The Forrester Wave™: Infrastructure-As-A-Service Platform Native Security, Q4 2020

The Seven Providers That Matter Most And How They Stack Up

by Andras Cser

December 7, 2020

Why Read This Report

In our 29-criterion evaluation of infrastructure-as-a-service platform native security (IPNS) providers, we identified the seven most significant ones — Alibaba, Amazon Web Services (AWS), Google, Huawei, IBM, Microsoft, and Oracle — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Key Takeaways

Google And Amazon Web Services Lead The Pack
Forrester's research uncovered a market in which Google and Amazon Web Services are Leaders; Microsoft and IBM are Strong Performers; and Oracle, Alibaba, and Huawei are Contenders.

Policy Posture Management And Guest OS Protection Are Key Differentiators
As IPNS technology matures to cover infrastructure-as-a-service (IaaS) providers' own IaaS platforms as well as those of other vendors, effective, multicloud policy posture management; guest OS protection; and integration of threat intel sources to reduce the attack threat surface will dictate which providers lead the pack. Vendors that can provide comprehensive IPNS, not only for their own platforms but also for competing public and private cloud and on-premises workloads and platforms, position themselves to successfully evolve into their customers' security central nervous systems.

The Forrester Wave™: Infrastructure-As-A-Service Platform Native Security, Q4 2020

The Seven Providers That Matter Most And How They Stack Up

by Andras Cser
with Merritt Maxim, Benjamin Corey, and Peggy Dostie
December 7, 2020

Table Of Contents

Related Research Documents

Assess Your Cloud Security Readiness

Best Practices: Cloud Governance

How Cloud Identity Governance Can Help Mitigate Access And Entitlement Risks

FORRESTER®

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

Cross-Cloud Posture Management And Guest OS Protection Matter

Today's cloud IPNS capabilities go a lot further than they did two or three years ago. We're seeing all vendors investing in overall infrastructure security, including secure boot of hypervisors and better data protection and encryption capabilities as well as simplified identity management and policy change management that don't compromise on security. Customers are also looking for IPNS components to provide as much coverage as possible for the IaaS platform's compute, storage and network offerings — and this is the area where we're going to see the greatest improvements in the next 18 to 24 months.

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

- **Offer comprehensive cloud policy posture management.** A sizeable chunk of recent data breaches in the cloud have resulted from improper and insecure configurations of cloud administrator identities and cloud resources. Examples include unencrypted object and file storage in IaaS, wide-open machines with unnecessary access to cloud instances from the public internet, and customers that don't fully manage identities from the cloud provider's admin console. Creating a cloud security posture management regime around these configuration artifacts, including ensuring that only authorized admins can make auditing changes and continually tracking and remediating deviations of the as-is configuration set from the to-be set, can greatly help reduce the likelihood and impact of a breach.
- **Provide native guest OS protection.** Agent-based or agentless malware protection, privilege escalation, and file integrity monitoring are a formidable line of defense against compromises. Customers increasingly want to deploy IaaS platforms that offer guest OS, container platform, and container orchestration capabilities that can identify suspicious network activity between compute and container instances and the processes running on them. Container image vulnerability scanning and API-based monitoring of IaaS platform activity are gaining ground to allow for an effective protection layer of minimally resource-intensive, agentless defenses.
- **Integrate multiple audit and threat intel sources.** Security and risk professionals are looking to IPNS providers to migrate their security analytics and aggregation systems from on-premises to the cloud to monitor cloud activity. Customers increasingly mention the importance of having a single-pane-of-glass view into all their public and private cloud platforms and the ability to use and alert on the IPNS vendor's own as well as third-party threat intel sources, including CVEs, best practices policy templates, and emerging threat information. To provide a lower ratio of false-positive alerts and decrease alert-investigation fatigue, integration between the IPNS and existing user behavior or security analytics platform is gaining importance. IPNS, just like other security products and technologies, is beginning to expose supervised and unsupervised machine learning analytics to end-user administrators. Exposing analytics tuning to customer administrators reduces false positives and allows clients to tune or switch off the analytics components.

