The Forrester Wave™: Cloud Workload Security, Q4 2019

The 13 Providers That Matter Most And How They Stack Up

by Andras Cser

December 9, 2019

Why Read This Report

In our 30-criterion evaluation of cloud workload security (CWS) providers, we identified the 13 most significant ones — Alert Logic, Aqua Security, Bitdefender, Cavirin, Check Point, Cisco, CloudPassage, Kaspersky, McAfee, Palo Alto Networks, Qualys, Symantec, and Trend Micro — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals select the right one for their needs.

Key Takeaways

Trend Micro, McAfee, And Bitdefender Lead The Pack

Forrester's research uncovered a market in which Trend Micro, McAfee, and Bitdefender are Leaders; Kaspersky, Qualys, Check Point, Palo Alto Networks, and CloudPassage are Strong Performers; and Symantec, Cisco, Aqua Security, Cavirin, and Alert Logic are Contenders.

Support For Containerization And OS-Level Protection Are Key Differentiators

As on-premises security suites technology becomes outdated and less effective to provide comprehensive support for cloud workloads, improved broad coverage support for guest/host OS; API-level connectivity to the infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) platform; and container orchestration and runtime platforms will dictate which providers lead the pack. Vendors that can provide cloud and on-premises-based CWS solutions position themselves to successfully deliver comprehensive cloud workload protection and posture management to their customers.

The Forrester Wave™: Cloud Workload Security, Q4 2019

The 13 Providers That Matter Most And How They Stack Up

by Andras Cser
with Merritt Maxim, Matthew Flug, and Peggy Dostie
December 9, 2019

Table Of Contents

Related Research Documents

The Forrester Wave™: Cloud Security Gateways, Q1 2019

Hybrid Cloud Security Best Practices

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Comprehensive Coverage Differentiates Offerings In The CWS Market

Customer needs in securing workloads are changing. Old-school, on-premises security tooling (security analytics/SA/SIEM), old endpoint detection and response (EDR) solutions, and vanilla password vaulting no longer cut it: Today's organizations must not only monitor and control the proliferation of cloud workloads but also do it comprehensively across multiple tiers.

As a result of these trends, cloud workload security customers should look for providers that:

- **Offer solutions for guest operating system native protection.** Many of the threats in workloads are still traditional changes to configuration files and network intrusions. S&R pros should look for CWS solutions that offer tools-file integrity monitoring, memory integrity monitoring, host-based firewalls, and intrusion detection/prevention and allow for scalable deployment of protection to a large number of workloads without interruption. Leading solutions also start to apply and expose machine learning algorithms and their tuning for admins.
- **Provide templatized API-level configuration management to IaaS and PaaS platforms.** You can't control Amazon Web Services (AWS), Azure, or Google Cloud Platform (GCP) using old-school, on-premises CMDB tools. Instead, you want tight control over instance and storage creation and network connectivity. Best practices, vulnerability, and compliance templates (CIS, CVE, or HIPAA) built into and consistently updated by vendors for managing configurations are key differentiators in this area.
- **Secure container runtimes and orchestration platforms natively.** With Kubernetes and Docker becoming de facto container environments mainly deployed on cloud platforms, S&R professionals need to be sure that: 1) they scan container images pre-runtime and runtime; 2) there are controls for any configuration drifts at the container level; and 3) they monitor network communications and system calls among containers as well as between containers and the underlying host operating system. Other differentiators include vendor-supplied and constantly updated best practices and compliance templates as well as agentless and agent-based container architectures.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and doesn't represent the entire vendor landscape. You'll find more information about this market in our reports on CWS.[1]

