RUN SECURITY

RUNTIME APPLICATION SECURITY

# RS PREVENT: ALWAYS ACTIVE & POWERED BY EBPF

**Always-active runtime security across your application ecosystem—delivering continuous visibility into all runtime traffic, services, and vulnerabilities.**

## TRADITIONAL APPSEC SOLUTIONS HAVE REACHED THEIR LIMITS

Run Security was founded to drive the next evolution of Application Security, solving problems where traditional scanning and monitoring solutions fall short. Today's AppSec tools weren't built for modern, fast-moving software teams—and it shows. As applications rapidly evolve, legacy tools like scanners leave apps unattended for most of their lifecycle, generating high false positives, and lack the context needed for effective prioritization. Monitoring solutions compound this by providing an outside-only view, with limited observability into internal processes and the extensibility needed to cover APIs. Besides the downstream impacts to DevOps and Security workflows, sunk licensing costs, and growing tech debt, tooling limitations also introduce increased business risk. This risk stems from an incomplete view of service inventory, consistent vulnerability exposure, and limited visibility into application traffic patterns and behaviors. Run Security delivers what first-gen AppSec tools cannot – always-active runtime security that never leaves an application unobserved, service unmanaged, or vulnerability undetected.

## RUNTIME SERVICE DISCOVERY & INVENTORY

Asset management is a moving target with Engineering, Security, and Compliance teams, all striving to meet critical deadlines and increasing regulatory requirements. Given the scope and velocity most businesses operate, maintaining an accurate catalog of all endpoints, methods, parameters, and authentications is a lofty expectation. RS Prevent continuously discovers and inventories every API and service running across their containerized, multi-cloud environments – at runtime. At any time, view a comprehensive rollup of your Services by APIs, owners, vulnerabilities, and more. Whether satisfying auditor requirements, reducing shadow IT costs, triaging a production issue, or gaining insights into your attack surface, Run Security delivers accurate, always-active visibility to the business while alleviating operational overhead and guess work.

## RUNTIME ANOMALY DETECTION & RESPONSE

Stopping exploitation attempts is a mission-critical part of any organization's application security strategy. As modern applications scale and evolve, attackers move quickly to exploit points of exposure. To stay ahead, security teams need runtime context to cut through the noise and confidently respond to anomalous behavior. RS Prevent provides a clear view into exploitation attempts targeting services and APIs in production. By correlating runtime activity with threat intelligence, security teams can quickly triage incidents and prioritize response efforts. With comprehensive runtime event logs capturing deep context, RS Prevent enables thorough forensic analysis – giving teams the critical visibility and evidence they need to rapidly investigate, respond, and mitigate threats.

RUN SECURITY

REQUEST A DEMO BY VISITING RUNSECURITY.COM

# TAKE THE NEXT STEP TODAY!

**Run Security is redefining what runtime application security should be: always-active, deeply observable, and designed to empower both DevOps and Security without slowing innovation. See for yourself and request a demo today.**

## RUNTIME EXPOSURE MANAGEMENT

Traditional tools like scanners run periodically, yielding high false positives, undetected flaws, and static reports. The impact: more vulnerabilities are being pushed into production every day – leaving user's data and organizations at risk.

RS Prevent accurately detects and validates vulnerabilities the moment they emerge – not after a scan or deployment cycle. No more guesswork, false positives, and wasted efforts — just continuous security that keeps pace with your applications. Stay ahead of vulnerabilities across dev, preprod, and production environments for precise, risk-based prioritization. Integrated remediation workflows reduce manual effort, streamlines response, and empowers DevOps and Security teams to fix what matters—faster and more effectively.

## RS PREVENT ARCHITECTURE