

RS Prevent — Runtime CNAPP

Cloud Application Detection & Response

Attackers don't wait to exploit vulnerable applications—stop giving them the runtime advantage. CADR captures what's happening now, not what already happened.

Stopping exploitation attempts is a mission-critical part of any organization's 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 stop runtime attacks, fast. RS Prevent provides a clear view into exploitation attempts targeting services and APIs in production. With comprehensive runtime, cloud, and Kubernetes logs capturing deep context, RS Prevent gives AppSec teams the critical visibility and evidence they need to rapidly investigate, respond, and mitigate threats.

CADR is the runtime defense layer of CNAPPs. It's purpose-built to detect and respond to active attacks as they happen. It's an essential layer for securing modern cloud applications—because if you actually want to stop attackers at runtime, you need to see them and stop them immediately.

RUNTIME MONITORING & DETECTION STACK

**See what's running. Know what's targeted.
Stop what matters - with Run Security**

RS Prevent detects all runtime threats and vulnerabilities putting your business-critical applications at risk.

By leveraging Extended Berkeley Packet Filter (eBPF) to monitor all processes, API calls, and syscalls—along with cloud signals like CloudTrail and Kubernetes logs—RS Prevent delivers comprehensive, real-time detection across your runtime environment.

Why eBPF?

- Low-latency, high fidelity monitoring across any cloud or containerized environments
- Continuous visibility into kernel-level activity that other tools don't capture
- Minimal performance impact compared to traditional agents or kernel modules



Cloud-to-Application Detection

See the Full Attack — Unify Cloud and Application Events for Full-Stack Visibility

Modern attacks don't stop at the cloud—they move laterally, escalate privileges, and exploit vulnerable applications. RS Prevent delivers Cloud-to-Application detection by correlating logs across cloud infrastructure, Kubernetes, and kernel-level runtime behavior to expose the full scope of an attack.

RS Prevent maps the full progression of an attack so security teams can detect and respond before damage is done. It correlates telemetry from multiple layers: cloud activity logs like CloudTrail, Kubernetes orchestration data, and deep runtime insights from eBPF monitoring.

As seen in the incident example, RS Prevent flags suspicious activity like privilege escalation, policy changes, and unauthorized session access across services like Lambda, S3, EC2, and VPC. Simultaneously, it detects high-risk behaviors inside the application—such as memory access anomalies and data exfiltration attempts—with context-aware severity scoring.

By connecting cloud-context to what's happening at runtime within production apps, RS Prevent gives AppSec teams end-to-end visibility and high-fidelity detection that spans from infrastructure to code—without the noise.

INC-2024-0116-002



Critical Memory-Based Credential Theft Attack

eBPF runtime monitoring detected sophisticated memory-based ...

Critical

Active

20 events

Security Team
us-east-1

Event ID	Severity ID	STATUS	SERVICE & RESOURCE	Risk Score
Lambda Function Environment Variable Exposure DataExfiltration	High	Investigating	eBPF Security Monitor prod-payment-api Lambda	88
Suspicious Lambda Function Memory Access Pattern RuntimeAnomaly	Critical	Investigating	eBPF Runtime Monitor prod-payment-api Lambda	95
Lambda Function Privilege Escalation Attempt UnauthorizedAPICall	High	Investigating	CloudTrail prod-payment-api Lambda	78
Security Group Rule Modification SecurityGroupRuleViolation	Medium	New	Config prod-api-security-group VPC	76
External Access Policy Modification ResourcePolicyViolation	High	New	Config prod-sensitive-data-bucket S3	89
Remote Command Execution via SSM MaliciousCommandExecution	Critical	New	CloudTrail prod-api-server EC2	94
Unauthorized SSM Session Establishment UnauthorizedSessionAccess	High	New	CloudTrail prod-api-server EC2	86
Suspicious Data Exfiltration Traffic DataExfiltrationSuspicious	Critical	New	VPC Flow Logs prod-vpc-main VPC	92

Runtime Response & Remediation Workflows

Stop What Matters — With Actionable Insights from All Layers

When a threat is detected, the speed and accuracy of your investigation determine how quickly you can contain it. RS Prevent gives security teams instant access to runtime context—capturing what was running, who triggered it, and what it impacted—so they can move from detection to root cause in seconds, not hours.

With RS Prevent, teams can:

- Correlate cloud activity with runtime behavior
- Trace an attack path across Lambda, EC2, S3, and VPC without switching tools
- See the exact function, process, or API that was exploited
- Identify if a vulnerability was actively targeted or just passively present

By combining deep runtime observability with cloud-native telemetry, RS Prevent enables teams to reconstruct incidents with confidence—reducing investigation time and eliminating alert fatigue.

Once a threat is confirmed, RS Prevent enables fast, precise remediation with zero guesswork. Security teams can immediately take action—killing malicious processes in real time to halt active exploitation, or quarantining affected applications to contain the threat and prevent lateral movement. Integration with tools like Jira allows teams to notify developers with clear, contextual details about what function was vulnerable and how it was targeted. Meanwhile, real-time alerts in Slack keep cross-functional teams aligned and ready to respond. With RS Prevent, every remediation step is informed by runtime evidence—reducing risk, minimizing impact, and ensuring threats are stopped before they escalate.



**Unify DevSecOps.
Operate in Lockstep.**



**Align Teams with
Cloud-to-App Content**



**Contain Threats.
Stop Real Risks.**



- Integrating with Jira allows both; SecOps and AppSec teams to push details about potentially affected or vulnerable functions being called at runtime, helping accelerate triage, and streamline collaboration.



- Ensure teams are instantly notified when new runtime threats are detected or vulnerabilities are identified, in Slack.
- Delivering high-fidelity alerts to existing communication workspaces, teams can be notified faster and stay aligned with runtime context. Reduce MTTD and MTTR—without switching tools.



- Stop active exploits in their tracks by killing malicious processes, preventing further damage and containing a threat in real time.
- Prevent lateral movement and isolate an impacted application, reducing the blast radius of an attack