Solution Brief

BlueRock

Not Network. Not Perimeter. Built into Compute. Built to Block

The NEXT Next-Gen ~~Network~~ Compute Firewall.

The Firewall Isn't Dead. It's in the Wrong Place.

The Firewall Isn’t Dead. It’s in the Wrong Place.

Traditional network firewalls were once security’s front line. But in today’s cloud-native world, the line has shifted. Firewalls can’t stop what doesn’t cross a perimeter—and modern exploits don’t play by perimeter rules.

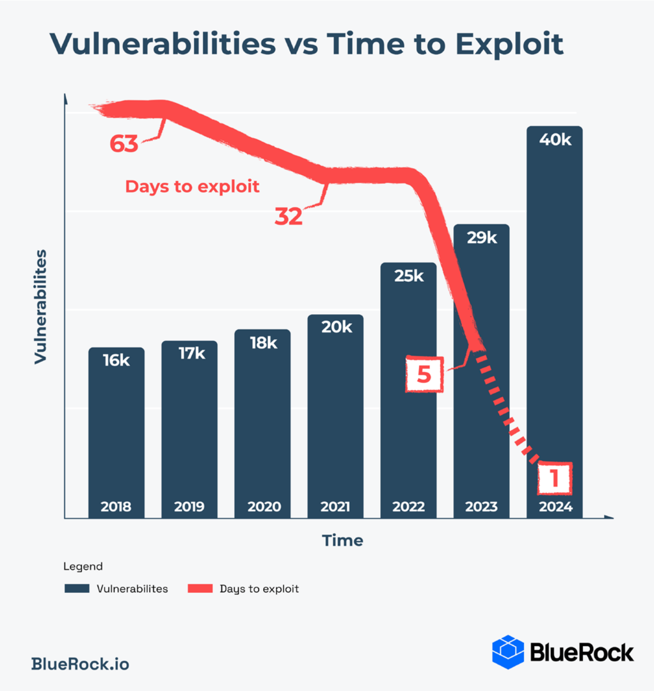
Meanwhile, we’ve piled on tools: SAST, CSPM, CNAPP, SIEM, CDR, ADR. These detect, monitor, and correlate—but they either operate pre-runtime or can’t enforce reliably at runtime. Even emerging tools that promise enforcement still fall short of real-time protection.

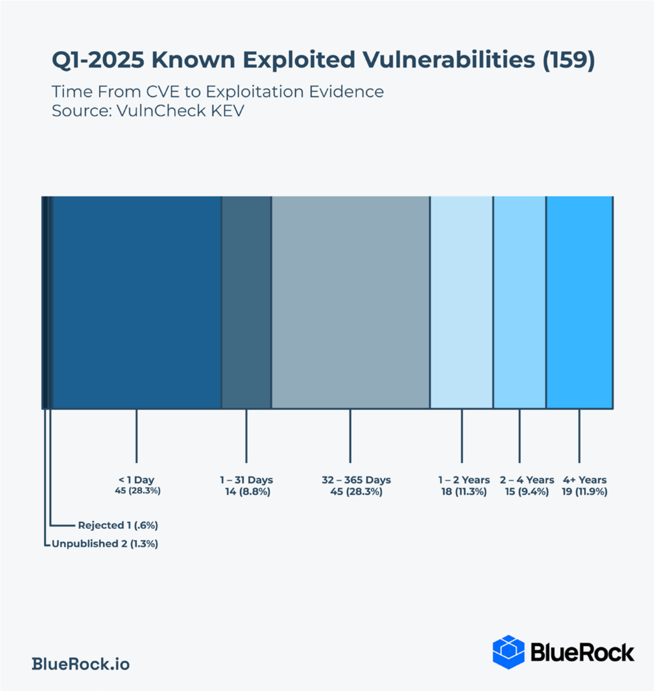
This is a problem.

Exploits Now Arise at AI Speed & Scale

Attackers aren’t waiting days or weeks anymore. In the last year, we’ve seen CVEs **exploited within minutes** of disclosure[1]. And in the first quarter of 2025, it has been reported that **28% of Known Exploited Vulnerabilities (KEV) were exploited within 24 hours** of disclosure[2].

If a firewall can’t stop them, and detection tools only alert after the fact, we have a serious enforcement gap.


