Maximum Security, Minimal Effort
Secure Code-To-Cloud

If you had one hour, how would you materially improve your cloud security posture?

Cloud estates are a complex interconnection of technologies, architectures, and environments often managed by independent, autonomous team.

Answering essential questions, like

1. "Where do I have publicly exposed servers with high privileges and vulnerabilities".

2. "What databases are exposed to the internet".

Answering these simple questions is painfully difficult. The reason is that current approaches require multiple tools that create a fragmented view of risk, perpetuate operational silos, and force teams to manually correlate thousands of alerts.

CloudDefense.AI has fundamentally reimagined security in the cloud by unifying visibility across the entire stack and weaving together interconnected risk factors.

CloudDefense.AI tells you what needs your immediate attention, bridges the gap between security and development teams, and eliminates the need for specialized analysts - enabling every business to build faster and more securely.

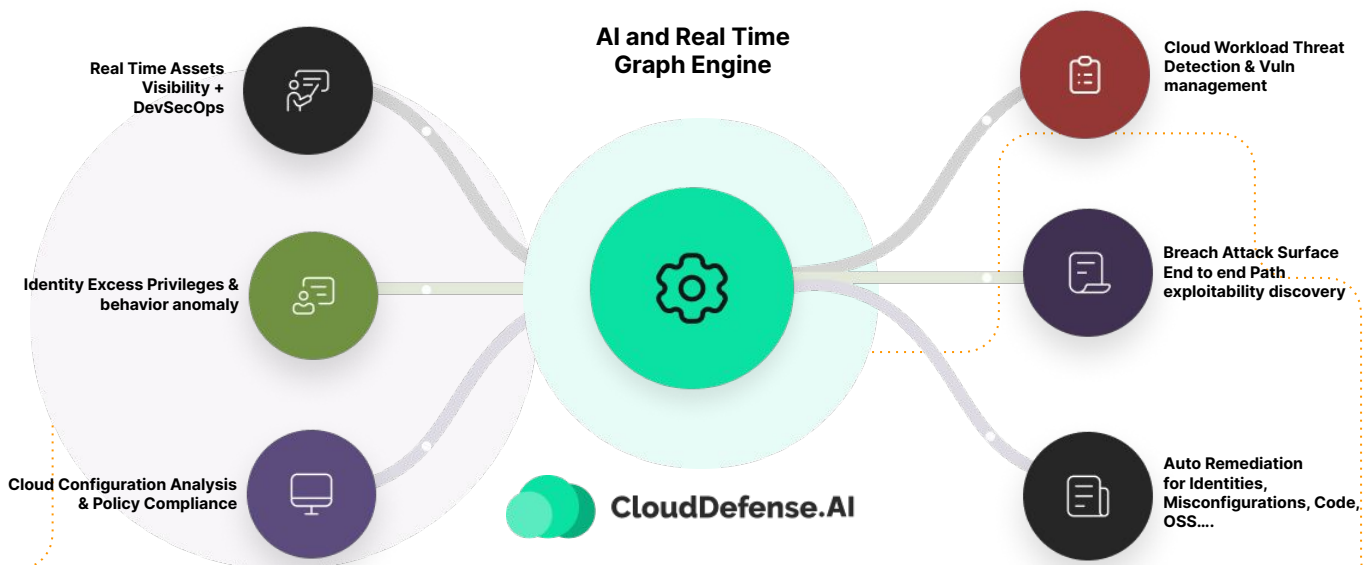## 5 mins deployment and comprehensive analysis of your cloud environment

- **CloudDefense.AI** scales effortlessly to any cloud environment with zero impact on resource or workload performance
- It connects in minutes via a single API per cloud and Kubernetes environment and achieves complete coverage immediately - no agents required
- It then collects information from every layer of your cloud stack without disrupting your business operations or requiring ongoing maintenance.
- The CloudDefense.AI Security Graph displays all cloud resources along with their fields and interconnections in near real-time to uncover the attackers view to a breach.

Prioritize Meaningful Risks: Direct Your Attention to What Truly Counts

- **CloudDefense.AI** reduces alert fatigue by 90%. Using CloudDefense.AI attack graph, you can focus on the most critical risk. No need to go through thousands of alerts.

Say Goodbye to Breaches

- **CloudDefense.AI**'s propriety's algorithm analyzes the behaviour of your cloud and able to detect zero day attacks
- Streamline Security Issue Resolution with Guided Remediation and One-Click Auto-Remediation Setup

AI and Real Time Graph Engine

Real Time Assets Visibility + DevSecOps

Identity Excess Privileges & behavior anomaly

Cloud Configuration Analysis & Policy Compliance

Cloud Workload Threat Detection & Vuln management

Breach Attack Surface End to end Path exploitability discovery

Auto Remediation for Identities, Misconfigurations, Code, OSS....

CloudDefense.AI

Key Capabilities

Cloud Security and 40+ Compliance

CloudDefense.AI: Comprehensive Discovery, Continuous Assessment, and Unmatched Compliance Monitoring for your cloud estate.

Container and Kubernetes security

CloudDefense.AI analyzes clusters on two complementary levels. First, host VMs and container images are scanned to identify vulnerabilities, malware, and exposed secrets across packages, libraries, and applications. Second, cluster APIs are interrogated directly to map cluster architecture, configuration, and more.

