ΛRMO

Creators of Kubescape

The First Behavioral Cloud Application Detection and Response Platform

ARMO Platform is the only platform that continuously minimizes cloud attack surface based on runtime insights, while actively detecting and responding to cyberattacks with real cloud risk context.

ARMO is the **creator and main maintainer of Kubescape**, the world's fastest growing & most adopted open-source Kubernetes security project (an official CNCF Project).

{Kubernetes-first} Cloud Posture

Powered by Kubescape

- CSPM (Agentless scanning)
- KSPM
- Runtime-based Vulnerability management (in-use/reachability)
- IaC security
- Identity security (CIEM) & RBAC

Behavioral Threat Detection & Response

Powered by eBPF

- Cloud Application Detection & Response (CDR, ADR)
- CWPP
- API security
- Container security

ΛPD™ Application Profile DNA Composition

{ Cloud & Kubernetes }

Cloud events logs
CRDs
IAMs
Cloud APIs
VMs and Nodes
KubeAPI & Control Plane
IAMs & RBAC

{ Containers & Workloads }

Container images Registries
System calls
Networking
SBOM
Files access
Code and configuration
Manifest files & IaC
Process execution

{ Applications }

Code
Stack traces
Functions
APIs
Call stack
L4 & L7

Multi-Cloud, On-Premises and Air-Gapped

> “ARMO has been a game-changer for us, empowering us to navigate the complex landscape of cloud-native security with ease and confidence”

Zois Pagoulatos
Principal DevOps Engineer @ KYOS

“ARMO Ensures Secure Infrastructure”

Erlend Hoel
Senior Systems Engineer @ Business

ARMO Behavioral Cloud Application Detection & Response

ARMO's Behavioral Cloud Runtime security platform addresses the complexities of novel cloud attacks. Our unique multi-layered solution combines data from:

Applications

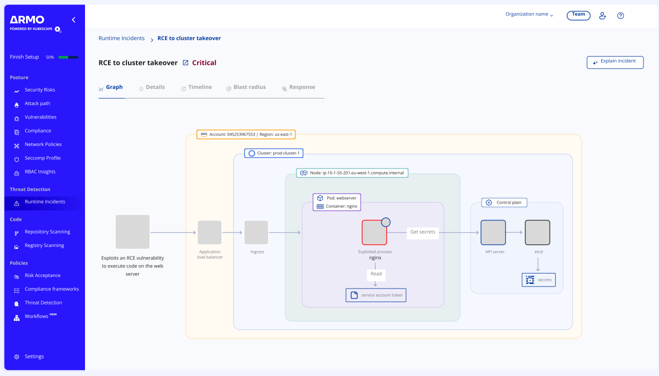
By monitoring code and function level activities, network traffic, layer 7 data, and API calls, our eBPF sensor provides unprecedented insight into the behavior of your applications, code libraries, functions, call stacks and stack traces.

Cloud & Kubernetes

Extract data from Cloud logs and APIs, Kubernetes APIs and control plane, IAMs and RBAC, manifest files etc, through our widely used open source project, Kubescape, eBPF runtime sensor and cloud agentless scanning.

Containers & Workloads

The eBPF sensor continuously monitors container and workload behavior, providing insights into the running processes and events.



Runtime Incidents > RCE to cluster takeover

RCE to cluster takeover Critical

Exploits an RCE vulnerability to execute code on the web server

By cross-correlating and analyzing these data streams across the entire cloud stack, we detect and trace sophisticated threats, including zero-day attacks, malware, and emerging security risks. We generate a fully explainable and traceable attack trail that provides deep visibility into potential security incidents. Furthermore, we proactively identify high-risk misconfigurations and pinpoint reachable and exploitable vulnerabilities across the cloud environment.

ARMO CADR offers key benefits for cloud security professionals

01 **Provide holistic, explainable & traceable runtime security stories:** Detecting complex, multi-stage attacks across your entire cloud-native stack. Providing clear, traceable, explainable attack trails with relevant stack traces.

02 **Detect zero-days attacks:** Based on constant learning of normal application runtime behavior, ARMO CADR detects anomalies and malicious activities that have never been seen before without prior exposure or reliance on after-the-fact rules.

03 **Minimize potential attack blast radius:** with rapid identification and response to threats through consolidation of multi-dimensional security events into a single, actionable incident. Enables mitigation of active threats, with a host of automatic and manual responses - Kill, Stop, Pause and Soft Quarantine while teams work to solve the root cause of the incident.

04 **Eliminate CVE-Shock:** by prioritizing relevant and high-risk vulnerabilities across the cloud-native application and infrastructure lifecycle using reachability and exploitability runtime analysis.

05 **Gain performant and efficient visibility:** with real-time kernel-level visibility that consumes less than 2% CPU and memory, while enjoying simple helm-based installation for quick and efficient implementation.

204%	ROI in first year
81%	MTTD reduction
87%	MTTR reduction
90%	Reduction in total incident analysis time and cost
46%	Increase in compliance score in less than 2 weeks
>90%	Less vulnerabilities to investigate

* Data from ARMO existing customers

Let’s talk

Learn more

See ARMO in action