

Graphion™ | Map Every Threat. Secure Every Connection.

Vulnerability Discovery & Management

Ocean of Code & Dependencies



Ocean of Infrastructure

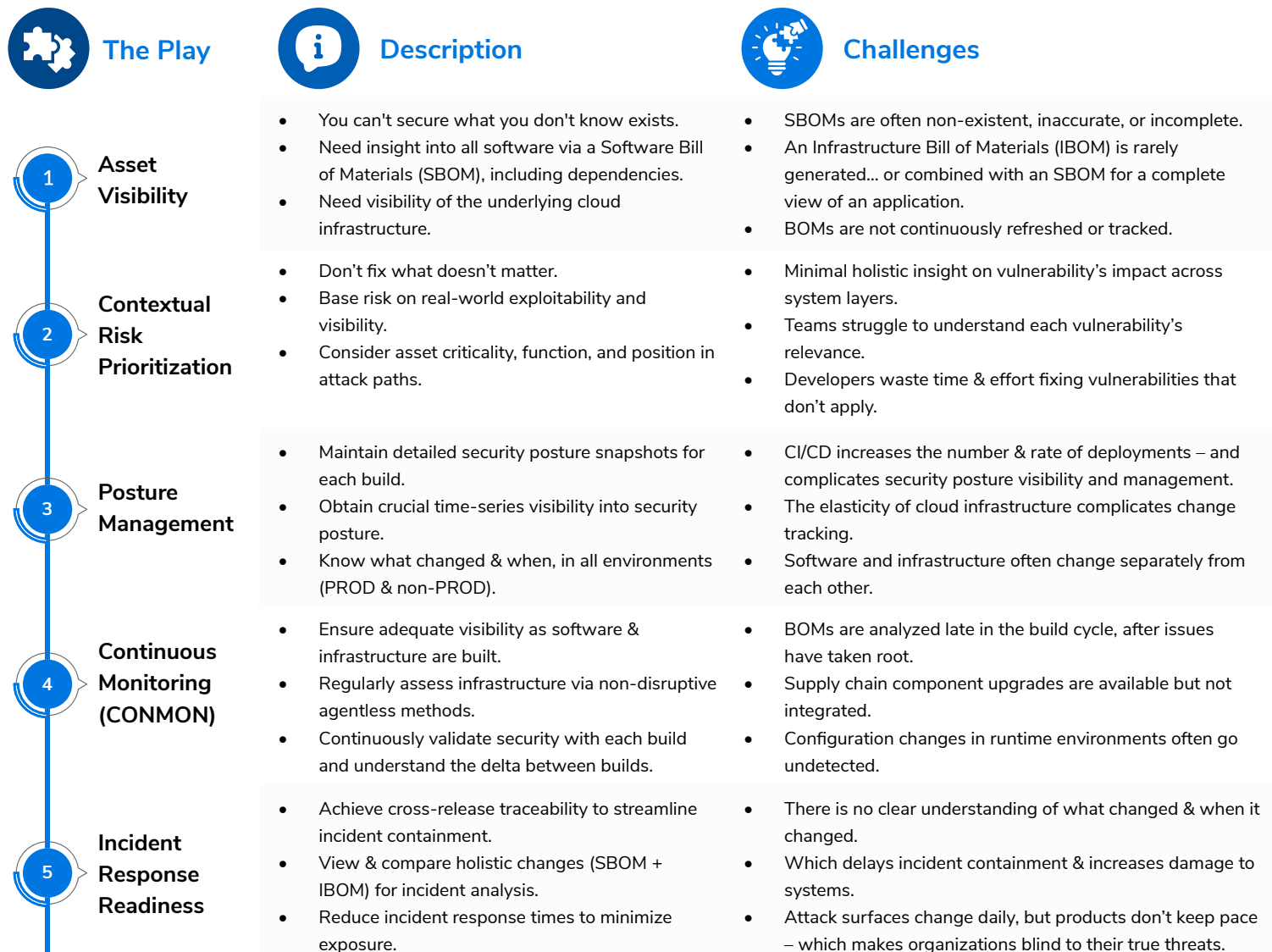


Ocean of Vulnerabilities



Vulnerability Discovery & Management is the essential foundation to implementing and maintaining a strong security posture within your entire application portfolio, covering software as well as infrastructure. However, most organizations struggle to build this foundation, which puts the entire operation at risk – primarily due to the ever-growing volume of code to manage (including open-source), dynamic cloud infrastructure, and unceasing vulnerabilities. Graphion provides a solution to help you navigate these rough waters, based on a few key tenets...

