



Chris Ray
Jan 15, 2025

GigaOm Radar for Cloud Workload Security^{v2.0}

Table of Contents

- [1. Executive Summary](#)
- [2. Market Categories and Deployment Types](#)
- [3. Decision Criteria Comparison](#)
- [4. GigaOm Radar](#)
- [5. Solution Insights](#)
- [6. Analyst's Outlook](#)
- [7. Methodology](#)
- [8. About Chris Ray](#)
- [9. About GigaOm](#)
- [10. Copyright](#)

1. Executive Summary

Cloud workload security (CWS) has evolved into an essential enterprise security framework, providing comprehensive protection for diverse cloud workloads across major cloud service providers and on-premises environments. CWS solutions deliver critical capabilities in policy enforcement, threat detection, and automated response mechanisms, which are particularly vital for containerized and Kubernetes environments.

The imperative for CWS adoption stems from the increasing complexity of cloud environments and the escalating sophistication of cyberthreats. For C-suite executives, CWS represents a strategic investment in risk management and operational efficiency. The financial implications of security breaches and compliance violations can be severe, with costs extending beyond immediate financial losses to long-term reputational damage. CWS solutions address these concerns by providing advanced threat prevention, detection, and response capabilities that surpass native cloud provider security controls.

The 2024 market analysis focuses exclusively on vendors offering comprehensive CWS solutions that can be deployed across multiple cloud environments. A significant evolution in this year's assessment reflects the market's technological advancement, particularly in artificial intelligence (AI) and automation capabilities. Notably, workload policy management has become a standard offering, while remediation powered by large language models (LLMs) and

these concerns by providing advanced threat prevention, detection, and response capabilities that surpass native cloud provider security controls.

The 2024 market analysis focuses exclusively on vendors offering comprehensive CWS solutions that can be deployed across multiple cloud environments. A significant evolution in this year's assessment reflects the market's technological advancement, particularly in artificial intelligence (AI) and automation capabilities. Notably, workload policy management has become a standard offering, while remediation powered by large language models (LLMs) and integrations with CI/CD tools have emerged as key differentiating features.

The scope of evaluation has expanded to acknowledge the convergence of security and development workflows, reflecting the industry's shift toward integrated DevSecOps practices. This evolution addresses the growing demand for security solutions that can operate at cloud scale while maintaining operational efficiency. The market has matured significantly, with vendors now offering more sophisticated capabilities in automated threat response, compliance management, and risk assessment.

These refinements in evaluation criteria align with enterprise requirements for more robust, automated security solutions that can protect cloud workloads effectively while supporting business agility and innovation. The emphasis on advanced features demonstrates the market's progression toward more sophisticated, AI-driven security solutions that can address the complexities of modern cloud environments

This is our second year evaluating the CWS space in the context of our Key Criteria and Radar reports. This report builds on our [previous analysis](#) and considers how the market has evolved over the last year.

This GigaOm Radar report examines 17 of the top CWS solutions and compares offerings against the capabilities (table stakes, key features, and emerging features) and nonfunctional requirements (business criteria) outlined in the companion Key Criteria report. Together, these reports provide an overview of the market, identify leading CWS offerings, and help decision-makers evaluate these solutions so they can make a more informed investment decision.

GIGAOM KEY CRITERIA AND RADAR REPORTS

The GigaOm Key Criteria report provides a detailed decision framework for IT and executive leadership assessing enterprise technologies. Each report defines relevant functional and nonfunctional aspects of solutions in a sector. The Key Criteria report informs the GigaOm Radar report, which provides a forward-looking assessment of vendor solutions in the sector.

2. Market Categories and Deployment Types

To help prospective customers find the best fit for their use case and business requirements, we assess how well CWS solutions are designed to serve specific target markets and deployment models (Table 1).

For this report, we recognize the following market segments:

- **Small-to-medium business (SMB):** In the SMB segment, CWS solutions offer cost-effective protection for cloud workloads, addressing budget constraints while safeguarding critical data from cyberthreats. These are scalable solutions that empower smaller organizations to secure their cloud assets efficiently.
- **Large enterprise:** Large enterprises benefit from the robust capabilities of CWS solutions, ensuring the security and compliance of complex cloud workloads at scale. With advanced features like AI-guided remediation and real-time insights, CWS solutions help enterprises stay ahead of evolving threats and maintain a strong security posture.
- **Public sector:** The public sector relies on CWS solutions to meet stringent compliance requirements while securing sensitive data in cloud environments. CWS solutions tailored to government regulations and cybersecurity standards provide essential protection against cyberthreats for government agencies and other organizations in the public sector.

In addition, we recognize the following deployment models:

- **SaaS:** SaaS deployment involves accessing CWS solutions hosted and managed by the vendor. Operators access the service over the internet, eliminating the need for on-premises hardware or software installation.
- **Self-hosted:** Self-hosted deployment allows organizations to install and manage CWS solutions on their own infrastructure. It provides greater control over data and customization but requires in-house hardware and software management.
- **Hybrid:** Hybrid deployment combines SaaS and self-hosted models, offering flexibility. Some components of the CWS solution may be hosted in the cloud (SaaS), while others run on the organization's infrastructure (self-hosted). This approach suits organizations with diverse security requirements and infrastructure setups.

Table 1. Vendor Positioning: Target Market and Deployment Model

GIGAOM					
VENDOR POSITIONING: TARGET MARKET AND DEPLOYMENT MODEL					
VENDOR	TARGET MARKET			DEPLOYMENT MODEL	
	SMB	Large Enterprise	Public Sector	SaaS	Se

VENDOR	SMB	Large Enterprise	Public Sector	SaaS	Se
Aqua Security	—	✓	✓	✓	
Broadcom	✓	✓	✓	✓	
Check Point	✓	✓	✓	✓	
Cisco	✓	✓	✓	✓	
CrowdStrike	✓	✓	✓	✓	
Fortinet	✓	✓	✓	✓	
IBM	—	✓	✓	✓	
Orca Security	✓	✓	✓	✓	
Palo Alto Networks	✓	✓	✓	✓	
Qualys	✓	✓	✓	✓	
SentinelOne	✓	✓	✓	✓	
Sophos	✓	✓	✓	✓	
Sysdig	✓	✓	✓	✓	
Tenable	✓	✓	✓	✓	
Trellix	—	✓	✓	✓	
Trend Micro	✓	✓	✓	✓	
Wiz	✓	✓	✓	✓	

Source: GigaOm 2024

Table 1 components are evaluated in a binary yes/no manner and do not factor into a vendor's designation as a Leader, Challenger, or Entrant on the Radar chart (**Figure 1**).

"Target market" reflects which use cases each solution is recommended for, not simply whether that group can use it. For example, if an SMB could use a solution but doing so would be cost-prohibitive, that solution would be rated "no" for SMBs.

3. Decision Criteria Comparison

All solutions included in this Radar report meet the following table stakes—capabilities widely adopted and well implemented in the sector:

- Multicloud support
- Support for various workloads
- Real-time workload security insights
- Workload vulnerability assessment
- Workload configuration assessment
- Workload policy management

Tables 2, 3, and 4 summarize how each vendor in this research performs in the areas we consider differentiating and critical in this sector. The objective is to give the reader a snapshot of the technical capabilities of available solutions, define the perimeter of the relevant market space, and gauge the potential impact on the business.

- Key features differentiate solutions, highlighting the primary criteria to be considered when evaluating a CWS solution.
- Emerging features show how well each vendor implements capabilities that are not yet mainstream but are expected to become more widespread and compelling within the next 12 to 18 months.
- Business criteria provide insight into the nonfunctional requirements that factor into a purchase decision and determine a solution's impact on an organization.

These decision criteria are summarized below. More detailed descriptions can be found in the corresponding report, "GigaOm Key Criteria for Evaluating CWS Solutions."

Key Features

- **Hybrid environment support:** This feature enables organizations to secure workloads seamlessly across both on-premises and cloud environments, ensuring consistent protection.
- **Workload detection and response:** This capability empowers organizations to promptly identify and respond to security threats and vulnerabilities within their cloud workloads, ensuring real-time protection.
- **Auto-discovery of workloads:** This feature simplifies the process of identifying and categorizing cloud workloads, streamlining security management.
- **Automated compliance checks:** This capability automates the process of assessing and ensuring compliance with both industry regulations and

- **Workload detection and response:** This capability empowers organizations to promptly identify and respond to security threats and vulnerabilities within their cloud workloads, ensuring real-time protection.
- **Auto-discovery of workloads:** This feature simplifies the process of identifying and categorizing cloud workloads, streamlining security management.
- **Automated compliance checks:** This capability automates the process of assessing and ensuring compliance with both industry regulations and internal security policies.
- **CI/CD integrations:** CI/CD integrations in CWS solutions enable automated security checks and controls throughout the software development lifecycle, ensuring continuous protection and compliance during deployment and updates of cloud-based applications and services.
- **Automated configuration enforcement:** This feature automates the implementation and enforcement of security configurations, reducing the risk of misconfigurations.

Table 2. Key Features Comparison

Exceptional

Superior

Capable

**

Limited

*

Poor

-

Not Applicable

KEY FEATURES

	AVERAGE SCORE	Hybrid Environment Support	Workload Detection & Response	Auto-Discovery of Workloads	Automated Compliance Checks
VENDOR	↕	↕	↕	↕	↕
Aqua Security	4.3	*****	*****	*****	*****
Broadcom	3.7	*****	*****	*****	***
Check Point	4.7	*****	*****	*****	*****
Cisco	4.3	****	*****	*****	***
CrowdStrike	4	****	*****	*****	***
Fortinet	4	***	*****	*****	*****
IBM	3.2	***	*****	***	***
Orca Security	3.8	**	*****	*****	*****
Palo Alto Networks	4.5	****	*****	*****	*****
Qualys	4.5	*****	*****	*****	*****
SentinelOne	3.8	****	*****	***	***
Sophos	3	**	*****	***	***
Sysdig	4.7	*****	*****	*****	*****
Tenable	3.7	***	*****	*****	***
Trellix	3.3	****	***	***	***
Trend Micro	3.7	****	***	***	*****
Wiz	4.5	****	*****	*****	*****

Source: GigaOm 2024

Emerging Features

- **Workload microsegmentation:** Workload microsegmentation is a security approach that divides cloud environments into isolated segments, limiting communication between workloads to reduce attack surfaces. This granular control enhances security by containing potential breaches, minimizing lateral movement, and enforcing the principle of least privilege across cloud infrastructures.
- **Serverless function checks:** Serverless function checks are security measures designed to assess and protect serverless computing environments from potential vulnerabilities and threats.
- **LLM-powered remediation suggestions:** LLM-powered remediation suggestions in CWS solutions use advanced AI models to provide intelligent, context-aware recommendations for addressing security issues and enhancing incident response and risk mitigation in cloud environments.

Table 3. Emerging Features Comparison



EMERGING FEATURES COMPARISON

VENDOR	AVERAGE SCORE	EMERGING FEATURES		
		Workload Microsegmentation	Serverless Function Checks	LLM-Powered Remediation Suggestions
Aqua Security	3.7	★★★★	★★★★★	★★★
Broadcom	1.3	—	★★★★★	—
Check Point	4.3	★★★★★	★★★★★	★★★★★
Cisco	2.7	★★★★★	★★★	—
CrowdStrike	2.7	★★	★★★	★★★
Fortinet	2	—	★★★	★★★
IBM	1.3	★★	★★	—
Orca Security	2.7	—	★★★★★	★★★★★
Palo Alto Networks	3.3	★★★★★	★★★★★	—
Qualys	2.7	★★	★★★★★	★★
SentinelOne	3	—	★★★★★	★★★★★
Sophos		—	—	—
Sysdig	3.3	★★★	★★★	★★★★★
Tenable	2.3	—	★★★	★★★★★
Trellix	2	★★★★	★★	—
Trend Micro	4	★★★★★	★★★	★★★★★
Wiz	3.3	—	★★★★★	★★★★★

Source: GigaOm 2024

Business Criteria

- **Scalability:** Scalability refers to the ability of a CWS solution to adapt and expand its security measures seamlessly to accommodate the growing and evolving cloud workloads within an organization's infrastructure.
- **Cost:** When evaluating cost, we look at the financial impact of implementing a CWS solution and whether it aligns with an organization's budget and resource constraints.
- **Flexibility:** Flexibility assesses a CWS solution's adaptability to diverse cloud workload scenarios and its ability to accommodate varying deployment models, market categories, and use cases.
- **Ease of use:** This criterion evaluates how user-friendly and intuitive a CWS solution is, considering factors like user interface design, simplicity of configuration, and accessibility of features.
- **Ecosystem:** For this criterion, we assess the compatibility and capabilities of a CWS solution for integration with other security tools, cloud platforms, and third-party applications.