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

FIGURE 1 Forrester Wave™: Cloud Workload Security, Q4 2019

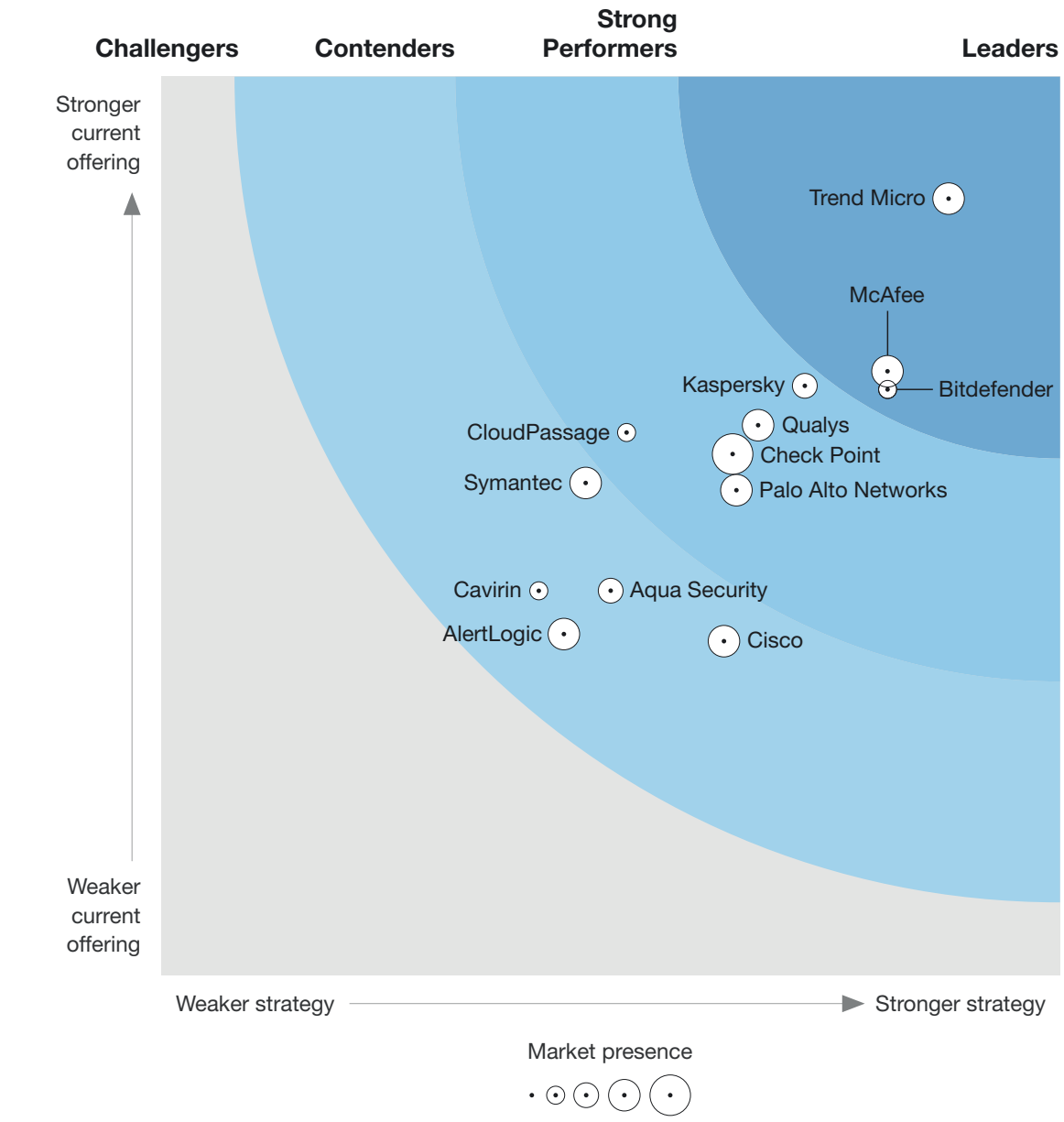

FIGURE 2 Forrester Wave™: Cloud Workload Security Scorecard, Q4 2019

	Forrester's weighting	Alert Logic	Aqua Security	Bitdefender	Cavirin	Check Point	Cisco	CloudPassage
Current offering	50%	1.90	2.14	3.26	2.14	2.90	1.86	3.02
Setup, configuration, and data integration	8%	1.00	3.00	5.00	1.00	3.00	1.00	3.00
Users and roles	8%	1.00	3.00	1.00	1.00	5.00	3.00	1.00
Operating system-level workload protection	10%	1.00	3.00	5.00	1.00	1.00	3.00	3.00
API-level connectivity and control for IaaS and PaaS	10%	3.00	1.00	3.00	5.00	5.00	1.00	5.00
Containerization and container orchestration platform protection	10%	1.00	5.00	0.00	3.00	1.00	3.00	5.00
Hypervisor protection	10%	0.00	0.00	5.00	0.00	0.00	0.00	0.00
Integration and reporting	8%	1.00	1.00	3.00	3.00	5.00	5.00	3.00
Scalability: protected cloud instances	8%	5.00	0.00	3.00	5.00	5.00	0.00	5.00
Scalability: protected containers	8%	3.00	5.00	0.00	1.00	3.00	0.00	5.00
Scalability: protected hypervisors	8%	0.00	0.00	5.00	0.00	0.00	0.00	0.00
Navigation, integrated environment	8%	5.00	3.00	5.00	3.00	5.00	5.00	3.00
Context-sensitive help	4%	3.00	1.00	5.00	3.00	3.00	1.00	3.00

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

FIGURE 2 Forrester Wave™: Cloud Workload Security Scorecard, Q4 2019 (Cont.)