Threat Detection and Response (CDR)

CloudDefense.AI analyze system's behavior by using machine learning and artificial intelligence technique and able to prevent ZERO DAY attacks by 99% accuracy.

Attack Paths Analysis

CloudDefense.AI automatically analyzes the toxic combinations and analyze potential vulnerable attack path and able to remediate vulnerable assets automatically. CloudDefense.AI is able to reduce alert fatigue by 90% so that your team can focus on the most important issues.
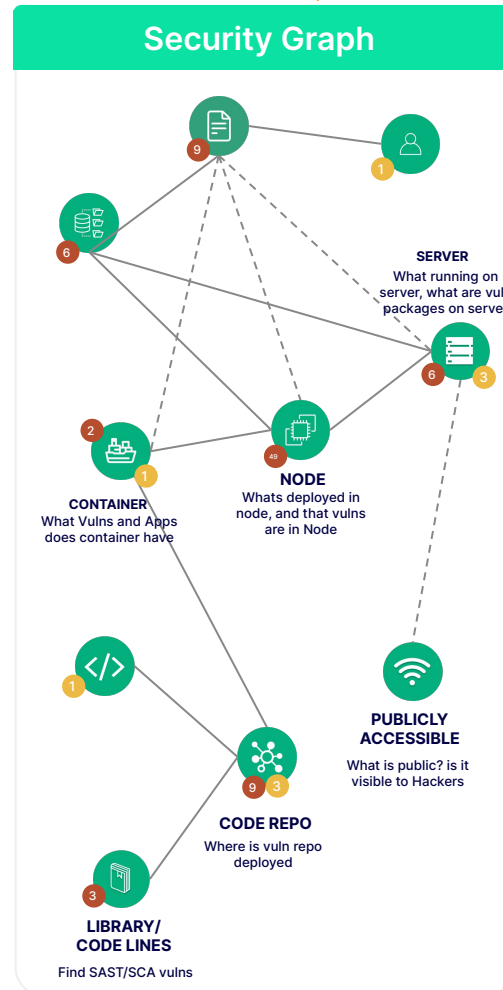
Cloud entitlements (CIEM)

CloudDefense.AI compiles the complex interactions between principals, resources, and boundaries to easily answer complex questions like "who can modify the infrastructure?" or "*Who can do credential exposure to your organization*?" and able to generate **ZERO TRUST** policies by analyzing user's behavior.

Application Security

CloudDefense.AI has full fledged DevSecOps solution is able to analyze SCA, SAST, DAST, API, IAC, HELM Chart by connecting your GitHub, Gitlab, Bitbucket etc. CloudDefense.AI is the only solution which is able to reduce false positive by 90%.

Automations and integrations

CloudDefense.AI offers dozens of out-of-the-box integrations for common SIEM, SOAR, ticketing, and messaging tools. It also integrates with CI/CD tools like Jenkins or Azure DevOps and offers a fully extensible API for unlimited workflow customizations.

Security Graph

SERVER
What running on server, what are vuln packages on server

CONTAINER
What Vulns and Apps does container have

NODE
Whats deployed in node, and that vulns are in Node

PUBLICLY ACCESSIBLE
What is public? is it visible to Hackers

CODE REPO
Where is vuln repo deployed

LIBRARY/ CODE LINES
Find SAST/SCA vulns

About CloudDefense.AI

Our mission is to empower organizations in effectively mitigating risks within their Cloud and Kubernetes environments. CloudDefense.AI is specifically designed to address the intricate challenges posed by multi-environment, multi-workload, and multi-project cloud estates. By intelligently correlating crucial risk factors, our platform provides timely and actionable insights that optimize efficiency. Say goodbye to wasted time and embrace a proactive risk reduction approach with CloudDefense.AI.

Why CloudDefense.AI

The advent of the cloud has revolutionized the way engineering teams and businesses operate, enabling unprecedented speed and efficiency. However, this progress has introduced a whole new realm of complexity for security teams to navigate. The most pressing challenge lies in the knowledge and visibility gap that emerges within organizations.

CloudDefense.AI was created by cloud security veterans who worked at companies like **AMAZON, MICROSOFT, VMWARE, CHARLES SCHWAB** to fix the fundamental problems of existing approaches and deliver the cloud native experience customers need. Since founders have worked at Amazon, Microsoft, they understand the complexity and the elasticity of the cloud. CloudDefense.AI empowers all companies to effectively reduce cloud risk and easily build scalable, predictable workflows that work for all teams.

"CloudDefense.AI provides the context to the security team they need to mitigate risks and improve ROI. Securing resources in the cloud requires a fundamentally new approach. Siloed security tools and scanners even the best in class simply can't provide the perspective that today's security professionals need."

Anshu Bansal CEO, CloudDefense.AI

"I've been doing security for 15+ years, and I've never had a security tool deploy faster than CloudDefense.AI, let alone return this much value. The mean time to value was under a half hour."

Bhargava Gorthy: Director of Cyber Security, Columbia University

"CloudDefense.AI replaced our incumbent and instantly got us out of chasing false positives and into identifying and remediating critical risks... scaling the Infosec team's reach and velocity"

Chetan K, Cyber-Security Head, Piramal Finance