

CoreStack Graphion

Correlate Signals. Control Outcomes.

Product Overview

Today's cloud-native applications are built quickly using dozens of third-party components, and deployed into constantly evolving, ephemeral infrastructure. This approach leads to sprawling attack surfaces that are full of unseen risks, where a single missed vulnerability or misconfiguration can cascade into a breach or compliance failure.

Graphion is a Cloud-Native Application Protection Platform (CNAPP) that maximizes decision quality by fusing technical signals with business context. It is powered by CoreStack's Cloud Knowledge Model (CloudKM): an ontology-driven knowledge graph that encodes not just what exists in an environment, but how cloud objects, including assets, vulnerabilities, identities, and configurations relate to one another. CloudKM operates across two layers: a deterministic graph that serves as the auditable source of truth, and an LLM reasoning layer on top of it. That separation makes Graphion's answers traceable and evidence-backed rather than free-form inference over raw alert streams. CloudKM is queryable and defensible, ensuring that Graphion accurately reflects current cloud environments to deliver outcome-driven risk prioritization, remediation, and continuous compliance. Graphion serves as a single source of truth to provide multi-persona intelligence for engineering, security, and operations teams across regulated industries where audit-grade traceability, explainability, and cross-domain governance are non-negotiable.

Graphion covers the CNAPP surface from a single model, including:

- ⚡ Multi-cloud security posture management (CSPM)
- ⚡ Identity and access posture (CIEM)
- ⚡ Agentless workload visibility (CWP)
- ⚡ Kubernetes (KSPM)
- ⚡ Infrastructure-as-code posture (IaC)
- ⚡ Software supply chain security

By continuously pairing Software Bill of Materials (SBOM) with Infrastructure Bill of Materials (IBOM), Graphion creates a live inventory of the cloud resources, configurations, and runtime topology each application runs on.

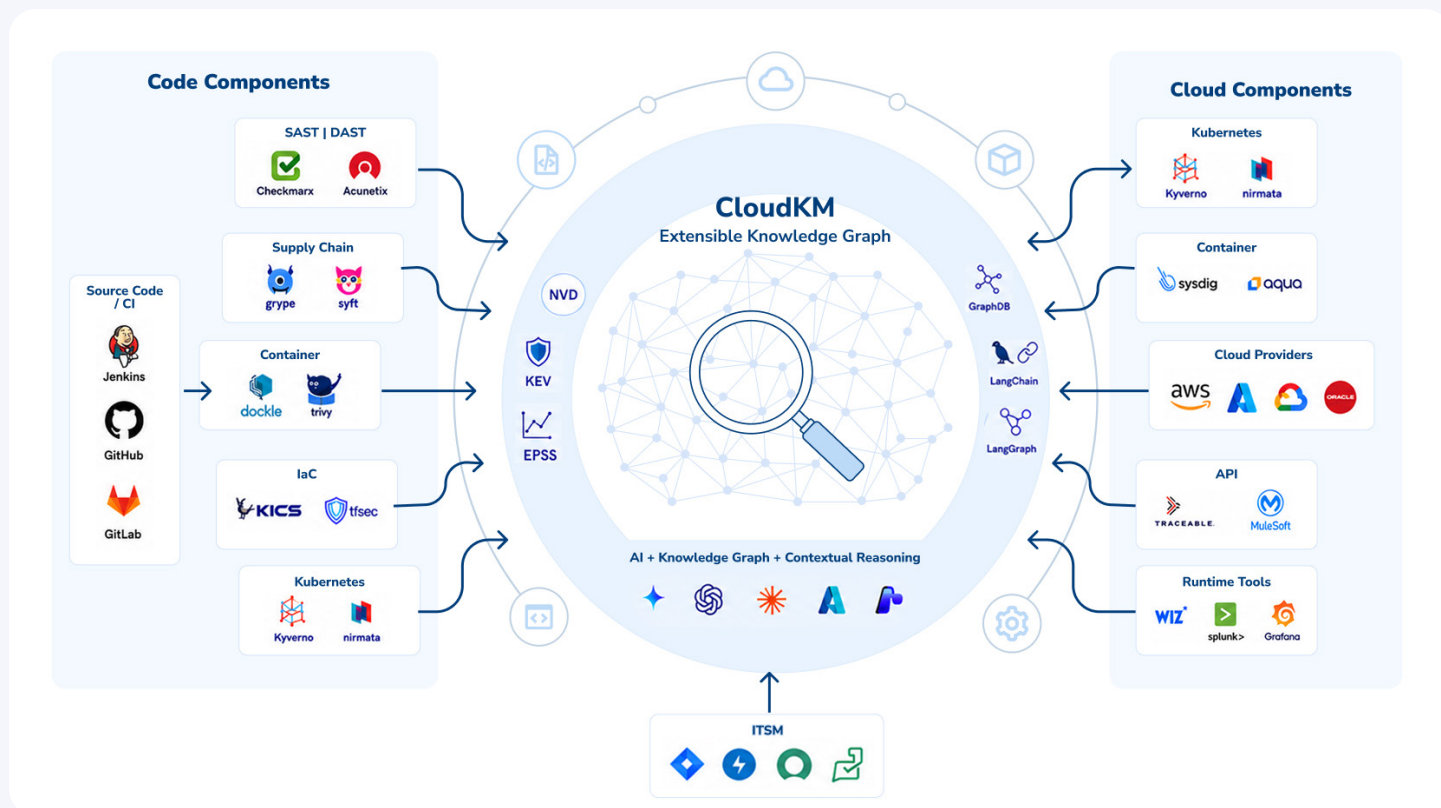
Graphion is available and can be deployed as SaaS, in a dedicated or air-gapped environment, or as a white-label OEM offering.