	Forrester's weighting	Alert Logic	Aqua Security	Bitdefender	Cavirin	Check Point	Cisco	CloudPassage
Strategy	50%	2.24	2.50	4.04	2.10	3.18	3.13	2.59
Centralized agent framework plans	8%	1.00	1.00	5.00	3.00	3.00	3.00	5.00
API control for IaaS and PaaS plans	8%	1.00	3.00	3.00	3.00	3.00	5.00	5.00
Containerization protection plans	8%	1.00	5.00	3.00	1.00	5.00	3.00	3.00
Hypervisor protection plans	8%	0.00	0.00	5.00	1.00	0.00	3.00	0.00
Threat detection and auditing plans	8%	3.00	1.00	1.00	1.00	3.00	3.00	3.00
Solution delivery	9%	3.00	5.00	3.00	3.00	1.00	5.00	3.00
Vendor's RFP response	8%	1.00	3.00	5.00	3.00	3.00	3.00	3.00
Vendor's PoC and demonstration	8%	1.00	3.00	5.00	3.00	5.00	3.00	3.00
Services and partners	7%	5.00	1.00	5.00	1.00	3.00	0.00	0.00
Development staffing	7%	5.00	3.00	5.00	1.00	5.00	5.00	1.00
Sales staffing	7%	3.00	1.00	5.00	1.00	3.00	3.00	1.00
Support staffing	7%	3.00	3.00	3.00	1.00	3.00	1.00	1.00
Pricing terms and flexibility	7%	3.00	3.00	5.00	5.00	5.00	3.00	5.00
Market presence	0%	3.20	2.60	2.00	1.60	4.60	3.80	1.60
Total vendor revenue	20%	2.00	1.00	2.00	1.00	4.00	5.00	1.00
CWS revenue	20%	5.00	2.00	1.00	1.00	5.00	4.00	2.00
CWS revenue growth	20%	1.00	5.00	1.00	4.00	5.00	4.00	2.00
CWS direct installed base	20%	5.00	3.00	1.00	1.00	5.00	4.00	2.00
CWS indirect installed base	20%	3.00	2.00	5.00	1.00	4.00	2.00	1.00

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

FIGURE 2 Forrester Wave™: Cloud Workload Security Scorecard, Q4 2019 (Cont.)

