# From Posture to Process: A Comparative Architectural Analysis of Wiz and CrowdStrike Container Security

## Executive Summary

The market for container security is defined by a fundamental choice between two distinct architectural philosophies: the "context-first" Cloud-Native Application Protection Platform (CNAPP) and the "detection-first" Endpoint Detection and Response (EDR) model. This report provides an exhaustive comparative analysis of Wiz and CrowdStrike, two market leaders who exemplify this divergence.

Wiz represents the context-first CNAPP approach. Its foundation is a broad, "agentless-first" capability 1 that connects to cloud APIs to map the entire cloud estate. This data populates a central "Wiz Security Graph" 2, which provides comprehensive Attack Path Analysis (APA) to prioritize risks.2 The optional Wiz Runtime Agent (Wiz Sensor) 3 is not a standalone EDR tool; it is a strategic data source that feeds this central graph. This integration enables uniquely powerful, context-aware threat detection and, most notably, "vulnerability validation" to identify which vulnerable packages are actually "loaded into memory".4 The primary value proposition of the Wiz model is *holistic risk prioritization*.5

CrowdStrike represents the detection-first EDR model. Its foundation is a market-leading, "best-in-class" agent 6 that provides deep, "behavior-based" threat detection. This capability is powered by advanced Artificial Intelligence (AI), Machine Learning (ML), and a massive global "CrowdStrike Threat Graph®" that correlates trillions of events per week.7 Its container security solution is a direct extension of this powerful EDR, offering unparalleled depth in runtime telemetry and forensic investigation.8 The primary value proposition of the CrowdStrike model is *specialized threat interdiction*.

This analysis reveals a critical distinction in how each platform is "far-reaching." Wiz's "far-reaching" nature is its *breadth of context*, enabling it to connect a single runtime event to posture, identity, and data risks across the entire cloud stack.9 CrowdStrike's "far-reaching" nature is its *depth of telemetry*, allowing it to identify a sophisticated, novel attack based on subtle behaviors deep within a single workload.7

The choice between them is one of strategic priority. Organizations seeking a unified platform to manage alert fatigue and prioritize vulnerabilities based on business-centric attack paths will find Wiz's model highly strategic. Organizations with a mature Security Operations Center (SOC) that prioritizes best-of-breed, real-time threat blocking and requires deep forensic data will favor CrowdStrike's specialized agent. For many, a "posture-first, runtime-second" strategy 9—which aligns with the Wiz platform's layered design—is the most effective path forward.

## Part 1: The Wiz Security Model: From Agentless Posture to Runtime Protection

The Wiz platform is architected in two distinct, yet deeply integrated, layers. The first is its foundational agentless platform, which provides broad, high-speed visibility. The second is an optional runtime agent, which provides deep, real-time protection. Understanding this dual-layered architecture is essential to grasping its strategic value.

### Chapter 1.1: Foundational Agentless Visibility: The "What" and "Where"

This foundational capability is the core of the Wiz platform and what it is most known for. It is an agentless, API-driven model designed to provide a comprehensive security posture assessment without installing any software on workloads.11

#### Core Mechanism: Agentless, API-Driven Scanning

The Wiz platform connects to multi-cloud environments—including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—in minutes via read-only API connectors.3 This "agentless-first" approach 1 is designed to achieve 100% coverage of all cloud assets, including virtual machines, containers, serverless functions, and Platform-as-a-Service (PaaS) resources.13

The scanning mechanism itself is "out of band," meaning it takes snapshots of resources and scans them on the Wiz backend.11 This model has zero performance impact on the production environment, as it does not consume the customer's compute resources for scanning.11 This elimination of friction is a core value proposition. Traditional agent-based models require deployment, maintenance, updates, and troubleshooting, which can create friction with DevOps and infrastructure teams. The agentless model bypasses this, enabling security teams to achieve full visibility in as little as 30 minutes, a process that could take days or weeks with agents.15 This rapid, frictionless visibility builds the trust necessary for effective security-developer collaboration.12

#### Key Feature: Cloud and Kubernetes Security Posture Management (CSPM/KSPM)

The primary function of the agentless scanner is proactive risk identification, which manifests as Cloud Security Posture Management (CSPM). The platform scans for thousands of cloud misconfigurations, such as public-facing storage buckets, unencrypted databases, or overly permissive Identity and Access Management (IAM) roles.16

