WAVE REPORT

The Forrester Wave™: Cloud Workload Security, Q1 2024

The 13 Providers That Matter Most And How They Stack Up

January 29, 2024



Andras Cser

with Merritt Maxim, Caroline Provost, Christine Turley

Summary

In our 21-criterion evaluation of cloud workload security (CWS) providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals select the right one for their needs.

Topics

CWS Consolidation Require... | Evaluation Summary | Vendor Offerings | Vendor Profiles | ...

CWS Consolidation Requires Scrutinizing Configurations And Identities

The CWS market has been rapidly consolidating: Large CWS suite providers continue to augment their functionality with cloud infrastructure entitlement management (CIEM) and data protection capabilities for cloud infrastructure platforms (including AWS, Azure, and GCP). CWS vendors are also increasingly adding productized support for Oracle Cloud Infrastructure and Alibaba cloud platforms, especially around cloud security posture management (CSPM) functionality. Infrastructure as code (IaC) scanning — to ensure the foundational security of cloud and container environment build scripts — is also gaining adoption. CSPM capabilities for mapping configuration rules to compliance templates are becoming less differentiated.

As a result of these trends, CWS customers should look for providers that:

- **Offer configuration and activity-based CIEM capabilities.** Tracking and managing identities and their access to data in cloud infrastructure platforms can be complicated. Low privilege cloud admin user identities (there may be thousands even in a simple environment) may have access to high-privilege compute (virtual machines) that have access to sensitive data. This transitive access is not readily detectable using manual methods like “eyeballing” cloud

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

Accept cookies

orchestrators have admin identities whose access rights should remain least-privilege. Container admins should also use multifactor authentication in all environments to prevent stolen credential-based attacks. Container runtimes such as Docker also complicate network access policy enforcement and can make detection of data exfiltration more difficult. S&R professionals should have reliable methods for detecting and managing secrets embedded in containers, as well as for remediating or even preventing container pre-runtime vulnerabilities. IaC scanning also plays an important role here: If the scanner detects a security hole in pipelines like AWS CloudFormation, Azure Resource Manager, or Terraform, it can stop the entire deployment process and force DevOps to remediate the IaC misconfiguration.

- **Report trends in cloud security exposure, remediation, and compliance.** CWS tools have significantly improved how they present information to auditors, DevOps, IT security, and executive stakeholders. We see differentiation in: trends reporting (e.g., showing how the number of HIPAA compliant workloads change over time); productized reporting to create presentation-ready PDF documents describing to C-level execs the compliance and security state of cloud environments; and easy-to-configure dashboard panels. Forrester is starting to see and expects further proliferation of generative AI (genAI) and large language models in CWS tools for: 1) formulating and getting responses to queries ("What are my riskiest workloads, and why in this environment?") and 2) generating dynamic, context-aware remediation scripts.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market in our reports on CWS.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figures 1 and 2). Click the link at the beginning of this report on Forrester.com to download the tool.

Figure 1

Forrester Wave™: Cloud Workload Security, Q1 2024

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2

Forrester Wave™: Cloud Workload Security Scorecard, Q1 2024

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

This website uses **cookies** to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our **cookie policy** for mor details.

