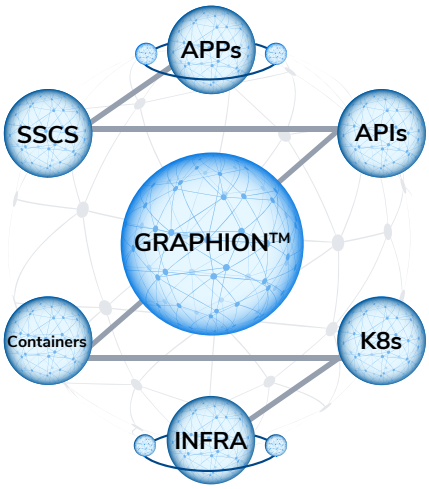
CORESTACK®

Graphion™ | Map Every Threat. Secure Every Connection.



Today's cloud-native applications are built fast, from dozens of third-party components, and deployed into constantly evolving, ephemeral infrastructure. The result? A sprawling software supply chain that's full of unseen risks—and where a single missed vulnerability can cascade into a breach or compliance failure.

CoreStack Graphion™ is a Cloud-Native Application Protection Platform (CNAPP) purpose-built for this new reality. It constructs a real-time, multi-layered graph of your entire cloud environment—integrating Software and Infrastructure Bills of Materials (SBOM + IBOM), policy enforcement, and AI-driven remediation. This living graph reveals not just what's vulnerable, but what's connected, what's at risk, and what to do next.

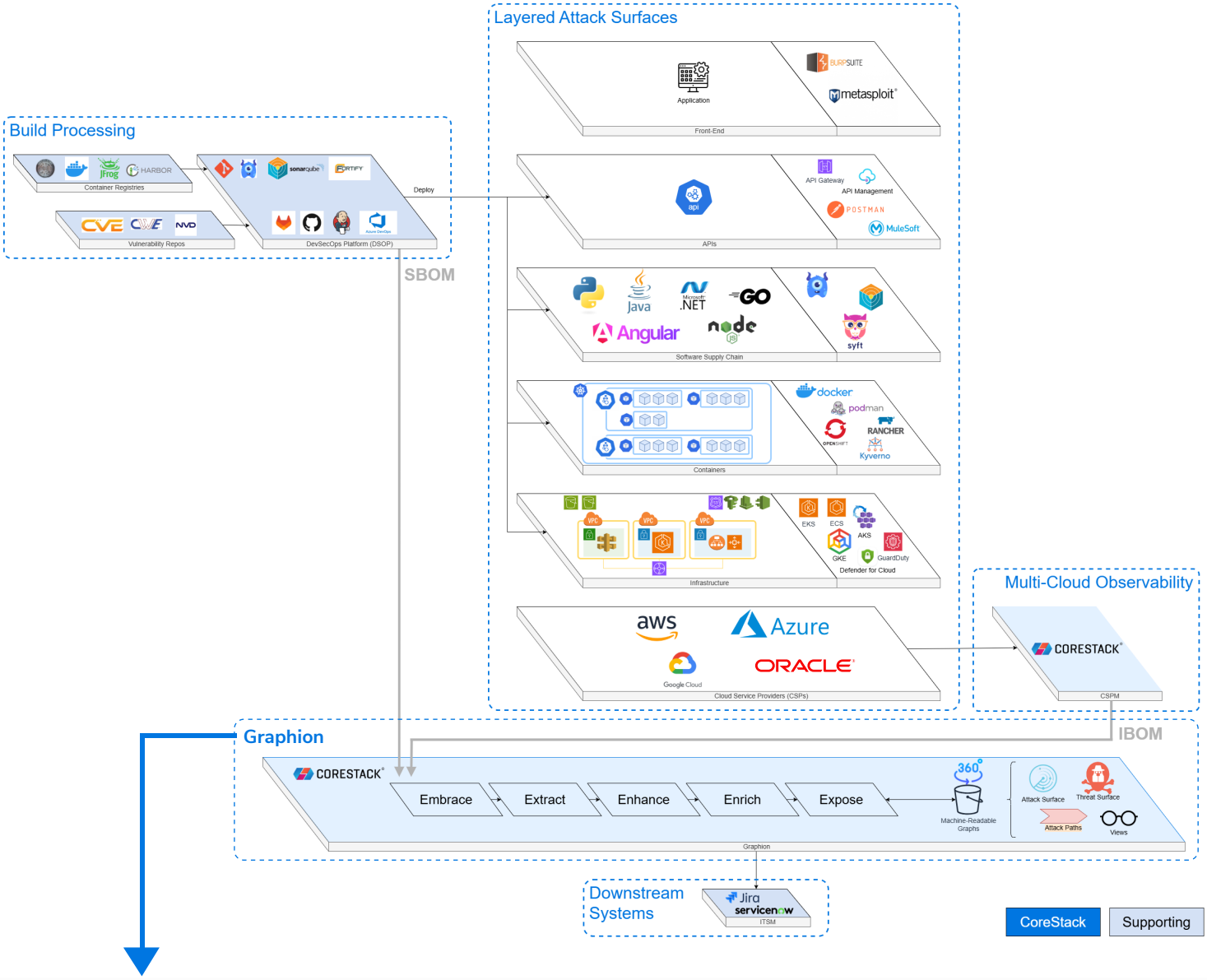
The urgency is real: with growing Zero Trust mandates, executive orders, and escalating attacks on the supply chain, Graphion gives security leaders the intelligence and automation to act now.

