeia de fornecimento permite que atores mal-intencionados se movam por toda parte”. Para combater esta ameaça, a comunidade de segurança cibernética precisa se concentrar em proteger o ciclo de vida de desenvolvimento de software (SDLC).

E o custo de não proteger adequadamente seus aplicativos contra os diversos riscos é maior do que nunca. Com toda essa complexidade, muitos fornecedores começaram a oferecer varredura de segurança, monitoramento e ferramentas de observabilidade para aplicações nativas da nuvem, tudo em uma única plataforma unificada em vez de um conjunto integrado de produtos com um propósito único.
Cunhado pela primeira vez pelo Gartner, o termo “plataforma de proteção de aplicativos nativos da nuvem” (CNAPP) refere-se a **“um conjunto integrado de recursos de segurança e conformidade projetados para ajudar a proteger aplicativos nativos da nuvem em todo o desenvolvimento e produção.”**

Mas muitas vezes, a promessa do CNAPP não corresponde ao que os fornecedores oferecem. Neste material, iremos ajudá-lo a escolher de uma vez por todas a melhor solução CNAPP para o seu negócio.

Top 10 considerações ao escolher uma solução CNAPP



1. Abordagem holística

O ambiente de nuvem está sujeito a uma ampla gama de ameaças, incluindo ataques de negação de serviço (DDoS), ataques de injeção de código, violações de dados e muito mais. Uma abordagem holística permite que a solução CNAPP detecte todas essas ameaças de maneira coordenada e eficaz.

2. Visibilidade

Você não pode proteger o que não vê. Ter visibilidade completa dos ativos e dados do ambiente de nuvem é fundamental.

Dada a complexidade e a natureza dinâmica dos aplicativos e o ecossistema em que são executados, rastrear ativos e fluxos de dados pode parecer uma missão impossível, certo? Sua plataforma CNAPP deve fornecer a todas as partes envolvidas uma visão centralizada, abrangente e em tempo real da segurança das aplicações.

3. Zero Trust

Escolha uma solução que permita manter uma confiança zero. Na prática, esse conceito de segurança assume que todas as solicitações de acesso à rede são suspeitas, mesmo que venham de dentro da organização. Em outras palavras, o Zero Trust não assume que um usuário autenticado em um dispositivo seguro é automaticamente confiável. Sua ferramenta CNAPP deve ajudá-lo a impor acesso com privilégio mínimo.

4. Automação

Em todo o SDLC e em ambientes de produção, a plataforma deve automatizar processos manuais de segurança de aplicativos demorados, tediosos e propensos a erros. Deve, por exemplo, aplicar automática e dinamicamente os controles de segurança e melhores práticas do setor, bem como detectar, alertar e, sempre que possível, corrigir configurações incorretas de segurança.

5. Ambiente agnóstico

A sua plataforma CNAPP deve funcionar perfeitamente em qualquer lugar. Ou seja, deve ser projetada para ser agnóstica em relação ao ambiente de execução: local, em vários provedores de nuvem e em infraestruturas híbridas. Isso proporciona flexibilidade aos desenvolvedores e operadores para implantar e migrar aplicativos conforme necessário, sem ficarem presos a um único ambiente de execução.

6. Arquitetura independente

A plataforma CNAPP precisa ser capaz de funcionar com todas as arquiteturas modernas atuais, incluindo microsserviços, contêineres e funções sem servidor, aplicando políticas de segurança e governança automaticamente. As ferramentas de segurança legadas não conseguem aplicar efetivamente controles de segurança em cargas de trabalho de nuvem flexíveis e dinâmicas, que são iniciadas e encerradas em escala e velocidade, com pouca ou nenhuma intervenção humana.

É aí que entra o CNAPP, garantindo consistência em todas as suas políticas de segurança.

7. Pipeline de segurança

Uma plataforma CNAPP deve ajudá-lo a desenvolver com mais rapidez e segurança, verificando modelos, scripts e imagens em busca de falhas de segurança antes que as vulnerabilidades possam ser propagadas para todos os aplicativos ou ambientes de tempo de execução que usam o pipeline.

