PRODUCT BRIEF

deepfence

Unified Cloud Native Security Observability

Protect Kubernetes, serverless, and more

Modern Applications Demand Modern Protection

The rush to deliver new applications and services is pushing organizations to adopt modern platforms and modern architectures. Containers, VMs, and serverless technologies unlock unprecedented speed and agility, but bring with them new and challenging security problems.

How can developers confidently trust and secure software that depends extensively on open source components?

How can operations teams know that their production platforms are secure and in compliance with best practices?

How can security teams identify threats and protect the enterprise across platforms and cloud boundaries?

How can you achieve this without slowing down the rate of innovation, impacting your customers, or sacrificing security along the way?

Comprehensive Protection Across All Your Cloud Workloads

Deepfence ThreatMapper is a full lifecycle security solution for modern applications. It observes and secures your applications from development to production.

Deepfence ThreatMapper's unique deep packet inspection (DPI) engine captures all traffic in your infrastructure – North/South and East/West – for out-of-band analysis. Unlike traditional proxy-based solutions that are complex to deploy and impact application performance, ThreatMapper is non-intrusive and does not impede your application's fast data path, enabling you to protect your infrastructure without degrading application performance or the user experience.

ThreatMapper Benefits

Visibility across all cloud environments, including cloud-native, multi-cloud, and hybrid cloud

Security for the entire CI/CD lifecycle, without slowing down innovation or your application

Protection across the cloud native continuum: Kubernetes, serverless, virtual machines, and more

Real-time threat and exploit detection using an advanced correlation engine that analyzes traffic patterns and application behavior

> *"We chose Deepfence after carefully evaluating options due to Deepfence's ability to perform Deep Packet Inspection of inter container and inter virtual machine traffic without adding additional latency to our data path. Deepfence is lightweight, scales well, and is the only solution that protects the entire cloud native continuum of Kubernetes, virtual machines, and serverless."*
>
> **KEVIN PAIGE,**
> CISO, Flexport

Full Lifecycle Security Observability & Protection

Identify

Recognize threats in real time

- Advanced out-of-band DPI
- Intrusion detection
- Sensors not proxies to keep fast data path intact
- Alert correlation and analytics

Analyze

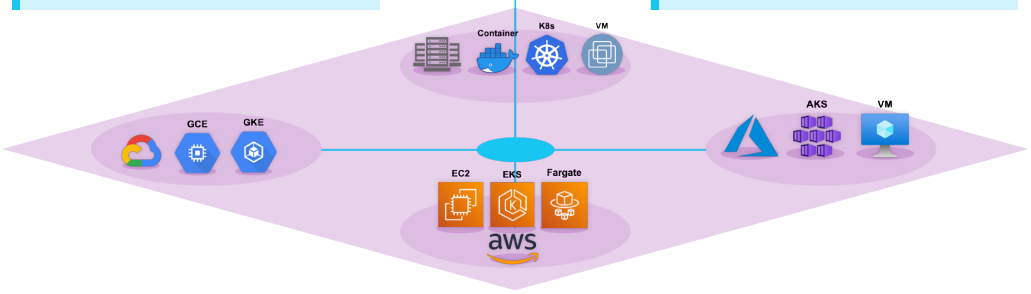
Understand your known attack surface

- Visibility & protection across all clouds
- Vulnerability and registry scanning
- CI/CD automation
- Compliance automation

Protect

Safeguard your workloads

- Automated protection policies
- Prevent potential lateral spread
- Defense against zero day attacks



About Deepfence

Deepfence is headquartered in California with offices in India and the UK. The founding team brings together deep expertise in application and network security, networking, virtualization, and DevOps, having worked in companies such as FireEye, Cisco, Juniper, and NGINX. Deepfence's Unified Cloud Native Security Observability Platform is radically changing the way cloud native workloads are protected. To learn more visit **www.deepfence.io**

Key Benefits

For development teams

Deepfence ThreatMapper runs in your Continuous Integration pipeline, cross-referencing components and dependencies against multiple threat and CVE lists, so that you can avoid releasing code and dependencies with known vulnerabilities into production

For operations teams

Deepfence ThreatMapper scans registries and deployment platforms, looking for misconfigurations and evaluating them against benchmarks, so that you can be confident you're following established best practices and demonstrate you're meeting compliance goals

For security teams

Deepfence ThreatMapper gathers and correlates multiple signals and analyzes network traffic, identifying and alerting on suspicious activity and zeroing in on known exploits, giving you immediate visibility of threats and exploits across cloud and on-premises estates

Key Features

Out-of-band DPI engine

- Inspects all traffic – North/South, East/West, plain text, and encrypted – at runtime to provide visibility into potentially malicious activities
- On-prem analysis so that sensitive application data never needs to leave your secured perimeter

Attack and exploit alerting

- Continuously processes runtime traffic and events using powerful machine learning algorithms
- Correlation engine analyzes signals and identifies attacks as they evolve

Management console

- Deep insights presented in an intuitive interface
- Easily see network activity, resource access patterns, and overall application and system health

Lightweight control plane

- Easily deployed as a DaemonSet on Kubernetes or as a sidecar container on hosts running containers
- Lightweight footprint to provide state-of-the-art security with minimal impact on application performance

Easy to deploy & manage

- Get up and running in just 30 minutes
- Orchestrate and scale in exactly the same manner as your other containers