Challenge	Problem	Solution
Overwhelming Risk Signals in Dynamic Cloud Environments	Security data from fragmented tools overwhelms teams with noise and lacks context, making it hard to prioritize what matters.	Graphion unifies signals using a real-time threat graph enriched with SBOM + IBOM correlation.
Manual, Time-consuming SDLC Security Assessments	Security reviews at ingest, deploy, and operate stages are slow and disconnected—especially for ATO and cATO processes.	Graphion automates evidence generation and embeds continuous attestation into DevSecOps pipelines.
Fragmented and Context-Free Vulnerability Management	Traditional tools identify vulnerabilities in isolation, ignoring exploitability, criticality, and dependency impact.	Graphion uses Agentic AI and graph-based modeling to prioritize vulnerabilities based on real-world risk.
Static and Reactive Compliance Processes for ATO	Checklist-driven compliance can't keep up with agile cloud changes, leading to trust and audit gaps.	Graphion enables real-time policy validation and continuous ATO with OSCAL-aligned artifact generation.
Lack Of Practical Execution for Zero Trust Strategies	Many organizations struggle to enforce Zero Trust principles across workloads, assets, and connections.	Graphion continuously validates identity, configuration, and access policies across the cloud-native stack.

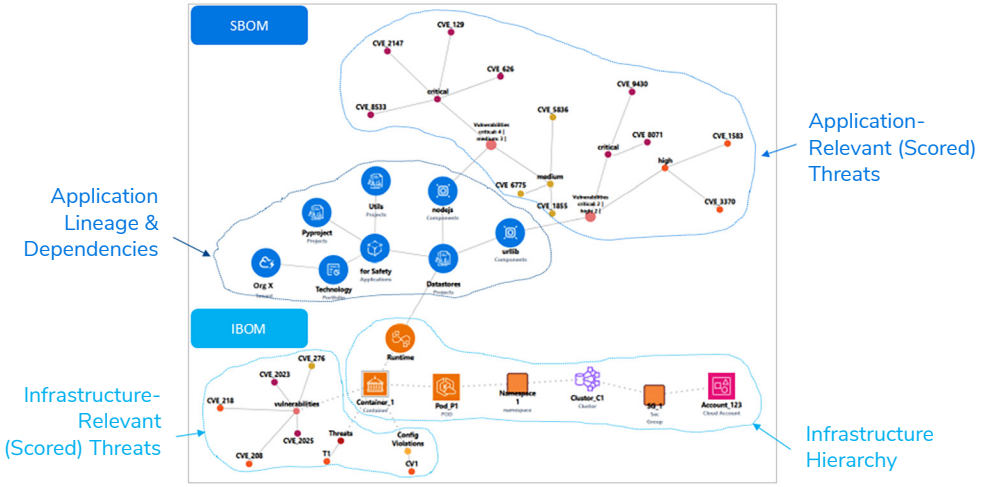
Your Long-Awaited 360° Vulnerability View

