

CoreStack Graphion

Ontology-Driven CNAPP. Govern Security from Code-to-Cloud.

Security Market Snapshot

The cloud security market has matured rapidly as enterprises now have deep visibility into assets, vulnerabilities, and attack paths across multi-cloud environments. Decision capacity is the new mandate as AI-accelerated development expands the software supply chain faster than triage can keep up. Security teams are struggling to move from detection coverage to decision quality: knowing which findings are consequential, why they matter, and which team needs to act to remediate vulnerabilities before they become incidents. Graphion delivers security at the speed of development.



Challenges Security Teams Face

Vulnerability findings arrive without context, and the gap between what was built and what is running keeps widening.



Why It Matters

Most security tools scan in isolation across code, containers, and cloud assets, generating findings without understanding how they relate. A CVE's risk depends entirely on where it is deployed, what data it can reach, how it is networked, and who can access it. While the SBOM records what went into the build, nobody reconciles it against what is deployed and reachable today, leading teams to rely on CVSS to rate risk severity. Working off long, manual backlogs, with no way to show which vulnerability is most critical to address, makes it impossible to remediate risk at scale.



How Graphion Helps

Graphion tracks two intersecting axes critical to cloud security: the delivery lifecycle (CI/CD, Registry, and Runtime) and the attack surface stack (code, IaC, identity, container, and API). By continuously reconciling SBOMs with IBOMs, Graphion produces a living map of what is running where, under what configuration, with what entitlements, and on which network paths. Teams can discover in seconds which application contains the risky component, where it is deployed, whether it is exposed, if it touches sensitive data, and who owns it, so they can act swiftly to remediate.

Siloed tools and remediation leave attack paths undetected, which is exacerbated when AI is bolted onto flat data and generates insights.

Conventional security tools treat inventory as a flat list. They record that a workload and a database both exist, but not that a permission change on one exposes the other, so the attack path between them is never surfaced. When an AI layer is added onto that same flat data, it returns insights without a traceable basis, making it hard for security teams to implement changes based on defensible, auditable data. This creates a compliance issue as findings only capture a point-in-time snapshot that is almost immediately out of date.

CloudKM, Graphion's ontology-driven knowledge model, defines how cloud objects are permitted to relate and interact. It contains two layers: a deterministic graph as the auditable source of truth, and an LLM reasoning layer above it. From this, Graphion builds a real-time graph of the behavioral and structural relationships between identities, running application code, and live infrastructure, so risky combinations and multi-hop attack paths are easily discoverable without teams needing to create or maintain correlation rules. The ontology constrains what the AI can conclude, making sure generated findings are repeatable and defensible, which enables continuous compliance.

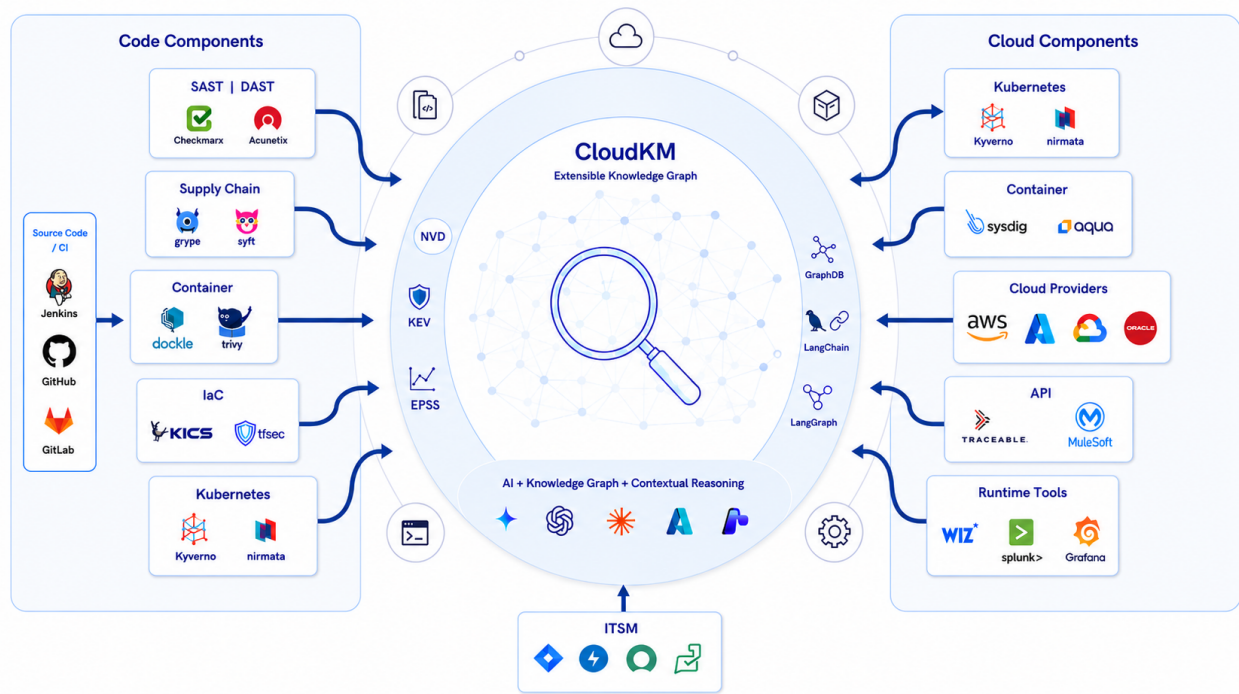
Risk is managed in silos across teams, making it hard for enterprises to see a complete and true risk position or where remediation investment pays back.

