

## DETECT, PROTECT, AND REMEDIATE CLOUD ATTACKS

Deepfence solutions protect cloud-native applications in production by finding vulnerabilities, observing attack behavior, and neutralizing sophisticated threats in real-time. Whether your cloud-native applications run in single, multiple, or hybrid clouds, or use Kubernetes, Docker, serverless, or virtual machines, Deepfence protects your applications and data and reduces your risk exposure.



### DEEP OBSERVABILITY



See across clouds + hosting modalities

- See all activity across cloud, containers, and hosts
- Cloud, network, and application context for all alerts
- Continuous compliance monitoring across environments

### MAP ATTACK SURFACE



See live attack vectors + reduce alert fatigue

- Prioritized risk analysis for security scans
- One console for all critical security scans (vuln, malware, CSPM, secret)
- Up to 90% reduction in non-critical security alerts

### PROTECTION IN RUNTIME



Stop threat actors in their tracks

- Next-gen traffic filtering to prevent attackers from reaching their targets
- Network and host-level blocking
- Ability to map protection to threat actor TTPs

*"There's a lot of cloud-native security solutions out there, but none cut down the alert fatigue and do it with the lightweight footprint that Deepfence does."*

Matt Lehman  
Head of Payment Security  


# CLOUD-NATIVE APPLICATION PROTECTION WITHOUT THE NOISE

The Deepfence CNAPP ensures complete security visibility for clouds, workloads, containers, and serverless. It reduces costs and alerts by consolidating the key features of cloud workload protection (CWPP) with the latest in cloud security posture management (CSPM).

*"Deepfence is rolling out another credible open source win for the industry - ThreatGraph, which provides a substantive range of threat detection, and more - combined into a single, easy-to-use open source tool."*

Nick Reva  
Head of Corporate Security Engineering  
**Snap Inc.**

## KEY BENEFITS AND USE CASES

### Cloud, Network, and Application Observability

Get deep observability into your applications, exposing vulnerabilities and observing attack behavior in real time by capturing observability data across cloud, network, and application vectors.

### Runtime Protection for all Cloud Environments

Deepfence offers dynamic runtime protection for all environments - from Kubernetes to serverless, single to hybrid clouds - stopping threat actors in their tracks and defending your digital fortress.

### Turn Security Noise into Actionable Intelligence

Lost in the cacophony of security alerts? Deepfence's prioritized attack surface analysis filters through the noise, highlighting the most critical threats and allowing you to focus on what truly matters.

### Continuous Compliance in a Multi-Cloud World

Compliance and security regulations are increasingly prevalent so Deepfence simplifies the complexity of multi-cloud compliance to maintain compliance throughout the year as environments change.

## THREATMAPPER

ThreatMapper is an open-source, cloud-native, security observability platform. Scan for vulnerabilities, malware, compliance misconfigurations, exposed secrets and prioritize these critical cloud security alerts by exploitability. ThreatMapper works across all clouds and workload types.

### Open Source

- ✓ Vulnerability & Compliance Scanning
- ✓ Malware and Secret Scanning
- ✓ Attack Surface Prioritization
- ✓ Integrations
- ✓ Community Support

**TRY IT ON GITHUB**

## THREATSTRYKER

Meet ThreatStryker, our premium enterprise CNAPP that offers real-time cloud detection and response capabilities allowing you to neutralize threats to your environment in real-time. Unlock advanced features and receive dedicated support.

### Enterprise

- ✓ All of the features in ThreatMapper
- ✓ Realtime Detection and Response
- ✓ Runtime Attack Analysis
- ✓ Managed SaaS Available
- ✓ Dedicated Support

**FREE FOR 14 DAYS**