Cloud Security Challenges

CHALLENGE	IMPACT	HOW GRAPHION HELPS
Teams face an overwhelming amount of risk signals across dynamic cloud environments.	Fragmented data from security tools overwhelms teams with noise. Much of this data lacks context, making it hard to prioritize remediating the most consequential findings.	Graphion unifies data using an ontology-driven security graph, enriched with SBOM + IBOM correlation, to relate findings to the assets, identities, and owners they affect and to show teams where to prioritize remediation.
Manual, time-consuming security assessments are required both pre- and post-deployment.	Security reviews across initial ingestion, deployment, and operation stages are slow and disconnected, especially for ATO FedRAMP, and ongoing authorization.	Graphion automates evidence generation and embeds continuous attestation into DevSecOps pipelines to reduce time and efforts needed to run assessments.
Fragmented and non-contextualized vulnerability management tools make it hard to see a unified view of risk.	Traditional tools identify vulnerabilities in isolation, ignoring exploitability, criticality, and dependency impact.	Graphion combines business-context risk scoring with attack path analysis and reachability context over an ontology-driven graph. It prioritizes remediation recommendations by presence, prevalence, and real-world exploitability rather than CVSS severity alone.
Manual, reactive compliance and ATO is time-consuming and impossible to scale.	Checklist-driven compliance can't keep up with agile cloud changes, leading to trust and audit gaps when it comes to demonstrating ATO.	Graphion supports continuous ATO by embedding controls, attestation logic, and policy validation directly into DevSecOps workflows, with continuous evidence against 27 standards and a custom policy engine. Compliance becomes a live, auditable, and reportable capability rather than a point-in-time snapshot.
Maintaining supply chain security is a constant need.	Many organizations struggle to implement and continuously enforce critical security principles across the full supply chain (workloads, assets, and connections).	Graphion continuously validates dependencies, configurations, and policies across the SDLC and throughout the cloud-native stack.

How Graphion Works

A code-to-cloud 360° view of risk with CloudKM as the foundation



Every layer is ingested in context

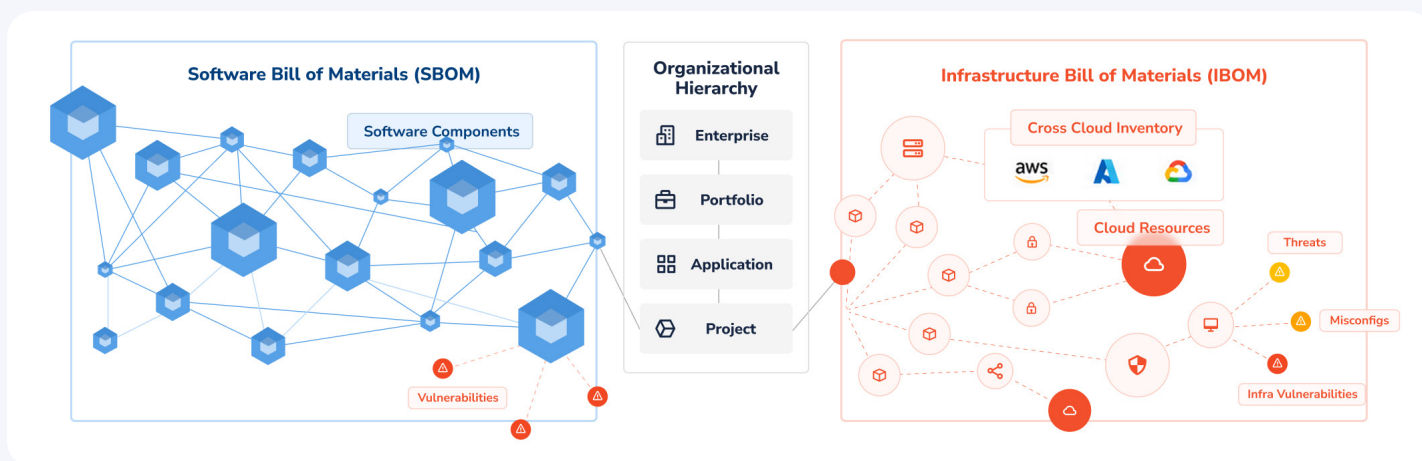
Graphion embraces signals across the full stack: build artifacts and SBOMs, applications and APIs, supply chain, containers, Kubernetes, infrastructure, and multi-cloud.

