Cybersecurity
INSIDERS

O Guia do CISO para

Proteção de aplicativos nativos da nuvem

Estratégias para proteger ambientes multinuvem num mundo híbrido

FORTINET®

Resumo executivo

O perímetro da sua nuvem já foi violado. Você só ainda não encontrou o ponto de entrada.

As arquiteturas nativas da nuvem proporcionaram velocidade e escala, mas expandiram exponencialmente a superfície de ataque. As identidades (máquinas e humanas) evoluem constantemente, e as APIs criam novas vulnerabilidades. A Gartner relata que os ataques motivados por identidade agora superam as violações de perímetro em quase 3 para 1, com as configurações incorretas da nuvem ainda sendo o principal vetor de ataque.

Ferramentas de segurança tradicionais, como SIEMs e plataformas de Service Organization Controls legadas, não foram criadas para a escala e complexidade dos ambientes em nuvem. Eles sobrecarregam as equipes com alertas de baixo valor, fornecendo visibilidade limitada das atividades na nuvem e falta de informações contextuais necessárias para correlacionar riscos com comportamentos ou automatizar respostas oportunas. É isso que as ameaças nativas da nuvem exigem hoje em dia e o que as ferramentas tradicionais não conseguem oferecer. As plataformas de proteção de aplicativos nativas da nuvem (CNAPP resolvem essas lacunas. O Lacework FortiCNAPP™ da Fortinet foi desenvolvido nativamente para a nuvem a partir da tecnologia Lacework e integrado ao Fortinet Security Fabric. Sua arquitetura garante menos falsos positivos, investigações mais rápidas de ameaças, redução significativa do ruído operacional e maior produtividade dos desenvolvedores.

Relatórios independentes validam esses resultados:

- **Investigações de ameaças até 80% mais rápidas**
  (Estudos de caso interno da Fortinet® internal case studies, 2024)
- **95% menos falsos positivos**
  (implantações validadas por clientes, 2024)
- **Apenas 1,4 alertas críticos por dia, em média**
  (Métricas do setor da Fortinet®, 2024)

À medida que os ambientes em nuvem se tornam cada vez mais complexos, adotar uma estratégia CNAPP não é opcional. É imperativo.

Um novo modelo para uma nova era

O modelo convencional de segurança na nuvem continua reativo e fragmentado:

As ferramentas CSPM detectam configurações incorretas, o CWPP detecta malware e o CIEM gerencia direitos, mas nenhuma delas conecta os pontos.