"It's not what you look at that matters, it's what you see."

- Henry David Thoreau



Graphion -Generated Insights



Key Features

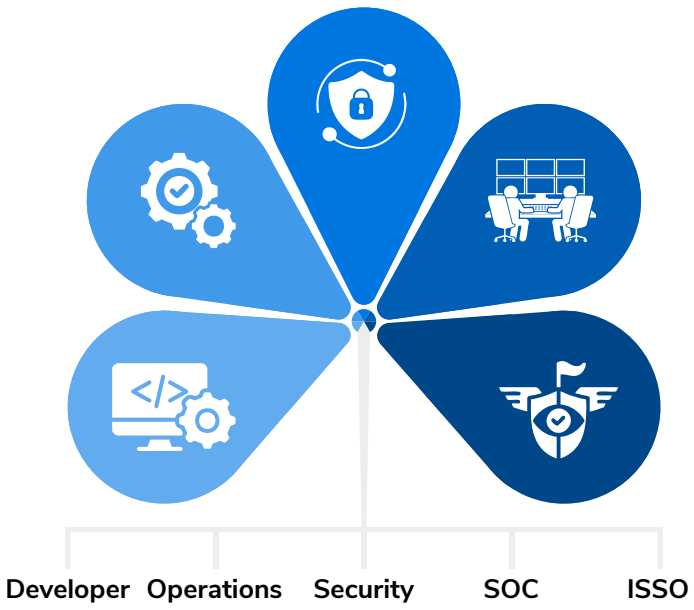
- Fused Tool Data – Blends together data from multiple tools used across the SDLC
- Contextualized Threat Scoring – Considers application-specific characteristics to assess the relevance of threats
- Multi-Layered Graphs – Creates holistic views for deeper insights

Key Technical Capabilities – Supporting the Federal Security Mission

Vulnerability Discovery & Management | ATO, Continuous ATO, Security Operations Center (SOC) | Zero Trust: Applications & Workloads