	Forrester's weighting	Kaspersky	McAfee	Palo Alto Networks	Qualys	Symantec	Trend Micro
Current offering	50%	3.28	3.36	2.70	3.06	2.74	4.32
Setup, configuration, and data integration	8%	5.00	1.00	1.00	3.00	1.00	3.00
Users and roles	8%	3.00	5.00	3.00	5.00	3.00	3.00
Operating system-level workload protection	10%	5.00	5.00	1.00	3.00	1.00	5.00
API-level connectivity and control for IaaS and PaaS	10%	3.00	5.00	3.00	5.00	5.00	3.00
Containerization and container orchestration platform protection	10%	1.00	3.00	5.00	3.00	1.00	5.00
Hypervisor protection	10%	5.00	5.00	0.00	0.00	0.00	5.00
Integration and reporting	8%	5.00	1.00	1.00	1.00	1.00	5.00
Scalability: protected cloud instances	8%	1.00	3.00	0.00	5.00	3.00	5.00
Scalability: protected containers	8%	1.00	3.00	5.00	5.00	5.00	5.00
Scalability: protected hypervisors	8%	5.00	3.00	5.00	0.00	5.00	5.00
Navigation, integrated environment	8%	1.00	3.00	5.00	3.00	5.00	3.00
Context-sensitive help	4%	5.00	1.00	5.00	5.00	5.00	5.00

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

FIGURE 2 Forrester Wave™: Cloud Workload Security Scorecard, Q4 2019 (Cont.)

	Forrester's weighting	Kaspersky	McAfee	Palo Alto Networks	Qualys	Symantec	Trend Micro
Strategy	50%	3.58	4.04	3.20	3.32	2.36	4.38
Centralized agent framework plans	8%	1.00	5.00	1.00	3.00	3.00	5.00
API control for IaaS and PaaS plans	8%	5.00	5.00	1.00	3.00	3.00	3.00
Containerization protection plans	8%	3.00	3.00	5.00	5.00	3.00	3.00
Hypervisor protection plans	8%	5.00	5.00	0.00	5.00	1.00	5.00
Threat detection and auditing plans	8%	3.00	5.00	3.00	3.00	3.00	3.00
Solution delivery	9%	1.00	3.00	5.00	5.00	1.00	5.00
Vendor's RFP response	8%	5.00	1.00	3.00	1.00	1.00	5.00
Vendor's PoC and demonstration	8%	5.00	3.00	3.00	1.00	3.00	5.00
Services and partners	7%	3.00	5.00	3.00	5.00	3.00	5.00
Development staffing	7%	3.00	3.00	3.00	3.00	5.00	5.00
Sales staffing	7%	5.00	5.00	5.00	3.00	1.00	5.00
Support staffing	7%	5.00	5.00	5.00	5.00	1.00	5.00
Pricing terms and flexibility	7%	3.00	5.00	5.00	1.00	3.00	3.00
Market presence	0%	2.80	3.00	3.40	3.20	3.60	3.80
Total vendor revenue	20%	3.00	4.00	5.00	3.00	5.00	3.00
CWS revenue	20%	2.00	3.00	4.00	3.00	3.00	5.00
CWS revenue growth	20%	1.00	3.00	3.00	2.00	5.00	3.00
CWS direct installed base	20%	3.00	1.00	4.00	5.00	2.00	3.00
CWS indirect installed base	20%	5.00	4.00	1.00	3.00	3.00	5.00

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

Vendor Offerings

Forrester included 13 vendors in this assessment: Alert Logic, Aqua Security, Bitdefender, Cavirin, Check Point, Cisco, CloudPassage, Kaspersky, McAfee, Palo Alto Networks, Qualys, Symantec, and Trend Micro.

Vendor Profiles

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

Leaders

- **Trend Micro builds a comprehensive CWS solution.** The Trend Micro Deep Security solution started with agent instrumentation at the guest OS level but has expanded into protecting hypervisors, container build, and pre-runtime scanning and orchestration platforms as well. The vendor plans to: 1) enhance data collection and managed detection; 2) improve container security and cloud file storage scanning (e.g., AWS S3 buckets); and 3) add serverless and runtime application protection as well as cloud security posture management.