For containerized environments, this capability extends to **Kubernetes Security Posture Management (KSPM)**. This provides zero-footprint, API-based discovery of Kubernetes clusters, their configurations, and their deployments.18 It delivers complete visibility into the security posture of container registries, cluster-level configurations, and the network settings surrounding them.16 The KSPM module leverages a built-in rules engine to evaluate configurations against security best practices and compliance standards, such as the Center for Internet Security (CIS) Kubernetes benchmarks.20 This analysis covers critical areas like Role-Based Access Control (RBAC) for access management, network segmentation policies, and container isolation settings.20

However, the KSPM function is not a standalone tool that just generates lists of findings. It is explicitly designed to be leveraged by the Wiz Security Graph, which is used to "analyze and prioritize risk with full context".16 This integration demonstrates that even at the posture level, the platform's goal is not merely *finding* misconfigurations but *contextualizing* their true risk.

#### Key Feature: Pre-Deployment Vulnerability Scanning

The agentless scanner also provides "shift-left" security capabilities by identifying known vulnerabilities (CVEs) before they reach production. Wiz scans container images *within* the build systems, CI/CD pipelines, and container registries where they are stored.19 This provides a comprehensive vulnerability assessment, covering dozens of operating systems and over 120,000 supported vulnerabilities.14 This allows security teams to identify and remediate issues early in the software development lifecycle (SDLC), reducing the attack surface of deployed applications.3

#### Key Feature: Attack Path Analysis (The Wiz Security Graph)

The "major strength" of the Wiz agentless platform is its Attack Path Analysis (APA), which is powered by the **Wiz Security Graph**.2 This graph database is the central engine of the platform. It ingests all the data from the API-based scans—assets, misconfigurations, vulnerabilities, identities, network exposures—and builds a model of the entire cloud environment.2

The Security Graph's purpose is to connect these seemingly isolated data points to reveal the "toxic combinations" 2 or "paths of least resistance" 2 that an attacker could chain together to compromise sensitive assets. This is the platform's primary answer to alert fatigue. Traditional tools provide disparate lists of findings, leaving security teams to manually determine which of the 10,000 vulnerabilities or 5,000 misconfigurations matter. The Security Graph provides *context*. It automatically elevates a seemingly low-risk vulnerability to "Critical" if that vulnerability exists on a machine with an exposed internet-facing service, which in turn has an overly permissive IAM role that provides access to a "crown jewel" database containing sensitive data.9

This *prioritization-by-context* is the central pillar of the agentless platform. It moves the security team away from managing endless lists and toward focusing on the few, critical attack paths that pose a genuine, exploitable risk to the business.2

#### Limitations of the Agentless-Only Approach

Despite its power, the agentless model has inherent limitations, which the platform acknowledges. By its nature, agentless scanning is a "snapshot-in-time".11 While these snapshots are taken regularly, they do not provide a real-time, millisecond-by-millisecond view of ephemeral activity *inside* a running workload.11

Most critically, an agentless service, by definition, has no ability to perform **runtime protection**. It cannot "actively protect your hosts by making configuration changes or quarantining suspicious packages".12 It is a purely proactive identification and posture management solution, not a reactive *threat response* tool.16 This gap—the "residual risk" of an active, real-time attack 9—is what led to the development of the platform's second layer: the Wiz Runtime Agent.

### Chapter 1.2: The Wiz Runtime Agent: The "How" and "Now"

The Wiz Runtime Agent, also known as the **Wiz Sensor**, is the optional component that addresses the "snapshot-in-time" limitation of the agentless-only model.3 This component is an explicit "add-on to Wiz Cloud".3 Its introduction strategically expands the platform from a pure posture management and risk-reduction tool into a full-fledged Cloud Detection and Response (CDR) solution.9

#### Core Technology: Lightweight eBPF Sensor

The Wiz Runtime Agent is a lightweight sensor that leverages **eBPF (extended Berkeley Packet Filter)** technology.1 The choice of eBPF is deliberate and significant. It allows the sensor to be "purpose-built for cloud environments" with a "kernel-safe architecture" and "negligible performance impact".1 By hooking directly into the Linux kernel, eBPF provides deep, granular visibility into system calls, network connections, file activity, and running processes 29, all without the instability or performance overhead of traditional, kernel-module-based agents.