8. Abordagem Shift left

Uma cultura de segurança Shift left facilita o feedback contínuo para que a segurança das aplicações e a proteção da carga de trabalho possam ser ajustadas e otimizadas ao longo do tempo. A abordagem consiste em antecipar e incorporar medidas de segurança desde as fases iniciais do SDLC.

9. Prevenção proativa de ameaças

Sua plataforma CNAPP deve ir além da detecção precoce de ameaças. Em primeiro lugar, precisa ser capaz de prevenir ameaças de forma proativa. As políticas somente de detecção dão aos agentes de ameaças bastante tempo para comprometer seus sistemas e ativos (minutos ou até horas) após a detecção e antes da correção. É por isso que você precisa de proatividade.

Procure recursos robustos de inteligência contra ameaças e análise comportamental que identifiquem riscos de maneira confiável.

10. Score de risco

Lidar com vários alertas de um conjunto completo de ferramentas de segurança em nuvem desconectadas é complicado. Para trabalhar de forma mais inteligente, uma solução CNAPP deve fornecer uma gestão de risco (ERM) eficaz, utilizando IA contextual para fornecer recomendações acionáveis, permitindo-lhe concentrar-se nos riscos de maior prioridade.

Procure uma plataforma que forneça um contexto profundo, permitindo que você se concentre em 1% das tarefas essenciais que não podem ser negligenciadas.

Quais as funcionalidades de uma solução CNAPP?

É importante deixar claro que nem todos os “produtos CNAPP” contêm os mesmos componentes. Como não há padronização, os fornecedores são livres para oferecer uma combinação de recursos.

A princípio, pode parecer uma sopa de letrinhas, mas cada um desses recursos tem uma função separada e útil para proteger todo o seu ambiente de desenvolvimento e produção. E, muitas vezes, não há como integrar todas essas partes móveis e fazê-las funcionar juntas. Isso é um problema quando você avalia 10 ou mais plataformas semelhantes e tenta escolher o que funcionará melhor para a sua empresa.

Componentes básicos que oferecem proteção mínima

Os itens a seguir devem ser considerados recursos básicos. Ou seja, o mínimo que você deve procurar ao considerar uma solução CNAPP. Olhando para isso de uma perspectiva geral, você deve (no mínimo) **ter a capacidade de monitorar e controlar sua postura de segurança na nuvem e seus aplicativos.**

CSPM: Gerenciamento da Postura de Segurança da Nuvem

Parte essencial de qualquer solução CNAPP, as soluções CSPM oferecem governança automatizada em ativos e serviços multinuvem. Isso abrange a detecção de configurações incorretas, a aplicação das melhores práticas de segurança e a adesão às estruturas de conformidade, bem como a visualização e avaliação da sua postura geral de segurança.

CSNS: Segurança de Rede na Nuvem

Este é o equivalente em nuvem das defesas de rede tradicionais baseadas em perímetro usadas para proteger a infraestrutura local, como firewalls tradicionais, uma vez que estes não funcionam no domínio “livre de perímetro” da nuvem e, portanto, não podem atender aos requisitos de segurança empresarial.

O CSNS permite que as empresas alcancem o mesmo nível de monitoramento de segurança e prevenção de ameaças que existe em seu ambiente local, sem o perímetro local tradicional. Isso permite garantir total segurança cibernética corporativa e conformidade regulatória usando segurança de rede em nuvem e segmentação de rede Zero Trust.

AppSec com IA

Isso permite substituir WAFs (Web Application Firewalls) legados por automação e inteligência. Em troca, você obtém prevenção precisa contra ameaças para poder interromper os 10 principais ataques do OWASP, evitar ataques de bots e detectar qualquer tentativa de interação maliciosa com seus aplicativos e APIs, em qualquer ambiente.

Proteção de Cargas de Trabalho na Nuvem

Com os aplicativos sendo criados e implantados na velocidade atual, a segurança costuma ser deixada de lado, levando a vulnerabilidades e comprometimentos de segurança. A proteção de carga de trabalho na nuvem descobre cargas de trabalho em execução em tempo real e, em seguida, executa uma verificação de vulnerabilidade para garantir que nada foi perdido, seja devido a práticas de codificação inadequadas ou à falta de segmentação de rede correta.