Table 4. Business Criteria Comparison

</

VENDOR	BUSINESS CRITERIA				
	Scalability	Cost	Flexibility	Ease of Use	Ec
Aqua Security	✓	✓	✓	✓	
Broadcom	✓	✓	✓	✓	
Check Point	✓	✓	✓	✓	
Cisco	✓	✓	✓	✓	
CrowdStrike	✓	✓	✓	✓	
Fortinet	✓	✓	✓	✓	
IBM	✓	✓	✓	✓	
Orca Security	✓	✓	✓	✓	
Palo Alto Networks	✓	✓	✓	✓	
Qualys	✓	✓	✓	✓	
SentinelOne	✓	✓	✓	✓	
Sophos	✓	✓	✓	✓	
Sysdig	✓	✓	✓	✓	
Tenable	✓	✓	✓	✓	
Trellix	✓	✓	✓	✓	
Trend Micro	✓	✓	✓	✓	
Wiz	✓	✓	✓	✓	

Source: GigaOm 2024

4. GigaOm Radar

The GigaOm Radar plots vendor solutions across a series of concentric rings with those set closer to the center judged to be of higher overall value. The chart characterizes each vendor on two axes—balancing Maturity versus Innovation and Feature Play versus Platform Play—while providing an arrowhead that projects each solution’s evolution over the coming 12 to 18 months.



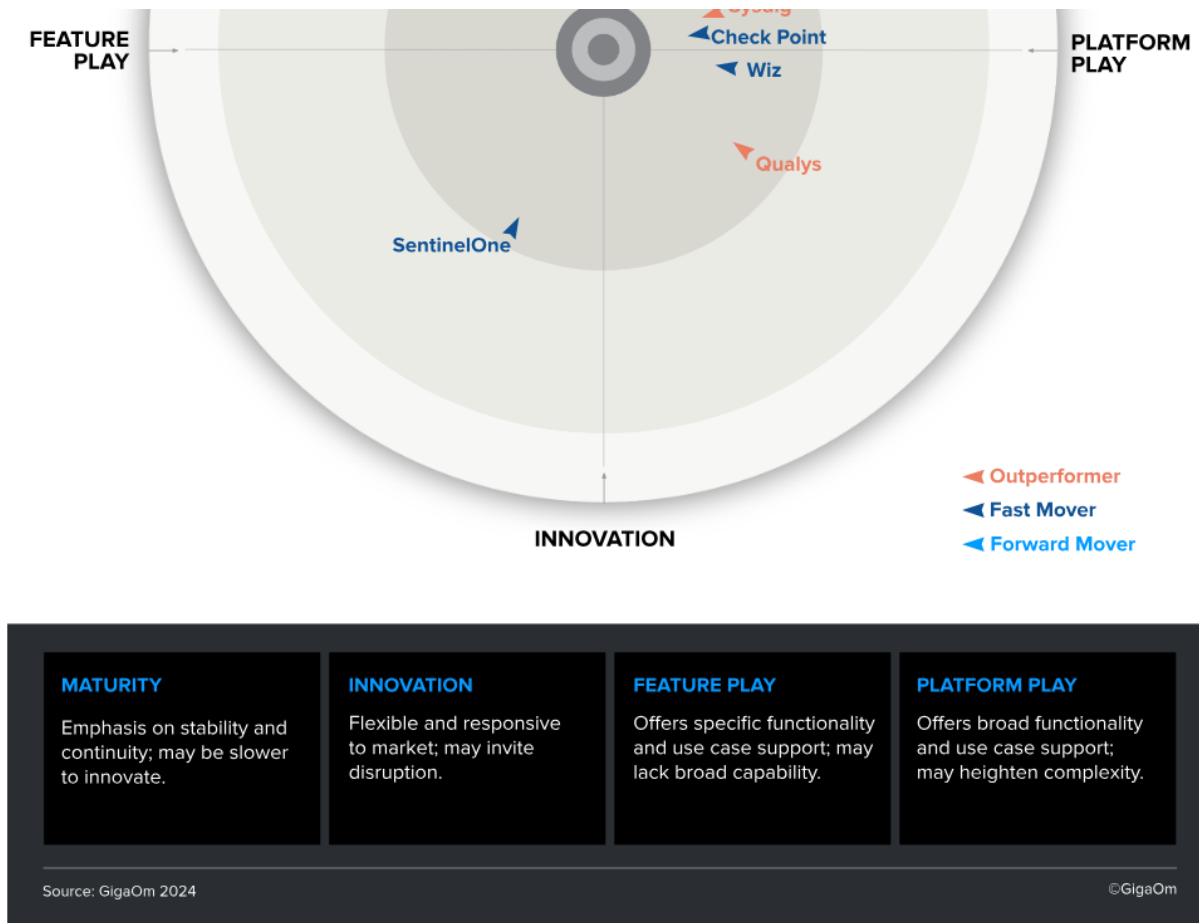


Figure 1. GigaOm Radar for CWS

As you can see in **Figure 1**, this Radar chart reveals interesting dynamics in the CWS solution market. The distribution shows a clear trend toward platform-based solutions, with more vendors positioned on the Platform Play side of the chart. This reflects the industry's broader shift from point solutions to integrated security platforms.

The positioning along the Maturity/Innovation axis is imbalanced, with the majority weighted toward Maturity. This suggests a market that values proven solutions that deliver the same value year over year. The clustering of vendors in the Maturity/Platform Play quadrant indicates that vendors are successfully transitioning from feature-specific offerings to comprehensive security platforms. This occurs either through acquisition or rapid execution on roadmap features that broaden the use cases for the solution.

Only two Outperformers appear in this report, and both reside in the Platform Play hemisphere, showing that platform strategies are currently driving market success. Fast Movers are more distributed among different quadrants, underscoring that there are multiple viable solutions to select from, each bringing its own strengths and weaknesses.

The year-over-year movement shows a gradual progression toward platform approaches, with several vendors successfully transitioning from feature-focused positions. The presence of multiple Leaders in the Maturity/Platform Play segment suggests this is a well-established market with clear best practices and proven approaches. Also worth noting is a change since the previous report in the way vendors are determined to be a Feature Play or Platform Play, which has resulted in some vendors migrating horizontally as well.

The chart shows a pair of Entrants in this competitive field, and these vendors are actually quite capable, depending on the use cases prioritized by the buyer. The positioning of Challengers across different quadrants suggests there are still opportunities for disruption through various strategic approaches.

The overall distribution pattern indicates a market that's consolidating around Platform Plays while maintaining space for specialized solutions in specific niches. This balanced ecosystem supports both established players and innovative newcomers, though the trend clearly favors comprehensive platform offerings over point solutions.

In reviewing solutions, it's important to keep in mind that there are no universal "best" or "worst" offerings; every solution has aspects that might make it a better or worse fit for specific customer requirements. Prospective customers should consider their current and future needs when comparing solutions and vendor roadmaps.

INSIDE THE GIGAOM RADAR

To create the GigaOm Radar graphic, key features, emerging features, and business criteria are scored and weighted. Key features and business criteria receive the highest weighting and have the most impact on vendor positioning on the Radar graphic. Emerging features receive a lower weighting and have a lower impact on vendor positioning on the Radar graphic. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and roadmaps.

To create the GigaOm Radar graphic, key features, emerging features, and business criteria are scored and weighted. Key features and business criteria receive the highest weighting and have the most impact on vendor positioning on the Radar graphic. Emerging features receive a lower weighting and have a lower impact on vendor positioning on the Radar graphic. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and roadmaps.

Note that the Radar is technology-focused, and business considerations such as vendor market share, customer share, spend, recency or longevity in the market, and so on are not considered in our evaluations. As such, these factors do not impact scoring and positioning on the Radar graphic.

For more information, please visit our [Methodology](#).

5. Solution Insights

Aqua Security

Solution Overview

Aqua Security is a cloud security vendor that specializes in protecting applications and infrastructure throughout their lifecycle. Its cloud native application protection platform (CNAPP) integrates security from code to cloud, focusing on containerized and serverless workloads.

The Aqua Platform is a unified solution comprising multiple integrated components for cloud security, including cloud security posture management (CSPM), cloud workload protection platform (CWPP), and supply chain security. These components work together to provide visibility and protection across cloud-native environments.

As a Platform Play vendor positioned in the Maturity half of the Radar, Aqua Security prioritizes stability and consistency in its approach to cloud security. The solution emphasizes methodical improvement and structured advancement, focusing on enhancing existing capabilities rather than pursuing rapid, potentially disruptive changes. This strategy is evident in its continuous refinement of container security features, compliance frameworks, and cross-platform compatibility.

Aqua Security's incremental improvements concentrate on expanding integration capabilities, strengthening compliance controls, and increasing platform availability. Its approach ensures that customers experience minimal disruption while benefiting from steady enhancements to core functionality, particularly in areas of container security, vulnerability management, and cloud workload protection.

Aqua Security is positioned as a Challenger and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Aqua Security scored well on a number of decision criteria, including:

- **Hybrid environment support:** The vendor earned a top score for uniform support across OpenShift, Tanzu Kubernetes Grid (TKG), Rancher, and Tanzu, alongside public cloud services like AWS, Azure, and Google Cloud Platform (GCP). Typical hybrid environments require moderate changes to the architecture to support deployments. However, because of the numerous deployment methods offered, this is not the case with Aqua Security's approach.
- **Automated configuration enforcement:** The vendor earned another top score for effective, easy-to-implement enforcement features. Enforcement can be achieved using out-of-the-box templates that can be further modified. The primary reason for the excellent score, however, is that enforcement can be enabled very easily through the deployment of the Aqua Enforcer daemon set for Kubernetes.
- **Workload microsegmentation:** The vendor earned a very good score for identity-based firewall rules and automated network connection management. This burgeoning technology is likely to deliver reliable security controls by using network segmentation (a reliable, proven method). The Aqua Security approach keeps implementation simple yet effective.

Challenges

Aqua has room for improvement in a few areas, including:

- **Workload detection and response:** The vendor earned a very good score. While its response policies demonstrate strong effectiveness once implemented, the configuration process presents significant complexity for users.
- **LLM-powered remediation guidance:** The vendor earned a good score due to its implementation of a privately hosted ChatGPT model that allows for user interaction and provides code snippets. However, the system lacks context awareness in its recommendations.
- **Workload microsegmentation:** Organizations with highly dynamic, frequently changing microservices architectures may face implementation challenges. While Aqua's microsegmentation capabilities are robust, enterprises with rapid deployment cycles and constant service updates might find the initial rule creation and ongoing maintenance process resource-intensive. The manual intervention required for additional rule creation could become a bottleneck in environments where hundreds or thousands of services are being updated daily.

Purchase Considerations

While the solution scales effectively for large enterprises, the approach to its pricing could be prohibitive for SMBs, warranting careful consideration of budget constraints.

The solution demonstrates strong technical flexibility, supporting multiple cloud environments and on-premises workloads. However, the user experience presents notable challenges, particularly when implementing advanced features. The poorly documented interface and frequent interface changes often necessitate support engagement for routine operations, potentially increasing operational overhead and time to value.

From an integration perspective, the vendor offers standard connectivity with common enterprise technologies, though the ecosystem depth is comparable to market alternatives. The platform's scalability is a notable strength, particularly for large-scale deployments, though smaller organizations may find the scaling mechanisms less than optimal for their needs.

Use Cases

Aqua Security demonstrates broad industry vertical coverage, effectively serving financial services, healthcare, technology, retail, and manufacturing sectors.

to market alternatives. The platform's scalability is a notable strength, particularly for large-scale deployments, though smaller organizations may find the scaling mechanisms less than optimal for their needs.

Use Cases

Aqua Security demonstrates broad industry vertical coverage, effectively serving financial services, healthcare, technology, retail, and manufacturing sectors. The platform architecture adapts well to diverse regulatory requirements and compliance frameworks specific to each industry, including HIPAA, PCI-DSS, and SOX.

The solution supports comprehensive use cases across the cloud security spectrum, including security for containers and Kubernetes, cloud infrastructure security, compliance management and reporting, and threat detection and response.