Map relationships, not just findings

Graphion preserves how each layer connects to the next, so a finding in a dependency, a misconfigured container, and an exposed cloud resource is understood as a single attack path.

One graph across surfaces

The same underlying model powers attack-surface views, attack-path analysis, and threat-surface scoring, to feed downstream systems such as Jira and ServiceNow with prioritized, context-rich work rather than raw noise.



Technical Capabilities

Graphion's capabilities are organized around three reinforcing pillars: a unified graph that sees everything, contextual reasoning that prioritizes what matters, and continuous assurance that ensures decisions are defensible.

Unified Visibility & Inventory

One connected model of your application and infrastructure estate.

CAPABILITY	DESCRIPTION
Code-to-Cloud Asset Graph	A single graph model that unifies SBOM (applications, components, dependencies) and IBOM (cloud resources, configurations, runtime topology) across AWS, Azure, Google Cloud, and Oracle Cloud — replacing fragmented inventories with one queryable source of truth.
Supply Chain Posture (SBOM)	View your supply chain inventory from SBOMs, including direct and transitive dependencies, so vulnerabilities are discovered and addressed before they reach higher environments.
Dynamic Runtime Posture (IBOM)	Continuous, on-demand ingestion of cloud resource inventory and metadata is dynamically updated to map interdependencies, so every finding is anchored in your evolving infrastructure.
Vulnerability & Threat Intelligence Fusion	Integrates external vulnerability signals (CVE, KEV, EPSS, vendor advisories) with internal telemetry, enriching every node in the graph with relevant threat context.
Extensible Graph Data Model	An open, extensible ontology allows you to incorporate custom asset types, telemetry, and security signals, so the graph reflects how your organization is actually structured.

Contextual Risk & Prioritization

A reasoning layer turns thousands of findings into a small, actionable set of explainable risks.

CAPABILITY	DESCRIPTION
Application-Aware Risk Scoring	Risk scores combine asset criticality, configuration state, and vulnerability characteristics specific to each application, shifting teams from “finding everything” to fixing what matters.
Attack Path Analysis	Surface multi-step attack paths that span code, container, infrastructure, and cloud layers to expose chained risks that single-tool scans miss.
Reachability & Exploitability Context	Determine whether a vulnerable component is reachable and prioritize accordingly to eliminate the noise of theoretical vulnerabilities that pose no real exposure.
Vulnerability Prevalence	Analyze how a given vulnerability propagates across applications, portfolios, and the broader supply chain, so a single remediation resolves risk at scale.
Posture Over Time	Maintain detailed posture snapshots by build and environment, providing time-series visibility into how security posture is trending across development, test, and production.

Continuous Assurance & Action

Turn prioritized risk into defensible decisions and downstream action.

CAPABILITY	DESCRIPTION
Continuous Policy Validation	Validate dependencies, configurations, and infrastructure state against selected policies as applications and environments evolve to flag drift as soon as it happens.
Compliance & Audit Evidence	Generate audit-ready evidence aligned to the frameworks that govern your industry — including HIPAA, SOC 2, ISO 27001, PCI DSS, NIST SP 800-53, and FedRAMP — compressing assessment cycles and supporting continuous authorization.
Downstream Workflow Orchestration	Push prioritized, context-enriched findings into the tools your teams already use, such as Jira, ServiceNow, and other ITSM and DevSecOps platforms, so remediation work arrives with relevant context.
Agentic Reasoning on the CloudKM	CoreStack’s proprietary CloudKM provides the reasoning layer over the graph — answering complex risk and compliance questions in natural language, with full traceability back to the underlying evidence.

Role-Based View of Risk

Graphion resolves the same CloudKM graph into role-specific views, so every stakeholder sees what they need to act without losing the shared context that makes cross-functional governance possible.

- ⚡ **Developers:** See prioritized fixes, in-pipeline, to quickly assess what matters for each code and dependency by owner.
- ⚡ **Security:** View a ranked queue across the full attack surface where every score traces back through the graph to the evidence behind it, including exposure, blast radius, exploitability, and business criticality from initial triage through correlated incident investigation.
- ⚡ **Operations:** Understand infrastructure drift, configuration change, and release-over-release changes, with finding attributeds to the team that owns the affected service.
- ⚡ **Leaders:** Gain continuous control attestation and audit-ready evidence drawn from the same graph the engineers work from, aligned to HIPAA, SOC 2, ISO 27001, PCI DSS, NIST SP 800-53, and FedRAMP for board-ready insights.



With Graphion, every risk view is generated from the same graph-powered model, enabling entire teams to work from a shared source of truth. Turn security complexity into clear, defensible decisions for cloud and security team members across your organization.

“CoreStack delivered immediate impact with substantial cost savings and cloud optimization across our entire environment. The platform integrates beautifully with our existing tools, and our independent analysts validated the security capabilities. We’re excited about what’s on the roadmap as we embrace a strong stance with additional automation and agentic AI enablement.”

MICHAEL LEE, VICE PRESIDENT, TAYLOR FARMS

About CORESTACK

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.