This "low-friction" design philosophy mirrors that of the agentless platform. As noted by the Wiz CTO, the platform's architecture allows the Runtime Sensor to remain a "lightweight eBPF agent".9 Because the heavy-lifting of vulnerability and configuration scanning is *still* performed by the agentless scanner, the sensor is freed to focus *only* on collecting true runtime signals. For Kubernetes environments, the sensor is typically deployed as a **DaemonSet**, which automatically places a sensor on every node in the cluster to monitor all containers running on it.31

#### Key Feature: Real-time Threat Detection and Blocking

This is the primary benefit of the agent. The Wiz Sensor monitors for suspicious behavior *within* running containers and on the hosts themselves.28 This includes detecting real-time threats such as:

* Unexpected or malicious processes (e.g., cryptocurrency miners, ransomware).28
* Suspicious file modifications or log tampering.1
* Malicious network connections, reverse shells, or network scanning.1
* Container escape attempts.1

This detection is powered by a tri-force of threat intelligence: the **Wiz Reputation Service** (for known malicious files, IPs, and domains), the **Wiz Rule Engine** (for known malicious behaviors), and **Wiz anomaly detection** (for activity that is atypical for that specific workload).28

Crucially, the Wiz Sensor provides **active blocking capabilities**.1 It is not a detect-only tool. Security teams can create custom detection rules that "trigger specific response actions, such as generating a finding... or **blocking the behavior**" in real-time.33

#### Key Feature: Vulnerability Validation (The "Loaded in Memory" Prioritizer)

This is a standout feature of the Wiz platform and a key point of integration between its two layers. The Runtime Agent's visibility is used to validate the findings of the agentless vulnerability scanner.

The sensor can see which vulnerable packages are *actually being loaded into memory* and actively used by a running application.1 This is a profound and practical solution to the problem of "vulnerability noise".34 Security teams are often overwhelmed with thousands of CVEs identified by scanners. However, many of these vulnerabilities may exist in packages or libraries that are on-disk but are *never executed* by the application.

The Wiz Sensor "validates vulnerabilities in runtime" 4, allowing teams to filter out these "irrelevant vulnerabilities" 35 and "prioritize remediation efforts on **active vulnerabilities**".4 This provides an immediate, data-driven prioritization filter that drastically reduces the number of "critical" vulnerabilities that need to be sent to development teams, improving the mean-time-to-remediate (MTTR) for the risks that truly matter.24

#### Key Feature: Incident Response and Forensics

To support investigations, the agent collects "deep execution context".1 This detailed telemetry, including process execution history, network activity, and file access records, is centralized for analysis.4 This data is used for "runtime hunting" 33 and forms the basis of Wiz's **Cloud Investigation and Response Automation (CIRA)** capability, which correlates this workload-level forensic data with the broader cloud context.32

#### Wiz's Strategic Rationale (Agentless-First, Agent-Add-on)

The decision for an "agentless-first" company to launch an agent was a deliberate, strategic move. As explained by the Wiz CTO, the platform's strategy was to *first* solve *prevention* and *posture* with its "agentless, API-centered approach".9 This addresses the largest, most common sources of risk.

The Runtime Sensor was then introduced to address the "residual risk" of active, in-progress attacks, providing the "workload runtime context" needed for a complete CDR solution.9

The most important part of this strategy is the integration. The Runtime Agent's signals are not analyzed in a silo. They are "well-integrated with the surrounding cloud and Kubernetes activity, as well as the **Wiz Security Graph context**".9 Therefore, the Wiz Runtime Agent is not just a competing EDR. It is a *runtime data feed* for the central Security Graph. This unique architecture allows Wiz to "correlate runtime activity with cloud context to surface real attacks" 36 and "uncover attacker movement across layers" 9—a capability that a siloed, workload-only agent cannot provide.

## Part 2: Comparative Analysis: Wiz Runtime vs. CrowdStrike Container Security

This analysis now pivots to a direct comparison with CrowdStrike. The core of the comparison is not a simple feature-by-feature checklist but a fundamental difference in architectural philosophy. This is best understood by defining what "far-reaching" means for each platform.

### Chapter 2.1: The Core Architectural Distinction: Defining "Far-Reaching"

The "far-reaching" nature of each product is the key to understanding their differing value propositions: one is defined by the *breadth of its context*, the other by the *depth of its telemetry*.