The platform's flexibility allows organizations to implement security controls consistently across multiple cloud providers and on-premises environments, making it particularly suitable for enterprises with complex, hybrid infrastructures. The solution's modular approach enables organizations to activate specific capabilities as their security needs evolve, though this can impact initial deployment complexity.

Broadcom: Carbon Black Cloud Workload*

Solution Overview

Broadcom delivers CWS through the Carbon Black Cloud Workload platform, leveraging Carbon Black's extensive virtualization expertise and cloud infrastructure capabilities. Following Broadcom's acquisition of VMware in 2023, the solution continues to evolve while maintaining its focus on comprehensive workload protection across hybrid environments.

Carbon Black Cloud Workload operates as part of the broader Broadcom security portfolio, integrating workload protection with vulnerability management and compliance monitoring. The platform's architecture leverages deep integration with VMware's virtualization infrastructure while supporting multicloud environments through its cloud-native security controls.

The solution combines traditional endpoint security capabilities with cloud workload protection, offering modules for workload security and CSPM.

Positioned in the Maturity half of the market, Broadcom demonstrates a methodical approach to solution development. The vendor prioritizes stability and proven security practices, focusing on systematic improvements to existing capabilities rather than rapid feature iteration. This strategy emphasizes reliable performance and consistent user experience, particularly in areas such as threat detection, compliance management, and virtualization security controls.

Broadcom is positioned as a Challenger and Fast Mover in the Maturity/Feature Play quadrant of the CWS Radar report.

Strengths

Broadcom scored well on a number of decision criteria, including:

- **Hybrid environment support:** Broadcom earned a top score due to its comprehensive approach that combines Carbon Black agent deployment with agentless cloud connections. The solution's ability to integrate with other VMware tools like Aria enables exceptional monitoring and control capabilities across public clouds, private clouds, and on-premises environments, providing consistent security coverage regardless of workload location.
- **Serverless function checks:** Broadcom earned a very good score for delivering robust multicloud protection through real-time visibility, misconfiguration detection, and least privilege enforcement. The solution's pre-runtime vulnerability assessment across the development lifecycle demonstrates strong security controls for serverless environments.
- **Workload detection and response:** Broadcom earned a strong score because it offers effective protection against both known and unknown threats, including malware, fileless attacks, and living off the land techniques. The solution shows some limitations in Azure and GCP environments compared to VMware and AWS deployments.

Challenges

Broadcom has room for improvement in a few areas, including:

- **CI/CD integration:** Broadcom scored poorly due to significant limitations in development pipeline security capabilities. While the solution offers automatic CI/CD generation through Chef, Puppet, and Ansible support and maintains a partnership with CloudBees CI for VMware Tanzu integration, these capabilities fall notably short of competitor offerings in terms of scope and sophistication.
- **LLM-powered remediation suggestions:** Broadcom earned no score due to lacking this feature.
- **Workload microsegmentation:** Broadcom earned no score due to the capability not being available within the solution.

Purchase Considerations

The solution demonstrates moderate scalability through its support for both agent-based and agentless deployment models. However, limitations in CI/CD integrations and a strong focus on the VMware ecosystem may impact scaling strategies in diverse environments. While the platform supports configuration management tools like Puppet, Chef, and Ansible, the implementation details and integration depth require careful evaluation.

The vendor employs a straightforward per-asset pricing model with quantity discounts, including standard support in the base cost. Implementation considerations reveal mixed characteristics. The unified console provides efficient management across Carbon Black products, and VMware environment deployments benefit significantly from automated tooling integration. The automated policy creation features reduce expertise requirements, though these advantages primarily benefit organizations heavily invested in VMware infrastructure.

A notable limitation exists in ecosystem integration because the vendor's VMware-first approach may create challenges for organizations using diverse technology stacks. While this focus provides excellent value for VMware-centric environments, organizations with heterogeneous infrastructure should carefully evaluate integration requirements against their existing technology investments.

Use Cases

Broadcom's Carbon Black Cloud Workload demonstrates particular strength in serving organizations heavily invested in VMware infrastructure, especially those managing hybrid cloud environments. The solution excels in scenarios requiring deep integration with VMware vSphere and VMware Cloud environments, making it particularly valuable for enterprises transitioning workloads between on-premises and cloud deployments.

Use Cases

Broadcom's Carbon Black Cloud Workload demonstrates particular strength in serving organizations heavily invested in VMware infrastructure, especially those managing hybrid cloud environments. The solution excels in scenarios requiring deep integration with VMware vSphere and VMware Cloud environments, making it particularly valuable for enterprises transitioning workloads between on-premises and cloud deployments.

The solution specifically addresses use cases focused on unified security management across VMware ecosystems, including automated workload protection, compliance monitoring, and threat detection. Its tight integration with VMware tools enables efficient security operations for organizations prioritizing VMware-based infrastructure. While the platform offers broader cloud security capabilities, its distinctive value lies in providing seamless security controls across VMware environments, though organizations primarily focused on non-VMware clouds may find more suitable alternatives.

Check Point: CloudGuard

Solution Overview

Check Point delivers cloud security through its CloudGuard platform, integrating comprehensive cloud security capabilities into the company's broader security architecture. The solution takes a holistic approach to protecting cloud assets by combining cloud network security, workload protection, and posture management into a unified framework.

As part of Check Point's unified security platform, CloudGuard operates through integrated components that encompass network security, workload protection, and posture management. This integration ensures comprehensive cloud security coverage while maintaining consistency with Check Point's established security framework, providing enterprises with robust protection across multiple environments.

Check Point's position in the Maturity half of the market stems from its methodical approach to solution development. The vendor emphasizes stability and established security practices, focusing on incremental improvements to existing capabilities rather than pursuing rapid, potentially disruptive innovation. This measured strategy prioritizes reliable performance and consistent user experience across threat detection, compliance management, and multicloud security controls.

The solution continues to evolve through strategic enhancements to integration capabilities with existing security infrastructure, compliance framework coverage and reporting mechanisms, workload security controls and automation features, and cross-platform compatibility with consistent policy management. This deliberate development approach ensures stability and reliability while maintaining competitive capabilities in the dynamic cloud security landscape.

Check Point is positioned as a Leader and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Check Point scored well on a number of decision criteria, including:

- **Hybrid environment support:** Check Point earned a top score due to its comprehensive coverage through a sophisticated combination of physical and virtual firewalls, agent-based protection, Helm charts, and dedicated security appliances. This multilayered approach enables seamless security management across diverse infrastructure environments, providing organizations with consistent protection regardless of workload location.
- **Workload detection and response:** Check Point earned another excellent score due to its superior coverage across all workload types, both in cloud and on-premises environments. The integration with CloudGuard Risk Management enhances this functionality by enabling intelligent prioritization of response activities, streamlining security operations and improving incident response effectiveness.
- **Automated configuration enforcement:** Check Point earned an excellent score due to its straightforward implementation process and intuitive policy management interface. Users can easily modify existing enforcement policies or create new ones, reducing operational complexity while maintaining robust security controls. This combination of simplicity and effectiveness makes the solution particularly valuable for organizations managing complex security requirements across diverse environments.

Challenges

For organizations seeking exception execution on specific key features, there are a few areas where Check Point could improve. These are:

- **LLM-powered remediation suggestions:** Check Point earned a very good score due to its measured approach to AI-driven security recommendations. CloudGuard implements LLM technology with careful constraints, prioritizing security through deterministic algorithms. While this approach ensures reliable risk assessment through effective risk management analysis, attack path evaluation, and real-time threat intelligence integration, the limited scope of LLM implementation may restrict some advanced remediation capabilities that competitors offer.
- **Serverless function checks:** Check Point earned a very good score for its serverless security features, including continuous scanning, runtime protection, and behavioral profiling. The implementation of function self-protection mechanisms, identity and access management (IAM) checks, and exposure minimization demonstrates strong technical capability. While the integration with CI/CD pipelines adds valuable security controls, opportunities remain for enhanced automation and deeper integration with cloud-native development workflows.
- **Automated compliance checks:** Check Point earned a very good score due to its comprehensive out-of-the-box compliance checks that apply broadly across infrastructure and workloads. While the customization options provide good flexibility for adapting to specific compliance requirements, there may be room for more advanced automation features and deeper integration with compliance reporting workflows.

Purchase Considerations

Check Point offers clearly defined pricing models across different components: CWS functionality is priced per asset, code security is available on a per-seat basis at competitive rates, and cloud detection and response capabilities are billed based on network data ingestion volumes. This flexible pricing strategy makes the solution accessible to organizations of all sizes, from SMBs to large enterprises and public sector entities.

The solution demonstrates exceptional scalability, employing robust horizontal scaling principles that maintain consistent performance regardless of utilization levels. The auto-scaling functionality ensures reliable operation as workload demands fluctuate, representing a more resilient approach compared to traditional vertical scaling methods.

Implementation and operational considerations are notably positive. The vendor provides comprehensive documentation and free training resources while leveraging AI/ML capabilities to streamline routine tasks. This commitment to user enablement significantly reduces the learning curve and operational overhead typically associated with enterprise security solutions.

to traditional vertical scaling methods.

Implementation and operational considerations are notably positive. The vendor provides comprehensive documentation and free training resources while leveraging AI/ML capabilities to streamline routine tasks. This commitment to user enablement significantly reduces the learning curve and operational overhead typically associated with enterprise security solutions.

The platform's extensive ecosystem integration capabilities further enhance its value proposition. Native integrations span critical operational tools, including security information and event management (SIEM) systems, incident management platforms, CI/CD tools, and cloud-native services. The availability of API and webhook integrations enables custom workflow development, providing organizations with the flexibility to adapt the solution to their specific operational requirements.

Use Cases

The solution effectively serves regulated industries, including financial services, healthcare, and government sectors, while also meeting the demands of retail, manufacturing, and technology companies. This broad vertical support is achieved through its robust compliance framework, industry-specific security controls, and adaptable security policies.

Check Point excels in addressing diverse use cases through its integrated approach to cloud security. Key scenarios include hybrid cloud protection leveraging physical and virtual firewalls, comprehensive workload security spanning cloud and on-premises environments, and automated compliance management. The platform's strengths in workload microsegmentation, CI/CD security integration, and serverless function protection demonstrate its versatility in supporting modern cloud-native architectures. CloudGuard's automated discovery capabilities and configuration enforcement features enable efficient security management across complex environments, while its integration with risk management tools ensures effective threat prioritization and response.

Cisco: Secure Workload*

Solution Overview

Cisco delivers CWS through its Secure Workload offering, leveraging the company's extensive networking expertise and security capabilities. The solution integrates workload protection with broader security controls.

Secure Workload operates as part of Cisco's broader security ecosystem, working in concert with other Cisco security products while maintaining standalone functionality. The solution combines workload protection, microsegmentation, and compliance monitoring through a unified console, enabling consistent security policy enforcement across diverse environments.

Cisco positions Secure Workload as a security solution particularly suited for organizations requiring sophisticated network segmentation and workload protection capabilities.

Positioned in the Maturity half of the Radar chart, Cisco demonstrates a methodical approach to solution development. The vendor prioritizes stability and proven security practices, focusing on systematic improvements to existing capabilities rather than rapid feature iteration. This strategy emphasizes reliable performance and consistent user experience, particularly in areas such as network segmentation, compliance management, and workload protection controls.

The solution shows ongoing enhancement in established areas, including integration capabilities, policy management, and automated controls, reflecting the vendor's commitment to the steady, purposeful advancement of core functionalities.

Cisco is positioned as a Leader and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Cisco scored well on a number of decision criteria, including:

- **Workload detection and response:** Cisco earned a top score because the solution performs sophisticated behavioral analysis to establish baselines, monitors process and communication activities for malicious behaviors, and leverages the MITRE ATT&CK framework for detection accuracy. The ability to maintain complete software inventory tracking while mapping known vulnerabilities to observed behaviors enables real-time event correlation, further enhanced by seamless integration with SIEM and SOAR platforms.
- **Automated configuration enforcement:** Cisco earned another excellent score because the solution offers fully automated enforcement mechanisms with flexible policy definition options, supporting both agent-based and agentless deployments. The solution's ability to generate policy recommendations and implement dynamic, context-aware policy models demonstrates advanced automation capabilities that adapt to evolving security requirements.
- **Workload microsegmentation:** Cisco earned an excellent score because the implementation leverages application behavior and communication patterns to establish zero-trust-based microsegmentation across AWS, Azure, GCP, and on-premises environments. The solution's support for dynamic, attribute-based policy definition within a hierarchical model enables sophisticated network security controls across diverse infrastructure environments.