	Forrester's weighting	Aqua Sec	Check Po Technolog	CrowdStr	Lacework	Microsoft	Orca Secu	Palo Alto Networks
Current offering	50%	3.10	3.10	3.30	2.20	3.00	2.70	3.70
Admin identity and access management	10%	3.00	5.00	3.00	3.00	5.00	5.00	5.00
Cloud security posture management (CSPM)	10%	3.00	5.00	3.00	1.00	1.00	3.00	5.00
Configuration templates	10%	3.00	3.00	3.00	3.00	3.00	3.00	5.00
Cloud infrastructure entitlement mgmt.	10%	1.00	3.00	1.00	1.00	3.00	3.00	1.00
Agent-based cloud workload protection	10%	1.00	1.00	3.00	3.00	5.00	1.00	3.00
Agentless cloud workload protection	10%	5.00	3.00	5.00	1.00	1.00	3.00	3.00
Container runtime protection	10%	5.00	1.00	5.00	3.00	3.00	1.00	5.00
Container orchestrator protection	10%	5.00	5.00	3.00	3.00	1.00	1.00	3.00
IaC scanning	5%	1.00	3.00	5.00	3.00	3.00	5.00	3.00
Detection and response	5%	3.00	1.00	5.00	3.00	5.00	1.00	5.00
Reporting and auditing	5%	1.00	5.00	3.00	1.00	5.00	3.00	5.00
Scale	5%	5.00	1.00	1.00	1.00	3.00	5.00	1.00
Strategy	50%	2.40	2.90	4.00	2.30	3.40	3.20	3.60
Vision	20%	1.00	5.00	5.00	1.00	1.00	3.00	3.00
Roadmap	20%	1.00	1.00	1.00	5.00	3.00	5.00	5.00
Community	10%	3.00	0.00	3.00	1.00	5.00	1.00	5.00
Innovation	10%	3.00	3.00	5.00	3.00	5.00	1.00	5.00
Partner ecosystem	10%	5.00	5.00	5.00	1.00	1.00	5.00	1.00
Adoption	15%	3.00	5.00	5.00	3.00	5.00	3.00	3.00
Pricing flexibility and transparency	15%	3.00	1.00	5.00	1.00	5.00	3.00	3.00
Market presence	0%	1.00	1.50	4.00	2.00	4.00	2.00	4.00
Product revenue	50%	1.00	2.00	3.00	1.00	4.00	3.00	5.00
Number of customers	50%	1.00	1.00	5.00	3.00	4.00	1.00	3.00

	Forrester's weighting	Qualys	Rapid7	Sysdig	Tenable	Trend Micro	Wiz
Current offering	50%	2.30	2.50	3.10	2.70	2.50	3.90
Admin identity and access management	10%	1.00	3.00	1.00	1.00	1.00	1.00
Cloud security posture management (CSPM)	10%	3.00	3.00	3.00	3.00	1.00	3.00
Configuration templates	10%	1.00	3.00	3.00	5.00	3.00	5.00
Cloud infrastructure entitlement mgmt.	10%	1.00	3.00	5.00	5.00	1.00	5.00
Agent-based cloud workload protection	10%	5.00	3.00	1.00	3.00	5.00	5.00
Agentless cloud workload protection	10%	1.00	3.00	3.00	1.00	5.00	5.00
Container runtime protection	10%	3.00	1.00	5.00	1.00	3.00	3.00
Container orchestrator protection	10%	1.00	1.00	5.00	3.00	1.00	5.00
IaC scanning	5%	3.00	1.00	1.00	3.00	1.00	5.00
Detection and response	5%	1.00	3.00	3.00	3.00	5.00	3.00
Reporting and auditing	5%	5.00	3.00	1.00	1.00	3.00	1.00
Scale	5%	5.00	3.00	5.00	3.00	1.00	5.00
Strategy	50%	2.50	2.60	2.10	2.50	3.50	2.40
Vision	20%	1.00	1.00	3.00	1.00	3.00	3.00
Roadmap	20%	5.00	3.00	1.00	3.00	3.00	1.00
Community	10%	5.00	5.00	3.00	5.00	1.00	3.00
Innovation	10%	1.00	3.00	3.00	1.00	5.00	1.00
Partner ecosystem							

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

Figure 3

Evaluated Vendors And Product Information

Vendor	Product evaluated
Aqua Security	Aqua Cloud Native Security Platform: SaaS 2310
Check Point	Check Point CloudGuard
CrowdStrike	Falcon Cloud Security
Lacework	Lacework Polygraph Data Platform
Microsoft	Microsoft Defender
Orca Security	Orca Cloud Security Platform
Palo Alto Networks	Prisma Cloud: 5
Qualys	Qualys TotalCloud
Rapid7	Insight Platform
Sysdig	Sysdig Secure
Tenable	Tenable One
Trend Micro	Trend Vision One, Trend Cloud One
Wiz	Wiz Cloud Security Platform

