OFFLOAD SECURITY

How Offload Compares: A Capability Guide Across Leading Security Tools

July 2026 · For prospective-customer evaluation

How to read this document

Every vendor here is excellent at its core domain — this is not a claim that Offload beats specialists at their specialty. It is an honest map of what one unified platform covers versus a stack of point solutions, including the areas where a specialist remains the deeper choice (Section 5). Competitor information is based on publicly available documentation as of July 2026 and should be re-verified during your evaluation; the Offload column reflects shipped product capabilities, not roadmap.

1. The Comparison Frame

Offload is a unified security and compliance platform: cloud security posture (AWS, GCP, Azure), application security (SAST, SCA, secrets, IaC, SBOM), container and Kubernetes security, unified vulnerability management, and compliance/risk automation in a single product with a single data model. The vendors below each lead a category that Offload spans:

Vendor	Primary category	Typical role in a security stack
Wiz	CNAPP (cloud-native application protection)	Cloud posture, workload scanning, attack paths
Prisma Cloud / Cortex Cloud (Palo Alto)	CNAPP + runtime protection	Cloud posture and workload defense
Snyk	Developer security (AppSec)	Code, dependency, and container scanning in the developer loop
Tenable	Vulnerability & exposure management	Infrastructure VM, cloud security, exposure analytics
Vanta	Compliance automation	SOC 2 / ISO evidence collection and audit readiness
Lacework (FortiCNAPP, Fortinet)	CNAPP with behavioral analytics	Cloud posture plus anomaly-based runtime threat detection
Orca Security	Agentless CNAPP	Agentless cloud posture, workload scanning, and attack paths

The honest one-liner: specialists go deeper in their lane; Offload connects the lanes. If your priority is a single domain at maximum depth, a specialist may serve you better. If your priority is one consistent

view of risk across code, cloud, containers, Kubernetes, and compliance — without stitching four subscriptions together — that is what Offload is built for.

2. Capability Matrix

● Native capability ◐ Partial / lighter-weight ○ Not offered / not a focus

Capability	Offload	Wiz	Prisma / Cortex	Snyk	Tenable	Vanta	Lacework	Orca
Cloud misconfiguration & compliance posture (CSPM)	●	●	●	○	●	○	●	●
Cloud workload vulnerability scanning (agentless snapshots)	◐	●	●	○	●	○	●	●
Identity & entitlement management (CIEM)	○	●	●	○	●	○	◐	●
Attack path analysis	◐	●	◐	○	◐	○	◐	●
Static application security testing (SAST)	◐	◐	◐	●	○	○	○	○
Dependency scanning (SCA) with exploit intelligence	●	◐	◐	●	○	○	◐	◐
Malicious-package & typosquat detection	●	◐	○	●	○	○	○	○
Secrets detection	●	◐	◐	○	○	○	◐	◐
Infrastructure-as-code scanning	●	●	●	●	◐	○	◐	◐
Container image & registry scanning	●	●	●	◐	◐	○	●	●
Kubernetes posture & benchmarks	●	●	●	◐	◐	○	●	●
Runtime workload protection (sensors / eBPF)	○	●	●	○	◐	○	●	◐
Web & API dynamic testing (DAST)	◐	○	○	◐	◐	○	○	○
Unified vulnerability management (all sources, SLA, lifecycle)	●	◐	◐	◐	●	○	◐	◐
Automated fix pull requests	◐	○	○	●	○	○	○	○
Compliance automation, evidence & risk register	●	◐	◐	○	◐	●	◐	◐

Capability	Offload	Wiz	Prisma / Cortex	Snyk	Tenable	Vanta	Lacework	Orca
India regulatory frameworks (DPDP, RBI, SEBI CSCRF)	●	○	○	○	○	◐	○	○
Security questionnaire / vendor-assessment automation	●	○	○	○	○	●	○	○
Self-hosted / on-premises deployment	●	○	◐	○	●	○	○	○
AI-assisted analysis & remediation guidance	●	●	◐	●	◐	◐	◐	●

Ratings reflect breadth-level capability presence, not fine-grained depth; Section 3 adds the depth nuance per domain, including where a competitor's partial or full rating understates or overstates practical fit.

3. Domain Notes — Including Where They Beat Us

Cloud security

Offload provides multi-account CSPM across AWS, GCP, and Azure — misconfigurations, public exposure, compliance benchmarks, and scheduled scanning — with findings feeding the same vulnerability and risk workflow as every other domain. The CNAPP specialists go deeper on the cloud runtime side: Wiz, Prisma, and Orca offer agentless snapshot scanning of running VM workloads (a technique Orca pioneered), mature CIEM, and identity-aware attack paths, while Lacework's distinctive strength is behavioral anomaly detection on workloads via its Polygraph analytics. Offload's attack-path analysis is configuration-derived and does not yet model identity relationships; if CIEM or identity-aware attack paths are a primary requirement, a CNAPP specialist is currently the stronger choice.