CoreStack's Vulnerability Discovery & Management Playbook



Discovery

“Discovery consists not in seeking new landscapes, but in having new eyes.”

- Marcel Proust

1 Asset Visibility

It's imperative to obtain data for all assets under your organization's control – software as well as the infrastructure that runs it. Without that data, the subsequent analysis cannot be fully trusted; and no amount of AI will help. Graphion uses SBOMs and IBOMs as the fuel for our vulnerability analysis engine.

Contents

Creation

SBOM

All components in applications, including third party dependencies (full supply chain).

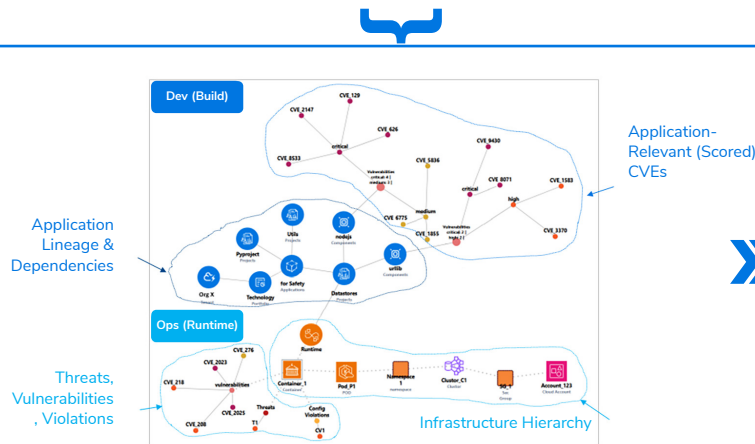
Software suppliers create an SBOM for each build, using COTS tools in their CI/CD pipeline to do so (e.g., Gype and Syft). Once generated, suppliers automatically submit the SBOM via Graphion's API to trigger insights processing.

IBOM

Infrastructure components included in the cloud-based runtime environment that hosts the application.

Rarely generated or refreshed by organizations. Requires specialized knowledge of cloud environments across all major Cloud Service Providers. CoreStack, with years of Cloud Security Posture Management (CSPM) experience, creates IBOMs on an agentless basis.

Graphion's discovery process provides immediate benefits by highlighting the right things to fix in the context of each application. Additionally, it is the genesis of each application's tailored AI model that will be used & further improved in subsequent vulnerability assessments.



BOMs are accurate, integrated, and refreshed

2 Contextual Risk Prioritization

Graphion combines SBOMs and IBOMs to establish a unique framework for clear, powerful, and holistic insights into an application.

By tracking software deployments to specific infrastructure components, Graphion provides several crucial capabilities for effective vulnerability remediation:



Graphion's flexible scoring algorithm is based (in part) on industry standards such as CISA's Stakeholder-Specific Vulnerability Categorization (SSVC).

- **Enhanced Contextual Scoring:** Graphion only assesses vulnerabilities that match characteristics of the runtime environment (e.g., specific Operating Systems).
- **Radical Prioritization:** Contextual scoring based on an application's 360° view pinpoints the highest risk vulnerabilities to fix, for each application/project.
- **Attack Surface Visibility:** Software overlaid on host infrastructure, combined with vulnerability information, collectively identify the attack surfaces and paths open to bad actors – then scored to ascertain the most important to remediate.
- **Posture Over Time:** Graphion tracks the software and infrastructure posture of every application/project/build over time, providing a highly valuable platform for runtime troubleshooting (e.g., SOC-led incident response and containment).
- **BOM Diffs:** Visualization of differences between application versions (for software and infrastructure) streamlines incident analysis – and provides trend data to feed Agentic AI.

Management

Once you see clearly, protection becomes precise tactical execution – not guesswork.

3 Posture Management

Without a continuous, accurate, and complete series of application changes, operations becomes time-consuming detective work when runtime problems occur... making it difficult to perform analysis, with or without AI.