  The OS-level, agent-based protections are very strong and include malware and memory protection, file integrity monitoring, host-based firewall, intrusion detection/intrusion prevention, log inspection, and application binary control. Role-based access control (RBAC) is very flexible for administrators. Container runtime and pre-runtime checks are comprehensive, and the solution exposes a broad API for deep security policy control. However, there is no functionality to protect VPNs with agents. The API-level IaaS control is missing AWS and Azure storage configuration controls and GCP instance creation controls.[2] Compliance (PCI and HIPAA) profiles are somewhat behind the competition and are available for Red Hat 7 but not for Ubuntu (this is planned). The solution's North American revenue split proportions are markedly smaller than those of the competition. The solution is ideal for large firms with broad CWS needs across workloads, hypervisors, and containers.

- **McAfee covers guest OS and API platforms.** The solution's ePolicy Orchestrator offers comprehensive and centralized control of CWS policies. The solution covers guest OS workloads and provides API connectivity to IaaS platforms. The vendor plans to: 1) improve container app security via auto discovery; 2) enhance single-click deployment of security to workloads; and 3) extend Zero Trust to serverless (functions) compute resources.

  The vendor offers comprehensive memory integrity monitoring, DLP scans for sensitive information for AWS S3 buckets, and Azure blobs as well as automatic warning of vulnerabilities based on fingerprinting good container images. The vendor offers only a price list for perpetual licenses (subscription is planned). Attempted unauthorized login discovery to workloads, patch deployment, and GCP storage policies are weaker than those of the competition. The solution has no

container-level system calls detection and lacks support for Docker engine protection. Continuous improvement/continuous delivery (CI/CD) integration with container protection was not available at the cutoff time.[3] The solution is a good fit for existing McAfee ESS/EDR and CSG customers.

› **Bitdefender excels in database, user, and agent rollout management.** Bitdefender builds on its malware, memory, and hypervisor protection/introspection legacy to craft a broad CWS solution. The vendor plans to: 1) expand the range of capabilities in the software-as-a-service (SaaS) version of GravityZone; 2) improve attack detection and response for Linux systems; and 3) release container protection modules, including image scanning and configuration drift/anomaly detection.

The solution has extensive configuration capabilities for setting up its back-end data stores and provides a very usable agent bulk rollout mechanism, configurable malware protection, and binary privilege escalation control. The stack includes HyperDetect, a custom-tunable machine learning engine for threat detection. It can scan for and install missing patches and offers very strong hypervisor introspection capabilities and good API-based policy management as well as configurable dashboards. However, it includes no shift-left container scanning, external threat feed integration, file integrity monitoring, or vulnerability scanning. Support for GCP is weaker than that of competitors. The solution today lacks container and container orchestration support. The solution is a match for organizations requiring very strong hypervisor control capabilities in hybrid clouds.

Strong Performers

› **Kaspersky covers CWS with an organically grown product portfolio.** While hampered in North America due to past concerns over the company's allegiances, Kaspersky offers a versatile and technologically competent CWS solution. The vendor plans to: 1) implement a SaaS model for CWS solution delivery; 2) extend vendor partnerships and introduce support for GCP and VMware Cloud on AWS; and 3) deepen security support and integration with native IaaS storage and serverless functions.

The solution provides comprehensive user management capabilities, has strong guest OS-level support (including one of the strongest memory protection and file integrity monitoring capabilities across vendors in this Forrester Wave), and has an effective remediation policy set against hardening standards. However, the solution has no SaaS delivery form factor and a minimal North American customer installed base, and its Linux workload coverage is weaker than its Windows workload coverage. It has no explicit support for container runtimes and orchestration platforms and is rather unintuitive. The solution is ideal for organizations that are seeking an alternative to US-based CWS solutions or that don't have concerns regarding Kaspersky's allegiances.

› **Qualys allows admins to project and control cost of cloud workloads.** The Qualys CWS tool is a security solution platform that supports network agents, agents, containers, and API-based cloud collectors. The vendor plans to: 1) enhance its DevOps-centric functionality, focusing on

baselining and drift detection of cloud platform instances; 2) passively monitor and provide visibility into network traffic flow between cloud environments; 3) and cover cloud edge instances, cloud databases, storage, and API gateways and provide vulnerability assessments on these assets.

