sysdig

CHECKLIST

Sysdig vs. CrowdStrike

Industry Leading Cloud-Native Application Protection Platform (CNAPP), Powered By Runtime Insights

Organizations need an efficient, comprehensive, and deeply-rooted cloud security solution to protect cloud innovation. CrowdStrike Cloud brings a retrofitted XDR approach without the depth needed to secure cloud infrastructure.

Why Customers Choose Sysdig

Sysdig unifies CNAPP security capabilities into a single, comprehensive solution so teams can effectively protect their cloud environments. CrowdStrike's cloud approach leaves cloud environments exposed without adequate vulnerability management and cloud security posture management capabilities.

Sysdig's approach dominates with multi-domain correlation to uncover hidden attack paths across vulnerabilities, configurations, entitlements, and runtime insights. Real-time detection and runtime insights further enable organizations to rapidly identify and prioritize high risk items like in-use vulnerabilities and permissions. Industry leading incident response and forensic capabilities accelerate and enhance security audits and root-cause analysis. These capabilities are delivered through a fully configurable and transparent platform built on Open Standards, such as Falco and OPA.

CrowdStrike can't compete.

With Sysdig, you can:

- ✓ Uncover hidden risks and attack paths with multi-domain correlation.
- ✓ Real-time detection and runtime insights help prioritize risks.
- ✓ Fully configurable and transparent platform built upon Open Standards.

Compare Sysdig to CrowdStrike

This checklist provides a comparison of CNAPP features across container and cloud security between Sysdig and CrowdStrike.

01 User Experience and Enterprise Grade Functionalities

Capabilities	sysdig	CrowdStrike
Unified security dashboards to visualize and address risks across cloud, containers, Kubernetes clusters, third-party apps, and code repos.	✓	✗
Simplified agentless cloud onboarding that allows teams to immediately assess and address security risks.	✓	◐
Fully configurable and transparent platform built upon Open Standards (e.g., Falco, OPA, etc.).	✓	✗
API/CLI-first platform that integrates with third-party tools, processes, and platforms (e.g., SIEM, CI/CD, ITSM, pagers etc.).	✓	◐
Enterprise Scale.	✓	✓
Option between kernel-module and eBPF-powered instrumentation for deployment flexibility with no compromises on runtime visibility.	✓	✓
Role Based Access Control (RBAC) and resource grouping with Zones for granular assignment of responsibilities.	✓	◐
Single Sign-On (SSO) with SAML support for controlled and seamless authentication.	✓	✓

02 Vulnerability Management

Capabilities	sysdig	CrowdStrike
Container images scanned for vulnerabilities in registries, CI/CD pipeline, and at runtime (including serverless containers).	✓	◐
Risk-based vulnerability policies that cover vulnerability scoring, image misconfigurations, and secrets detection.	✓	✗
Scheduled, on-demand, and event-triggered image re-checks to avoid vulnerability blind spots.	✓	✗
Integrated external CVE feeds that provide industry validated vulnerability assessment.	✓	✗
Vulnerability prioritization based on in-use packages.	✓	✗
Enhanced vulnerability prioritization filters and reporting, such as on fix availability, exploitability, etc.	✓	✗
Agent-based and agentless scanning options to host vulnerability management.	✓	◐

03 Cloud Detection and Response

Capabilities	sysdig	CrowdStrike
Unified policy language to detect threats across hosts, containers, Kubernetes, cloud, and third-party apps (e.g., Okta, GitHub).	✓	✗
Managed detection and response rules updated and curated by threat researchers.	✓	✗
Detection rules with out-of-the-box support for compliance frameworks and attack tactics tagging (e.g., SOC2, PCI, HIPAA, CIS, MITRE, etc.).	✓	◐
Deepest level of visibility for attacks in the cloud with Extended Process Trees for context enrichment and correlation of events from the wider context.	✓	✓
Extended FIM capabilities for real-time detection of both file-based and fileless attacks across hosts and containers' filesystems and memory.	✓	✗
Multi-layered approach that combines machine learning, drift prevention, and image profiling with detection policies based on Falco.	✓	✗
Rapid response shell into suspicious workloads based on MITRE ATT&CK context from Live mapping of infrastructure and workloads.	✓	✓
Detailed and actionable data capture for incident response and forensic teams for security audits and root-cause analysis.	✓	✗

04 Cloud Security Posture Management

Capabilities	sysdig	CrowdStrike
Agentless cloud scanning via snapshots.	✓	✗
Remediation of insecure cloud deployments at IaC source with automated GitOps pull requests.	✓	✗
Compliance reports with support for industry benchmarks and regulatory compliance frameworks, enhanced by accurate MITRE risk mapping.	✓	◐
Controlled acceptance of lower risk violations for specific policies or cloud assets for flexible remediation planning.	✓	✗
Risk Prioritization to identify, rank, and address risks combining static posture and vulnerability checks with runtime context from in-use vulnerabilities, permissions, and active threats.	✓	✗
Clear visual representation of risks through Attack Graphs overlaying active events to vulnerabilities and misconfigurations for complete situational awareness in both prevention and response scenarios.	✓	◐
Unified cloud asset inventory to track assets from IaC to production. Filter with runtime insights such as public exposure, in-use packages, failing controls, etc.	✓	◐

05 Permissions and Entitlements Management

Capabilities	sysdig	CrowdStrike
Basic user accounts and roles security hygiene enforced by identifying risky user profile settings.	✓	✓
Simplified posture hardening for accounts and roles via guided remediation of excessive permissions with recommended IAM policies.	✓	✗
Least privilege enforcement based on analyzing in-use permissions.	✓	✗

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights, a unique AI architecture, and open source Falco. Sysdig delivers live visibility by correlating signals across cloud workloads, identities, and services to uncover hidden attack paths. By knowing what is running, teams can prioritize the vulnerabilities, misconfigurations, permissions, and threats that matter most. From prevention to defense, Sysdig helps enterprises move faster and focus on what matters: innovation.

Sysdig. Secure Every Second.

To learn more about Sysdig, visit **sysdig.com.**

REQUEST DEMO →

sysdig

COPYRIGHT © 2021-2023 SYSDIG, INC.
ALL RIGHTS RESERVED. CL-021 REV. C 10/23