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.

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™: Infrastructure-As-A-Service Platform Native Security, Q4 2020

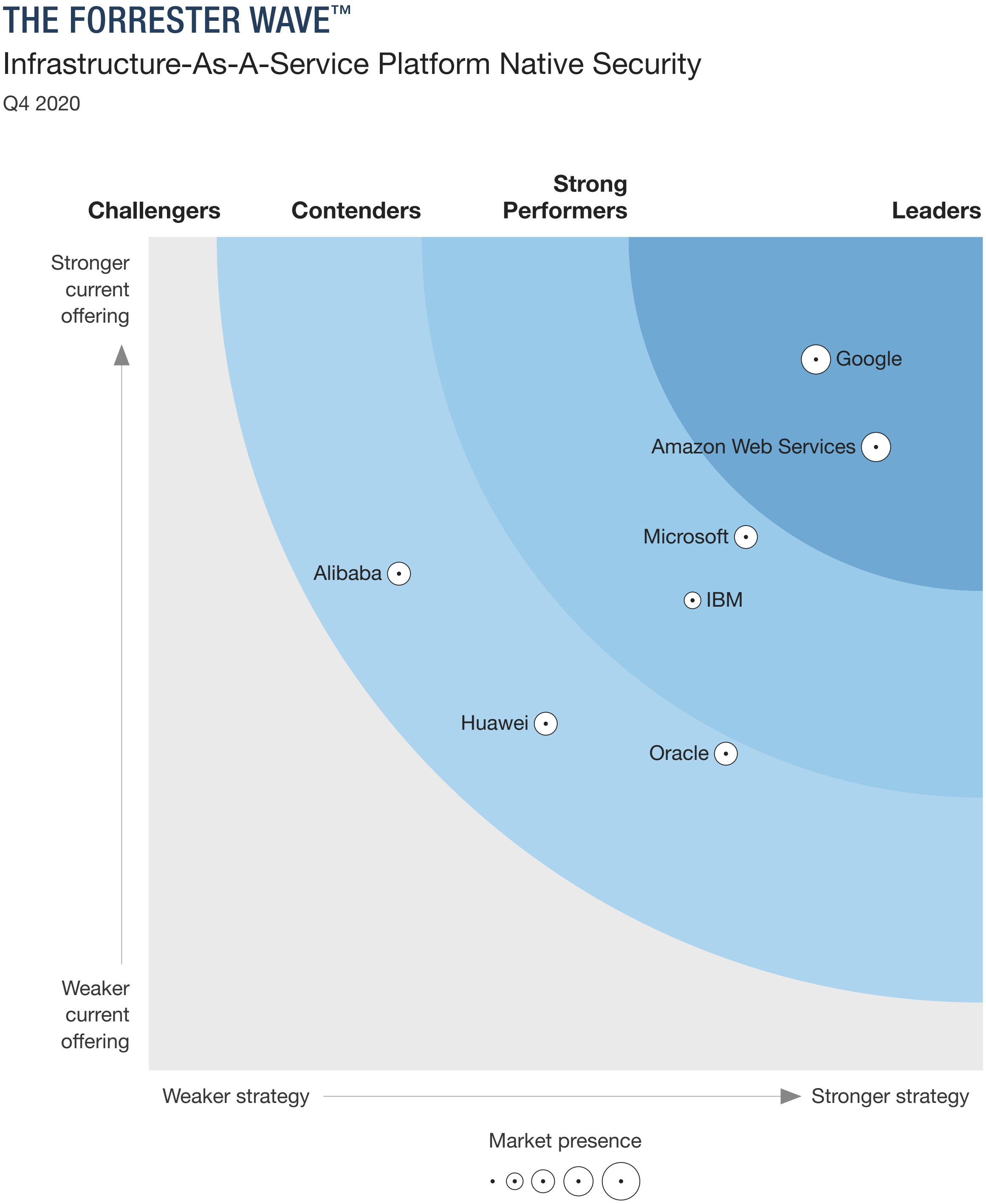

FIGURE 2 Forrester Wave™: Infrastructure-As-A-Service Platform Native Security Scorecard, Q4 2020

