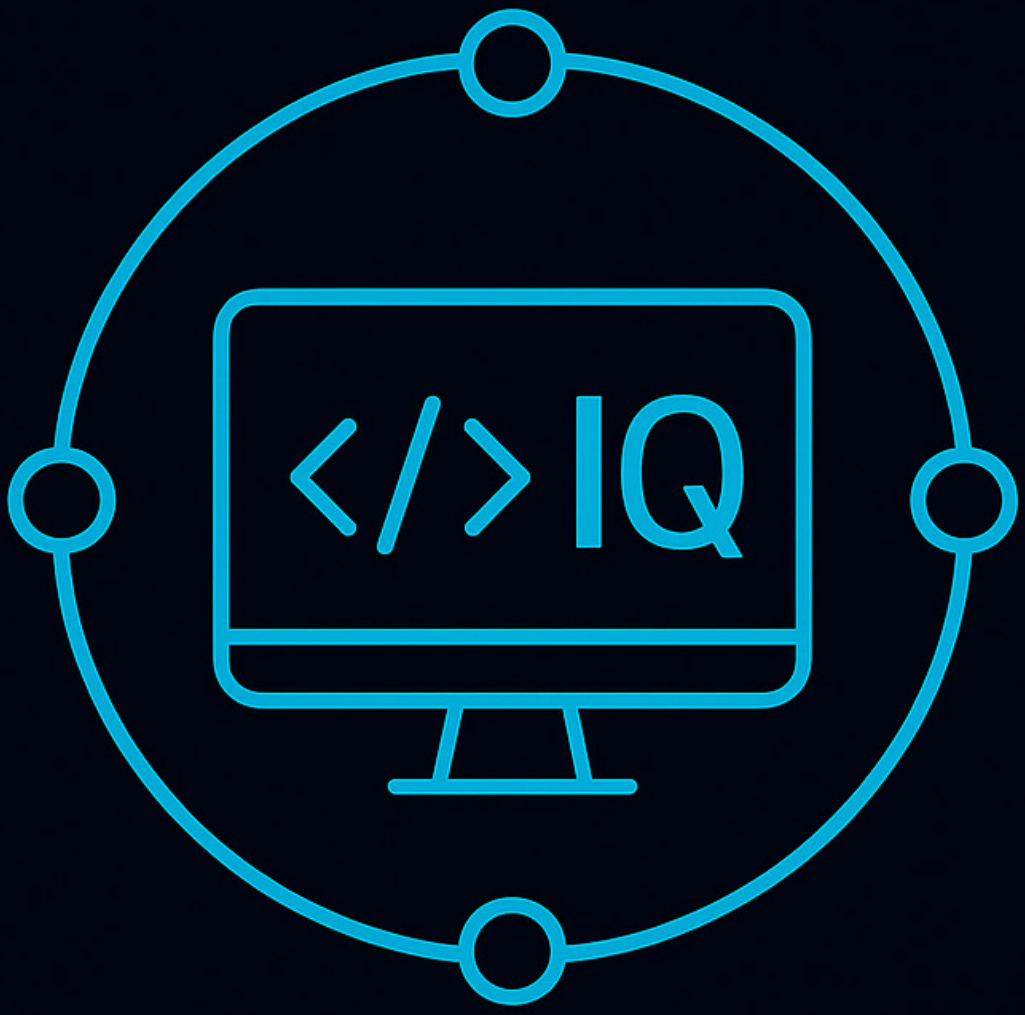
Solution Brief

BlueRock

From Noise to Actionable Risk Reduction

BlueRock Runtime Reachability IQ (RRIQ)



BlueRock

Solving the Problem of Vulnerability Overload

Problem:	Explosion of code and libraries, creates vulnerability overload.
Cause:	SCA, SAST, DAST run behind, are based on theoretical risk, and are not prioritized by what actually runs.
Impact:	Increase risk to business, compounded further by the rise of AI-speed attacks.
Solution:	BlueRock Runtime Reachability IQ (RRIQ), seamlessly integrated as part of the BlueRock Compute Firewall, reveals what is actually loaded and run by apps, enabling teams to focus on the vulnerabilities that truly matter. BlueRock RRIQ is an integrated and integral part of BlueRock runtime machine images and represents the first step in the Compute Firewall movement.
Benefit:	Saves significant developer time, prioritizing fixes for *runtime vulnerabilities*

Introduction:

In modern application development, security teams are overwhelmed. Traditional vulnerability scanners produce a deluge of alerts, often listing thousands of CVEs (Common Vulnerabilities and Exposures) within an application's dependencies. Further, the time to exploit vulnerabilities is decreasing dramatically, while the amount of code generated is increasing – both accelerated by AI capabilities – exposing a larger attack surface.