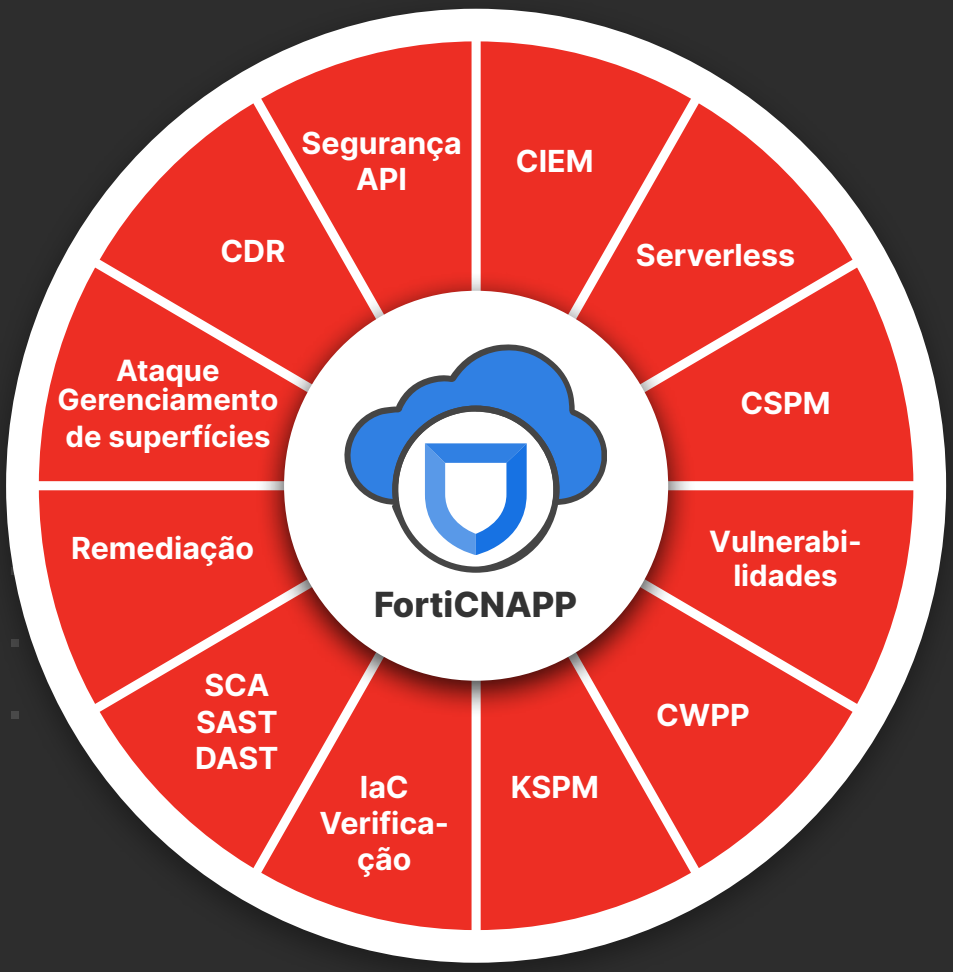


Figura 1: O CNAPP unifica uma variedade de ferramentas de segurança na nuvem

As plataformas modernas de proteção de aplicativos nativos da nuvem (CNAPP) exigem mais do que visibilidade

Os CNAPP modernos, como o Lacework FortiCNAPP, se destacam por correlacionar sinais estáticos e dinâmicos, criando um rico reconhecimento contextual e automatizando respostas em todo o ciclo de vida dos aplicativos em nuvem. Em vez de reagir a alertas, o FortiCNAPP permite uma intervenção proativa para conter e eliminar ameaças antes que causem danos significativos.

SC Awards TRUST AWARD WINNER 2025

Segurança do ciclo de vida do código para a nuvem

A segurança eficaz na nuvem deve começar antes da implantação do código. O Lacework FortiCNAPP™ integra-se diretamente aos pipelines de Infraestrutura como Código (IaC), permitindo a detecção precoce de vazamentos de segredos e configurações incorretas, além de aplicar políticas de segurança.

As ferramentas integradas de Static Application Security Testing (SAST), análise de composição de software (SCA) e lista de materiais de software (SBOM) garantem um desenvolvimento robusto e seguro, sem interromper os fluxos de trabalho. Ao contrário dos fornecedores que dependem de aquisições pouco integradas, o FortiCNAPP foi projetado de forma nativa, oferecendo cobertura contínua do código à nuvem com escalabilidade superior, integração mais estreita e complexidade significativamente reduzida.