Challenges

Cisco has room for improvement in a few areas, including:

- **Automated compliance checks:** Cisco earned an average score due to limitations in its compliance framework coverage. While the solution offers basic compliance monitoring capabilities and explicitly supports NIST standards, documentation lacks clear reference to support for other major frameworks such as CIS, HIPAA, PCI, FISMA, and GDPR.
- **LLM-powered remediation suggestions:** Cisco earned no score because the feature is missing from the solution.

Purchase Considerations

The solution demonstrates exceptional scalability through its hybrid deployment approach. The agentless architecture for cloud environments combined with a unified agent model for other workloads streamlines deployment and operational management. This efficiency extends to security operations through powerful workload detection and response capabilities that reduce manual triage requirements. The automated discovery features further enhance operational efficiency by eliminating labor-intensive manual processes.

Implementation considerations reveal strong usability characteristics. The platform's visual query interface reduces learning complexity, while centralized

with a unified agent model for other workloads streamlines deployment and operational management. This efficiency extends to security operations through powerful workload detection and response capabilities that reduce manual triage requirements. The automated discovery features further enhance operational efficiency by eliminating labor-intensive manual processes.

Implementation considerations reveal strong usability characteristics. The platform's visual query interface reduces learning complexity, while centralized workload management simplifies operations across diverse environments. The automated microsegmentation capabilities provide sophisticated security controls, though organizations should carefully evaluate their comfort level with automated policy enforcement.

The solution's ecosystem integration capabilities are exceptional, benefiting from Cisco's extensive market presence. Strategic partnerships with major technology providers (Intel, Oracle, Red Hat, VMware, and SAP) and comprehensive integration support for key operational platforms (Kubernetes, ServiceNow, and AWS) enable seamless incorporation into existing enterprise environments.

Use Cases

The platform addresses workload security use cases through its unified approach, leveraging Cisco's extensive networking expertise for cloud workload protection, container security, and network security. The solution particularly excels in complex deployment scenarios, including hybrid environments, cloud-native application security, and network microsegmentation. The platform's automated risk assessment and threat detection capabilities make it especially effective for organizations requiring comprehensive security coverage with strong operational efficiency.

Cisco's focus on integrated security operations and network security expertise provides particular value for enterprises prioritizing advanced threat detection capabilities across their cloud infrastructure.

CrowdStrike*

Solution Overview

CrowdStrike's Falcon platform extends its endpoint security expertise into comprehensive cloud workload protection through its Falcon Cloud Security module. The solution leverages CrowdStrike's threat intelligence and detection capabilities to protect cloud workloads, containers, and Kubernetes environments across multiple cloud providers.

The Cloud Security module operates as an integrated component of the broader Falcon platform, incorporating cloud workflow protection, container security, CSPM, ASPM, and DPM. These capabilities are delivered through a unified console, providing visibility and control across cloud environments. Key Falcon Cloud Security components include CWPP, Container Security, and CSPM.

CrowdStrike's approach emphasizes real-time threat detection and response, leveraging its extensive threat intelligence network and automated response capabilities. The solution falls on the Maturity half of the chart, reflecting CrowdStrike's established position and methodical approach to solution development. The vendor prioritizes stability and reliability, focusing on incremental improvements to core capabilities while maintaining a consistent user experience.

The platform demonstrates ongoing enhancement in critical areas, including threat detection accuracy, integration capabilities with cloud-native services, and automated response mechanisms.

CrowdStrike is positioned as a Leader and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

CrowdStrike scored well on a number of decision criteria, including:

- **Workload detection and response:** CrowdStrike earned a top score due to the exceptional integration of threat intelligence sources with AI capabilities. The solution's ability to complement automated detection with optional human threat hunting services provides a comprehensive security approach that addresses sophisticated threats effectively.
- **Hybrid environment support:** CrowdStrike earned a very good score because it distinguishes itself through strategic partnerships with key technology providers like Red Hat for OpenShift integrations. This collaborative approach enhances its hybrid cloud security capabilities, providing robust protection across diverse infrastructure environments.
- **Auto-discovery of workloads:** CrowdStrike earned another very good score for providing efficient API-based discovery mechanisms for major cloud platforms while leveraging the Falcon platform's capabilities for on-premises workload discovery. This dual approach ensures comprehensive visibility across complex enterprise environments.

Challenges

CrowdStrike has room for improvement in a few areas, including:

- **Serverless function checks:** CrowdStrike earned an average score due to its runtime-focused approach to serverless security. While the solution provides visibility into serverless functions across major cloud providers and includes CI/CD integration, there are opportunities to enhance predeployment security checks and expand coverage beyond the basic action and service relationship monitoring.
- **Workload microsegmentation:** CrowdStrike scored poorly. The solution provides visibility into cloud and container network traffic patterns, but it lacks active segmentation capabilities and doesn't offer policy recommendations for network isolation.

Purchase Considerations

CrowdStrike's licensing approach demonstrates notable transparency with a straightforward pricing model based on workload count and repository numbers. This clear structure enables organizations to accurately forecast costs and scale their investment according to their security needs. The solution's packaging is well defined, making it straightforward for organizations to understand which capabilities they're acquiring and how they align with security requirements.

The platform demonstrates strong scalability, leveraging its cloud-native architecture to support multiple deployment types effectively. This architecture particularly benefits larger enterprises, though the solution remains accessible to midsize organizations. As a Platform Play, Falcon Cloud Security requires consideration as a primary security solution, potentially necessitating the displacement of existing tools to fully leverage its integrated capabilities.

Implementation considerations reveal moderate complexity. While the user interface is intuitive and streamlined, this simplification occasionally results in reduced visibility of important operational details. The solution's deployment model focuses effectively on major cloud providers and common deployment

particularly benefits larger enterprises, though the solution remains accessible to midsize organizations. As a Platform Play, Falcon Cloud Security requires consideration as a primary security solution, potentially necessitating the displacement of existing tools to fully leverage its integrated capabilities.

Implementation considerations reveal moderate complexity. While the user interface is intuitive and streamlined, this simplification occasionally results in reduced visibility of important operational details. The solution's deployment model focuses effectively on major cloud providers and common deployment scenarios, though it may lack some specialized capabilities for unique use cases.

Use Cases

The solution's architecture accommodates diverse compliance requirements while maintaining consistent security controls across different industry contexts.

The platform addresses key cloud security use cases through its unified approach, supporting cloud-native workload protection, container security, and hybrid cloud environments. Its strengths in threat detection and response, coupled with extensive threat intelligence capabilities, make it particularly effective for enterprises requiring comprehensive security coverage. The solution excels in complex deployment scenarios, including multicloud environments, containerized workloads, and DevSecOps integration, though smaller organizations may find the full feature set exceeds their requirements.

CrowdStrike's focus on automated security operations and integrated threat intelligence provides particular value for organizations prioritizing advanced threat detection and incident response capabilities across their cloud infrastructure.

Fortinet: Lacework FortiCNAPP*

Solution Overview

Fortinet's Lacework FortiCNAPP delivers cloud security through its data-driven platform, focusing on automated threat detection and continuous monitoring of cloud environments. Following its recent acquisition by Fortinet in August 2024, the solution is positioned to integrate with Fortinet's broader security ecosystem while maintaining its distinctive cloud-native security approach.

Fortinet's Lacework FortiCNAPP Cloud Security Platform operates as a unified solution encompassing CSPM, CWPP, SCA, IaC, SAST, SBOM, and cloud infrastructure entitlement management (CIEM). These capabilities are delivered through a single platform that leverages ML for anomaly detection and behavioral analysis across cloud environments.

The solution's core components include Polygraph Data Platform for active threat detection and behavioral analysis, Workload Security for runtime protection, and Cloud Configuration Assessment for compliance monitoring. This integrated approach reflects Fortinet's strategy of providing comprehensive cloud security through automated, data-driven insights.

The acquisition by Fortinet is well underway, and technical integrations have already occurred with the Fortinet Security Fabric with solutions like FortiSOAR and FortiGUARD. Further expansion across the Security Fabric is expected soon.

Fortinet is positioned as a Challenger and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Fortinet scored well on a number of decision criteria, including:

- **Workload detection and response:** Fortinet earned a top score because the solution offers streamlined implementation for cloud workload protection, enabling rapid deployment and operational effectiveness. Its threat detection feature uses behavioral analysis, threat intelligence, and anomaly detection and covers a wide range of workload types (both cloud and on-premises). The resulting output of this feature is a composite alert that considers all inputs and multiple, often less important alerts, when viewed individually, into one easy to understand comprehensive risk score.
- **Auto-discovery of workloads:** Fortinet earned a very good score for the way it implements a dual approach using both API and agent-based discovery methods, providing comprehensive visibility across major cloud providers, including AWS, Azure, GCP, and Oracle Cloud Infrastructure (OCI). The solution extends its discovery capabilities to open source infrastructure components such as Kubernetes and OpenShift, ensuring broad coverage of modern cloud-native environments.
- **CI/CD integration capabilities:** Fortinet earned a very good score due to leveraging webhooks and scripts, avoiding tool-specific limitations, and enabling seamless integration with diverse CI/CD toolchains. The platform's native integration with major code repositories like GitHub, GitLab, and Bitbucket, combined with proactive security issue remediation in build pipelines and IDE extensions demonstrates strong DevSecOps alignment.

Challenges

Fortinet has room for improvement in a few areas, including:

- **Hybrid environment support:** Fortinet earned an average score due to limitations in its architectural approach. While the platform employs API-based security for cloud environments, it relies on agent-based protection for on-premises Kubernetes clusters and virtual machines (VMs). This bifurcated approach may introduce operational complexities and potential coverage gaps in hybrid deployments.
- **LLM-powered remediation suggestions:** Fortinet earned a satisfactory score because of its "Smart Fix" feature, which shows promise in addressing CVE remediation for third-party and open source software. The system's ability to evaluate and recommend remediation paths demonstrates thoughtful implementation, but its limitation to code and build security contexts significantly restricts its utility across broader CWS scenarios.
- **Workload microsegmentation:** Fortinet earned no score due to the feature being absent in Lacework FortiCNAPP. The broader Fortinet Security Fabric offers FortiWEB integrations that can enable similar features.

Purchase Considerations

The solution demonstrates above-average flexibility through comprehensive platform coverage and extensive integration capabilities. Fortinet's broad ecosystem support includes partnerships with major cloud providers (AWS, GCP, Azure, IBM) and seamless integration with DevOps tooling and SIEM systems, enabling robust security workflows across diverse environments. This extensive integration framework makes the platform particularly valuable for organizations with complex multicloud infrastructures.

From an implementation perspective, Lacework FortiCNAPP stands out for its intuitive user interface and streamlined onboarding process. The platform's ease of use significantly reduces training requirements and accelerates time to value, though the API and agent-based scaling approach, while effective, aligns with industry standards rather than exceeding them.

From an implementation perspective, Lacework FortiCNAPP stands out for its intuitive user interface and streamlined onboarding process. The platform's ease of use significantly reduces training requirements and accelerates time to value, though the API and agent-based scaling approach, while effective, aligns with industry standards rather than exceeding them.

The solution's architecture supports standard deployment scenarios through API and agent-based implementations, providing reliable but conventional scalability options. Organizations should consider their specific scaling requirements and evaluate how Fortinet's approach aligns with their operational models and growth projections.

Use Cases

Lacework FortiCNAPP, now part of Fortinet, delivers comprehensive cloud security capabilities across a broad spectrum of industry verticals. The platform particularly excels in automated threat detection and response, leveraging ML capabilities for behavioral analysis across cloud environments. The solution effectively handles complex deployment scenarios, including multicloud environments, cloud-native application security, and DevSecOps integration, making it suitable for enterprises requiring comprehensive cloud security coverage with strong automation capabilities.

The platform's data-driven approach and automated security controls make it particularly effective for organizations prioritizing operational efficiency alongside robust security measures.

IBM*

Solution Overview

IBM leverages its extensive enterprise security expertise and cloud capabilities to provide comprehensive CWS solutions. IBM combines threat management, application security, data security, and IAM to provide comprehensive protection for cloud workloads across hybrid environments.

The solution operates as part of IBM's broader security ecosystem. Key components include Security Guardium Insights, Cyber Threat Management Services, and Guardium Data Protection, all integrated through a unified management console. These modules work in concert with IBM's QRadar SIEM and broader security portfolio to provide end-to-end visibility and control.