Componentes avançados que oferecem proteção elevada

Os componentes CNAPP a seguir são considerados recursos avançados que estão se tornando disponíveis em algumas soluções de funcionamento superior.

Gerenciamento de direitos de infraestrutura em nuvem (CIEM)

Na nuvem, não há perímetro, por isso as permissões são mais importantes do que nunca para proteger ativos confidenciais. Mas não termina aí. Além dos usuários comuns, também lidamos com entidades efêmeras, como cargas de trabalho (contêineres, sem servidor) que aumentam e diminuem sob demanda. Para evitar problemas com permissões, as equipes de DevOps geralmente atribuem direitos excessivos para promover a agilidade, mas isso deixa sua organização vulnerável.

O CIEM fornece uma imagem real da sua infraestrutura e do gerenciamento de acesso, eliminando suposições e aplicando automaticamente o mínimo de privilégios. Uma solução CIEM verdadeiramente eficaz não atrapalhará o trabalho do desenvolvedor; em vez disso, ele funciona em segundo plano para tornar o trabalho deles ainda mais fácil.

A solução de CNAPP, fornecida pela CG One, com CIEM ajuda a reduzir o seu TCO com:

- Correção automática de risco de identidade;
- Aplicação automática de privilégio mínimo;
- Elimina a necessidade de pesquisar, localizar e remover manualmente contas de usuário redundantes;
- Permite que você adote facilmente as melhores práticas de segurança.

Tudo sem afetar a funcionalidade ou o ritmo de desenvolvimento. Você consegue segurança e insights valiosos, sem dor de cabeça.

Visibilidade da postura de segurança

A proteção de carga de trabalho na nuvem (CWP) fornece visibilidade profunda da postura de segurança em todos os processos em execução: hosts, contêineres e microsserviços. Muitos fornecedores de soluções CWP dirão que isso não pode ser feito sem adicionar agentes às cargas de trabalho, mas isso acrescenta muito trabalho para os desenvolvedores e aumenta o atrito entre as equipes de desenvolvimento e segurança. Como a agilidade do desenvolvedor é um objetivo estratégico importante de qualquer organização de software, o ideal é procurar uma solução de postura de carga de trabalho sem agente (AWP) que funcione em segundo plano, sem interferir nos processos DevOps existentes. Isso garante segurança e permite que suas equipes continuem trabalhando normalmente.

A nossa solução de CNAPP com AWP fornece proteção de carga de trabalho que integra segurança diretamente nas aplicações nativas da nuvem, proporcionando-lhe:

- Cobertura total, desde o desenvolvimento até o tempo de execução e do código até a nuvem;
- Automação total para começar a trabalhar rapidamente, com confiança zero e mínimos privilégios;
- Segurança total em todos os seus ambientes de nuvem, em qualquer arquitetura de carga de trabalho e em todo o ciclo de vida do aplicativo;
- Fácil acesso para definir políticas de segurança, aplicar e criar perfis de funções e bloquear atividades maliciosas.

O AWP permite incorporar segurança na construção com verificação contínua de código, incluindo infraestrutura como código (IaC).

Segurança do pipeline

A maneira como construímos código mudou. Em vez de criar aplicativos do zero, os desenvolvedores os reúnem a partir de uma mistura de componentes, bibliotecas e APIs de código aberto. Isso introduz novos tipos de vulnerabilidades em toda a sua cadeia de fornecimento de software. A segurança do pipeline oferece uma maneira mais fácil e eficiente de criar testes estáticos de segurança de aplicativos (SAST) para código-fonte, juntamente com a verificação de infraestrutura como código (IaC).