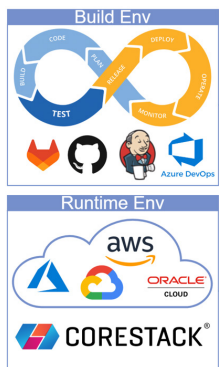
In today's hyperconnected digital ecosystem, the traditional network perimeter has exploded into a complex mesh of cloud services, remote access points, IoT devices, and third-party integrations – plus microservices, containers, and serverless computing. With expanded and layered attack surfaces, adversaries can choose from a plethora of methods to take advantage of exploitable vulnerabilities & misconfigurations, constructing attack paths that progress through the layers of your architecture to arrive at high-value assets (HVAs).

Graphion blends time series of SBOMs & IBOMs, application characteristics, and vulnerability data into our Large Cloud Governance Model (LCGM™) ontology. Applying Agentic AI, our algorithms identify Threat Surfaces and Attack Paths across your architecture layers – scoring them to reveal the most critical components and paths to remediate. This capability – unique to Graphion – sets a new bar for Posture Management.

4 Continuous Monitoring (CONMON)

Integration into CI/CD pipelines via Graphion's API achieves CONMON of the build process through SBOM analysis; and with ongoing CSPM, Graphion refreshes IBOMs. BOM updates continuously trigger holistic (SBOM+IBOM) risk & trend analysis.

Given the critical nature of BOMs to Graphion's insights algorithms, CoreStack engineered the product to continuously receive and process BOM data using the following methods:



» Graphion easily integrates into CI/CD pipelines in major COTS DevSecOps platforms, permitting a continuous feed of SBOMs as they're created during an application's build process.

» Through CoreStack's agentless CSPM capabilities, Graphion scans an application's cloud-based runtime environment on a scheduled basis, then creates an IBOM which defines the infrastructure in that environment.

These automated BOM streams allow Graphion to continuously supply your organization with up-to-date recommendations to protect your portfolio's security posture, including trend analytics between builds.

5 Incident Response Readiness

While significantly curbing the number of system issues, reality dictates that issues will still occur. Graphion has you covered with automated 360° analytics, associated recommendations, and the basis for Agentic AI and auto-remediation.

Graphion empowers Security and Ops Teams to:

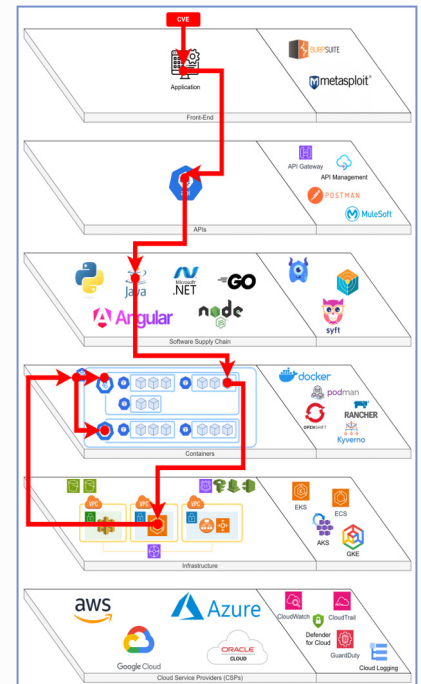
- » **Assess Your Attack Surface:** By identifying all potential entry points that an unauthorized user might exploit, you gain a clearer understanding of vulnerabilities, conceptualize the risks they pose, and prioritize their remediation.
- » **Pinpoint Root Causes:** Move beyond superficial symptoms to uncover the underlying vulnerabilities and misconfigurations that enable an attack.
- » **Quickly Synthesize Location & Prevalence Data:** Understand where assets reside and how widely they are used – which helps responders determine the impact of a cyber attack, prioritize containment, assess exposure, and implement effective remediation strategies.

With Graphion, organizations can shift from reactive, isolated incident response to proactive, holistic security management.

>60%

of organizations now unknowingly rely on at least one compromised open-source component in their software

- 2025 Supply Chain Threat Landscape



Attack Surfaces lead to Attack Paths that often span multiple layers of an application's architecture. This is where Graphion's innovative layered view comes to the rescue... supporting Attack Surface Analysis which allows users to visualize the system connections that an attacker can traverse after exploiting a vulnerability. Without this fundamental capability, threat hunting and attack path analysis is cumbersome and potentially incomplete – which could be catastrophic.

