Executive Brief

Runtime Security for Business Critical Applications

Today's businesses are rapidly developing and scaling cloud-native architectures, built on APIs, micro-services, and containers. As innovation accelerates, these businesses have challenges with accurate service inventory, vulnerabilities, and threats that multiply at the application layer. Legacy tools like CNAPPs, XDRs, and scanners are not designed for modern, application first infrastructure. Consequentially, organizations are more vulnerable to application layer threats, as modern attackers increasingly target applications directly and bypass infrastructure-layer defenses.

Observability Gaps: Costs & Business Risk

- 87% of organizations cite a lack of runtime application visibility as a top challenge in securing cloud workloads.
    - *ESG Research, 2024*
- 80% of data breaches now involve data stored in the cloud while traditional tools miss over 45% of application layer threats.
    - *Gartner 2024 Cloud-Native Security Hype Cycle*
- The average cloud breach costs $4.75M, with response time >200 days due to lack of visibility across APIs, services, and ephemeral workloads.
    - *IBM, 2023; Ponemon Institute*
- 70% of security teams report alert fatigue from infrastructure tools while still missing critical application-layer attacks that exploit logic flaws and insecure service-to-service interactions.
    - *SANS Institute Cloud Security Survey, 2024*

Run Security delivers CADR by design.

Built for modern environments and your most critical assets, Run Security empowers Security and DevOps teams with always-on application-layer protection that complements CNAPPs and closes the visibility gap that attackers increasingly exploit.

Key Solutions and Capabilities

Continuous Runtime Visibility

Gain full observability into every service, API, and component running across containerized, hybrid, and multi-cloud environments. Discover shadow, zombie, and undocumented APIs in real time—without manual tagging or custom instrumentation.

Real-Time Risk Validation

Instantly detect exploitable vulnerabilities and suppress false positives by observing how applications behave in production. Stop chasing “hypothetical” issues and prioritize what's truly exploitable and under threat.

Active Threat Detection & Response

Monitor kernel-level runtime activity to detect and block exploitation attempts before they escalate. Correlate behavior with threat intelligence and trigger virtual patches, alerts, or auto-ticketing into developer workflows.

Built for DevSecOps

Run Security natively integrates into CI/CD pipelines and developer tools. Remediation becomes part of your agile process with runtime insight feeding directly into triage and fix workflows. Complimenting CNAPP with CADR.

Cloud-Native Application Protection Platforms (CNAPPs) are designed to secure infrastructure and configurations but most miss what happens inside the application once it's running.

This is where CADR and Run Security fill the gap:

CNAPP = Prevent misconfigurations, enforce policy, scan containers

CADR = Detect and respond to live application threats and exploit attempts

Together = Full stack defense, from cloud posture to runtime behavior

Run Security seamlessly integrates with CNAPP strategies to give organizations end-to-end visibility and protection extending runtime defense into the application layer.

How Run Security Delivers Value

Capability	Business Outcome
Always-On Runtime Security	Continuous coverage eliminates scan gaps, reducing breach risk during deployments or updates
False Positive Elimination	Teams save time and reduce friction by acting only on exploitable, context-rich alerts
Faster Incident Response	Reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) with kernel visibility
Attack Path Clarity	Understand the full blast radius of exploits, trace data flows, and validate what's reachable and at risk
Full Traceability	Granular visibility into runtime events and service behavior enables audit-ready investigation and faster forensic response
Streamlined Compliance	Runtime visibility supports audit prep, configuration validation, and operational assurance
Low Total Cost of Ownership	Lightweight instrumentation delivers protection with minimal overhead and maintenance needs

Rethink Runtime Security

Proof Points from the Field

- Up to 90% reduction in time spent chasing false positives
- Instant detection of zero-day exploitation attempts
- <1% technical overhead with no kernel changes or code rewrites
- Deploy in days with full support for Kubernetes, VMs, and bare metal environments
- Reduce operational burden with real-time asset inventory and no manual tracking
- Low TCO: Full deployment in days, <1% technical overhead, and <0.1 FTE ongoing maintenance, and rapid time-to-value

Run Security provides a new layer of defense—purpose-built for the dynamic, fast-moving nature of cloud-native applications. By embedding deep observability directly into the runtime layer, organizations can:

- Maintain a live inventory of all Cloud Services, Applications, and APIs,
- Protect applications continuously
- Eliminate alert fatigue
- Empower developers with trustworthy, actionable insights
- Lower costs and complexity with a minimal-footprint, low-TCO solution

CADR is the missing piece of your cloud security stack—and Run Security brings it to life. Whether you're defending customer-facing platforms or internal micro-services, Run Security helps your team move faster, with confidence.

RUN SECURITY

visit runsecurity.com | info@runsecurity.com