O nosso CNAPP com segurança de pipeline Spectral oferece uma maneira mais fácil e eficiente de construir SAST para código-fonte, juntamente com varredura IaC, permitindo:

- Gerenciar políticas de segurança a partir de um único painel central;
- Aplicar verificação de rotina de código e repositórios;
- Proteger aplicativos desde o código até a nuvem de forma integrada;
- Automatizar a proteção secreta, malware e detecção de vulnerabilidades por meio do SDLC;
- Eliminar pontos cegos públicos e aplicar políticas em todo o SDLC.

O Spectral foi criado pensando nos desenvolvedores, portanto, como acontece com todo o conjunto CNAPP, seu foco é deixá-los fazer seu trabalho.

ERM: unindo tudo

Com todos os componentes que exploramos até agora em seu CNAPP, você já sabe que precisa reunir as informações de todas as suas soluções de segurança. Você quer se concentrar nos riscos que são importantes para seu negócio e não distrair suas equipes com questões de menor prioridade, certo? Para o ajudar a fazer isso mais facilmente, o nosso CNAPP oferece uma gestão de risco (ERM) eficaz, fornecendo-lhe não apenas dados, mas também contexto profundo e insights que lhe permitem agir rapidamente:

- IA contextual e pontuação de risco;
- Superfície de ataque reduzida, para que você possa se concentrar nos riscos de maior prioridade;
- Auto remediação baseada em “ações mínimas eficazes”.

O que queremos dizer com “ação mínima eficaz”? Na prática, é a resolução de problemas de segurança seguindo recomendações do “tamanho certo”: se for muito pouco, a resolução não resolverá o problema; se for demais, você desperdiçará recursos fazendo trabalhos desnecessários com menor ROI.

Portanto, otimize o foco da sua equipe de segurança para proteger os ativos e processos mais importantes.

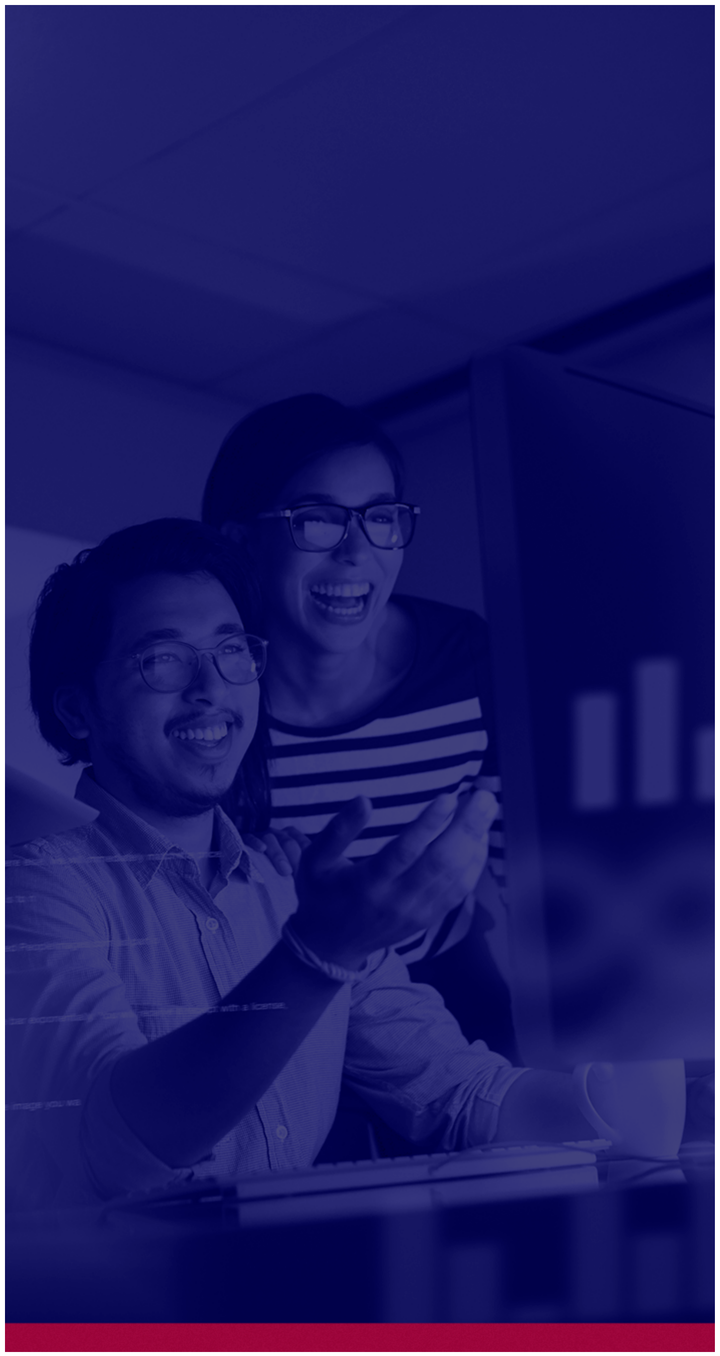
É apenas mais uma forma de o CNAPP colocar você no comando, com controle total sobre sua segurança, adaptado às suas prioridades.