IBM's position in the Maturity half of the Radar chart reflects its methodical approach to solution development. The vendor emphasizes stability and proven security practices, focusing on systematic improvements to existing capabilities rather than rapid feature iteration. This approach prioritizes reliability and consistent performance, particularly in areas such as threat detection, compliance management, and enterprise integration capabilities.

IBM is positioned as an Entrant and Fast Mover in the Maturity/Feature Play quadrant of the CWS Radar report.

Strengths

IBM scored well on a number of decision criteria, including:

- **Workload detection and response:** IBM earned a strong score due to its advanced ML capabilities for threat detection combined with an integrated data security broker from its Baffle acquisition. The solution's CLI-based rapid response functionality enables swift connection to any system, enhancing incident response effectiveness.
- **CI/CD integrations:** IBM earned a very good score because its solution provides automated security scanning, including both static application security testing (SAST) and dynamic application security testing (DAST) capabilities, while delivering cloud-native security features that ensure continuous protection throughout the application lifecycle.
- **Auto-discovery of workloads:** IBM earned a good score for implementing a hybrid approach that combines agent-based discovery for on-premises and Kubernetes environments with cloud connector-based discovery.

Challenges

IBM has room for improvement in a few areas, including:

- **LLM-powered remediation suggestions:** IBM earned no score due to a complete absence of documented LLM-powered capabilities.
- **Automated configuration enforcement:** IBM scored poorly because the enforcement mechanisms are restricted to cloud resources and agent-equipped Linux hosts, notably excluding on-premises Kubernetes clusters and OpenShift environments without agents.
- **Serverless function checks:** IBM scored poorly because while the solution provides static analysis during CI/CD processes and offers runtime visibility, it lacks reactive controls for addressing identified risks in executing functions.

Purchase Considerations

The licensing model employs a graduated pricing structure by which per-node costs decrease with larger deployments, making the solution more cost-effective for extensive implementations. However, the pricing structure's complexity and variability in evaluation pricing availability may create challenges in accurate cost forecasting.

The solution's scalability presents certain limitations, particularly in on-premises environments where the absence of Helm charts restricts deployment options. While API-driven scaling works effectively for cloud environments, the agent-based approach for on-premises workloads may impact scalability in hybrid scenarios. The platform's flexibility demonstrates strong cloud coverage but shows limitations in on-premises Kubernetes support, a consideration that's particularly relevant for organizations with significant hybrid infrastructure.

The user experience varies significantly across the platform, with modern interface elements contrasting sharply with legacy components. While comprehensive documentation helps mitigate these inconsistencies, the mixed interface design may impact operational efficiency and user adoption. Integration capabilities align with industry standards, though the dependency on feature releases for new integrations requires careful evaluation of existing partnerships against organizational requirements.

Use Cases

IBM's strengths in workload detection and response, CI/CD integration, and auto-discovery of workloads make it an ideal choice for organizations seeking robust security solutions in dynamic environments. With advanced ML capabilities and a CLI-based rapid response system, IBM excels in threat detection and incident response. It supports continuous application security through automated SAST and DAST scans, benefiting DevOps teams focusing on CI/CD pipelines.

IBM's strengths in workload detection and response, CI/CD integration, and auto-discovery of workloads make it an ideal choice for organizations seeking robust security solutions in dynamic environments. With advanced ML capabilities and a CLI-based rapid response system, IBM excels in threat detection and incident response. It supports continuous application security through automated SAST and DAST scans, benefiting DevOps teams focusing on CI/CD pipelines.

IBM's hybrid discovery approach caters to both on-premises and cloud environments, making it a strong candidate for organizations with diverse IT infrastructure, particularly those in industries with stringent security needs, such as finance and healthcare.

Orca Security

Solution Overview

Orca Security delivers security through its agentless platform, focusing on visibility and risk management across cloud environments. The company's innovative SideScanning technology enables deep workload inspection without requiring agent deployment.

The Orca Cloud Security Platform operates as a unified solution, offering integrated capabilities for workload protection, vulnerability management, compliance monitoring, and cloud security posture management. The platform's architecture leverages read-only access to cloud provider APIs and workload runtime block storage, enabling comprehensive security coverage without operational impact.

Orca's approach emphasizes simplified deployment and reduced operational overhead through its agentless architecture while maintaining visibility into CWS risks.

Positioned in the Maturity half of the Radar chart, Orca Security demonstrates a steady progression of features and enhancements that looks and feels the same year over year. The platform's continuous evolution focuses primarily on expanding cloud provider coverage, enhancing detection capabilities, and strengthening integration with enterprise security workflows, demonstrating Orca's commitment to innovation in CWS.

Orca is positioned as a Leader and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Orca scored well on a number of decision criteria, including:

- **Automated compliance checks:** Orca earned a top score due to leveraging its SideScanning technology and comprehensive API checks to monitor compliance across more than 125 frameworks, including PCI, SOC 2, HIPAA, FedRAMP, and ISO standards.
- **LLM-powered remediation suggestions:** Orca earned a very good score due to its effective use of major cloud AI services to generate contextual remediation instructions for security alerts.
- **Serverless function checks:** Orca earned a strong score for applying its core security capabilities successfully to serverless functions with the same level of effectiveness as traditional workloads.

Challenges

Orca has room for improvement in a few areas, including:

- **Workload microsegmentation:** Orca earned no score because it is not available in the solution.
- **Hybrid environment support:** Orca scored poorly due to its limitations with hybrid environments. Although visibility is achieved, Orca is unable to react or control actions in hybrid environments.

Purchase Considerations

The vendor's licensing model demonstrates exceptional transparency, earning a perfect score for its straightforward pricing structure and well-defined support services. This clarity in pricing and support terms enables organizations to forecast costs and resource requirements accurately.

The solution shows strong scalability for cloud-hosted workloads, effectively serving both large and small organizations. However, hybrid environment capabilities, while improving with recent agent-based features, currently lag behind market leaders. This consideration is particularly relevant for organizations with significant hybrid infrastructure requirements.

Implementation and operational aspects are notably positive. Orca's intuitive user interface and straightforward SideScanning deployment methodology significantly reduce operational complexity. The integration of LLM technology for remediation guidance further enhances usability, streamlining security management processes.

The platform's ecosystem integration capabilities are comprehensive, featuring strong partnerships with major DevOps platforms (GitHub, Jenkins, GitLab, CircleCI) and extensive SIEM and security orchestration, automation, and response (SOAR) integrations. This broad integration framework enables seamless incorporation into existing security and development workflows.

Use Cases

Orca Security's platform particularly excels in environments requiring stringent compliance monitoring and risk management because of its exceptional compliance checking feature.

The platform addresses key cloud security use cases through its agentless architecture, supporting cloud workload protection, vulnerability management, and compliance monitoring. The SideScanning technology enables effective coverage across multicloud environments, container security, and cloud-native application protection. The solution's automated risk prioritization and remediation capabilities make it particularly effective for organizations prioritizing operational efficiency alongside robust security measures, though some hybrid environment use cases may require additional consideration due to evolving agent-based capabilities.

Palo Alto Networks: Prisma Cloud*

Solution Overview

Palo Alto Networks delivers comprehensive cloud security through its Prisma Cloud platform, representing the company's strategic focus on cloud security. The solution integrates cloud workload protection with broader cloud security capabilities, leveraging the vendor's extensive security solution set and threat intelligence network.

Solution Overview

Palo Alto Networks delivers comprehensive cloud security through its Prisma Cloud platform, representing the company's strategic focus on cloud security. The solution integrates cloud workload protection with broader cloud security capabilities, leveraging the vendor's extensive security solution set and threat intelligence network.

Prisma Cloud operates as a unified platform offering multiple integrated modules, including Workload Security, CSPM, CIEM, and Cloud Network Security. These components work in concert to provide comprehensive protection across cloud environments while maintaining consistency with Palo Alto Networks' established security framework.

The vendor positions Prisma Cloud as a CNAPP, targeting organizations requiring sophisticated cloud security controls across multiple environments. This approach aligns with the strategy of providing integrated security solutions that address the full spectrum of cloud security requirements.

Positioned in the Maturity half of the Radar, Palo Alto Networks demonstrates a methodical approach to solution development. The vendor prioritizes stability and proven security practices, focusing on systematic improvements to existing capabilities rather than rapid feature iteration. This strategy emphasizes reliable performance and consistent user experience, particularly in areas such as threat detection, compliance management, and cloud-native security controls.

Palo Alto Networks is positioned as a Leader and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Palo Alto Networks scored well on a number of decision criteria, including:

- **Workload microsegmentation:** Palo Alto Networks earned a top score for its comprehensive microsegmentation capabilities. The solution provides identity-based microsegmentation for containerized workloads through both virtual and physical firewall integrations. Its policy builder uses a GUI-based model with predefined identities, which are discovered through Kubernetes analysis, enabling straightforward policy creation and effective implementation.
- **Automated compliance checks:** Palo Alto Networks earned an excellent score because it demonstrates comprehensive coverage with 75 industry standards and 1,500 prebuilt checks and policies.
- **Serverless function checks:** Palo Alto Networks earned a top score because its solution integrates threat detection, compliance monitoring, and vulnerability management capabilities with DevOps processes, ensuring consistent security coverage for serverless functions.

Challenges

Palo Alto Networks has room for improvement in a few areas, including:

- **Hybrid environment support:** Palo Alto Networks scored very well. Although hybrid environments are generally well supported, the reliance on physical or virtual firewalls to achieve this could be a challenge for organizations that are unable to employ Palo Alto Networks firewalls.
- **Workload detection and response:** While Palo Alto Networks' consistent detection and response (D&R) capabilities across on-premises and cloud environments is generally a strength, this unified approach could present challenges for organizations undergoing gradual, phased cloud migrations. Companies that need to maintain different security postures or compliance requirements between their on-premises and cloud environments (common in regulated industries like healthcare or finance) may find the "one-size-fits-all" approach too rigid.

Purchase Considerations

The vendor's licensing model demonstrates standard market transparency, with costs tracking through the Prisma portal and including basic 8x5 support coverage. While pricing aligns with market averages, the clear cost visibility helps organizations accurately forecast their security investments.

The solution excels in scalability, earning top marks for its versatile deployment options across both cloud and on-premises environments. This architectural flexibility, combined with multiple collection methods, including agent-based approaches and firewall integration, enables efficient scaling to meet diverse enterprise requirements. The platform's unified interface across the Prisma ecosystem significantly reduces the learning curve, while automated workflows and dynamic visualizations streamline common security operations.

The consistent user interface across Prisma products accelerates adoption for organizations already using other Palo Alto Networks solutions. Integration capabilities are exceptional, benefiting from the vendor's extensive ecosystem partnerships and broader platform capabilities.

The solution's deployment model effectively supports both cloud and hybrid environments through agent-based protection and firewall collection capabilities.

Use Cases

The platform addresses core cloud security use cases through an integrated approach, supporting cloud workload protection, container security, and CSPM. The solution particularly excels in complex deployment scenarios, including multicloud environments, cloud-native application security, and DevSecOps integration. The platform's automated risk assessment and threat detection capabilities make it especially effective for organizations requiring comprehensive security coverage with strong compliance controls and operational efficiency.

Prisma Cloud's focus on automated security operations and integrated threat intelligence provides particular value for enterprises prioritizing advanced threat detection and response capabilities across their cloud infrastructure.

Qualys: TotalCloud

Solution Overview

Qualys delivers CWS through its TotalCloud platform, leveraging the company's extensive vulnerability management expertise to provide comprehensive cloud security capabilities.

TotalCloud operates as part of Qualys's Cloud Platform, offering integrated modules for cloud workload protection, container security, cloud detection and response (CDR), cloud identity and entitlement management (CIEM), cloud workflow automation, SaaS security posture management, and CSPM. The platform architecture combines agent-based and agentless approaches, including snapshot-based scanning, network scanning, and CSP API scanning, to provide comprehensive visibility and control across multicloud and hybrid environments.

TotalCloud operates as part of Qualys's Cloud Platform, offering integrated modules for cloud workload protection, container security, cloud detection and response (CDR), cloud identity and entitlement management (CIEM), cloud workflow automation, SaaS security posture management, and CSPM. The platform architecture combines agent-based and agentless approaches, including snapshot-based scanning, network scanning, and CSP API scanning, to provide comprehensive visibility and control across multicloud and hybrid environments.

Qualys positions TotalCloud as particularly suited for organizations requiring sophisticated vulnerability management and automated security controls. Positioned in the Innovation half of the Radar chart, Qualys demonstrates an aggressive approach to platform development. The vendor frequently introduces new capabilities and feature enhancements, particularly in areas of automated vulnerability assessment and cloud-native security controls. Its rapid development cycle and focus on emerging technologies indicate a solution that will likely evolve significantly over the contract lifecycle.

