

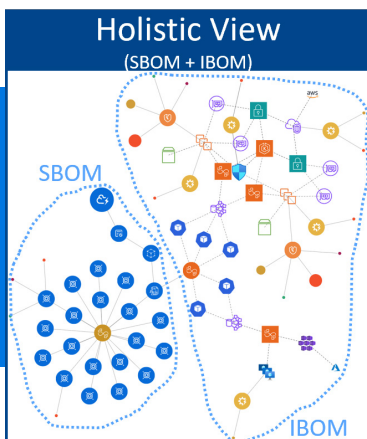
# Graphion™ | Map Every Threat. Secure Every Connection.

## FedRAMP 20x: Continuous Vulnerability Management (CVM) Standard

As part of the FedRAMP 20x initiative, RFC-0012 proposes requirements for a Continuous Vulnerability Management standard – with the intent “to ① ensure providers **promptly detect and respond** to critical vulnerabilities ② by considering the **entire context** over Common Vulnerability Scoring System (CVSS) risk scores alone, ③ prioritizing **realistically exploitable** weaknesses, ④ and encouraging **automated vulnerability management**... ⑤ (and) to facilitate the use of existing commercial **tools for cloud service providers** ⑥ and **reduce custom government-only reporting** requirements.”

CoreStack’s Graphion solution helps product and cloud suppliers achieve and maintain FedRAMP certification via **continuous, proactive, automated, contextual, and cumulative** system assessments.

Graphion Features	Description	RFC Intentions					
		1	2	3	4	5	6
<b>Holistic View</b>	Overlays each application’s software on dynamic cloud infrastructure, showing exactly what runs on each component in the connected operational cloud ecosystem and thus helps ascertain vulnerability prevalence; continuously builds this view from (a) an application’s Software Bill of Materials (SBOM) produced by CI/CD pipelines and (b) the Infrastructure Bill of Materials (IBOM) generated by Cloud Security Posture Management (CSPM) as modifications occur within the monitored runtime environment.	✓	✓	✓	✓	✓	
<b>Context-Based Scoring</b>	Quantifies risks by combining asset criticality, configuration state, and relevant vulnerability analyses – supporting prioritization based on each application’s holistic view and unique characteristics, shifting focus from "finding everything" to fixing what matters most.	✓	✓	✓	✓		✓
<b>History &amp; Trends</b>	Presents the timeline of modifications to each cloud component, including software, infrastructure, and configurations – thus providing security posture trends, Configuration Management (CM) for infrastructure and software, and the identification of past-due remediations.	✓		✓	✓		✓
<b>Agentic AI</b>	Constructs, continuously enhances, and leverages an ontology based on unique data derived specifically from a customer’s application portfolio.	✓	✓	✓	✓		
<b>Reports</b>	Leverages data extracted from SBOMs and IBOMs, subsequently enhanced and enriched, then stored to support Agentic AI and reports – assisting with troubleshooting, analysis, and compliance (e.g., with NIST 800-53), as well as Authorization to Operate (ATO), risk assessment, and Plan of Action and Milestones (POA&M).	✓			✓		✓



### Context-Based Scoring

Graphion score is based on the KEV status, EPSS, CVSS, age of the vulnerability, and Business Criticality score of your application.

Issue ID	Graphion Score	CVSS	Severity	EPSS	Is KEV
CVE-2025-27363	8.7	8.1   V3.1	High	65.21%	Yes
CVE-2020-11023	7.55	6.1   V3.1	Medium	21.67%	Yes
CVE-2025-48384	6.9	8   V3.1	High	4.08%	Yes

### Vulnerability Prevalence

CVE-2025-27363 - Prevalence

- Affected Supply Chain Prevalence: **94**
- Affected Infra Resources: **7**
- Affected Organizational Entities: **47**

Supply Chain Prevalence

Component Type	Component Name [(Version)]	Project Name
library	freetype (2.10.4-9.e19)	cs-external-api_cr
library	freetype (2.10.4-9.e19)	broker__preview
library	freetype (2.10.4-9.e19)	notification__previe
library	freetype (2.10.4-9.e19)	compliance__cnapp
library	freetype (2.10.4-9.e19)	cost__preview