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **CrowdStrike shines in agentless CWP and container runtime protection.** From its agent-based behavioral malware detection roots, CrowdStrike has been expanding on its AI/ML rails into CSPM and IaC scanning. CrowdStrike shows a convincing CWS vision, and its innovation potential as indicated by technical employee staffing is ahead of the competition. CWS revenue contribution from the partner network is also ahead. The size of the vendor's CWS user community is on par. However, its CWS roadmap lags others evaluated. The vendor's CWS roadmap includes: 1) integrating its September 2023 Bionic application security posture management (ASPM) acquisition into its CWS offering, 2) moving asset discovery to be event-based and thus real time, and 3) extending cloud workload protection (CWP) to the entire cloud, irrespective of workload type.

  CrowdStrike offers strong agent-based CWP for Linux and Windows and robust container runtime protection. IaC scanning is versatile and effective. Cloud detection and response

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

platform.

- **Palo Alto Networks provides comprehensive CSPM.** Palo Alto Networks' solution consists of organically developed components (CWP) and acquired pieces (CSPM), with some other functionality distributed across various CWS components. Palo Alto Networks has a large mindshare with end users and competitors. Its CWS roadmap is very strong. The size of the vendor's CWS user community is ahead of others, as is innovation potential as indicated by technical employee staffing. However, CWS revenue contribution from the partner network is behind. The vendor's CWS adoption acceleration strategy is on par with others evaluated. Its CWS roadmap includes: 1) integrating AI into the Prisma Cloud Copilot, 2) unifying XDR/CWP into a single cloud security agent, and 3) addressing open-source vulnerabilities and license compliance issues.

  Palo Alto Networks' admin identity and access management (IAC), including role-based access control, is powerful. CSPM and its accompanying configuration and compliance templates are broad and deep. Container runtime protection, reporting and auditing, and detection and response are ahead. However, agent-based and agentless CWP are only on par. CIEM capabilities and the largest number of workloads protected by the vendor's agentless CWP are behind. Reference customers said the reporting and auditing was significantly above their expectations but also mentioned that the tool sometimes lacks the capability to mature and move into enterprise operations and workflows. Palo Alto Networks is a great fit for organizations looking to extend network-based cloud security to agentless cloud visibility and compliance.

Strong Performers

- **Microsoft provides usable AWS and GCP CWS capabilities but lacks OCI support.** Microsoft has been enhancing its Azure CWS controls to extend Azure into AWS and Google Cloud Platform (GCP). The result is a multicloud-capable CWS solution that can detect and mitigate risks in other public clouds — something that AWS or GCP cannot yet do to the same level of functionality. The vendor's CWS user community is ahead of others, and innovation potential as indicated by technical employee staffing and CWS adoption acceleration strategy distinguish the vendor. However, the partner network's CWS vision and CWS revenue contribution are behind. Its CWS roadmap is on par and includes: 1) container security enhancements, including drift detection; 2) multicloud and DevOps support for Oracle Cloud Infrastructure (OCI) and GitLab; and 3) holistic enterprise security exposure management.

  Microsoft's administrative user identity and access management (IAM) is strong (it's based on the vendor's core Entra IAM offering), and IaC scanning is versatile. Detection and response (risky user detection) and reporting and auditing are ahead. However, non-Azure CSPM, agentless CWP, and container orchestrator protections are behind. Reference customers said the Defender for Cloud is a good tool to have in a Microsoft Azure environment, and the ability to include other cloud environments is a plus. They also mentioned that ongoing changes in Defender for Cloud make it difficult to determine which agents to use. Microsoft is a solid fit for enterprises that have a large Azure cloud infrastructure presence and want to curb spending on standalone solutions for cloud security and CWS.

- **Wiz excels in agentless CWP but lags in admin user management.** Wiz has traditionally been

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

2) continuous cloud threat detection and response, and 3) cloud management platform (reliability, engineering, and cost management) developments.