The TotalCloud platform shows continuous innovation in key areas, including vulnerability detection accuracy, compliance automation, and cloud-native security controls. This reflects Qualys's commitment to advancing CWS through technological innovation. The vendor's focus on rapid feature development and integration of emerging technologies positions it well for addressing evolving cloud security challenges.

Qualys is positioned as a Leader and Outperformer in the Innovation/Platform Play quadrant of the CWS Radar report.

Strengths

Qualys scored well on a number of decision criteria, including:

- **Hybrid environment support:** Qualys earned a top score due to its comprehensive multicloud, on-premises, legacy, and containerized scanning capabilities. The unique implementation of network scanning combined with agent-based, agentless, and API-driven approaches provides unmatched visibility across diverse environments, setting Qualys apart from competitors in hybrid infrastructure protection.
- **Auto-discovery of workloads:** Qualys earned an excellent score due to its sophisticated combination of configurable inventory scanning, internet-facing asset discovery, network sensors, and agent-based detection. This multilayered approach, particularly the integration of attack surface management (ASM)-style internet scanning with network telemetry, delivers superior asset discovery capabilities across complex environments.
- **Automated configuration enforcement:** Qualys earned an excellent score due to its ability to enforce configurations consistently across cloud and on-premises environments, supported by an extensive library of ready-to-use enforcement actions. The integration of QFlow for custom remediation workflows further enhances this capability, providing granular control over security policy implementation.

Qualys is classified as an Outperformer based on its exceptional momentum in platform development and feature innovation. The vendor's aggressive development roadmap has yielded significant advancements in cloud workload protection capabilities, particularly in the areas of automated threat response and vulnerability management.

Challenges

Qualys has room for improvement in a few areas, including:

- **LLM-powered remediation suggestions:** Qualys earned a subpar score due to limitations in its implementation of AI-driven security guidance. While the solution employs LLM and neural network technology to generate predefined remediation recommendations, it includes deep learning CDR capabilities which are able to provide guided remediation steps based on user input. This restriction in user interaction reduces the practical utility of the AI-powered features, particularly when security teams need to understand complex remediation scenarios or adapt recommendations to specific environments.
- **Workload microsegmentation:** Qualys did not score well due to reliance on eBPF for identity-based zero-trust workload policies, which, while technically sophisticated, presents limitations in comprehensive network security control. The absence of direct creation or suggestion capabilities for network access control lists (ACLs), firewall rules, and web application firewall (WAF) configurations restricts organizations' ability to implement comprehensive microsegmentation strategies.

Purchase Considerations

The vendor's token-based pricing model (QLUs) for cloud resources demonstrates exceptional transparency and flexibility. It allows organizations to reallocate capabilities without requiring relicensing. This approach, combined with comprehensive try-before-buy access to features, enables accurate cost forecasting and risk-free evaluation.

The solution shows moderate scalability characteristics, particularly in microsegmentation capabilities, due to eBPF-based implementation limitations. While remediation guidance is robust, the absence of interactive LLM capabilities may increase operational overhead for security teams managing complex environments. However, the platform's three-step onboarding process, supported by Terraform and CloudFormation automation, significantly streamlines deployment.

Implementation considerations reveal positive benefits, with the TruRisk Insights dashboard enabling rapid identification and remediation of security issues. The API-driven architecture with role-based access controls (RBAC) facilitates comprehensive integration with CI/CD tools (Jenkins, Bamboo, CircleCI, Azure DevOps), SIEM platforms, and ServiceNow for IT service management (ITSM), demonstrating strong enterprise readiness.

While the solution's flexibility is impacted by limitations in LLM-powered remediation and eBPF-based approaches, it remains robust due to strong performance across other key features. Organizations should carefully evaluate these considerations alongside their specific requirements for CWS, particularly noting the balance between automated capabilities and potential operational overhead.

Use Cases

The vendor's extensive vulnerability management heritage enables robust compliance controls and automated security measures across hybrid environments.

The solution demonstrates particular strength in vulnerability management use cases, leveraging its extensive scanning capabilities and threat intelligence network for comprehensive risk assessment. Qualys's automated vulnerability prioritization and remediation workflows make it especially effective for organizations requiring sophisticated vulnerability management across diverse environments, while its network scanning capabilities provide unique visibility advantages over competitors.

SentinelOne

organizations requiring sophisticated vulnerability management across diverse environments, while its network scanning capabilities provide unique visibility advantages over competitors.

SentinelOne

Solution Overview

SentinelOne delivers cloud workload protection through its Singularity Cloud platform, extending the company's endpoint security expertise into comprehensive workload security. The solution integrates cloud-native security capabilities with SentinelOne's established threat detection and response framework, leveraging its AI-driven approach to security.

Following the acquisition of Attivo Networks in 2022, SentinelOne enhanced its cloud security capabilities with advanced identity protection and deception technology. The Singularity Cloud platform operates as part of the broader Singularity security ecosystem, offering integrated modules for cloud workload protection, container security, and CSPM.

The vendor positions Singularity Cloud as particularly suited for organizations requiring sophisticated threat detection and automated response capabilities across cloud environments. This approach aligns with SentinelOne's strategy of providing AI-powered security solutions that address evolving cloud security challenges.

SentinelOne's position in the Innovation half of the Radar reflects its aggressive approach to platform development. The vendor demonstrates a commitment to rapid feature advancement, particularly in AI/ML-driven security capabilities and automated response mechanisms. Its development strategy emphasizes frequent updates and new feature releases, indicating a solution that will likely evolve significantly over the contract lifecycle.

SentinelOne is positioned as a Leader and Fast Mover in the Innovation/Feature Play quadrant of the CWS Radar report.

Strengths

SentinelOne scored well on a number of decision criteria, including:

- **Workload detection and response:** SentinelOne earned a top score due to the sophisticated implementation of multiple AI engines covering static analysis, behavioral monitoring, and application control.
- **LLM-powered remediation suggestions:** SentinelOne earned another top score due to its innovative "Purple AI" technology, which provides transparent, secure remediation guidance without compromising customer data.
- **Serverless function checks:** SentinelOne earned a very good score by applying the same comprehensive security scrutiny to serverless functions as to traditional workloads, ensuring consistent protection across all deployment models.

Challenges

SentinelOne has room for improvement in a few areas, including:

- **Auto-discovery of workloads:** SentinelOne earned an average score due to its unique but potentially limited eBPF-based discovery approach, which is less comprehensive than leading solutions.
- **Workload microsegmentation:** SentinelOne earned no score due to the complete absence of this capability.
- **Automated compliance checks:** SentinelOne earned an average score for providing coverage of major compliance frameworks like HIPAA, PCI, and SOC 2 while lacking support for less common regulatory requirements.

Purchase Considerations

The vendor's licensing model demonstrates standard market transparency, with per-workload pricing and basic product support included. While professional services are available, the pricing structure aligns with industry averages, enabling straightforward cost forecasting for most organizations.

The solution shows strong scalability despite the inherent limitations of its eBPF agent-based architecture. The integration of Purple AI technology enhances operational efficiency by reducing the need for specialized expertise, while comprehensive CI/CD integrations enable automated security processes. This combination helps organizations scale their security operations effectively, though the agent deployment requirement should be considered in large-scale implementations.

Implementation considerations are positive. The platform's intuitive user interface, enhanced by Purple AI capabilities, significantly reduces operational complexity and enables less experienced teams to maintain robust security practices. This emphasis on usability, combined with comprehensive risk coverage, accelerates time to value and reduces training requirements.

The solution's ecosystem integration capabilities are exceptional, featuring extensive partnerships with major security and IT operations platforms. Native integrations span SIEM, SOAR, secure access service edge (SASE), identity providers, and threat intelligence platforms, including industry leaders like Splunk, ServiceNow, and Mandiant. This broad integration framework enables seamless incorporation into existing security workflows.

Use Cases

The solution excels in specific use cases, including automated threat detection and response, particularly through its Purple AI implementation, which enhances security operations efficiency. The platform particularly appeals to organizations prioritizing automated security operations and those requiring sophisticated threat detection capabilities. The solution's strength in runtime protection and container security makes it effective for organizations with containerized workloads and those implementing DevSecOps practices, though organizations seeking comprehensive cloud security coverage may need to supplement with additional solutions.

The vendor's focus on AI-driven security operations and automated response capabilities provides particular value for security teams seeking to enhance operational efficiency while maintaining robust protection.

Sophos*

Solution Overview

Sophos delivers cloud workload protection through its Cloud Native Security platform, leveraging the company's extensive experience in endpoint security and threat detection.

Solution Overview

Sophos delivers cloud workload protection through its Cloud Native Security platform, leveraging the company's extensive experience in endpoint security and threat detection.

The solution operates as part of Sophos's unified security ecosystem, with Cloud Workload Protection integrating with its broader security portfolio. The solution combines workload protection, container security, and CSPM through a centralized management console, Sophos Central. This integration enables comprehensive visibility and control across cloud environments while maintaining consistency with existing Sophos security frameworks.

Sophos positions its CWS solution as particularly suited for organizations requiring advanced threat detection and automated response capabilities. This approach aligns with a strategy of providing integrated security solutions that leverage the vendor's extensive threat intelligence network.

The solution shows progress in key areas, including advanced threat detection, automated response capabilities, and integration with cloud-native services.

Sophos is positioned as an Entrant and Forward Mover in the Maturity/Feature Play quadrant of the CWS Radar report.

Strengths

Sophos scored well on a number of decision criteria, including:

- **Workload detection and response:** Sophos earned a very good score due to its strong agent-based detection and response capabilities for both Linux and Windows environments. The solution's Linux agent can be deployed as a daemon set, and the solution offers integration capabilities to perform image scanning predeployment.
- **CI/CD integration:** Sophos earned a satisfactory score because it offers good support for major container registries (ECR, ACR, Docker Hub) and infrastructure-as-code platforms (Terraform, CloudFormation, Ansible, Kubernetes, ARM) while maintaining essential source control integrations with GitLab and GitHub.
- **Automated configuration enforcement:** Sophos earned a good score due to its policy enforcement capabilities through its Sophos Protection for Linux agent (SPL) and its Sophos Linux Sensor (SLS), though the reliance on two agents for implementation introduces some limitations compared to API-driven or side-scanning alternatives available in the market.

Challenges

Sophos has room for improvement in a few areas, including:

- **Serverless function checks:** Sophos earned no score due to this feature being absent in the solution, though it is a roadmap item expected soon.
- **LLM-powered remediation suggestions:** Sophos earned no score due to this feature being absent in the solution, but it is a roadmap item expected soon.
- **Workload microsegmentation:** Sophos earned no score because this emerging feature is not found in the solution.

Sophos was classified as a Forward Mover because it was missing LLM-powered remediation suggestions, workload microsegmentation features, and serverless function checks, while earning average scores on other key features.

Purchase Considerations

The vendor's licensing model demonstrates good transparency, offering straightforward pricing structures and support packages at competitive rates. This pricing approach particularly benefits existing Sophos customers, who can leverage their current investments to expand into CWS.

The solution's scalability presents moderate challenges due to its reliance on dual agent deployment (sensor and traditional agent) for comprehensive protection. While the agent-based architecture provides reliable security coverage and flexibility in some situations, it may introduce deployment complexity and potential operational overhead in large-scale environments. This dual-agent requirement also impacts the solution's flexibility, potentially limiting its applicability in certain use cases and deployment scenarios.

Implementation considerations reveal standard market complexity. While the user interface is intuitive and well designed, this level of usability aligns with industry standards rather than exceeding them.

The platform's ecosystem integration capabilities demonstrate average depth and breadth, offering standard connectivity with common enterprise technologies without notable advantages or disadvantages compared to competitors.

Use Cases

The solution does well in endpoint-based workloads. Its emphasis on runtime protection and vulnerability management makes it effective for organizations prioritizing compliance automation. While the platform offers good security capabilities, its strength in container security and compliance automation makes it particularly valuable for organizations focusing on these specific requirements, though those seeking comprehensive cloud security coverage may need to supplement it with additional solutions.

Sysdig: Secure

Solution Overview

Sysdig delivers cloud-native security through its Secure platform, focusing on container and Kubernetes security with an emphasis on runtime threat detection and response. The company's expertise in container security and deep system visibility sets it apart in the CWS market.