94 total  
1 - 5 of 94

Infrastructure: Prevalence +

Prevalence across Organizational Entities +

# Graphion's core features cover the categorized FedRAMP Requirements (FRR) presented in RFC-0012

		Graphion Features						
ID	Requirement Summary	How Graphion Helps		HV	CBS	H&T	AI	R
CVM	Blanket requirements for the Continuous Vulnerability Management (CVM) standard		HV = Holistic View; CBS = Context-Based Scoring; H&T = History & Trends; AI = Agentic AI; R = Reports					
01	Establish and maintain programs that <b>detect, evaluate, report</b> , mitigate, and remediate vulnerabilities in the relevant timeframes, leveraging CISA's guidelines.	<ul style="list-style-type: none"> <li>Continuously identifies the most important vulnerabilities to remediate for each application, factoring in contextual data.</li> <li>Shows progress (or lack thereof) in that remediation.</li> </ul>	✓	✓	✓	✓	✓	
02	Create and maintain vulnerability reports showing <b>vulnerability management activity</b> , including specific information about all detected vulnerabilities within the FedRAMP Authorized offering.	<ul style="list-style-type: none"> <li>Leverages the combined view of software &amp; infrastructure (esp. the internet-reachability of resources) to assess each vulnerability's credibility &amp; exploitability.</li> <li>Presents time series tracking of changes to a system, including vulnerabilities per build &amp; diffs between those builds.</li> </ul>	✓		✓		✓	
03	Make vulnerability reports available to all necessary parties in human-readable and machine-readable formats.	<ul style="list-style-type: none"> <li>Uses configurable Role-Based Access Control (RBAC) for report access.</li> <li>Permits the secure export of report data on an ad hoc or scheduled basis.</li> </ul>					✓	
04	Adjust the risk and severity of vulnerabilities by <b>using CVSS and contextual information</b> (to determine <b>exploitability</b> and the <b>potential adverse impact of exploitation</b> ).	<ul style="list-style-type: none"> <li>Considers application-specific characteristics when evaluating vulnerability credibility for the app (macro level).</li> <li>Considers resource reachability and the potential impact of exploitation when evaluating vulnerability credibility for each asset (micro level).</li> </ul>	✓	✓		✓		
05	Address vulnerabilities <b>within the relevant timeframes</b> or create a POA&M.	<ul style="list-style-type: none"> <li>Shows progress (or lack thereof) in remediations for identified vulnerabilities, with respect to (WRT) the applicable response timeframe.</li> </ul>			✓		✓	
06	Maximize <b>automation</b> to identify, mitigate, and/or remediate <b>credibly exploitable</b> vulnerabilities in <b>internet-reachable information resources</b> .	<ul style="list-style-type: none"> <li>Runs vulnerability assessment for each build (SBOM-based).</li> <li>Runs vulnerability assessment for each CSPM-generated IBOM.</li> <li>Uses context-based scoring to assess vulnerability relevance.</li> </ul>	✓	✓		✓		
07	Do NOT share sensitive information about vulnerabilities; but do share sufficient information for <b>oversight, tracking, analysis, action, and risk assessment</b> with all necessary parties.	<ul style="list-style-type: none"> <li>Presents time series tracking of changes to a system, covering software and infrastructure.</li> <li>Maintains data for maximum &amp; cumulative insights.</li> </ul>					✓	
08	<b>Maintain records</b> of all false positives and <b>exclude</b> validated ones from reports.	<ul style="list-style-type: none"> <li>Stores a history of vulnerability data relevant to each application.</li> <li>Provides report filters at the row and column levels.</li> </ul>			✓		✓	
09	Group similar vulnerabilities <b>detected across different resources</b> .	<ul style="list-style-type: none"> <li>Tracks vulnerability metadata across the cloud ecosystem.</li> <li>Supports reports that group resources by that metadata.</li> </ul>	✓			✓	✓	
TM	Requirements for timeframes							
01	Continuously provide <b>up-to-date vulnerability reports</b> to all necessary parties at least monthly.	<ul style="list-style-type: none"> <li>Allows users to create scheduled or ad hoc reports.</li> <li>Gives users the ability to distribute reports on a scheduled basis.</li> </ul>					✓	
02	Make <b>historical vulnerability reports</b> available to all necessary parties.	<ul style="list-style-type: none"> <li>Stores raw data as well as derived data.</li> <li>Utilizes the results for reporting and AI purposes.</li> </ul>			✓		✓	