Embrace	**Multi-Cloud Support**	Deliver consistent, comprehensive security and visibility across all your cloud environments by providing full feature parity and unified management across major cloud service providers.	●
	AI-Enablement	Leverage deep AI integration across all features, enabling customers to dive deep into security issues without onerous research or cross-enterprise data calls.	●
	Out of the Box Integrations	Accelerate your security operations with our readily available, critical integrations for leading vulnerability intelligence sources, along with essential ITSM platforms.	● ● ●
	Modularity	Reduce adoption friction by offering highly modular capabilities, making it easy to integrate into existing systems and workflows.	●
Extract	**Asset Visibility**	Gain a comprehensive and continuously updated inventory of your software supply chain components, cloud resources, and interdependencies, providing the foundational insights essential for robust security posture and proactive risk management.	● ● ●
	Supply Chain Posture (SBOM)	Extract deep supply chain inventory using your SBOMs, including direct and transitive dependencies, to discover and address vulnerabilities before they impact higher environments.	● ● ●
	Dynamic Runtime Posture (IBOM)	Leverage continuous, on-demand ingestion of cloud resource inventory and metadata, dynamically updating interdependencies to contextualize all vulnerabilities within your evolving infrastructure.	● ● ●
	Automated Dependency Validation	Automatically determine the security posture of your application's dependencies by continuously validating your software supply chain inventory against defined policies, ensuring they are up-to-date, secure, and free from known vulnerabilities.	● ● ●
	Dynamic Assessments Support	Continuously capture and analyze your cloud resource inventory, metadata, associated vulnerabilities, identified threats, and policy violations to dynamically pinpoint and prioritize potential attack paths, streamlining your remediation efforts.	● ● ●
Enhance	**Vulnerability Intelligence**	Bridge external vulnerability data with your application's unique context is affected by the threat – thus integrating supplier vulnerability data (e.g., CVEs, breaches, malicious updates) with internal telemetry to detect vulnerabilities in your software supply chain.	● ● ●
	Data Extensibility	Integrate your security data seamlessly with our highly extensible data model, empowering you to incorporate vulnerabilities, operational telemetry and any custom data for a unified and comprehensive security overview.	●
	Agentic AI	Leverage our proprietary Large Governance Cloud ModelTM (LCGM), which harnesses the power of Agentic AI to deliver highly contextualized and deep insights for your vulnerability management processes.	●
Enrich	**Radical Prioritization**	Quantify risks by combining asset criticality, configuration state, and relevant vulnerability analyses – allowing you to prioritize remediation based on each of your application's unique characteristics, shifting your focus from "finding everything" to fixing what matters most.	● ●
	Posture Over Time	Maintain detailed posture snapshots for each build, providing crucial time-series visibility into security improvements across your development, test, and production environments.	● ● ●
	What-ifs	Simulate remediation outcomes with our what-if capabilities, allowing you to maximize your impact-to-effort ratio. By analyzing factors such as vulnerability prevalence and potential attack paths, you can prioritize fixes that matter most, delivering the greatest security uplift.	● ●
Expose	**Graph Data Model**	Leverage our extensible graph data model that intelligently relates all types of security data, empowering highly customizable dashboards and reports to accelerate your remediation efforts.	● ●
	Assessments	Support self-attestations to improve adoption of your applications by your stakeholders, which includes dependency tracking as part of continuous assurance.	● ●
	Continuous Validation	Ensure continuous compliance with security standards by dynamically flagging non-compliant items as your application's software (including dependencies) and infrastructure evolve.	● ●
	Policy Compliance	Create an ongoing evidence pipeline to support audit-ready reporting for various industry standards and security requirements.	● ●

The Enterprise



Priority

Receive clear direction for the top issues that need to be corrected in the code base, including dependencies

Clarity

Understand what's changing and when – software and infrastructure – to adequately prepare for new releases

Stability

Easily see the security posture of entire portfolios, including the impact of specific threats across multiple applications

Traceability

Quickly view the holistic changes (SBOM + IBOM) across releases, streamlining incident response and containment

Auditability

Acquire assurance that the full contents of system releases can be easily identified – facilitating reports & the proactive identification of new threats

Graphion's Effectiveness (Examples)

- **Automatic Re-Assessments:** Continuously monitor a release baseline for new threats and the contextual relevance of those threats, proactively triggering recommendations to remediate when relevant
- **BOM Diff:** Easily visualize software and infrastructure differences between application versions, streamlining incident analysis, containment, and resolution – and permitting automated trend analysis to feed agentic AI
- **Cross-Layer Attack Paths:** Link every code dependency, container, configuration, and cloud asset to the risks they collectively create – allowing you to track and visualize vulnerabilities across architectural layers
- **What-If Analysis:** Prior to remediation, visualize the impacts of to-be-fixed vulnerabilities across your portfolio's security posture – allowing you to invest your team's time and effort (and your money) in the most impactful resolutions
- **Automatically Refreshed Views:** Detect changes to infrastructure and automatically trigger the generation of refreshed views and recommendations (vulnerabilities, attack paths, etc.)

CORESTACK®

CoreStack is an AI-powered NextGen Cloud Governance 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.