The Sysdig Secure solution operates as part of the broader Sysdig cloud-native security platform, which includes integrated modules for CSPM, vulnerability management, and compliance monitoring. The solution leverages Sysdig's open source Falco project for container runtime security, complemented by proprietary technologies for comprehensive workload protection.

Sysdig positions its security solution as a cloud-native first platform, particularly suited for organizations with significant container and Kubernetes deployments. This focused approach aligns with its strategy of providing specialized security solutions that address the unique challenges of cloud-native environments.

The platform shows continuous improvement in key areas like container runtime security, cloud-native threat detection, and Kubernetes-specific security

Sysdig positions its security solution as a cloud-native first platform, particularly suited for organizations with significant container and Kubernetes deployments. This focused approach aligns with its strategy of providing specialized security solutions that address the unique challenges of cloud-native environments.

The platform shows continuous improvement in key areas like container runtime security, cloud-native threat detection, and Kubernetes-specific security controls.

Sysdig is positioned as a Leader and Outperformer in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Sysdig scored well on a number of decision criteria, including:

- **Workload detection and response:** Sysdig earned a top score due to its agentless approach, combined with comprehensive identity protections, drift control, and attack lineage tracking, enabling organizations to reduce incident analysis time to (a claimed) five minutes.
- **Auto-discovery of workloads:** Sysdig earned a top score for implementing a hybrid approach that combines agentless cloud resource discovery with agent-based real-time monitoring. This dual methodology enables instant threat and vulnerability detection while enriching discovered workloads with contextual data from across the customer's environment, providing comprehensive visibility and control.
- **CI/CD integration:** Sysdig earned another excellent score due to offering comprehensive support for numerous DevOps platforms like GitHub, Jenkins, Backstage, Terraform, and leading container registries like ECR and Artifactory.

Sysdig was classified as an Outperformer based on its impressive feature release history and aggressive roadmap. Consistent delivery of new or enhanced capabilities and rapid response to emerging security challenges positions Sysdig at the forefront of CWS evolution.

Challenges

Sysdig has room for improvement in a few areas, including:

- **Serverless function checks:** Sysdig earned an average score because the solution provides vulnerability and threat detection for major serverless platforms, including AWS Lambda, Fargate, and Google Cloud Run, through Falco integration. However, the deployment options remain limited.
- **Workload microsegmentation:** Sysdig earned an average score because the microsegmentation features are primarily restricted to Kubernetes resources.

Purchase Considerations

The vendor's licensing model demonstrates strong transparency, with support services included in the base cost. Customer feedback consistently highlights frictionless setup processes that reduce implementation expenses and accelerate time to value.

The solution shows excellent scalability through its stateless microservices architecture, employing daemon sets for container workload scaling and agent-based protection for VMs. This approach enables efficient resource utilization while maintaining consistent performance across growing deployments. As a Platform Play, Sysdig requires consideration as a primary security solution, though its comprehensive feature set justifies the potential displacement of existing tools.

The platform's intuitive interface and streamlined deployment processes significantly reduce operational complexity. The integration of Sage AI technology enhances user expertise through contextual guidance and explanations, effectively supporting staff development while maintaining security effectiveness.

The solution's ecosystem integration capabilities are robust, featuring extensive partnerships with both Sysdig's native offerings and third-party security tools. This broad integration framework enables seamless incorporation into existing security workflows while maintaining flexibility for future adaptations.

Use Cases

The platform addresses core cloud security use cases through an integrated approach, leveraging its deep visibility capabilities for cloud workload protection, container security, and compliance monitoring. Its solution particularly excels in complex deployment scenarios, including multicloud environments, Kubernetes security, and DevSecOps integration. The platform's automated risk assessment and threat detection capabilities, enhanced by Sage AI, make it especially effective for organizations requiring comprehensive security coverage with strong operational efficiency.

Sysdig's focus on automated security operations and integrated threat intelligence provides particular value for enterprises prioritizing advanced threat detection and compliance capabilities across their cloud infrastructure.

Tenable: Cloud Security*

Solution Overview

Tenable delivers CWS through its integrated Cloud Security CNAPP platform, leveraging the company's extensive vulnerability management expertise. Following its strategic acquisition of Accurics in 2021 and Ermetic (a complete CNAPP solution) in 2023, Tenable has enhanced its cloud-native security capabilities, particularly in infrastructure as code (IaC) security and cloud configuration assessment.

The solution operates as part of Tenable's broader security portfolio or as a standalone solution. As a standalone CNAPP solution, it provides coverage across cloud workload protection, container security, CIEM, CSPM, KSPM, DSPM, AI-SPM, and IaC. The platform integrates with Tenable's vulnerability management capabilities, enabling unified visibility and control across cloud environments through a centralized console.

Tenable positions its Cloud Security offering as a solution particularly suited for organizations of any scale, enabling them to efficiently identify, prioritize, and address cloud and identity security risks across single and multicloud environments through a streamlined approach.

Positioned in the Maturity half of the Radar chart, Tenable demonstrates a methodical approach to solution development. The vendor prioritizes stability and proven security practices, focusing on systematic improvements to existing capabilities rather than rapid feature iteration.

Tenable is positioned as a Challenger and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Tenable scored well on a number of decision criteria, including:

Tenable is positioned as a Challenger and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Tenable scored well on a number of decision criteria, including:

- **Auto-discovery of workloads:** Tenable earned a strong score due to its comprehensive agentless-first approach, which combines cloud service integration, CMDB connectivity, and IaC template analysis to provide detailed asset discovery and correlation capabilities. This approach has additional potential for operational technology (OT) environment coverage through Tenable.ep integration.
- **CI/CD integration:** Tenable earned a very good score due to its robust integration with major Git repositories and pipeline solutions, enabling real-time security actions while maintaining seamless connectivity with ticketing systems, messaging platforms, and SIEM or data security posture management (DSPM) solutions.
- **Automated configuration enforcement:** Tenable earned a very good score for its strong policy management foundation that delivers effective enforcement actions integrated directly into security policies, ensuring consistent security control implementation across cloud environments.

Challenges

Tenable has room for improvement in a few areas, including:

- **Hybrid environment support:** Tenable earned an average score for its agent-based approach to hybrid environment management. The solution provides vulnerability management features across VMs, on-premises Kubernetes, hosted applications, and cloud environments through API connections. However, the reliance on agents for comprehensive coverage may create deployment and maintenance overhead, particularly in large-scale environments with diverse infrastructure components.
- **Workload microsegmentation:** Tenable earned no score due to the absence of this increasingly important security capability in the solution.

Purchase Considerations

The solution demonstrates strong scalability capabilities, enhanced by unique CIEM features. Additionally, it provides contextual intelligence unique to each customer's environment to provide better understanding around risks and asset risk relationships. This architecture effectively supports growing enterprise deployments, though the platform's flexibility shows some limitations in hybrid environment support and compliance checking compared to market leaders. Despite these constraints, the solution effectively addresses core cloud security use cases.

The vendor's licensing model presents some complexity, particularly in pricing structures. While standalone pricing is resource-based with volume discounts available, integration with Tenable One introduces more complex pricing calculations that may challenge accurate cost forecasting.

The platform's intuitive user interface and prominent placement of common features streamline adoption and daily operations. Tenable's extensive ecosystem integration capabilities are a standout strength developed through its long-standing market presence. The solution offers comprehensive integration with cloud providers, identity management platforms (Okta, OneLogin, Ping, and Azure AD), DevOps tools, container orchestration platforms, and enterprise systems, including ticketing, notification, and SIEM solutions.

Use Cases

The platform addresses core CWS use cases through its unified approach, leveraging its vulnerability management expertise for cloud workload protection, container security, and infrastructure assessment. The solution particularly excels in risk-based security scenarios, including vulnerability prioritization, compliance monitoring, CIEM, DSPM, and CSPM.

The platform's automated risk assessment and exposure management capabilities make it especially effective for organizations requiring comprehensive security coverage with strong compliance controls, though some specialized container security use cases may require additional consideration.

Trellix: Cloud Security*

Solution Overview

Trellix delivers CWS through its integrated XDR platform, leveraging the company's extensive threat detection and response capabilities. Following the merger of McAfee Enterprise and FireEye in 2021, Trellix has continued to evolve its cloud security offerings, combining advanced threat intelligence with comprehensive workload protection.

The solution operates as part of the broader Trellix XDR ecosystem, with Cloud Security representing a key component of the unified security platform. The architecture integrates cloud workload protection, container security, and CSPM through a centralized console, enabling comprehensive visibility and control across cloud environments.

Positioned in the Maturity half of the Radar, Trellix demonstrates a methodical approach to solution development. The vendor prioritizes stability and proven security practices, focusing on systematic improvements to existing capabilities rather than rapid feature iteration. This strategy emphasizes reliable performance and consistent user experience, particularly in areas such as threat detection, compliance management, and cloud security controls.

Trellix is positioned as a Challenger and Fast Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Trellix scored well on a number of decision criteria, including:

- **Hybrid environment support:** Trellix earned a strong score due to its comprehensive approach, combining the Trellix ePolicy Orchestrator (ePO) for agent management with an agentless cloud provider strategy. Through its integration of the Symantec acquisition, Trellix achieved feature parity across both on-premises and cloud environments.
- **CI/CD integration:** Trellix earned a very good score due to its strong implementation, which supports both hybrid and pure cloud environments through Puppet and Chef integration, comprehensive container image registry scanning, and native support for infrastructure-as-code platforms, including Terraform and CloudFormation.
- **Workload microsegmentation:** Trellix earned a very good score for its sophisticated capabilities, including ML-driven risk-based microsegmentation and quarantine features for malicious assets, with consistent support across all major cloud providers.

~ "

Terraform and CloudFormation.

- **Workload microsegmentation:** Trellix earned a very good score for its sophisticated capabilities, including ML-driven risk-based microsegmentation and quarantine features for malicious assets, with consistent support across all major cloud providers.

Challenges

Trellix has room for improvement in a few areas, including:

- **Serverless function checks:** Trellix earned a subpar score. While the solution can discover functions through API connections and monitor code in repositories during predeployment stages, its runtime monitoring capabilities are notably restricted.
- **Automated configuration enforcement:** Trellix earned an average score due to its basic enforcement mechanisms. Additionally, the solution lacks a comprehensive library of preconfigured enforcement actions.
- **LLM-powered remediation suggestions:** Trellix earned no score because of a complete absence of this emerging technology in its solution.

Purchase Considerations

The platform demonstrates moderate scalability, though some limitations exist. While the core solution scales effectively, the reliance on ePO agents for VM-based assets, rather than an API-first approach, introduces friction in scaling operations. Additionally, average capabilities in compliance checks and configuration enforcement may constrain scalability of security operations in larger environments.

The vendor's licensing model presents some challenges in transparency, with pricing details not publicly available and support services requiring additional investment. While the solution can be purchased standalone or bundled with other Trellix services at a discount, the lack of included support services may impact total cost calculations.

Implementation considerations reveal mixed characteristics. The solution's intuitive interface and straightforward setup process have garnered positive user feedback regarding ease of use. However, the agent-first approach for VMs may limit deployment flexibility in certain environments. Integration capabilities align with typical enterprise requirements, though access to the full range of over 450 integrations requires additional investment in the Trellix XDR solution.

Use Cases

The platform addresses numerous cloud workload use cases through its unified XDR approach, supporting cloud workload protection, container security, and CSPM. The solution excels in complex deployment scenarios, including multicloud environments, cloud-native application security, and DevSecOps integration. The platform's automated risk assessment and threat detection capabilities make it especially effective for organizations requiring comprehensive security coverage with strong compliance controls and operational efficiency.

Trend Micro: Vision One*

Solution Overview

Trend Micro delivers CWS through its Vision One platform, leveraging the company's cybersecurity expertise and threat intelligence network. The solution integrates cloud workload protection with broader security capabilities, providing comprehensive coverage across cloud environments and traditional infrastructure.

Vision One operates as a unified security platform, incorporating Cloud One Workload Security alongside complementary modules for container security, application security, and CSPM. These components work in concert through a centralized console, enabling security policy enforcement and threat detection across diverse environments.

Trend Micro positions Vision One as a solution suited for organizations requiring threat detection and automated response capabilities across hybrid environments. Positioned in the Maturity half of the Radar, Trend Micro demonstrates a methodical approach to solution development.

Trend Micro is positioned as a Challenger and Forward Mover in the Maturity/Platform Play quadrant of the CWS Radar report.

