xFabric
Unified Security Fabric Platform

WHITE PAPER TÉCNICO

CNAPP: arquitetura de referência

Postura, direito de acesso, workload e dado convergindo em caminho de ataque priorizado

Cobertura por camada, cálculo de permissão efetiva, construção do grafo de exposição e modelo de encaminhamento de remediação com dono e prazo, aplicável a AWS, Azure, Google Cloud e Kubernetes.

Documento técnico xFabric · revisão 2026.2 · uso corporativo

Contexto e fundamentação

Postura, workload, identidade e dado avaliados isoladamente produzem volume. Avaliados como grafo, produzem uma fila curta de exposições exploráveis com dono e prazo.

Por que a lista de achados não é priorização

Uma avaliação de postura sobre um patrimônio multicloud típico devolve dezenas de milhares de achados. A severidade emitida pelo verificador é uma propriedade da regra, não do ambiente: o mesmo controle vale o mesmo em uma conta de laboratório sem rota externa e em uma conta de produção com dado regulado.

Priorização exige contexto de alcance. Um achado só é acionável quando se sabe quem pode explorá-lo, a partir de onde e o que ele alcança depois de explorado.

As quatro camadas que precisam convergir

Um CNAPP entrega valor quando as quatro camadas escrevem no mesmo modelo de dados e se referenciam pelo mesmo identificador de recurso.

- Postura (CSPM): desvio de configuração frente a benchmark e política interna
- Direito de acesso (CIEM): princípios, papéis e permissões efetivas, não declaradas
- Workload (CWPP): vulnerabilidade em imagem, pacote em execução e comportamento de runtime
- Dado: classificação, sensibilidade e exposição efetiva de armazenamento

Permissão efetiva contra permissão declarada

A diferença entre a política escrita e o acesso efetivamente alcançável é onde a maior parte do risco de nuvem se acumula. Cadeias de assunção de papel, políticas de recurso, limites de permissão e federação de identidade compõem um alcance que nenhum documento descreve integralmente.

O cálculo de permissão efetiva percorre essas cadeias e devolve o conjunto real de recursos alcançáveis por princípio. É esse conjunto — não a política — que deve ser comparado ao princípio do menor privilégio.

Da exposição ao caminho de ataque

Um caminho de ataque é uma sequência verificável: ponto de entrada exposto, vulnerabilidade explorável em execução, credencial alcançável a partir do workload e recurso sensível ao final da cadeia. Cada elo é evidência estrutural derivada do inventário, não inferência.

Quando os caminhos são ordenados por sensibilidade do destino e por facilidade do ponto de entrada, a fila resultante costuma conter dezenas de itens, não dezenas de milhares. É uma fila que uma equipe de plataforma consegue drenar em ciclos de sprint.

Remediação com dono e prazo

A correção pertence a quem opera o recurso. O CNAPP deve derivar o responsável a partir da tag de propriedade, do repositório de infraestrutura como código e do histórico de deploy, e abrir o item diretamente no fluxo de trabalho da equipe dona — não em uma fila genérica de segurança.

Remediação verificável fecha o ciclo: o achado só é encerrado quando a próxima coleta confirma o estado corrigido na fonte, com registro de quem alterou e quando.

Cobertura por camada e por provedor

A avaliação de um CNAPP deve começar pela cobertura efetiva por camada em cada provedor em uso, incluindo Kubernetes gerenciado e ambientes on-premise conectados.

Camada	Objeto avaliado	Fonte de verdade
Postura	Configuração de serviço e política de recurso	API de configuração do provedor
Direito de acesso	Permissão efetiva por princípio	Grafo de papéis, políticas e federação
Workload	Imagem, pacote em execução, comportamento	Registro de imagens e telemetria de runtime
Dado	Classificação e exposição de armazenamento	Amostragem autorizada e metadados

Cálculo de permissão efetiva

O cálculo percorre cadeias de assunção de papel, políticas de recurso, limites de permissão e provedores federados, devolvendo o conjunto de recursos alcançáveis por princípio. O resultado é comparado ao propósito declarado do princípio para produzir a recomendação de redução de privilégio.

- Princípios humanos e de serviço tratados no mesmo grafo
- Cadeias de assunção resolvidas entre contas e entre provedores
- Permissão não utilizada em janela observada marcada para redução
- Recomendação emitida como política mínima aplicável, versionada

Grafo de exposição e ordenação de caminhos

Cada caminho é uma sequência verificável de elos derivados do inventário. A ordenação combina sensibilidade do destino, facilidade do ponto de entrada e existência de exploração pública conhecida para a vulnerabilidade envolvida.

Elo	Evidência exigida
Ponto de entrada	Exposição de rede efetiva e ausência de controle de borda
Execução	Vulnerabilidade presente em processo em execução
Credencial	Segredo alcançável a partir do workload

Destino	Recurso com dado classificado como sensível

Modelo de encaminhamento de remediação

- Dono derivado de tag de propriedade, repositório de IaC e histórico de deploy
- Item aberto no fluxo de trabalho da equipe dona, com prazo por severidade efetiva
- Correção proposta como alteração de infraestrutura como código quando aplicável
- Encerramento condicionado à confirmação do estado corrigido na próxima coleta
- Exceção formal com prazo, justificativa e aprovador nomeado

Pontos de decisão

- Severidade de regra não é risco; alcance e sensibilidade do destino são.
- Permissão efetiva calculada por grafo revela exposição que a política declarada esconde.
- Achado sem dono nomeado e prazo é inventário de dívida, não programa de remediação.