RoonCyber

RC PREVENT — RUNTIME APPLICATION SECURITY

RUNTIME DISCOVERY & SERVICE INVENTORY

What you can't see can hurt you. Uncover the APIs and services you didn't know were exposing your applications — and your business — to risk.

RUNTIME OBSERVABILITY & MONITORING

When it comes to application security, you can't secure what you can't see. Asset inventories and API schemas quickly became outdated and scanning-based solutions operate intermittently, creating dangerous blind spots. RC Prevent solves these challenges by offering an always-active, runtime observability and monitoring of all network, kernel, and syscall activity — with zero performance impacts.

With always-active, runtime observability your team can:

- Maintain continuous visibility into active services and APIs
- Gain clarity into how applications operate at runtime
- Catch issues before they impact users or production systems
- Maintain an up-to-date inventory with runtime context

Runtime observability helps security and engineering teams stay aligned, eliminate blind spots, response faster to threats and vulnerabilities, and maintain accurate inventories – even as environments shift and scale. RoonCyber delivers what first-gen AppSec tools cannot – always-active runtime security that never leaves an application unobserved, service unmanaged, or risks undetected.

SEE WHAT'S RUNNING BEFORE IT BECOMES A RISK

- Know what's live, where it's running, and whether it's exposing your business to risk. RC Prevent continuously identifies every API, service, and endpoint at runtime across cloud, containerized, and hybrid environments.

  At any time, teams can view a comprehensive rollup of Services by APIs, owners, vulnerabilities, methods, and more. With RC Prevent, teams can manage their attack surface, eliminate blind spots, and uncover hidden risks before they can impact users or production systems.

ALIGN SECURITY & DEV WITH RUNTIME CONTEXT

- Security and development teams often work with fragmented views of their company's application landscape — especially as environments shift and scale.

  Built for DevSecOps, RC Prevent helps teams maintain accurate and up-to-date inventories of their application services and APIs leveraging deep runtime context gathered by our eBPF-powered prevent sensor.

  It's not just about visibility — RC Prevent also detects vulnerabilities and threats, helping teams stay aligned on top risks and what matters most in their organization's application security posture.

SIMPLIFIED COMPLIANCE WITH MINIMAL EFFORT

- Keeping pace with compliance demands takes more than quarterly scans or static reports. RC Prevent simplifies compliance by providing a continuously updated, real-time inventory of all APIs, services, and endpoints — no scans, no spreadsheets, no effort required.

  RoonCyber's runtime-driven service catalog helps organizations meet requirements under PCI DSS, HIPAA, GDPR, and more. RC Prevent reduces manual effort, speeds up audit preparation, and minimizes the risk of non-compliance.

RooCyber

RUNTIME DISCOVERY & SERVICE INVENTORY

Asset management is a moving target — especially as Engineering, Security, and Compliance teams race to meet tight deadlines and increasing regulatory demands. At the speed most organizations operate, maintaining an accurate, up-to-date catalog of APIs, services, and system components is nearly impossible with traditional tools.

RC Prevent addresses this with continuous runtime discovery and inventorying of every API and service running across containerized, multi-cloud environments. Discovery is only the beginning, RC Prevent brings clarity through runtime data, showing not just what exists, but how each API and service behaves in production — including ownership, dependencies, communication patterns, and potential exposure points. This context helps teams trace data flows, validate configurations, and understand how services impact security posture and business risk.

At any time, teams can access a comprehensive view of services organized by APIs, owners, vulnerabilities, authentication methods, and more — helping them eliminate blind spots, reduce shadow IT, and respond to issues faster.

CAPTURE WHAT'S REALLY RUNNING WITH RUNTIME SCHEMA GENERATION

CLARITY IN PRODUCTION. CONFIDENCE IN COMPLIANCE. PRECISION IN TESTING.

Extended Berkeley Packet Filter (eBPF) is the foundation of RC Prevent's always-active, runtime application security. eBPF is a powerful kernel-level technology that allows programs to run safely and efficiently inside the Linux kernel — without requiring intrusive agents, kernel modules, or source code changes. This technology enables RC Prevent to capture real-time telemetry on API calls, service communications, system behavior, and data flows as your applications run.