Vulnerabilities vs Time to Exploit


Q1-2025 Known Exploited Vulnerabilities (159)

Time From CVE to Exploitation Evidence
Source: VulnCheck KEV

[1] https://www.bleepingcomputer.com/news/security/hackers-use-poc-exploits-in-attacks-22-minutes-after-release/

[2] https://vulncheck.com/blog/exploitation-trends-q1-2025

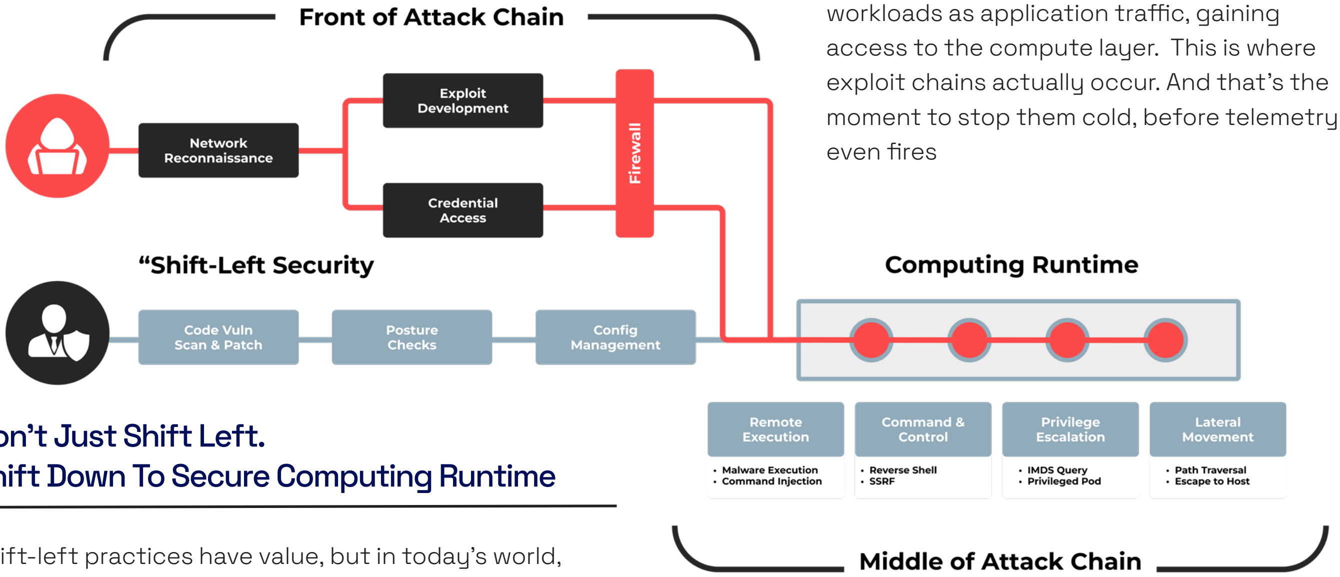
Real Enforcement Belongs in Compute

To close the enforcement gap, we need to move past agents and detection logic.
Enforcement needs to be:

- ☆ **Embedded in the compute layer**
- ☆ **Workload-transparent and tamper-resistant**
- ☆ **Realtime-preemptive, not after-the-fact reactive**

Stop Exploit Chains Where & When They Run

Modern attacks don't get blocked at network ingress. They interact with workloads as application traffic, gaining access to the compute layer. This is where exploit chains actually occur. And that's the moment to stop them cold, before telemetry even fires



Don't Just Shift Left. Shift Down To Secure Computing Runtime

Shift-left practices have value, but in today's world, they aren't enough. Developers are drowning in patch pipelines and scan alerts – no match for modern attacks running at AI-accelerated speed and scale. Shift Down Security means moving enforcement into the runtime layer—the infrastructure itself.

Security Agents Can't Fill The Gap

Runtime security tools rely on agents, telemetry and complex analysis to detect, then respond, to attacks. This makes agents a poor foundation for real-time enforcement:

- ☆ **Too Noisy — high volumes of alerts with poor signal-to-noise**
- ☆ **Too Slow — telemetry events arrive after behavior has already occurred**
- ☆ **Too Complex — tuning requires deep expertise and constant care**
- ☆ **Too Fragile — attackers can tamper with eBPF hooks or spoof telemetry**
- ☆ **Too Blind — many behaviors go undetected until it's too late**

The result? Most organizations are still watching—and hoping someone spots an attack and responds in time.

Introducing The NEXT Next-Gen ~~Network~~ Compute Firewall.

Evidence of Vulnerability Coverage (EVC)

Buy Time. Patch Smart.

Runtime eXploit Guardrails (RXG)

Respond Less. Block More.