#### Wiz's "Far-Reaching" Breadth of Context

Wiz's "far-reaching" nature stems from the **breadth of its holistic cloud context**.5 Its strength is connecting dots *horizontally* across the entire cloud estate. The Wiz Security Graph is the engine for this, providing an "interconnected view" that unifies disparate signals from posture, identity, data, code, and runtime.5

This architecture provides the answer to the "so what?" question of a security alert. When the Wiz Sensor (the "guard") detects a suspicious runtime event, that event is immediately correlated against the agentless posture data (the "blueprints"). The platform can therefore instantly distinguish a trivial event (a suspicious process on a non-critical, isolated test machine) from a critical one (the *exact same* suspicious process on a machine with a privileged IAM role, public-facing IP, and network access to a sensitive database).9 This "holistic risk prioritization" 37—the ability to *immediately* understand the "blast radius" 9 of a runtime event—is its core strength.

#### CrowdStrike's "Far-Reaching" Depth of Telemetry

CrowdStrike's "far-reaching" nature comes from the **depth of its Endpoint Detection and Response (EDR) capabilities** and its massive threat intelligence graph.6 Its strength is connecting dots *vertically*—deep into the kernel and behavior of the workload—and *globally*, by correlating a single, subtle event against its "CrowdStrike Threat Graph®." This graph processes "over 3 trillion endpoint-related events per week" 7 from all CrowdStrike agents worldwide.

CrowdStrike is the "highly trained security guard." It leverages its market-leading EDR technologies, including "Machine Learning (ML), Artificial Intelligence (AI), [and] Indicators of Attack (IOAs)," to "automatically defend against malware and sophisticated threats".8 Its power is identifying and stopping a "fileless attack" 8 or a novel, zero-day exploit *in real-time* based on its sophisticated behavioral analysis, regardless of that workload's cloud configuration. Its "far-reaching" nature is its ability to see an attack that no one else has ever seen before, based on its deep behavioral models.

### Chapter 2.2: In-Depth Feature, Philosophy, and Market Comparison

This fundamental distinction in philosophy—Breadth of Context vs. Depth of Telemetry—manifests across every aspect of the products. The following framework provides a detailed comparison of the two approaches.

| **Comparative Axis** | **Wiz Runtime Agent (Wiz Sensor)** | **CrowdStrike Container Agent (Falcon)** |
| --- | --- | --- |
| **Core Design Philosophy** | **Context-Driven CDR:** A runtime sensor designed to *feed data into* a broader, agentless-first CNAPP. | **EDR-Driven Workload Security:** A best-of-breed endpoint agent *extended and optimized* for cloud workloads. |
| **Primary Strength** | **Holistic Risk Prioritization:** Unifies runtime events with cloud posture, identity, and data context via the Wiz Security Graph.1 | **Best-in-Class Threat Detection & Response:** Mature, EDR-native capabilities for deep behavioral analysis and real-time threat blocking.6 |
| **Key Technology** | Lightweight eBPF sensor for runtime visibility 1; Security Graph (API-based) for prioritization.2 | Single lightweight agent leveraging behavioral AI, ML, and the CrowdStrike Threat Graph®.7 |
| **"Far-Reaching" Aspect** | **Breadth of Context:** Reaches *across* the entire cloud-native stack (code, posture, identity, runtime).5 | **Depth of Telemetry:** Reaches *deep into* the workload's execution behavior and leverages global threat intelligence.5 |
| **Vulnerability Validation** | A primary, explicit feature. Validates if a vulnerable package is *loaded into memory*, reducing alert fatigue.1 | Part of a broader runtime protection capability; strong at detecting exploitation *attempts* against vulnerabilities.8 |
| **Forensics & IR** | Provides deep telemetry 4 for investigation; context is correlated with the cloud graph.32 | Market-leading. Provides exceptionally deep process trees, threat hunting tools, and mature IR workflows.8 |
| **Market/User Perception** | "Cloud-native," "easy setup," "unified visibility".43 | "Best endpoint stuff," but cloud security can feel "bolted on" or "dated".44 |

#### Analysis: The Unified Platform (Wiz)

Wiz's core value is its "unified platform".1 It consolidates CSPM, CIEM, KSPM, vulnerability management, Data Security Posture Management (DSPM), and now Cloud Workload Protection (CWP) into a single, integrated interface.3 This "single pane of glass" simplifies security workflows. The Runtime Sensor's data is not treated as a separate product; it is a data source that enriches the main platform, allowing it to "correlate runtime activity with cloud context to surface real attacks".36 This unified approach is validated by user reviews, which give Wiz high scores for "Unified Visibility" across multi-cloud environments.43