The solution offers strong user and roles management (including RBAC), excellent agent rollout capabilities, nice vulnerability scanning, and strong API-level connectivity to IaaS platforms (AWS, Azure, and GCP storage security, instance creation, and AWS data protection). However, the vendor has no professional services and offers only a SaaS solution.[4] The solution has no purpose-built hypervisor protection, no guest OS memory protection, and no monitoring of user/admin logins. Dashboarding and integration are significantly weaker than those of its competitors. The solution is a fit for firms looking for strong vulnerability scanning options.

› **Check Point offers viable API-based cloud protection.** The solution provides checks against Center for Internet Security (CIS) benchmarks and other regulatory frameworks and also automates remediation of cloud workload configuration drifts using a single-pane-of-glass visibility and management console. The vendor plans to: 1) support containers using a dedicated agent; 2) make hygiene improvements and permission reductions for serverless function security and permission reduction; and 3) scan cloud storage to identify malicious files and other threats.

The solution provides a nice RBAC structure and configuration. Productized integration between the solution and help desk systems is above that of other vendors in this Forrester Wave. Security analytics (e.g., Splunk) integration is productized. The solution offers a very comprehensive compliance engine, complete textual explanations, and a compliance score. However, it has no agent-based deployment option by design and offers no patching of workload. GCP platform support is weaker than that of AWS and Azure. Support for containers and hypervisors and third-party threat feed integration lags that of competitors. The solution is a good fit for firms needing to maintain strict adherence to CIS benchmarks and other regulatory frameworks.

› **Palo Alto Networks extends CWS with container protection.** Palo Alto added Evident.io and Twistlock to its existing CWS portfolio to build out coverage for guest OS, API, and containers. The solution supports serverless cloud security as well. The vendor plans to: 1) integrate with RedLock as part of Prisma Cloud; 2) launch container security as a SaaS offering; and 3) continue improvements in layer 7 traffic filtering and layer 4 protection.[5]

The solution offers outstanding container security and protection, including monitoring the container orchestration and runtime platforms, ensuring regulatory and best practices compliance of containers (HIPAA, PCI, and CIS benchmarks), monitoring system calls between containers and the host OS, and inspecting network communications between containers. However, Twistlock's API connectivity to cloud platforms is weak, its cloud reputation services are not productized, and it offers no API support for cloud platform native storage configuration checks.[6] The vendor also has a minimal system integrator partner ecosystem. The solution lacks hypervisor security today, and its dashboarding is weaker than that of the competition. The solution is a good choice for firms requiring extensive container and network security.

› **CloudPassage expands to containerization and IaaS monitoring.** CloudPassage has focused on public cloud infrastructure and has been investing in building technical innovations in containerization and API-based IaaS monitoring. The vendor now provides an agent rollout tightly integrated with CI/CD pipeline platforms. The vendor plans to: 1) complete the unification of all asset types into a common workflow for discovery, inventory, and assessment; 2) convert operational data into KPIs; and 3) improve intelligent issue prioritization and workflow guidance based on machine learning algorithms.

CloudPassage Halo stands out with API IaaS connectivity cloud instance configuration management and containerization runtime and platform protection capabilities. It has a particularly strong instance monitoring and interception capability for AWS and Azure. Managing policies for the container orchestration platform is above that of most competitors. However, the user and role definitions are behind (there are only predefined roles), and support for GCP is missing (it's planned). The vendor has a limited system integrator ecosystem, and navigation is difficult, as there are multiple policy management interfaces. It also offers no hypervisor protection functionality. We recommend the solution to those clients that need a single vendor for agent-based and agentless protections for guest OSes, AWS and Azure compute, and containers.

Contenders

› **Symantec provides SaaS and on-premises cloud workload security.** The solution uses a single agent for vulnerability scanning, hardening, application isolation, antimalware protection, and file integrity monitoring. The vendor uses its DLP capabilities for detecting sensitive data in cloud workloads. The vendor plans to: 1) create a container-first dedicated front-end user interface for cloud security products; 2) create microsegmentation-dedicated UIs; and 3) expand storage security from AWS and Azure to GCP and Oracle.