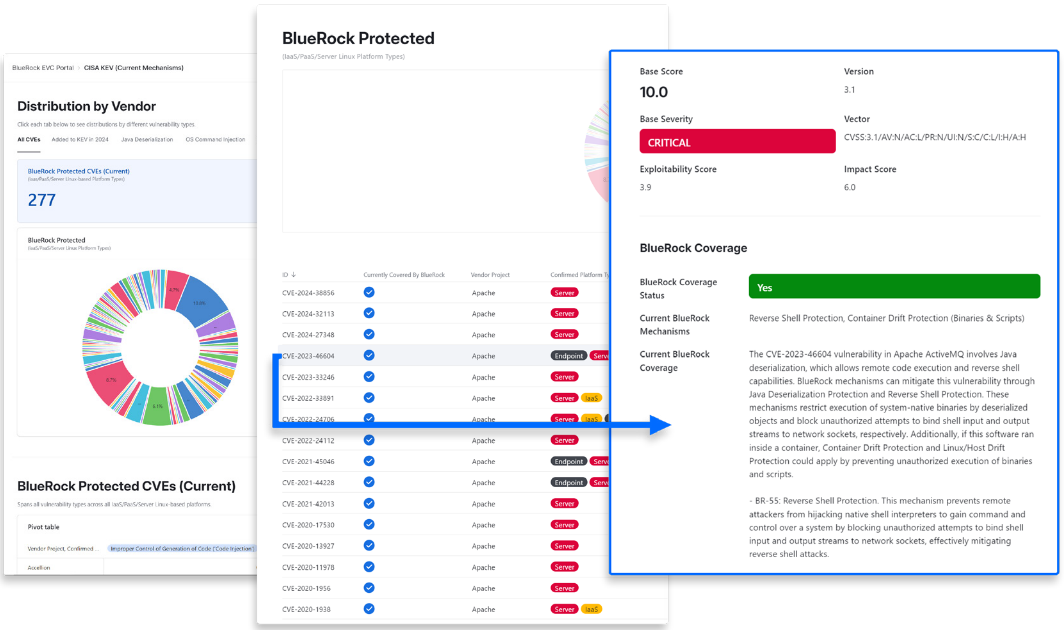
BlueRock EVC

Leveraging a multi-model AI inference system to analyze CVE characteristics and attack chains, EVC maps exploit exposure to BlueRock RXG security protections which provide a compensating control. This gives you the ability to prioritize which vulnerabilities are most critical to patch. BlueRock reduces the set of CVEs security teams need to juggle and helps prioritize the ones that matter most.

Trying to achieve or maintain SOC2, PCI, HIPAA, or ISO 27001 compliance? BlueRock EVC auto-documents explanations of vulnerability coverage to help you and your auditors accelerate certification and re-certification efforts.

- Rapid Response: AI-driven vulnerability insights—even when new zero-day threats emerge.
- Transparent Analysis: Detailed breakdowns of how each CVE is neutralized.
- Comprehensive Coverage: Not just the headline threat—EVC analyzes the full chain of vulnerabilities.
- Optimized for Your Workloads: Specifically tailored for Linux servers and container environments.

learn more at BlueRock.io/evc



BlueRock EVC Portal > CISA KEV (Current Mechanisms)

Distribution by Vendor

Click each tab below to see distributions by different vulnerability types.

All CVEs | Added to KEV in 2024 | Java Deserialization | OS Command Injection

BlueRock Protected CVEs (Current)
(Iaas/PaaS/Server Linux-based Platform Types)

277

BlueRock Protected
(IaaS/PaaS/Server Linux Platform Types)

BlueRock Protected CVEs (Current)

Spans all vulnerability types across all IaaS/PaaS/Server Linux-based platforms.

Pivot table

Vendor Project, Confirmed ... | Improper Control of Generation of Code ('Code Injection')

Accellion

BlueRock Protected
(IaaS/PaaS/Server Linux Platform Types)

ID ↓	Currently Covered By BlueRock	Vendor Project	Confirmed Platform Ty
CVE-2024-38856	✓	Apache	Server
CVE-2024-32113	✓	Apache	Server
CVE-2024-27348	✓	Apache	Server
CVE-2023-46604	✓	Apache	Endpoint Serv
CVE-2023-33246	✓	Apache	Server
CVE-2022-33891	✓	Apache	Server IaaS
CVE-2022-24706	✓	Apache	Server IaaS
CVE-2022-24112	✓	Apache	Server
CVE-2021-45046	✓	Apache	Endpoint Serv
CVE-2021-44228	✓	Apache	Endpoint Serv
CVE-2021-42013	✓	Apache	Server
CVE-2020-17530	✓	Apache	Server
CVE-2020-13927	✓	Apache	Server
CVE-2020-11978	✓	Apache	Server
CVE-2020-1956	✓	Apache	Server
CVE-2020-1938	✓	Apache	Server IaaS

Base Score	Version
10.0	3.1
Base Severity	Vector
CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H
Exploitability Score	Impact Score
3.9	6.0

BlueRock Coverage

BlueRock Coverage Status	Yes
Current BlueRock Mechanisms	Reverse Shell Protection, Container Drift Protection (Binaries & Scripts)
Current BlueRock Coverage	The CVE-2023-46604 vulnerability in Apache ActiveMQ involves Java deserialization, which allows remote code execution and reverse shell capabilities. BlueRock mechanisms can mitigate this vulnerability through Java Deserialization Protection and Reverse Shell Protection. These mechanisms restrict execution of system-native binaries by deserialized objects and block unauthorized attempts to bind shell input and output streams to network sockets, respectively. Additionally, if this software ran inside a container, Container Drift Protection and Linux/Host Drift Protection could apply by preventing unauthorized execution of binaries and scripts. - BR-55: Reverse Shell Protection. This mechanism prevents remote attackers from hijacking native shell interpreters to gain command and control over a system by blocking unauthorized attempts to bind shell input and output streams to network sockets, effectively mitigating reverse shell attacks.