Wiz provides leading agentless CWP and deployment scale as measured by the largest number of workloads protected by the vendor's agentless CWP. Compliance template mapping to policies, CIEM, agent-based CWP, and container orchestrator protections are also ahead. However, the solution is behind in the areas of admin user IAM and reporting and auditing. Reference customers said that agentless CWP is significantly above their expectations, however, agent-based CWP adoption is nascent and container protections are not used by all customers. Wiz is a good fit for organizations that need to prioritize agentless CWP and need attack path visualization but only minimal agent-based workload protections.

- **Check Point is ahead in container orchestrator protection but lags in agent-based CWP.** In addition to staple CWS features, Check Point Software Technologies provides container and serverless cloud security. Integration with continuous integration/continuous delivery (CI)/(CD) pipelines and catering to DevOps' needs are central to the vendor's CWS product vision, which shines. CWS revenue contribution of the partner network and CWS adoption acceleration strategy are also ahead. However, when it comes to the CWS roadmap and the size of a CWS user group (the vendor does not maintain a CWS-specific user group), the vendor lags. The vendor's CWS roadmap includes: 1) processing real-time alerts to identify aggregate risk, 2) monitoring application code for risk discovery, and 3) IaC and application code drift detection.

  Check Point's CSPM capabilities across multiple clouds are strong, including broad coverage for Oracle and Alibaba Cloud platforms. Container orchestrator protections are leading and are easy to use, but agentless CWP is behind. Cloud detection and response capabilities are also weaker than others evaluated. Reference customers said the solution's dashboards are easy to read. They also said that cloud detection and response meets expectations, but they are only starting to implement it. Check Point is a strong fit for shops that require comprehensive container orchestration coverage in their CWS portfolio.
- **Trend Micro has capable agent-based and agentless CWP but lags in CIEM.** Trend Micro has consolidated its cloud security solutions into the Trend Vision One platform. In addition to the cloud workload security solution, the vendor also offers managed detection and response (MDR) as well as endpoint security capabilities. Innovation potential as indicated by technical employee staffing, CWS revenue contribution from the partner network, and CWS adoption acceleration strategy are ahead of the competition. CWS vision and roadmap are on par with others evaluated, but the size of the vendor's CWS user group is behind. The vendor's CWS roadmap includes: 1) further platform consolidation; 2) extended agentless scanning and asset graph additions; and 3) attack surface risk management improvements in identity entitlements, APIs, and Kubernetes posture management.

  Trend Micro's agent-based and agentless CWP and risk detection and response are ahead of the competition. However, admin user management, CSPM, CIEM, container orchestrator protection, and IaC scanning lag. Reference customers mentioned that the solution "saved us more than once" but also expressed that they are not yet using agentless CWP. Trend Micro is

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

solution this year. The vendor's CWS roadmap is ahead of the competition, as is CWS revenue contribution from the partner network. CWS adoption acceleration strategies are on par. However, when it comes to innovation potential as indicated by technical employee staffing and the size of the vendor's CWS user group, the vendor is behind others. The vendor's CWS roadmap includes: 1) improving threat detection and response automation, especially in the DevOps area; 2) agent-based runtime protection for Linux and Windows virtual machines; and 3) expanding shift-left scanning security.

Orca's administrator IAM and IaC scanning are powerful and are ahead of the competition. The vendor's largest number of workloads protected by the vendor's agentless CWP is also ahead. However, agent-based CWP as well as container runtime and orchestrator protections are behind. Reference customers found the vendor willing to work with them on product improvements, but some of them mentioned that the solution currently lacks container runtime protections. Orca security is a strong fit for organizations that do not want to or cannot implement agent-based CWP and must work with agentless protections.