#### Analysis: The Best-in-Class Specialist (CrowdStrike)

CrowdStrike's value is its specialization. It is a recognized "Leader" in endpoint and workload security by major analyst firms like Forrester and Gartner.40 Its EDR capabilities are its core competency.6 The CrowdStrike container agent is a direct beneficiary of this deep, mature expertise, providing highly effective "behavioral AI and machine learning to identify and stop advanced threats in real-time".38

A significant differentiator for CrowdStrike is its forensic capability. The dynamic and ephemeral nature of containers means that when a container is terminated, "forensic evidence is lost".8 This is a critical problem for incident responders. CrowdStrike solves this by streaming all container activity, process events, and network connections to its platform in real-time.8 This enables "proactive threat hunting" and "powerful search" on historical data "even for ephemeral containers after they have been decommissioned".8 This is an exceptionally mature, SOC-centric capability that is fundamental to a best-of-breed EDR.

#### Market and User Perception (The "Bolted On" Conundrum)

Unfiltered user sentiment provides critical, real-world context that aligns perfectly with this "Breadth vs. Depth" analysis. While analyst reports rate CrowdStrike's *workload* security highly 40, user forums describe its *cloud posture* (CSPM) component as "awful," "dated," and "bolted on".44

In stark contrast, users describe Wiz as "cloud-first" and "solid," with a "cloud-native approach [that] really shows".45 This user sentiment reveals the origin story of each platform. CrowdStrike started with a market-leading agent (depth) and *added* cloud posture (breadth). Wiz started with a market-leading posture graph (breadth) and *added* an agent (depth). The "feel" of each product reflects its architectural foundation. As one analysis notes, "Wiz emphasizes broad, contextual visibility... whereas CrowdStrike's strength continues to be deep workload and endpoint visibility".5

## Part 3: Conclusion and Strategic Recommendation

The decision between the Wiz Runtime Agent and the CrowdStrike Container Agent is not a simple choice of a "better" product, but a strategic decision about security philosophy. It is the formalization of the "security guard" analogy.

### Revisiting the Core Choice (The "Security Guard" Analogy Formalized)

**CrowdStrike** is the **Specialized Threat Hunter**. It is the "highly trained security guard" whose expertise is focused entirely on *behavior*. It is a "best-of-breed runtime threat detection and response" solution.6 This is the correct choice for an organization that has a mature Security Operations Center (SOC), prioritizes stopping the most sophisticated, novel attacks *at the point of execution*, and requires the deep, standalone forensic data to conduct investigations.41

**Wiz** is the **Strategic Risk Manager**. It is the "security guard... [with] access to the blueprints of the entire building".5 Its power is *context*. The platform is designed for organizations whose primary challenge is not a lack of *alerts*, but a lack of *prioritization*. It definitively answers the question, "Of all the threats and vulnerabilities, which one *actually* matters to my business?" This is the "strategic option" for unifying security, development, and infrastructure teams around a single, prioritized view of risk.3

### The Recommended Strategy: Posture First, Runtime Second

For an organization beginning its container security journey, the most effective and efficient path is a layered, "posture-first, runtime-second" strategy. This approach is validated by Wiz's own strategic messaging.1

Phase 1: Prevention & Posture (The 80% Solution)

An organization can deploy Wiz's agentless scanner in minutes 3 to gain an immediate, comprehensive baseline of its entire cloud attack surface. This allows the security team to identify and "tackle [their] biggest posture problems first." This "prevention and security posture management" is "priority number one" 9 because it remediates the static, high-risk attack paths that attackers exploit.

Phase 2: Detection & Response (The 20% Solution)

Once the "noise" of widespread misconfigurations is managed, the team can "layer on real-time protection where it matters most".10 This is achieved by deploying the Wiz Runtime Agent selectively onto the most critical, high-risk workloads—the "crown jewel" applications.9

This "hybrid approach" 10 represents a modern, pragmatic model for cloud security. It balances the "comprehensive coverage" of agentless scanning with the "enhanced visibility" of a runtime agent.10 It avoids the "agent sprawl" 44 and operational overhead of a legacy EDR-everywhere model, while still providing the real-time blocking and deep context required to secure critical applications. This directly fulfills the strategic vision of solving *prevention* first (agentless), and then deploying a context-aware agent to handle the *residual risk* (runtime).9