Gestão de Riscos Corporativos (ERM)

A nossa solução CNAPP ajuda você a entender sua verdadeira postura de risco, que é mais do que apenas um número. O ERM vai além dos números, levando em consideração:

- O tipo de problema de segurança e sua gravidade;
- Modificadores de contexto, como exposição na rede;
- Modificadores de impacto, como o custo financeiro potencial para o seu negócio.

Essas informações capacitam sua equipe a agir, reduzindo o tempo total para remediação (TTR) e garantindo maior segurança de aplicativos de ponta a ponta.



Conclusão

O desenvolvimento moderno baseado em nuvem exige soluções de segurança projetadas desde o início para a nuvem.

O CloudGuard, fornecido pela CG One, é a única plataforma de segurança nativa da nuvem de ponta a ponta. Com proteção para todas as camadas da carga de trabalho do aplicativo, desde CI/CD até o tempo de execução, ele capacita equipes de segurança e equipes de DevOps a implantarem simultaneamente, com uma abordagem de segurança de confiança zero, ao mesmo tempo em que atende a todos os desafios do desenvolvimento moderno.

As soluções de segurança de aplicativos visam preencher lacunas de segurança e conformidade, fornecendo uma estrutura de segurança unificada e centralizada que oferece visibilidade de ponta a ponta e aplicação consistente de proteções de segurança e conformidade. As melhores soluções de segurança de aplicativos sustentam uma estratégia de segurança de confiança zero, fornecem altos níveis de automação e são independentes do ambiente e da arquitetura da carga de trabalho.

Esperamos que este guia prático seja útil em sua missão de escolher a melhor plataforma CNAPP para a sua organização.

CNAPP em ação

Quer uma demonstração gratuita de como a plataforma CNAPP fornecida pela CG One pode elevar sua segurança cibernética?

Agende agora

Todas as soluções de cibersegurança em um só lugar

Enquanto você se concentra em impulsionar o seu negócio, nossa equipe de especialistas está pronta para cuidar de todas as suas complexidades tecnológicas. Conte conosco para ser seu parceiro estratégico de segurança digital e riscos.

Network

Configuração, otimização e fortalecimento das infraestruturas de rede.

Security

Proteção de ativos críticos e prevenção de ataques cibernéticos.

Integrated Risk Management

Gerenciamento de riscos para melhorar a visibilidade e o processo de tomada de decisão.

Parceiros:

Akamai, algosec, Checkmarx, Check Point, Claroty, CyberArk, Cyrebro, Fortinet, GetGlobal, Keysight, netskope, OneTrust, proofpoint.

CG // One

Quer implementar o CNAPP?

Com mais de 40 anos de expertise no mercado, sabemos exatamente como proteger o seu negócio das mais avançadas ameaças cibernéticas. Desenvolvemos e gerenciamos soluções de **Redes, Segurança da Informação e Gerenciamento Integrado de Riscos, em conformidade com as práticas e os padrões de segurança do NIST® Cybersecurity Framework.**

Contamos com um time qualificado e certificado que já proporcionou operações seguras para mais de 500 empresas de diversos portes e setores, em todo o Brasil.

Converse agora
com um especialista