RoonCyber.AI

WHAT RUNTIME IS VS. WHAT RUNTIME ISN'T

RUNTIME SHOULD BE A TECHNOLOGY, NOT A BUZZWORD

Runtime security was built around a straightforward idea: security should keep pace with software while it is actually running. Modern technology has made it possible to deliver on that idea with always-active visibility into applications and workloads, providing the context needed to understand what is running, what it is doing, and what action should be taken when something goes wrong.

As runtime becomes a bigger part of the security conversation, however, the definition is starting to get stretched. Analyzing an event that occurred at runtime is not the same as having visibility into runtime itself. Sending activity to an LLM for analysis, periodically checking for changes, or inferring behavior from downstream events may provide useful security information, but those approaches should not be confused with continuously observing execution.

WHAT RUNTIME IS

✓ KERNEL-LEVEL VISIBILITY WITH EBPF

Modern runtime security can use technologies such as eBPF to continuously observe activity at the kernel level with minimal performance impact. This provides direct visibility into processes, API calls, syscalls, and application behavior as software executes.

✓ REAL-TIME INVENTORY OF PROCESSES, APIS, AGENTS & SERVICES

Because runtime visibility is always active, it can continuously discover what is actually running rather than relying solely on what has been configured, documented, or previously scanned. This becomes increasingly important as AI agents, services, APIs, and other components are created and changed at a faster pace.

✓ BLOCKING, CONTAINING & REMEDIATING THREATS

Deep runtime context gives security teams the evidence needed to move beyond detection. When malicious behavior occurs, teams can understand what happened and take action against the executing workload, including blocking processes, containing affected applications, and accelerating remediation.

WHAT RUNTIME ISN'T

✗ USING AN LLM TO "LISTEN" TO ACTIVITY

LLMs can provide valuable analysis, but using an LLM to interpret activity does not make the underlying security technology runtime. The distinction is whether the technology is directly and continuously observing execution or analyzing information collected through another mechanism.

✗ SENDING EVENTS TO AI FOR ANALYSIS

An event can occur at runtime without the technology analyzing it being a runtime security technology. AI can help interpret telemetry, correlate events, and identify suspicious patterns, but that analysis is different from directly observing what a workload is doing as it executes.

✗ INFERRING BEHAVIOR AFTER THE FACT

Runtime provides evidence of actual execution. Tools that reconstruct or infer behavior from downstream signals can still be valuable, but they do not provide the same level of continuous visibility and context into what actually occurred inside the running workload.

RoonCyber.AI

WHAT RUNTIME IS VS. WHAT RUNTIME ISN'T

WHY THE DISTINCTION MATTERS

Security spent years moving beyond point-in-time scanning toward continuous protection that could keep pace with modern software. As AI creates new ways to analyze security data, we shouldn't move backward by applying the runtime label to technologies that intermittently listen, scan, or analyze activity generated elsewhere.

> Analyzing an event that occurred at runtime is not the same as having visibility into runtime itself.

HOW ROONCYBER WORKS

Built around continuous runtime observability.

Using eBPF, RoonCyber monitors processes, API calls, syscalls, and other kernel-level activity in real time with minimal performance impact. That visibility provides the evidence needed not only to understand what happened, but to respond by blocking malicious processes or isolating impacted applications when threats are confirmed.

eBPF | processes | API calls | syscalls | real time

WHAT TO ASK ANY VENDOR

Understanding how the technology observes execution, whether that visibility is continuous, where the telemetry comes from, and what actions can be taken from it can help separate true runtime technology from another security capability carrying the runtime label.

01 **How does it observe execution?**

02 **Is that visibility continuous?**

03 **Where does the telemetry come from?**

04 **What actions can be taken from it?**

ASK HOW THEIR RUNTIME ACTUALLY WORKS

When evaluating a security product that claims runtime capabilities, the most important question may be the simplest: how does your runtime actually work?

contact@RoonCyber.com | RoonCyber.com/demo