







Why Graphion

 Challenge	 Traditional Tools	 Graphion Advantage
 Overwhelming Risk Signals	Existing tools flood teams with static lists of vulnerabilities and alerts, slowing remediation — especially in the age of AI-generated code.	Graphion consolidates and correlates risk signals across tools, teams, and applications — delivering contextual, prioritized, and explainable insights that enable remediation at the speed of development.
 Fragmented Risk Visibility	Supply chain and cloud security data remain siloed across SBOM, CSPM, and SIEM tools.	Graphion's unified Knowledge Model links SBOM, IBOM, vulnerabilities, misconfigurations, and threats for a single source of truth.
 Siloed Remediation	Disparate tools lead to isolated findings and uncoordinated fixes, resulting in sub-optimized security outcomes.	Graphion drives enterprise-wide, risk-based remediation by correlating data across domains so all teams share the same priorities and view of risk.

Core Value Propositions

End-to-End Supply Chain Security

Manage SBOMs across builds and correlates software and dependency risks, transforming fragmented data into actionable insights.

SecOps Visibility with Context

Provides comprehensive understanding of cloud inventory, vulnerabilities, threats, and compliance posture across multi-cloud environments in the context of Application.

Unified Knowledge Model

Integrates SBOMs, IBOMs, vulnerabilities, misconfigurations, and threats into a single, contextual graph — delivering a unified view of software and cloud risk.

Agentic AI for Security Teams

Ontology-driven, conversational AI that reasons across the knowledge graph to deliver explainable and contextual answers. Produces explainable insights across every layer of the attack surface, ensuring faster, data-backed decisions and measurable security outcomes.

Accelerated Remediation

Enables contextual understanding of risk that drives prioritization and remediation at the speed of development.

Common Vernacular Across Teams

Establishes a shared language across Dev, Sec, and Ops for coordinated, risk-based remediation.

Key Features

- Application Onboarding
- Cloud Security Posture Management (CSPM)
- Access Posture Management
- Compliance Posture Management
- SBOM Management Module
- Vulnerability Management (VM)
- Software Supply Chain Security (SSCS)
- Conversational AI & Agentic AI News Feed
- Container Security
- API security
- MCP Server
- Supports both SaaS or Dedicated Deployments



CoreStack is an AI-powered NextGen Cloud Governance & Security Platform that enables enterprises to embrace cloud with confidence, rapidly achieving continuous and autonomous cloud governance at scale. CoreStack helps 750+ global enterprises govern more than \$2B in annual cloud consumption. The company is a Microsoft Azure (Legacy) Gold Partner, Amazon AWS Technology Partner with Cloud Operations Competency, Oracle Cloud Build Partner, and Google Cloud Build Partner.