Correlação entre risco e ameaça

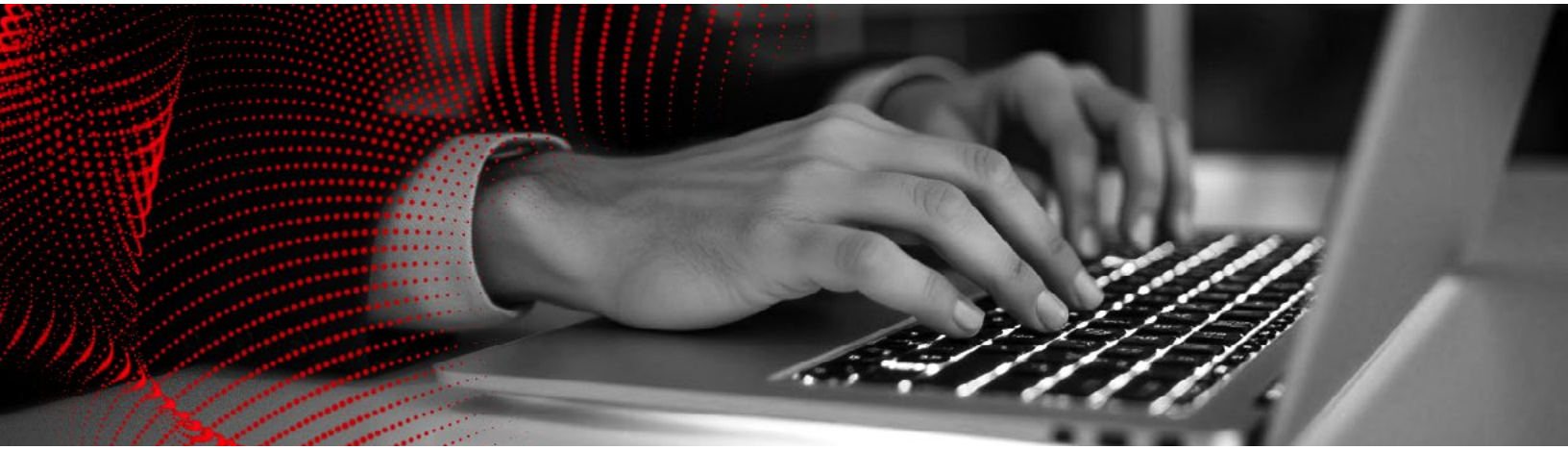
Nem todos os riscos são iguais. O CNAPP eficaz correlaciona as descobertas de postura com telemetria de ameaças em tempo real, identificando vulnerabilidades ativamente exploradas em seu ambiente.

FortiCNAPP, ao integrar CSPM, CWPP e CIEM, oferece dados prioritários sobre explorabilidade e impacto. Isso diminui consideravelmente a exaustão dos alertas e possibilita respostas ágeis e confiáveis.

Análise comportamental com inteligência artificial e resposta orquestrada

Os invasores sofisticados já não dependem de exploits conhecidos para evitar a detecção baseada em assinaturas.

O FortiCNAPP emprega uma poderosa plataforma de dados alimentada por IA para modelar o comportamento normal de usuários e entidades, permitindo a detecção rápida de ameaças desconhecidas, incluindo ameaças de dia zero, credenciais comprometidas, ameaças internas, ransomware e cryptojacking, sem precisar de assinaturas estáticas ou regras predefinidas. Essa abordagem comportamental é complementada por recursos de resposta orquestrada com o Fortinet® Security Fabric. As integrações automatizadas com FortiSOAR e FortiGuard permitem a contenção, correção e escalonamento de ameaças em tempo real, reduzindo o tempo de permanência do invasor de dias para segundos.



Operacionalização do CNAPP
Cenários do mundo real

O valor do CNAPP fica claro quando o contexto substitui a confusão. Considere estes casos documentados:

Prevenção de riscos a montante

Um provedor líder do setor da saúde integrou o FortiCNAPP diretamente em seus pipelines DevSecOps. Configurações IaC não conformes no GitHub e no Terraform foram identificadas e bloqueadas antes da implantação, evitando três violações significativas de conformidade somente no primeiro trimestre.

Triagem e redução de alertas

Um fabricante global sobrecarregado por milhares de alertas diários implementou o FortiCNAPP para correlacionar os dados do CSPM com a atividade em tempo de execução. Apenas 2% das configurações incorretas sinalizadas foram exploradas ativamente, permitindo que as equipes de segurança concentrassem seus recursos estrategicamente e reduzissem drasticamente o ruído operacional.

Detecção de ameaças baseada em comportamento

Durante um teste de penetração em uma empresa da Fortune 100, o FortiCNAPP identificou um contêiner verificando armazenamentos confidenciais e estabelecendo conexões de saída. A resposta automatizada do FortiCNAPP conteve e escalou a ameaça em 60 segundos, sem depender das assinaturas de ameaças tradicionais.

Resposta coordenada em ambientes híbridos

Uma instituição financeira sofreu movimentos laterais não autorizados dentro dos clusters do Kubernetes. O FortiCNAPP utilizou o Kubernetes Security Posture Management (KSPM) para detectar e isolar o pod comprometido, atualizar automaticamente as políticas e manter registros de auditoria abrangentes tudo isso executado em questão de minutos.