These two factors create a perfect storm where **traditional vulnerability remediation programs will never catch up**. As a result, security and development teams are left with an impossible task: trying to patch everything, everywhere, all at once.

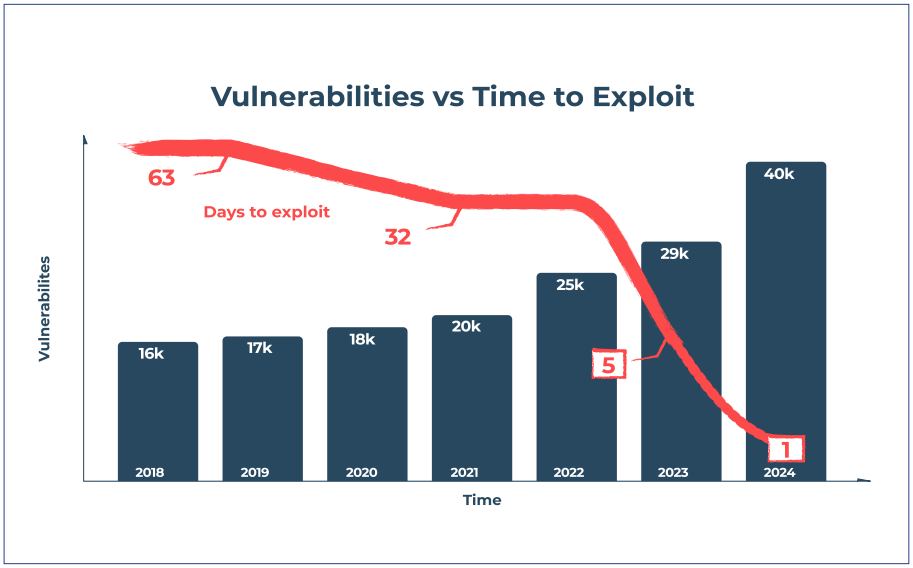
To further exacerbate the problem, the speed to exploit vulnerabilities has reduced from weeks or months, to days or even hours. And with the rise of AI-speed exploit development [1] the discrepancy between traditional scan/patch and attacker speed is only going to get worse.

1 https://sean.heelan.io/2025/05/22/how-i-used-o3-to-find-cve-2025-37899-a-remote-zeroday-vulnerability-in-the-linux-kernels-smb-implementation

The Need For Effective Prioritization

In the era of AI-speed attacks and shrinking remediation windows, SCA, SAST, and even DAST tools can't keep pace. **The traditional "scan-and-patch" model is broken.**

It treats a vulnerability in a library that is never used with the same urgency as one in a core, internet-facing function that runs with every app instance. This floods developers with huge vulnerability patch lists, creating "findings fatigue", wasted effort, and friction between security and development teams.



The real question:

Which of the thousands of vulnerabilities pose a real threat to my application?

The BlueRock Difference: Runtime Reachability IQ

Unlike traditional SCA, SAST and DAST tools that only scan static manifests and files on disk or test apps from the outside, BlueRock RRIQ has a unique vantage point, **observing the application as it executes at runtime.**

BlueRock RRIQ tracks which packages and libraries are actually loaded and executed. It then applies advanced agentic AI workflows to automate what is usually an incredibly complex and time consuming process for developers: cross-referencing software sources and vulnerability databases. This inverts the model, delivering a bottoms-up, evidence-based view of your true attack surface and highest-priority CVEs.