BlueRock RXG

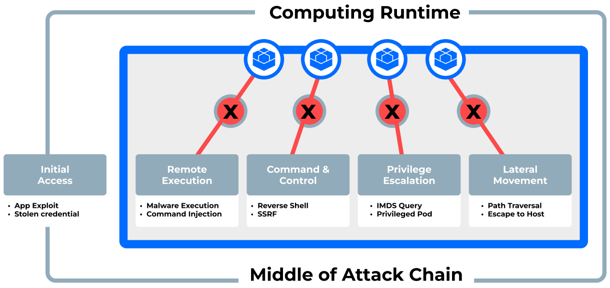
BlueRock RXG isn't a next-gen security agent. It's a compute-native enforcement layer that is capable of seeing and stopping attack chains before they execute.

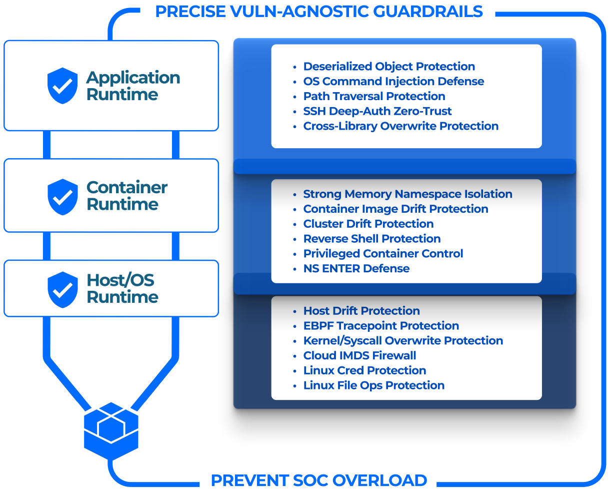
Pre-integrated into cloud-ready Linux and Container node images, BlueRock RXG delivers real-time attack prevention to protect apps, container, and host runtime environments. Always-on and transparent, BlueRock RXG removes the need to deploy yet another security agent and protects workloads without requiring developer code changes.

- Delivered as a BlueRock-supported Linux machine image based on what you already use.
- Enhanced with simple invariant-based runtime guardrails, BlueRock RXG is effective at blocking entire classes of exploit chains across Linux and container environments.
- Assures workload performance and security, without compromise.

BlueRock runtime execution guardrails can be configured to run in alert-only or real-time blocking mode. Instead of searching for needles in noisy telemetry haystacks, BlueRock RXG proactively enforces runtime **invariants**—precise guardrails capable of disrupting entire classes of attacker exploit chains. Such invariant-based rules flip the script on "detect and respond", clearly defining what should **never happen** in uncompromised workloads. Examples include running container apps that weren't part of the container image, binding shell interpreter IO streams to network sockets, or executing OS commands from deserialized runtime objects.

This approach enables BlueRock to see and stop attacker behavior and **avoid false positives**. It doesn't guess—it blocks only definitively malicious actions. And it does so with little to **no performance impact.**




PRECISE VULN-AGNOSTIC GUARDRAILS
Application Runtime
Container Runtime
Host/OS Runtime
• Deserialized Object Protection
• OS Command Injection Defense
• Path Traversal Protection
• SSH Deep-Auth Zero-Trust
• Cross-Library Overwrite Protection
• Strong Memory Namespace Isolation
• Container Image Drift Protection
• Cluster Drift Protection
• Reverse Shell Protection
• Privileged Container Control
• NS ENTER Defense
• Host Drift Protection
• EBPF Tracepoint Protection
• Kernel/Syscall Overwrite Protection
• Cloud IMDS Firewall
• Linux Cred Protection
• Linux File Ops Protection
PREVENT SOC OVERLOAD

BlueRock. Built to block.

Founded by cybersecurity industry veterans Ashar Aziz (Founder/CEO of FireEye) and Bob Tinker (Founder/CEO of MobileIron), BlueRock is delivering breakthroughs in runtime protection to build a stronger digital foundation for the apps and services the world relies on by giving the security teams the capabilities they need without slowing down DevOps.

Learn more at BlueRock.io

BlueRock