Application security

Offload's AppSec pillar covers SAST, SCA with CISA KEV and EPSS exploit enrichment, malicious-package and typosquat detection, secrets scanning, IaC scanning, SBOM generation with license compliance, governed finding triage, release gates enforceable as required GitHub status checks, and basic automated fix pull requests. Snyk remains deeper in the developer loop: a proprietary vulnerability database, dataflow-based SAST with AI autofix, function-level reachability analysis (Offload's reachability is import-level and advisory), and IDE plugins. Offload counters with capabilities Snyk lacks: secrets detection, attribution/NOTICE file generation for license compliance, audit-evidence-stamped gate decisions, and findings that land in the same risk register as cloud and Kubernetes issues.

Containers and Kubernetes

Offload scans registries and images (with scheduled re-validation), generates SBOMs, and runs continuous Kubernetes cluster assessments — configuration, RBAC, workloads, and CIS-style benchmarks. Wiz, Prisma, and Lacework add runtime sensors for in-workload detection and response

(Lacework's behavioral analytics being its historic core strength), and Orca offers a lightweight sensor alongside its agentless model; Offload has no runtime agent today. Buyers needing container detection-and-response should pair Offload with a runtime tool or choose a CNAPP with sensors.

Vulnerability and exposure management

This is Offload's center of gravity: findings from cloud, code, containers, Kubernetes, and integrated tools are normalized, de-duplicated, correlated, and managed through one lifecycle with ownership, SLA tracking, aging, and history. Tenable is the long-standing leader for infrastructure VM (network scanning, agent coverage, prioritization analytics) and is the better choice for deep traditional-infrastructure estates; Offload is the better choice when the estate is cloud/code/container-centric and the pain is aggregation across tools.

Compliance and risk

Offload treats compliance as connected to the technical layer: framework assessments (ISO 27001, SOC 2, SCF and others), technical findings mapped to controls, evidence collection, an enterprise risk register, business-impact analysis, and automated security-questionnaire answering. It is also one of the few platforms with first-class India regulatory coverage — the DPDP Act, RBI guidelines, and SEBI CSCRF. Vanta is stronger on breadth of business-control integrations (HR systems, MDM, identity providers) for pure audit-readiness automation; Offload is stronger where compliance must reflect actual technical security posture rather than run alongside it.

4. Deployment and Commercial Model

Dimension	Offload	Typical specialist stack
Deployment	SaaS or fully self-hosted / on-premises — all security data can remain in your environment	Predominantly SaaS-only (Wiz, Snyk, Vanta, Lacework, Orca); limited self-hosted options elsewhere
Data residency	Customer-controlled in on-prem model; single data store	Security findings distributed across multiple vendor clouds
Licensing	Platform license — not per-developer seats or percentage of cloud spend	Per-developer (Snyk), workload/spend-based (CNAPPs), per-asset (VM), per-framework (compliance)
Operational surface	One console, one data model, one workflow	4–5 consoles, manual cross-tool consolidation, or a separate aggregation layer

5. When a Specialist Is the Better Choice

We would rather tell you this now than have you discover it in a proof of concept:

- **Runtime workload protection:** Offload has no eBPF/agent sensor. For in-workload threat detection and response — especially behavioral anomaly detection, where Lacework's Polygraph is distinctive

— choose Wiz, Prisma/Cortex, Lacework, or a runtime specialist; Offload complements them at the posture and workflow layer.

- **Cloud identity entitlements (CIEM):** if least-privilege analysis across thousands of cloud identities is your primary problem, Wiz, Prisma, Orca, or Tenable are ahead of us today.
- **Agentless cloud coverage at maximum depth:** Orca and Wiz scan running VM workloads via snapshot analysis with no deployment effort; Offload's workload visibility comes through registries, images, and clusters rather than VM snapshots.
- **Maximum-depth SAST and reachability in the IDE:** Snyk's proprietary engine, function-level reachability, and IDE presence remain deeper than Offload's scanner-based SAST with import-level reachability.
- **Traditional network/host VM at scale:** Tenable's scanner and agent coverage of on-prem infrastructure estates is more mature.
- **Pure business-controls audit automation:** if you only need SOC 2 evidence collection from HR/MDM/IdP systems and no technical security platform, Vanta or Drata is the lighter path.

6. When Offload Is the Right Choice

- You want **one platform and one risk view** across cloud, code, containers, Kubernetes, vulnerability management, and compliance — instead of stitching together 4–5 tools.
- **Data sovereignty matters:** you need security findings, source-code excerpts, and evidence to stay in your own environment (on-premises deployment).
- **Compliance must reflect reality:** technical findings linked to controls, risk register, evidence, and auditor-ready reports in the same system that scans.
- **You operate under Indian regulations:** DPDP, RBI, and SEBI CSCRF coverage is native, not an afterthought.
- **Budget consolidation:** a single platform license replaces several per-seat, per-asset, and per-spend subscriptions and the engineering time spent integrating them.