API-level connectivity to IaaS platforms is very strong (areas that stand out here include insecure network configuration detection on AWS S3 buckets and Azure blob scans). Container scanning at runtime and Kubernetes configuration file protection is versatile. However, the vendor has no managed service hosting partners, and the solution has no threat feeds mapping or alert ingestion from third-party tools. Administrators cannot customize the RBAC system. The solution includes no shift-left container image scanning or checking container images against CIS benchmarks or PCI, HIPAA, and other regulatory compliance rules.[7] It also lacks hypervisor protection features. It's a nice fit for firms with advanced cloud data scanning and protection needs.

› **Cisco focuses on workload protection and DevOps audiences in cloud security.** The Cisco solution provides visibility and policy enforcement through two workload-based agent types, which customers can deploy separately. This allows for visibility-only deployments without taking on the additional footprint and CPU tax of enforcement agents. It also includes application segmentation, vulnerability assessments, and forensics. The vendor plans to: 1) enable cooperative security

practices between DevOps and security teams using CI/CD integration; 2) move security controls up the stack to layer 7 API whitelisting; and 3) move controls closer to the application itself using OS-level, container sidecar, and application performance monitoring controls.

The solution uses unsupervised machine learning controls to system administrators in guest OS agent-based operation and has very strong container segmentation and microsegmentation policy definition capabilities. It includes productized integration between the solution and the ServiceNow help desk.[8] However, it has a minimal system integrator partner ecosystem of integrators with a proven track record. RBAC and user management are behind those of the competition; API connectivity-based IaaS configuration controls are minimal; and it lacks hypervisor protection features. The solution is a great fit for customers looking to implement Zero Trust network and workload controls in a multicloud environment.

› **Aqua Security covers virtual machines as well as containers.** The solution is largely available as an on-premises deployment with per-VM and per-node annual subscription pricing.[9] The pricing covers the CI/CD pipeline, container runtimes, and orchestration platforms. The vendor plans to: 1) expand into securing cloud APIs; 2) add more controls to Kubernetes-based environments; and 3) use AI to analyze and prioritize vulnerabilities, threats, and attack indicators.

The solution has a scalable and flexible agent rollout mechanism. Admins can map the schema of an external threat feed to the solution. The tool allows for malware detection, memory integrity protection, and file integrity monitoring. Shift-left pre-runtime container scanning and container drift detection are ahead of other vendors in this Forrester Wave. However, the solution offers minimal API connectivity to IaaS, no hypervisor protection, and no productized help desk integration. An administrator's ability to define and run ad hoc reports is behind that of others in this Forrester Wave. Aqua's dashboards are currently not customizable, but the solution has integrations with SIEM and analytics tools. The solution is a fit for organizations that have containerized environments requiring pipeline protection and configuration drift detection and remediation.

› **Cavirin provides compliance packs for cloud platform services and instances.** The agentless solution provides first-line defense for the major public clouds, with hundreds of built-in and vendor-updated rules for checking for security and compliance of IaaS and PaaS instances against regulations such as PCI and HIPAA. The vendor plans to: 1) launch its SaaS offering; 2) improve monitoring for baseline configurations and compliance frameworks on AWS, Azure, and GCP; and 3) remediate for 80%-plus of already existing baseline configurations (misconfiguration prevention).

Detecting insecure storage in AWS and Azure is outstanding, with very user-friendly, detailed explanations. The solution has extensive firewall policy and vulnerability checks. Container orchestration configuration best practice checks are ahead of those of the competition. However, the solution has no SaaS-based policy server (it's planned), no data integration configuration, and no malware or memory integrity checks and lacks file integrity monitoring. It includes no host-based firewall, IDS/IPS, and runtime privilege escalation. Importantly, remediation automation is not yet built in for all detected misconfigurations (it's planned), and where it is built in, it requires

a separate user interface.[10] It includes no runtime container vulnerability scanning and hypervisor protection. The solution is a good fit for firms that have extensive compliance checklists for cloud services and instances but may use other remediation tools.