- **Aqua Security offers strong container orchestration protections but weaker CIEM.** Starting from heritage container protection, Aqua Security has been building out a CWS solution to cover CSPM, CIEM, and IaC scanning. It also maintains developer community for its open-source products to boost adoption of its paid solutions. The CWS revenue contribution of the partner network is greater than the competition. The vendor's user group size and innovation potential as indicated by technical employee staffing are on par. However, its CWS product vision and roadmap are behind other vendors in this evaluation. The vendor's CWS roadmap includes: 1) automatic creation of pull requests in source code to IaC, permission, and vulnerability issues; 2) more investment in CIEM; and 3) runtime container image admission controls based on code attestation checks.

  Aqua Security's container orchestration visibility and protection capabilities are outstanding. Scale, in terms of largest number of workloads protected by the vendor's agentless CWP, is also ahead. CSPM and admin user IAM capabilities are on par. However, CIEM, agent-based operating-system-level CWP, and IaC scanning are weak. Reference customers said that they use Aqua Security's container protections extensively to reason with their DevOps teams about container image vulnerabilities, but noted that the agent-based CWP only meets their expectations. Aqua Security is a solid fit for companies that do not yet require extensive IaC scanning or CIEM but have sizable and varied container runtime and orchestrator deployments to protect.

Contenders

- **Sysdig offers great container protections but lags in IaC scanning.** Sysdig's CWS solution provides coverage of vulnerabilities, detection, and posture management across cloud infrastructure, operating system, container runtime and orchestration, serverless, and IaC environments. Its CWS vision, innovation potential as indicated by technical employee staffing, pricing flexibility and transparency, and the size of its CWS user community are on par. However, its CWS roadmap, CWS revenue contribution from the partner network, and CWS adoption acceleration strategy lag. The vendor's CWS roadmap includes: 1) collecting and analyzing runtime signals to help prioritize security findings and their remediation, 2) using

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

vulnerability scans and file integrity monitoring), and IaC scanning (much less productized than competitors) fall behind. Reference customers said that they use container orchestrator protection extensively and it meets their expectations, however, some references said they do not or are only starting to use agentless CWP. Sysdig is a good fit for organizations requiring primarily container runtime protections (including shift-left scanning) and extensive container image admission control.

- **Tenable has great CIEM but falls behind in container runtime protection.** Based on its vulnerability scanning DNA, Tenable is creating a comprehensive exposure management platform that provides consolidated tooling for securing hybrid and multicloud environments. The vendor's acquisition of CIEM specialist Ermetic in October 2023 offers customers more identity-centric visibility into cloud platform configuration and data access. The size of the vendor's CWS user community and the CWS revenue contribution from the partner network are large and ahead of the competition. Its CWS roadmap is on par. However, CWS vision and innovation potential as indicated by technical employee staffing are behind others evaluated. The vendor's CWS roadmap includes: 1) expanding CIEM capabilities, 2) extending the vendor's own heritage vulnerability content to the cloud, and 3) using agent-based and agentless detection in cloud detection and response.

  Tenable provides great templates for satisfying regulatory compliance mandates and extensive CIEM capabilities that are ahead of the competition. Container orchestration protection and IaC scanning are functional and on par with others evaluated. However, administrative user IAM, agentless CWP, container runtime protection, and reporting and auditing lag. Customer references said that they primarily use the solution for posture monitoring and managing identity risk in cloud environments but are not using the solution for container runtime protection. Tenable is a good fit for firms looking to expand on-prem vulnerability scanning to the cloud and perform identity-centric threat detection.
- **Rapid7 offers a mostly on-par CWS solution but is behind in container protections.** Rapid7 provides contextual, transitive risk scoring for cloud identities, environments, applications, and infrastructure-layered context. The vendor acquired Minerva Labs in March 2023 to augment existing managed threat detection services. The size of the vendor's CWS user group is larger than that of competitors, and its CWS roadmap, innovation potential as indicated by technical employee staffing, and CWS adoption acceleration strategy are on par. However, its CWS vision and CWS revenue contribution from the partner network lag. The vendor's CWS roadmap includes: 1) improved runtime protection and detection and response, 2) integration and enhancement of its External Attack Surface Management service, and 3) expanded support for CI/CD and supply chain security.