#### Works cited

1. Protect any workload, anywhere — at runtime | Wiz, accessed November 11, 2025, <https://www.wiz.io/solutions/runtime-sensor>
2. What is Attack Path Analysis? | Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/attack-path-analysis>
3. Wiz Cloud: Manage Security Posture | Wiz, accessed November 11, 2025, <https://www.wiz.io/platform/wiz-cloud>
4. What is Container Runtime Security? | Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/container-runtime-security>
5. Wiz vs. CrowdStrike: 2025 Cloud security comparison | Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/wiz-vs-crowdstrike>
6. What is EDR? Endpoint Detection & Response Defined - CrowdStrike, accessed November 11, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/>
7. Breach protection for containers - CrowdStrike.com, accessed November 11, 2025, <https://www.crowdstrike.de/wp-content/uploads/2020/07/container-security-solution-brief.pdf>
8. FALCON CLOUD SECURITY: - CrowdStrike, accessed November 11, 2025, <https://www.crowdstrike.com/wp-content/uploads/2023/03/crowdstrike-falcon-cloud-security-container-security.pdf>
9. CTO Point of View: Why Wiz is launching a Runtime Sensor | Wiz Blog, accessed November 11, 2025, <https://www.wiz.io/blog/cto-point-of-view-why-wiz-is-launching-a-runtime-sensor>
10. Hybrid File Integrity Monitoring: Agentless & Runtime FIM | Wiz Blog, accessed November 11, 2025, <https://www.wiz.io/blog/a-hybrid-approach-to-file-integrity-monitoring-agentless-and-runtime-fim>
11. Agents are not enough: Why cloud security needs agentless deep ..., accessed November 11, 2025, <https://www.wiz.io/blog/agents-are-not-enough-why-cloud-security-needs-agentless-deep-scanning>
12. Agentless vs. Agent-Based Security: How do they compare? - Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/agentless-vs-agent-based-security>
13. Wiz cloud security platform, accessed November 11, 2025, <https://www.wiz.io/platform>
14. Agentless Cloud Vulnerability Management - Wiz, accessed November 11, 2025, <https://www.wiz.io/solutions/vulnerability-management>
15. Wiz's Agentless Scanning: Revolutionizing Cloud Security Management - Cytas, accessed November 11, 2025, <https://cytas.io/wizs-agentless-scanning-revolutionizing-cloud-security-management/>
16. What is Wiz? | Solution Overview | Enterprise Tech News EM360Tech, accessed November 11, 2025, <https://em360tech.com/tech-articles/solution-overview-what-wiz>
17. Wiz Cloud Security Platform - Threatscape, accessed November 11, 2025, <https://www.threatscape.com/wp-content/uploads/2021/06/Wiz-Datasheet-April-2021.pdf>
18. Agentless container posture in Defender CSPM - Microsoft Learn, accessed November 11, 2025, <https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-containers>
19. Container Registry 101: What You Need to Know - Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/container-registries>
20. Kubernetes Security Posture Management (KSPM) Explained - Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/kubernetes-security-posture-management-kspm>
21. What is Security Posture? Components, Assessment, Best Practices - Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/security-posture>
22. Wiz - Red Hat Ecosystem Catalog, accessed November 11, 2025, <https://catalog.redhat.com/en/software/vulnerability-scanner/detail/264007>
23. Identify and prioritize security risks with Wiz Security Graph and Google Cloud | Cloud Architecture Center, accessed November 11, 2025, <https://docs.cloud.google.com/architecture/partners/id-prioritize-security-risks-with-wiz>
24. Introducing Wiz for Exposure Management | Wiz Blog, accessed November 11, 2025, <https://www.wiz.io/blog/introducing-wiz-for-exposure-management>
25. CloudGuard Network NGFW & Wiz CNAPP - Check Point, accessed November 11, 2025, <https://www.checkpoint.com/cloudguard/wiz/>
26. How Does Wiz Work Without Agents? - BytePlus, accessed November 11, 2025, <https://www.byteplus.com/en/topic/414939>
