

August 2025 Release Notes

BlueRock v1.2.2 for Ubuntu 24.04 and 22.04 v1.2.2 - Release Notes

Release Date: August 28, 2025

We are thrilled to announce the release of **BlueRock v1.2.2 for Ubuntu!**

BlueRock for Ubuntu is our new offering designed to bring powerful runtime security to your cloud applications with zero friction. This release provides lightweight, standalone application sensors and pre-secured virtual machines and containers for cloud and modern AI/ML workloads. Get instant visibility and secure by default protection where it matters most—inside compute runtime.

What's New in v1.2.2

- **Standalone Python & Java Sensors:** Our new "Unplugged" sensors for Python and Java provide deep runtime protection without any dependency on kernel-level components. They are lightweight, easy to deploy, and perfect for containerized environments. These sensors protect against deserialization, remote code execution, and path traversal attacks.
 - **Embedded Compute Runtime Security:** Embedded in the Ubuntu distribution, BlueRock protects against a range of exploit tactics that attackers may use to compromise systems including: remote shell, script execution, rootkit installation, container capabilities modification, critical system configuration modification and more.
 - **Dual Mode Operation:** Run sensors in **Observe Mode** for event visibility and alerting or switch to **Block Mode** to actively stop threats in real-time.
 - **Event Monitoring and SIEM Integration:** BlueRock supports event streaming via OLTP and can be integrated with CloudWatch or virtually any other SIEM or event monitoring solution via OTEL collectors.
-

New Features in Detail

1. Lightweight, Standalone Application Runtime Sensors

You can now secure your applications from the inside out with minimal overhead. These sensors are designed to run independently, making them ideal for any environment, from a local Docker Desktop to a full-scale EKS cluster.

- **Python App Runtime Sensor:** Provides robust protection for Python applications against common runtime attacks.
- **Java App Runtime Sensor:** Delivers runtime security for Java applications, offering deep visibility into JVM behavior.

2. Embedded Compute Runtime Security

With the BlueRock Ubuntu distribution, you can detect and block a range of weaponized tactics that attackers may use to compromise your cloud instances. In addition to the application runtime security methods mentioned above, compute runtime security capabilities include:

- Remote Shell Detection and Blocking
- Memory Access Control
- Container Drift Detection and Blocking
- Container Capabilities Control
- Rogue Container Detection and Blocking
- NSenter Detection and Blocking
- Container Socket Protection
- Process Exec Restrictions
- Dynamic Library Exec Restriction

3. Dual Mode Operation: Observe and Block

You are in full control of the security posture.

- **Observe Mode (Default):** The sensor detects and logs all policy violations and suspicious activities without taking any blocking action. This is perfect for initial deployments to understand application behavior and evaluate potential security gaps without impacting performance.
 - **Block Mode:** When enabled, the sensor actively prevents threats as they happen, providing proactive protection for your critical applications.
-

Thank you for being part of our community. We are excited to see what you build and secure with BlueRock!

The BlueRock Team