Reducing CVEs to Patch

Saving Time with BlueRock RRIQ

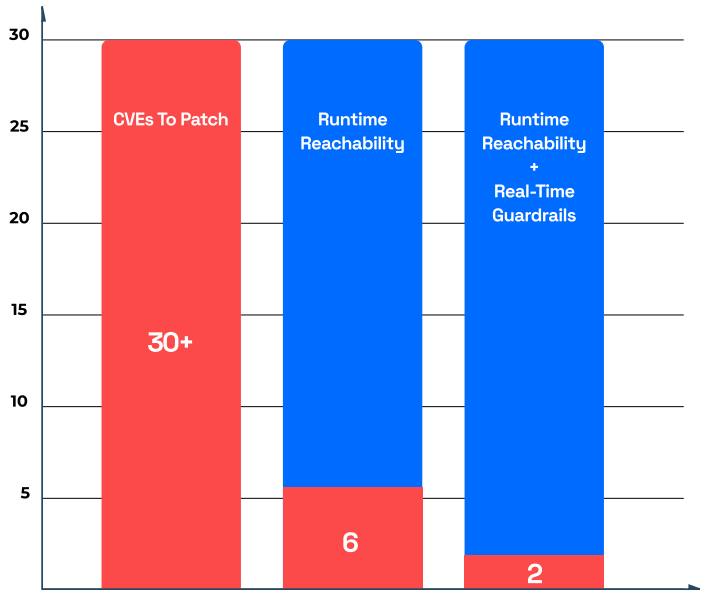
The result of BlueRock Runtime Reachability IQ is that every developer can drastically reduce the time they spend focusing on vulnerability patching.

BlueRock RRIQ saves Dev Teams
2-3 Days Per Sprint, Per Developer.

Without BlueRock: Devs must triage 30+ CVEs per sprint.

With Runtime Reach IQ (RRIQ) : Cuts triage to 6 by showing which libraries/functions matter.

With RRIQ + Enforcement: Drops to 2 by blocking exploit paths tied to critical CVEs.



Map What Matters:

From Static Code Analysis to Real Runtime Risk

Stop distracting developers with meaningless CVEs to triage and patch. Drive value to your business by giving developers more time to deliver meaningful innovation.

Key Benefits

Runtime Visibility	Gain visibility into what is actually executing in your cloud/app environments.
App development cost savings	Reduce your vulnerability patch list by 70 - 90%, saving time spent on false positive vulnerabilities on a continual basis.
Reduced Team Friction	Evidence-based reports align dev and security on what to fix first.
Real-Time CVE Intelligence	Identify which CVEs impact your runtime instantly—including zero-days.

Feature Breakdown:
BlueRock Runtime Reachability IQ

Real-Time Runtime Reachability Report	Dynamic Dependency Analysis	Goes beyond static analysis to show libraries that are actually loaded and executed at runtime.
	Loaded vs. On-Disk Visibility	Distinguishes between packages merely present in the environment and those actively loaded into memory.
	Simplified Reporting	Real-time reporting on running/reachable libraries. Supports Python and Java applications.
Actionable Risk Prioritization	Evidence of Vulnerability Coverage (EVC)	Enriches runtime data with vulnerability intelligence to prioritize true threats.
	Reachable Vulnerability Flagging	Flags CVEs in loaded components as “Reachable” and assigns them highest remediation priority.
Visual Attack Chain Analysis (Paid Feature)	Exploit Visualization	Maps exploited vulnerabilities to the MITRE ATT&CK framework. Shows how BlueRock Guardrails mitigate common exploitation methods.
	Enhanced Reporting Engine	Combines runtime + exploit intelligence. Generates reports in PDF/JSON formats.

About BlueRock

BlueRock is the leading Compute Firewall solution delivering breakthroughs in runtime reachability analysis and real-time protection against AI-speed attacks. The BlueRock Compute Firewall embeds runtime security directly into compute — not bolted on like legacy agents — so you can move at developer speed without friction.

BlueRock Runtime Reachability Intelligence (RRIQ) reduces the number of vulnerabilities that developers and app teams have to address by up to 90 percent. An integral part of the BlueRock Compute Firewall, RRIQ delivers results by inverting the vuln identification process. Unlike legacy code scanning of static source code repos, BlueRock RRIQ focuses on what is reachable and running, giving you real-time intelligence on what CVEs are most important to fix. This results in thousands of dollars in hard cost savings per developer per year, while freeing them up to do what they do best — driving innovation for your business.

BlueRock Runtime Security delivers a secure-by-default runtime that sees and stops AI-assisted attacks in real-time. Unlike legacy security agents that are complex to deploy, slow app performance, and introduce new attack surfaces, BlueRock Runtime Security ships as hardened AWS machine images (AMIs), delivered as part of the images you love: Amazon Linux, Bottlerocket, and Ubuntu. The result is frictionless integration into your existing CI/CD pipeline, requiring no app changes by developers and assuring breakneck performance of your apps.

Learn more at bluerock.io.

BlueRock