Esses cenários demonstram o papel fundamental do FortiCNAPP na redução da complexidade, na otimização das operações e na proteção decisiva de ambientes híbridos.

Benefícios do CNAPP

Figura 2: Como uma CNAPP melhora e apoia as tarefas fundamentais de segurança

Avaliando a maturidade do CNAPP: Um quadro estratégico

Para criar uma estratégia CNAPP eficaz, os CISOs precisam mais do que uma lista de recursos, eles precisam de um roteiro. A maturidade da segurança nativa da nuvem não é binária; ela evolui por meio de recursos interconectados, como visibilidade, detecção de ameaças e automação.

Essa estrutura divide a maturidade do CNAPP em cinco estágios progressivos, mapeados nas dimensões mais importantes: visibilidade e inventário, gerenciamento de riscos e vulnerabilidades, detecção de ameaças e resposta, conformidade e governança, e automação e orquestração. Use-o para avaliar sua situação atual, identificar lacunas que representam risco de segurança ou ineficiências e priorizar os recursos que proporcionarão os maiores ganhos em termos de segurança e operacionais em seu ambiente.

FASE 1
Controle fragmentado
(Inicial / Ad Hoc)

Nesta fase, os esforços de segurança na nuvem são reativos e isolados. Ferramentas como CSPM ou CWPP podem existir, mas são isoladas, produzindo alertas não correlacionados com alto ruído e pouco contexto.

- **Visibilidade e inventário:**
  Incompleto ou manual; limitado a varreduras periódicas ou painéis isolados.
- **Gestão de riscos e gerenciamento de vulnerabilidades:**
  A postura é estática; os riscos são registrados, mas não estão vinculados à explorabilidade ou aos dados de tempo de execução.
- **Detecção de ameaças e resposta:**
  Detecção baseada apenas em assinaturas; sem análise comportamental; triagem manual lenta.
- **Conformidade e governança:**
  As auditorias pontuais predominam; as lacunas de conformidade são descobertas após o incidente.
- **Automação e orquestração:**
  Mínimo ou nenhum; predominam os manuais de jogadas manuais.

FASE 2
Visibilidade conectada
(Fundamental)

As equipes de segurança consolidam o monitoramento em todas as contas na nuvem e começam a integrar ferramentas básicas.

- **Visibilidade e inventário:**
  Inventário centralizado e descoberta de ativos em ambientes de nuvem; ainda falta visibilidade em tempo real.
- **Gestão de riscos e gerenciamento de vulnerabilidades:**
  As configurações incorretas e vulnerabilidades surgiram de forma mais consistente, mas a triagem continua sendo manual.
- **Detecção de ameaças e resposta:**
  Algumas detecções básicas de anomalias começam a aumentar as regras; poucos falsos positivos são filtrados.
- **Conformidade e governança:**
  A visibilidade aprimorada ajuda na preparação para auditorias, mas a conformidade contínua continua sendo difícil.
- **Automação e orquestração:**
  Os fluxos de trabalho de alerta começam a alimentar os sistemas de emissão de tickets ou ferramentas SOAR, mas não são impulsionados dinamicamente pelo risco real.

FASE 3
Priorização contextual
(Proficiente)

As organizações começam a correlacionar a postura com a telemetria de ameaças em tempo real.

- **Visibilidade e inventário:**
  Inventário dinâmico com atualizações contínuas; cobertura em cargas de trabalho, contêineres e APIs.
- **Gestão de riscos e gerenciamento de vulnerabilidades:**
  O CNAPP correlaciona riscos de postura estática com dados de explorabilidade e caminhos de ataque; as equipes podem se concentrar no que é mais importante.
- **Detecção de ameaças e resposta:**
  A atividade em tempo real enriquece as descobertas; a linha de base comportamental identifica ameaças emergentes mais cedo.
- **Conformidade e governança:**
  Postura mapeada para estruturas de conformidade; as equipes podem identificar desvios antes que eles levem a violações.
- **Automação e orquestração:**
  Triagem baseada em políticas; integrações antecipadas com CI/CD e sistemas de tempo de execução começam a influenciar a prevenção.