ID	Requirement Summary	How Graphion Helps	HV	CBS	H&T	AI	R
<b>TM Requirements for timeframes</b>							
03	Remediate <b>Known Exploited Vulnerabilities (KEVs)</b> in accordance with CISA's timelines.	<ul style="list-style-type: none"> <li>Considers KEV status when scoring each vulnerability.</li> <li>Shows progress (or lack thereof) in remediations.</li> </ul>		✓	✓		✓
04	<b>Discover, analyze, and assess</b> all <b>internet-reachable resources</b> for vulnerabilities <b>continuously</b> .	<ul style="list-style-type: none"> <li>Creates holistic views for each SBOM &amp; IBOM.</li> <li>Evaluates &amp; scores vulnerabilities through the contextual lens of a holistic view.</li> </ul>	✓	✓			
05	Address <b>credibly exploitable</b> vulnerabilities in <b>internet-reachable resources</b> promptly.	<ul style="list-style-type: none"> <li>Shows progress (or lack thereof) in remediations for identified vulnerabilities, WRT the applicable response timeframe.</li> </ul>			✓		✓
06	<b>Discover, analyze, and assess</b> all resources that are <b>NOT internet-reachable</b> for vulnerabilities <b>continuously</b> .	<ul style="list-style-type: none"> <li>Runs vulnerability assessment for each build (SBOM-based).</li> <li>Runs vulnerability assessment for each CSPM-generated IBOM.</li> </ul>	✓	✓			
07	Address <b>credibly exploitable</b> vulnerabilities in resources that are <b>NOT internet-reachable</b> promptly, until or unless the <b>potential adverse impact</b> is Low or Very Low.	<ul style="list-style-type: none"> <li>Shows progress (or lack thereof) in remediations for identified vulnerabilities, WRT the applicable response timeframe.</li> <li>Continuously reassesses exploitability and impact.</li> </ul>			✓		✓
08	Address <b>credibly exploitable</b> (low) impact vulnerabilities in resources that are <b>NOT internet-reachable</b> promptly, until or unless the <b>potential adverse impact</b> is Very Low.	<ul style="list-style-type: none"> <li>Shows progress (or lack thereof) in remediations for identified vulnerabilities, WRT the applicable response timeframe.</li> <li>Continuously reassesses exploitability and impact.</li> </ul>			✓		✓
09	Address all remaining detected vulnerabilities on a regular basis.	<ul style="list-style-type: none"> <li>Shows progress (or lack thereof) in remediations for identified vulnerabilities, WRT the applicable response timeframe.</li> </ul>			✓		✓
<b>AY Provide guidance on the application of the standard</b>							
01	May share reports publicly or with other parties, barring the release of sensitive data.	<ul style="list-style-type: none"> <li>Allows users to create scheduled or ad hoc reports.</li> <li>Permits the secure export of report data on an ad hoc or scheduled basis.</li> </ul>					✓
02	May provide additional (non-required) data as deemed appropriate.	<ul style="list-style-type: none"> <li>Allows users to create scheduled or ad hoc reports.</li> <li>Permits the secure export of report data on an ad hoc or scheduled basis.</li> </ul>					✓
03	Follow FedRAMP's best practices and technical assistance on <b>continuous vulnerability management</b> and reporting.	<ul style="list-style-type: none"> <li>Continuously assesses apps for each build and CSPM run.</li> <li>Maximizes automation while securing data.</li> </ul>	✓	✓	✓	✓	✓
<b>EX Address exceptions</b>							
01	May be required to share additional data & reports at an alternative frequency per other legitimate agreements.	<ul style="list-style-type: none"> <li>Allows users to create scheduled or ad hoc reports.</li> <li>Permits the secure export &amp; sharing of report data on a scheduled basis.</li> </ul>					✓
02	May be required to provide sensitive data as part of review, response or investigation by necessary (authorized) parties.	<ul style="list-style-type: none"> <li>Allows users to create scheduled or ad hoc reports.</li> <li>Permits the secure export &amp; sharing of report data on a scheduled basis.</li> </ul>					✓



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.