  Rapid7's admin user IAM, CSPM, CIEM, configuration templates' breadth and depth, agent-based CWP, agentless CWP, detection and response to risky users in cloud environments, and reporting and auditing are on par. However, container runtime and orchestrator protections and IaC scanning are weak. Reference customers mentioned that cloud detection and response is somewhat above their expectations, but the vendor's agent-based CWP is significantly below their expectations. Rapid7 is a good fit for organizations looking for a no-frills, CSPM-first solution to cover primarily noncontainerized environments and workloads.

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

potential as indicated by technical employee staffing, CWS revenue contribution from the partner network, and pricing flexibility and transparency lag. The vendor's CWS roadmap includes: 1) providing contextual risk insight into assets; 2) prioritizing remediation using risk scores; and 3) broadening agentless snapshot inspection for vulnerabilities, secrets, and malware.

Agent-based CWP, especially vulnerability and malware detection; reporting and auditing; and scale as measured by the largest number of workloads protected by the vendor's agentless CWP are ahead. However, mapping configuration compliance templates to policies, CIEM capabilities, agentless CWP, container orchestration protection, and detection and response (especially risky user detection) are weak. Reference customers said they use the vendor's CWS solution's agent-based CWP functionality across their entire IT infrastructure for vulnerability scanning but do not use agentless capabilities as much. Qualys is a good fit for firms looking to build application risk assessment and mitigation frameworks spanning on-prem and cloud workloads.

- **Lacework shows promise in agent-based CWP but currently has weak CIEM.** Lacework realized early that vendors must offer both agent-based and agentless CWP deployment options. Its CWS solution focuses on developer team enablement and helps uncover and prioritize code-originated as well as runtime risks. Its CWS product roadmap is ambitious and ahead of the competition. Innovation potential as indicated by technical employee staffing and the vendor's CWS adoption acceleration strategy are on par. But CWS vision, the size of the vendor's CWS user group, CWS revenue contribution from the partner network, and pricing flexibility and transparency lag. The vendor's CWS roadmap includes: 1) revamping user experiences across user types, including using GPT-powered assistive technology; 2) improving proactive security to cover cloud infrastructure, platform as a service (PaaS), container runtimes and orchestration, identity, data, and serverless; and 3) continued investment in threat detection.

  Lacework's CWS admin IAM, compliance configuration templates' mapping to policies, agent-based CWP, and container runtime and orchestrator protections are on par. However, the vendor falls behind when it comes to CIEM, reporting and auditing, and the scale of deployment as indicated by the largest number of workloads protected by the vendor's agentless CWP. Reference customers said that deployment times were short (less than five days) and painless (performed by three to four practitioners), but they are not yet using container orchestration protections. Lacework is a good fit for firms looking to understand the transient nature of cloud workload configurations and, as a result, seeking "always-on," proactive cloud workload security.

Evaluation Overview

We grouped our evaluation criteria into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include admin identity and access management, CSPM, configuration templates, cloud infrastructure entitlement management, agent-based cloud workload protection, agentless cloud workload

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

pricing flexibility and transparency.

- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's product revenue and number of customers.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **A thought-leading, productized portfolio of cloud workload security products.** We included CWS vendors that demonstrate thought leadership and solution strategy execution by regularly updating and improving their productized and integrated CWS product portfolios. This includes a complete, productized CWS offering with a product roadmap that covers CWS components of cloud security posture management, cloud workload protection (OS and container), and IaC scanning.
- **Annual CWS revenues of at least $15 million.** We included vendors that have at least $15 million in annual revenues from CWS solutions.
- **Mindshare with Forrester's end-user customers.** The vendors we evaluated are frequently mentioned in Forrester end-user client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.
- **Mindshare with vendors.** The vendors we evaluated are frequently mentioned by other CWS vendors during Forrester briefings as viable and formidable competitors.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by December 5, 2023, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.

policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the integrity policy posted on our website.

© 2024, Forrester Research, Inc. and/or its subsidiaries. All rights reserved.

This website uses cookies to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our cookie policy for mor details.