FASE 4

Proteção automatizada

(Avançado)

Os programas de segurança tornam-se adaptáveis, combinando detecção baseada em IA com orquestração de respostas.

- **Visibilidade e inventário:**
  Visão completa e continuamente atualizada do código, infraestrutura em nuvem, identidades e dos fluxos de dados.
- **Gestão de riscos e gerenciamento de vulnerabilidades:**
  Riscos não apenas identificados, mas contextualizados e priorizados pelo comportamento real do invasor e pelo raio de ação.
- **Detecção de ameaças e resposta:**
  A análise avançada detecta ameaças desconhecidas, incluindo ameaças de dia zero e ameaças internas; a contenção automatizada é comum.
- **Conformidade e governança:**
  Conformidade contínua com controles ativos; violações de políticas acionam barreiras de proteção automatizadas ou medidas coercitivas.
- **Automação e orquestração:**
  O CNAPP aciona fluxos de trabalho de remediação completos, quarentena, eliminação e escalonamento com base na confiança e na gravidade.

FASE 5

Plano de Controle Estratégico

(Otimizado)

O CNAPP torna-se o centro nervoso das operações de segurança na nuvem

- **Visibilidade e inventário:**
  Visão unificada, desde o desenvolvimento até a produção, complementada com contexto empresarial e perspectivas de acesso.
- **Gestão de riscos e gerenciamento de vulnerabilidades:**
  Os riscos informam os modelos de ameaças e as estratégias de prevenção a montante (por exemplo, em IaC); as informações sobre ameaças reforçam a priorização.
- **Detecção de ameaças e resposta:**
  Totalmente integrado com SOAR, SIEM, EDR e sistemas de identidade para detecção e correção em ciclo fechado.
- **Conformidade e Governança:**
  Governança proativa por meio de políticas incorporadas como código; prontidão para auditoria integrada.
- **Automação e orquestração:**
  Os fluxos de trabalho autônomos mantêm a postura, bloqueiam ameaças, garantem a conformidade e reduzem o ruído, capacitando as equipes de segurança a operar em escala com precisão.

Ao identificar claramente o seu estágio atual e definir metas de melhorias, os CISOs podem garantir que seu CNAPP evolua e se adapte de forma eficaz para enfrentar os desafios modernos de segurança na nuvem.

CNAPP como o Plano de Controle Estratégico

As equipes de segurança não precisam de mais alertas. Eles exigem inteligência acionável e controle unificado. O CNAPP não deve adicionar outro produto, ele deve servir como base operacional da segurança na nuvem.

O Lacework FortiCNAPP da Fortinet exemplifica essas capacidades por meio de sua Security Fabric totalmente integrada e projetada de forma nativa, contrastando fortemente com soluções fragmentadas e adicionais. O FortiCNAPP simplifica a conformidade contínua ao mapear automaticamente os ativos para normas como PCI DSS, HIPAA, Service Organization Controls 2 e ISO 27001, simplificando significativamente as auditorias e reduzindo o desgaste da conformidade.

A questão estratégica não é se o CNAPP se tornará o pilar central da segurança na nuvem. Trata-se de avaliar se a sua estratégia atual de nuvem é forte o suficiente para resistir às ameaças direcionadas e automatizadas do futuro.

Questões críticas para avaliar os fornecedores de CNAPP:

- *Eles fornecem correlação em tempo real entre postura e comportamento de ameaça ativa?*
- *A plataforma deles é unificada em termos de código, cargas de trabalho, APIs e identidades?*
- *Eles conseguem realizar a detecção de ameaças e responder a elas sem depender exclusivamente de assinaturas predefinidas?*
- *Que tipo de automação está incorporada na detecção de ameaças, contenção e resolução de ameaças?*
- *A solução deles reduz significativamente a complexidade operacional e as despesas gerais?*

Explore mais

Saiba mais

Solicite uma demonstração

Faça um tour pelo FortiCNAPP