A severity score alone is not sufficient to tell teams the urgency to remediate a CVE. The same CVE in a live regulated system and in a sandbox environment arrive with the same score. The context that separates them lives outside the security tool, often in CMDBs, spreadsheets, and institutional memory, so every finding routes through a central team that is forced to rebuild its context manually.

Graphion embeds organizational context directly into prioritization, including application ownership, business criticality, financial impact, regulatory and compliance scope, supply chain risk, system resiliency, and data sensitivity. Ownership is inferred from how code is structured, how infrastructure is organized, and how teams operate, so it can be maintained as environments change. Remediation effort maps to business risk, not technical severity, helping teams know where to focus efforts to reduce risk to the most consequential findings.

Product Overview

Graphion is a Cloud-Native Application Protection Platform (CNAPP) that unifies code, supply chain, infrastructure, identity, and runtime context into a single intelligence layer. It is powered by CoreStack's Cloud Knowledge Model (CloudKM) — an ontology-driven knowledge graph that encodes what exists in your environment and how everything is related. Based on that context, Graphion fuses technical signals with business and organizational context to surface the most critical vulnerabilities, attributes each one to the team accountable for it, and applies policy-bound agents that recommend, explain, and prepare remediation inside the guardrails your security team defines. Every action captured as audit-grade evidence to help teams demonstrate continuous compliance.



Key Capabilities



Graph-Based Risk

Graphion builds a real-time, multi-dimensional map of your application and infrastructure ecosystem—linking every code dependency, container, configuration, and cloud asset to the risk it creates. Since the model is ontology-driven rather than rule-based, it captures what each relationship means and updates constantly as environments change, saving teams time on manually configuring relationship rules. This context-rich graph allows security teams to track not just individual vulnerabilities, but how they connect and cascade across environments.



360° Code-to-Cloud Visibility

Rather than treating SBOMs as compliance checkboxes, Graphion uses them as foundational intelligence. By continuously reconciling SBOMs and IBOMs, Graphion maintains a living map of what was built and where it's running, enabling security teams to quickly detect vulnerable components, drift, and misalignment between code and cloud. A single system allows teams to determine which applications contain a given vulnerable component, where it is deployed, whether it is internet-exposed, whether it touches sensitive data, and who owns it to strengthen security posture and remediate issues before they become incidents.



Agentic Remediation

Graphion's embedded AI learns about your environment, understands business criticality, and recommends precise, explainable remediations to improve risk posture, helping to turn noisy data into prioritized action. Since every agent reasons from the CloudKM rather than from raw alert streams, conclusions are traceable to the underlying evidence and defensible under scrutiny.



Continuous Compliance

Graphion comes with native support for NIST, FedRAMP, PCI DSS, CIS, HIPAA and GDPR — alongside a custom policy engine for requirements unique to your organization to help teams deliver real-time compliance artifacts and attestation reports. Every change, build, and deployment is validated against policy in real time to support boundary-enforced environments, secure-by-design principles, and traceable auditability.



DevSecOps Alignment Across the Full Lifecycle

Graphion integrates with your CI/CD pipeline to secure builds, infrastructure provisioning, and changes to operational environments to secure deployments, helping catch risk where it is cheapest to fix. Governance travels with the code rather than being applied after deployment.



Integrate With Your Existing Tech Stack

Security intelligence only changes outcomes if it reaches the people who can act on it. Using an MCP integration, Graphion exposes the CloudKM as a structured, governed data service that other systems and AI assistants can query directly, allowing prioritized, owner-attributed findings to show up in SIEM and SOAR platforms, ITSM systems, developer workflows, and other collaboration tools where remediation work is actually coordinated.



CoreStack is an agentic governance operating system for multi-cloud enterprises that unifies cost, security, compliance, and operations for cloud, SaaS, and AI systems into a single intelligent control plane. Purpose-built for regulated industries, CoreStack delivers CXO-grade financial, security, and SaaS governance outcomes at the speed of technology innovation. Trusted by 1,000+ global enterprises across 40+ countries, CoreStack governs \$3B+ in annual cloud consumption and oversees \$35B in annual SaaS transactions. CoreStack is a Microsoft Azure (Legacy) Gold Partner, Amazon AWS Technology Partner with Cloud Operations Competency, Oracle Cloud Build Partner, and Google Cloud Build Partner.