Strengths

Trend Micro scored well on a number of decision criteria, including:

- **LLM-powered remediation suggestions:** Trend Micro earned a strong score due to its Trend Companion AI assistant. This technology enhances security operations by accelerating risk identification and providing guided remediation.
- **Automated compliance checks:** Trend Micro earned a top score because the solution covers major standards, including AWS Well-Architected, Azure Well-Architected Framework, Google Cloud Architecture Framework, NIST 800-53, CIS benchmarks for major cloud providers, and industry-specific regulations like PCI, HIPAA, GDPR, and ISO 27001.
- **Automated configuration enforcement:** Trend Micro earned a very good score for leveraging its XDR integration to deliver detection and response capabilities that enhance workload configuration enforcement.

Challenges

Trend Micro has room for improvement in a few areas, including:

- **Auto-discovery of workloads:** Trend Micro earned an average score due to the solution's reliance on an agentless approach, which, while efficient for certain scenarios, inhibits comprehensive workload discovery. The presence of an agent doesn't contribute to discovery functionality, potentially leaving gaps in asset visibility across complex environments.
- **CI/CD integration:** Trend Micro earned an average score because, while the solution supports Azure DevOps pipelines and Jenkins, integration with other development platforms remains limited. Though the vendor indicates support for "leading container platforms," suggesting compatibility with Docker Hub, Nexus, and GitHub, the lack of explicit, comprehensive integration support may impact organizations with diverse development toolchains.
- **Serverless function checks:** Trend Micro earned an average score because the solution provides only fundamental runtime protection for serverless functions and guards against OWASP's top 10 vulnerabilities, offering visibility into serverless application attacks; these capabilities represent baseline functionality rather than advanced protection measures.

While Trend Micro maintains solid performance across key features, its classification as a Forward Mover reflects a slower pace of development compared to market peers. Its established feature set, while comprehensive, shows slower enhancement rates than competitors do.

functions and guards against OWASP's top 10 vulnerabilities, offering visibility into serverless application attacks; these capabilities represent baseline functionality rather than advanced protection measures.

While Trend Micro maintains solid performance across key features, its classification as a Forward Mover reflects a slower pace of development compared to market peers. Its established feature set, while comprehensive, shows slower enhancement rates than competitors do.

Purchase Considerations

As a Platform Play, the solution requires consideration as a primary security tool, potentially necessitating displacement of existing solutions to fully leverage its integrated capabilities.

The platform demonstrates moderate scalability through its agent-based architecture. While this approach ensures consistent security coverage, organizations must factor in agent management overhead when planning large-scale deployments. The solution's integration with Trend Micro's broader security ecosystem provides enhanced functionality, though this tight integration may influence deployment decisions for organizations not currently using other Trend Micro products.

User feedback from various sources indicates average usability, though the interface and operational experience align with industry standards rather than exceeding them. The solution's ecosystem integration capabilities are notable, featuring strong partnerships with technology providers and seamless integration within the Trend Micro portfolio.

Use Cases

This solution excels in environments requiring sophisticated compliance controls and automated security measures across hybrid infrastructures.

The platform particularly stands out in complex deployment scenarios where traditional agent-based security meets modern cloud-native requirements. Its XDR integration makes it especially effective for organizations prioritizing integrated threat detection and response across diverse environments. The platform's automated risk assessment and remediation capabilities make it particularly valuable for organizations with limited security expertise, as its AI-driven controls can effectively guide security operations teams through complex threat scenarios.

Wiz*

Solution Overview

Wiz delivers cloud security through its unified security platform, focusing on comprehensive visibility and risk management across cloud environments. The company has rapidly established itself as a significant player in cloud security, leveraging advanced analytics and automation to provide deep insights into cloud security posture.

The Wiz cloud security platform operates as a unified solution, offering integrated capabilities for cloud workload protection, vulnerability management, and security posture management. The solution's architecture emphasizes agentless deployment and API-driven security controls, enabling comprehensive coverage without operational overhead. Key components include CIEM, CSPM, and CWPP capabilities.

Wiz positions its platform as a cloud security solution suited for organizations requiring sophisticated risk analysis and automated security controls. This approach aligns with its strategy of providing comprehensive visibility and protection across cloud environments while maintaining operational simplicity.

Wiz is positioned in the Innovation half of the Radar chart and demonstrates an aggressive approach to platform development. Wiz frequently introduces new capabilities and features, particularly in areas of risk analysis, threat detection, and automated remediation. Its rapid development cycle and focus on emerging technologies indicate a solution that will evolve significantly over the contract lifecycle, reflecting a commitment to addressing emerging cloud security challenges through technological advancement.

Wiz is positioned as a Leader and Fast Mover in the Innovation/Platform Play quadrant of the CWS Radar report.

Strengths

Wiz scored well on a number of decision criteria, including:

- **Workload detection and response:** Wiz earned a top score due to its sophisticated graph-based threat detection approach. The solution combines agentless and agent-based telemetry to create comprehensive "issues" that incorporate multiple contextual elements, including internet exposure, CVSS scores, misconfigurations, adjacent vulnerabilities, and identity risks.
- **Auto-discovery of workloads:** Wiz earned an excellent score because it implements an agentless approach that ensures comprehensive coverage across all cloud assets. The solution excels in identifying complex relationships between assets, including network visibility, shared identities, resources, and events.
- **Automated compliance checks:** Wiz earned an excellent score due to offering extensive support for major compliance frameworks, including CIS, PCI, NIST, HIPAA, and GDPR. The solution performs automatic assessments against all frameworks across cloud configurations, operating systems, workloads, and applications.

Challenges

Wiz has room for improvement in a few areas, including:

- **Automated configuration enforcement:** While Wiz earned a strong score for its automated configuration enforcement capabilities, the solution's reliance on custom playbook creation may present challenges for organizations with limited cloud security expertise or resources. Organizations with rapid deployment cycles or those requiring frequent playbook updates may find the customization requirements time-consuming, despite the robust automation capabilities.
- **Workload microsegmentation:** Wiz earned no score due to the lack of microsegmentation, a feature that represents a significant gap in network security controls, particularly for organizations requiring granular network isolation and policy enforcement capabilities.

Purchase Considerations

Through its SaaS-first architecture, the solution exhibits excellent scalability characteristics. While the initial setup of on-premises components (Wiz Outpost, VMware integration) requires careful planning, these elements don't impede ongoing scaling. The platform's automation capabilities and graph-based visualization tools enhance operational efficiency, enabling effective security management even as deployments grow.

Purchase Considerations

Through its SaaS-first architecture, the solution exhibits excellent scalability characteristics. While the initial setup of on-premises components (Wiz Outpost, VMware integration) requires careful planning, these elements don't impede ongoing scaling. The platform's automation capabilities and graph-based visualization tools enhance operational efficiency, enabling effective security management even as deployments grow.

The vendor offers transparent pricing, with costs aligning favorably against feature availability. It also includes comprehensive support and sales engineer access during onboarding. This clarity in pricing structure enables accurate cost forecasting and ROI assessment for organizations of varying sizes.

Implementation considerations are notably positive. The platform's "issues" concept streamlines security operations by consolidating risk information into comprehensible, actionable events. Deployment flexibility through agentless options and preconfigured Helm charts for sensor deployment significantly reduces implementation complexity.

While the integration catalog is substantial, it may not cover all enterprise requirements without additional configuration.

Use Cases

Wiz demonstrates comprehensive coverage across major industry verticals through its agentless security platform. The platform addresses workload security use cases through its unified approach, supporting cloud workload protection, container security, and cloud security posture management.

Wiz particularly excels in risk-based security scenarios, including vulnerability prioritization, multicloud security, and automated compliance monitoring. The platform's graph-based architecture and automated risk assessment capabilities make it especially effective for organizations requiring additional security expertise.

6. Analyst's Outlook

The CWS market has reached a maturity inflection point characterized by the convergence of traditional security capabilities with emerging AI-driven features. Leading vendors now offer comprehensive platforms that combine vulnerability management, threat detection, and automated response capabilities. The market shows a clear differentiation between Platform Players offering comprehensive security suites and specialized vendors focusing on specific capabilities like container security or compliance automation.

Key market developments include the integration of AI/ML capabilities for threat detection and response, enhanced automation for security operations, and improved integration with DevOps workflows. The acquisition of Lacework by Fortinet signals continued market consolidation, suggesting enterprises should carefully evaluate vendor stability and long-term viability in their selection process.

Organizations evaluating CWS solutions should prioritize several critical factors. First, assess the alignment between your cloud infrastructure strategy and vendor capabilities, particularly in hybrid and multicloud scenarios. Consider the vendor's approach to agent deployment versus agentless monitoring, as this choice significantly impacts operational overhead and coverage completeness.

Integration capabilities with existing security tools and DevOps platforms should be a primary consideration because seamless workflow integration increasingly determines implementation success. Evaluate vendors' AI/ML capabilities pragmatically, focusing on concrete operational benefits rather than marketing promises.

Begin by conducting a comprehensive inventory of your cloud workload environment, including container deployments, serverless functions, and traditional VMs. Document specific security requirements across different workload types and compliance mandates.

Develop a clear evaluation framework that weighs vendor capabilities against your organization's specific needs, considering factors such as:

- Hybrid environment support requirements.
- Compliance automation needs.
- Requirements for integration with existing security tools.
- Operational capacity for security management.

The CWS market is evolving toward more automated, AI-driven security operations. Organizations should prepare for increased integration of security controls into development workflows and greater emphasis on automated remediation capabilities. The rise of LLM-powered security guidance suggests a future in which security operations become more intuitive and accessible to teams with varying expertise levels.

The successful implementation of CWS will depend increasingly on an organization's ability to balance comprehensive protection with operational efficiency, leveraging automation and AI-driven capabilities while maintaining appropriate human oversight and control.

To learn about related topics in this space, check out the following GigaOm Radar reports:

- CNAPP, CIEM, CSPM
- [GigaOm Radar for Cloud-Native Application Protection Platforms \(CNAPPs\) v1.0](#)
- [GigaOm Radar for Cloud Security Posture Management \(CSPM\) v2.0](#)
- [GigaOm Radar for Cloud Infrastructure Entitlement Management \(CIEM\) v1.0](#)

7. Methodology

*Vendors marked with an asterisk did not participate in our research process for the Radar report, and their capsules and scoring were compiled via desk research.

For more information about our research process for Key Criteria and Radar reports, please visit our [Methodology](#).

8. About Chris Ray

Chris Ray is a veteran of the cyber security domain. He has a collection of experiences ranging from small teams to large financial institutions. Additionally,

8. About Chris Ray

Chris Ray is a veteran of the cyber security domain. He has a collection of experiences ranging from small teams to large financial institutions. Additionally, Chris has worked in healthcare, manufacturing, and tech. More recently, he has acquired an extensive amount of experience advising and consulting with security vendors, helping them find product-market fit as well as deliver cyber security services.

9. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

10. Copyright

© [Knowingly, Inc.](#) 2025 "GigaOm Radar for Cloud Workload Security" is a trademark of [Knowingly, Inc.](#) For permission to reproduce this report, please contact sales@gigaom.com.

Interested in more content like this? Check out GigaOm Research Reports

[SUBSCRIBE NOW](#)

GIGAOM

Did you like this content?

Subscribe to GigaOm **Premium Research** for help making decisions and purchasing technologies

\$12/month

Billed Annually

[SUBSCRIBE NOW](#)

Already a subscriber? [Sign in](#)

Yearly individual access to the latest research for making decisions and purchasing technologies
Unlimited reports

GIGAOM

Knowingly Corporation

Subscribe to our monthly analyst insights newsletter

Stay on top of emerging trends by joining our

[SUBSCRIBE NOW](#)

Research

- > Methodology
- > Vendor Escalation Policy
- > Analyst Videos
- > AI, Data & Analytics
- > Security & Risk
- > Cloud, Infrastructure & Management
- > DevOps
- > Network & Edge
- > People, Processes, & Applications
- > View All Research

For Vendors

- > Research Calendar
- > Customer Centric Enablement and Activation
- > Total Cost of Ownership & Engineering Benchmarks
- > Radars
- > Key Criteria
- > Advisory Services
- > Enterprise Subscription
- > Value Engineering
- > Vendor Marketing Content Review
- > Assets Login
- > Research Access

Insights

- > Case Studies
- > Blog
- > Video
- > Press Room

Company

- > Why GigaOm
- > Our Team
- > Partners
- > Careers
- > Contact us



Feedback

How would you rate your experience?











Hate

Love

Next