› **Alert Logic provides threat management for cloud workloads.** The vendor offers 24x7 network traffic and log monitoring of customers' workloads in its security operations center (SOC), with curated threat intelligence and remediation guidance. The solution is a managed SaaS-only service with no setup requirements. The vendor plans to: 1) improve user experience; 2) increase the number of compliance reports in the solution, including ISO and GDPR reporting; and 3) enhance capabilities, including file integrity monitoring and cloud-based web application firewalls (WAFs).

The solution offers agent deployment and management for a large number of workloads and coverage for VPN connected workloads. Detection of insecure creation and deletion on AWS and built-in practice template libraries on Azure are strong. However, admin role definitions are fixed, and the solution includes no direct Active Directory-based admin user authentication.[11] There is minimal API connectivity only to Office 365 and IaaS platforms, and GCP support is much less functional than support for AWS or Azure. Shift-left and runtime container image scanning are also missing. The solution provides no hypervisor-specific protections, and dashboarding is behind that of competitors. The solution is a great fit for organizations that require managed cloud workload security services.

Evaluation Overview

We evaluated vendors against 30 criteria, which we grouped into three high-level categories:

› **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions: 1) setup, configuration, and data integration; 2) users and roles; 3) operating-system-level workload protection; 4) API-level connectivity and control for IaaS and PaaS; 5) containerization and container orchestration platform protection; 6) hypervisor protection; 7) integration and reporting; 8) scalability; 9) intuitiveness; and 10) help.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated vendors' development plans for: 1) centralized agent frameworks; 2) API control for IaaS and PaaS; 3) containerization protection; 4) hypervisor protection; and 5) threat detection and auditing. We also assessed: 1) solution delivery; 2) RFP response; 3) proof of capability and demonstration; 4) services and partners ecosystems; 5) development, sales, and support staffing; and 6) pricing terms and flexibility.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's: 1) total vendor revenue; 2) CWS revenue; 3) CWS revenue growth; and 4) CWS direct and indirect installed bases.

Vendor Inclusion Criteria

Forrester included 13 vendors in the assessment: Alert Logic, Aqua Security, Bitdefender, Cavirin, Check Point, Cisco, CloudPassage, Kaspersky, McAfee, Palo Alto Networks, Qualys, Symantec, and Trend Micro. Each of these vendors has:

- **A thought-leading, productized portfolio of products and services.** We included CWS vendors that demonstrated thought leadership and solution strategy execution by regularly updating and improving their productized product and model portfolio. Customers of vendors had to report that the solution is purpose-built for cloud workload protection and posture management.
- **Total annual CWS revenues of at least $3 million with at least 10% growth.** We included vendors that have at least $3 million in combined revenues from the CWS solution and at least 10% year-over-year growth in revenues.
- **An unaided mindshare with Forrester's end user customers.** The vendors we evaluated are frequently mentioned in Forrester end user client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.
- **An unaided mindshare with vendors.** The vendors we evaluated are frequently noted by other vendors during Forrester briefings as viable and formidable competitors.

Supplemental Material

Online Resource

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

The Forrester Wave Methodology

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

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

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by June 30, 2019, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

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

Endnotes

[1] See the Forrester report "Best Practices: Cloud Workload Security," see the Forrester report "Hybrid Cloud Security Best Practices," and see the Forrester report "Best Practices: Cloud Governance."

[2] This was released after the June 30, 2019 cutoff date.

[3] McAfee's acquisition of Nanosec provides CI/CD integration.

[4] The vendor offers a private cloud platform-based delivery of the solution on an as-needed basis.

[5] Plans 1 and 2 will likely be part of the generally available solution by November 18, 2019.

[6] Prisma Cloud/RedLock provides some of this capability.

[7] However, there are templatized compliance checks against cloud services.

[8] There are other integrations points as well, such as vCenter and Kubernetes.

[9] It's also available on demand as a PaaS-deployed solution.

[10] However, the vendor provides guidance on remediation steps.

[11] The vendor provides single sign-on integration instead.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.