27. WIZ is {insert your experience} : r/cybersecurity - Reddit, accessed November 11, 2025, <https://www.reddit.com/r/cybersecurity/comments/1c1s9r2/wiz_is_insert_your_experience/>
28. Wiz Sensor - Red Hat Ecosystem Catalog, accessed November 11, 2025, <https://catalog.redhat.com/en/software/container-stacks/detail/68a3700b800fe36691cf7bde>
29. Wiz Runtime Sensor for Linux | Wiz Blog, accessed November 11, 2025, <https://www.wiz.io/blog/wiz-runtime-sensor-for-linux>
30. Wiz Runtime Sensor - AWS Marketplace, accessed November 11, 2025, <https://aws.amazon.com/marketplace/pp/prodview-debmfdjvlvfvo>
31. Detect and respond to your security threats with Wiz and Google Cloud | Community, accessed November 11, 2025, <https://security.googlecloudcommunity.com/community-blog-42/detect-and-respond-to-your-security-threats-with-wiz-and-google-cloud-5561>
32. Wiz Defend: Respond to cloud threats, accessed November 11, 2025, <https://www.wiz.io/platform/wiz-defend>
33. Wiz Expands Runtime Protection to Serverless Containers | Wiz Blog, accessed November 11, 2025, <https://www.wiz.io/blog/wiz-expands-runtime-protection-to-serverless-containers>
34. I'm the CTO of Container Security at Wiz, AMA! : r/cybersecurity - Reddit, accessed November 11, 2025, <https://www.reddit.com/r/cybersecurity/comments/1iba3cp/im_the_cto_of_container_security_at_wiz_ama/>
35. From Cloud to Hybrid: 360° Runtime Protection, Anywhere You Run | Wiz Blog, accessed November 11, 2025, <https://www.wiz.io/blog/from-cloud-to-hybrid-360deg-runtime-protection-anywhere-you-run>
36. Dissecting Cloud Attacks and Attack Vectors: Types + Mitigation Steps | Wiz, accessed November 11, 2025, <https://www.wiz.io/academy/cloud-attacks-and-attack-vectors>
37. What is Cloud Network Security? - SentinelOne, accessed November 11, 2025, <https://www.sentinelone.com/cybersecurity-101/cloud-security/what-is-cloud-network-security/>
38. Preventing Container Escape Attempts with Falcon Cloud Runtime Security - CrowdStrike, accessed November 11, 2025, <https://www.crowdstrike.com/en-us/blog/preventing-container-escape-attempts-falcon-cloud-runtime-security/>
39. AI-Powered Behavioral Analysis in Cybersecurity | CrowdStrike, accessed November 11, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-powered-behavioral-analysis/>
40. Compare the CrowdStrike Falcon® Platform vs. Wiz, accessed November 11, 2025, <https://www.crowdstrike.com/en-us/compare/crowdstrike-vs-wiz/>
41. CrowdStrike Container Security | CloudProtectionWorks.co.uk, accessed November 11, 2025, <https://www.cloudprotectionworks.co.uk/Container-Security.php>
42. Digital Forensics and Incident Response (DFIR) Explained - CrowdStrike, accessed November 11, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/digital-forensics-and-incident-response-dfir/>
43. Compare CrowdStrike Falcon Cloud Security vs. Wiz - G2, accessed November 11, 2025, <https://www.g2.com/compare/crowdstrike-falcon-cloud-security-vs-wiz-wiz>
44. Wiz vs CrowdStrike for cloud security - which one actually works : r/cybersecurity - Reddit, accessed November 11, 2025, <https://www.reddit.com/r/cybersecurity/comments/1nngytw/wiz_vs_crowdstrike_for_cloud_security_which_one/>
45. Wiz vs CrowdStrike for cloud security - which one actually works : r ..., accessed November 11, 2025, <https://www.reddit.com/r/cybersecurity/comments/1nngytw/wiz_vs_crowdstrike_for_cloud_security_which_one_actually_works/>
46. Wiz: #1 Cloud Security Software for Modern Cloud Protection, accessed November 11, 2025, <https://www.wiz.io/>
47. Defend Agentless Workload Detection | Cloud Security Guide | Wiz Blog, accessed November 11, 2025, <https://www.wiz.io/blog/defend-agentless-workload-detection-bringing-visibility-to-blind-spots-in-threat>
48. Falcon Cloud Security Identifies AI-Driven Packages in Container Images - CrowdStrike, accessed November 11, 2025, <https://www.crowdstrike.com/en-us/blog/falcon-cloud-security-identifies-ai-driven-packages/>
49. What Is Container Security? | CrowdStrike, accessed November 11, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/container-security/>