Leveraging eBPF vs. Agents or Kernel Modules allows for:

- Low-latency, high-fidelity monitoring across any cloud or containerized environment
- Continuous visibility into application traffic and internal API calls that other tools miss
- Minimal performance impact compared to traditional application security agents or kernel modules

Powered by eBPF, RC Prevent delivers a foundationally better approach to observe and discover how your modern applications operate across environment and through dev stages into production. Whether you're tracking API behavior across dev, staging, and production or preparing for a compliance audit, RC Prevent empowers Security and Dev to work better together.

RoonCyber

WHAT CAN I SEE WITH RC PREVENT:

RUNTIME THREATS Detect and respond to live threats as they emerge — including exploitation attempts and anomalous behavior. RC Prevent monitors runtime activity at the kernel level to stop threats before they escalate.

VULNERABILITIES Identify exposed APIs and services in real time, enriched with live runtime context. RC Prevent automatically validates vulnerabilities to confirm exploitability and risk severity — giving security and development teams the shared context they need to prioritize critical issues and resolve them before they impact users.

APIS & SERVICES Discover all services and APIs running in your environment — including undocumented, shadow, or zombie APIs missed by traditional scanning tools. RC Prevent reveals ownership, behavior, and potential exposure points.

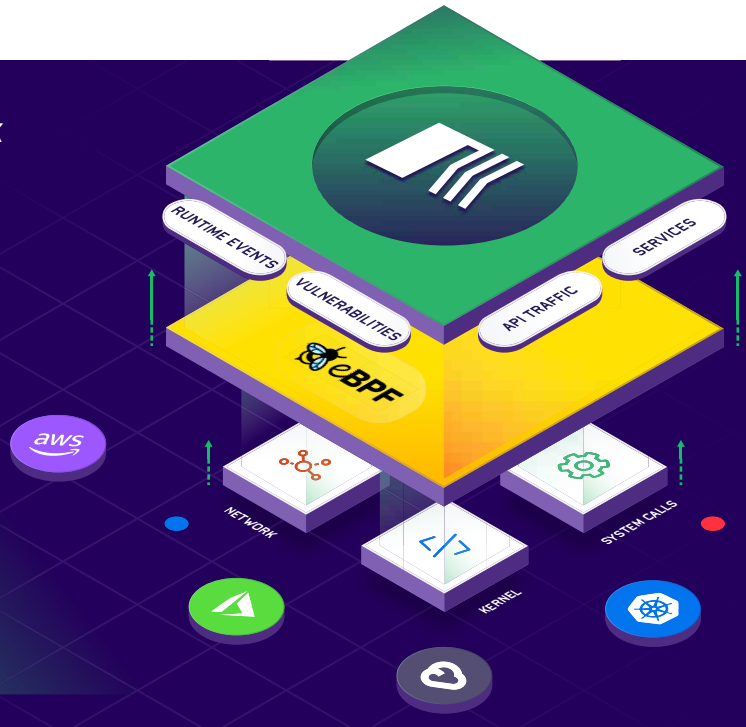
SENSITIVE DATA Track how services and APIs interact with sensitive or regulated data — such as PII, PHI, or cardholder info — in real time. RC Prevent provides visibility into data flows and access points to help meet compliance mandates like GDPR, HIPAA, and PCI DSS.

VULNERABILITIES Automatically generate and update accurate API and service schemas from real runtime activity — creating a live, source-of-truth inventory required for compliance frameworks like PCI DSS, HIPAA, and GDPR. RC Prevent eliminates the need for manual documentation by capturing actual behavior in production, streamlining audit preparation, strengthening data flow visibility, and improving test coverage.

Always-active Discovery. Runtime clarity. Effortless compliance — RC Prevent leverages always-active, runtime observability to maintain visibility, provide clarity on how application operate, identify issues before impacting users, and maintain an always-up- to-date inventory so teams can stay aligned and easily meet compliance and audit requirements.

RUNTIME OBSERVABILITY & DISCOVERY STACK

RoonCyber 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.



TAKE THE NEXT STEP.

REQUEST A DEMO!