	Forrester's weighting	Alibaba	Amazon Web Services	Google	Huawei	IBM	Microsoft	Oracle
Current offering	50%	2.98	3.74	4.26	2.08	2.82	3.20	1.90
Global data centers	9%	5.00	5.00	5.00	3.00	1.00	3.00	1.00
Identity and access management	9%	3.00	5.00	3.00	3.00	3.00	5.00	3.00
Policy change and posture management	10%	1.00	5.00	3.00	1.00	3.00	5.00	1.00
Hardware and hypervisor security	9%	3.00	5.00	3.00	1.00	3.00	1.00	1.00
Guest OS and container protection	9%	5.00	1.00	5.00	1.00	3.00	3.00	1.00
Storage and data security	9%	3.00	3.00	5.00	5.00	3.00	3.00	1.00
Network security	9%	5.00	3.00	3.00	1.00	3.00	3.00	3.00
Auditing, threat intel, and integration	9%	5.00	3.00	5.00	1.00	1.00	5.00	1.00
Solution delivery	9%	1.00	3.00	5.00	5.00	5.00	3.00	3.00
Navigation and integrated environment	9%	1.00	3.00	5.00	1.00	3.00	3.00	3.00
Static and contextual documentation	9%	1.00	5.00	5.00	1.00	3.00	1.00	3.00

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

FIGURE 2 Forrester Wave™: Infrastructure-As-A-Service Platform Native Security Scorecard, Q4 2020 (Cont.)

	Forrester's weighting	Alibaba	Amazon Web Services	Google	Huawei	IBM	Microsoft	Oracle
Strategy	50%	1.50	4.36	4.00	2.38	3.26	3.58	3.46
Execution roadmap	7%	1.00	5.00	5.00	1.00	5.00	3.00	1.00
Market approach: total employees	6%	1.00	5.00	1.00	5.00	5.00	3.00	3.00
Market approach: developers	6%	1.00	5.00	5.00	3.00	1.00	5.00	3.00
Market approach: sales	6%	3.00	5.00	5.00	5.00	3.00	5.00	5.00
IPNS R&D investment	7%	3.00	5.00	3.00	5.00	5.00	5.00	3.00
Identity and access management plans	7%	1.00	5.00	3.00	3.00	1.00	1.00	3.00
Security posture management plans	7%	1.00	1.00	5.00	1.00	3.00	1.00	3.00
Hypervisor security plans	6%	3.00	3.00	5.00	3.00	3.00	3.00	5.00
Guest OS and container plans	6%	1.00	3.00	5.00	1.00	5.00	5.00	3.00
Storage and data security plans	6%	1.00	5.00	3.00	1.00	5.00	3.00	5.00
Network security plans	6%	1.00	5.00	5.00	3.00	1.00	3.00	3.00
Auditing and threat intel plans	6%	1.00	5.00	3.00	1.00	5.00	3.00	1.00
Support engineers	6%	3.00	5.00	3.00	1.00	1.00	5.00	5.00
Professional services staffing	6%	1.00	5.00	3.00	1.00	3.00	5.00	5.00
Partner ecosystem	6%	1.00	5.00	5.00	1.00	3.00	5.00	5.00
Commercial model	6%	1.00	3.00	5.00	3.00	3.00	3.00	3.00
Market presence	0%	3.00	4.00	3.50	3.00	1.50	3.00	3.00
IPNS revenue	50%	1.00	5.00	3.00	1.00	2.00	5.00	4.00
IPNS revenue growth	50%	5.00	3.00	4.00	5.00	1.00	1.00	2.00

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

Vendor Offerings

Forrester included seven vendors in this assessment: Alibaba, Amazon Web Services, Google, Huawei, IBM, Microsoft, and Oracle. We invited Century Link, Salesforce, and SAP to participate in this Forrester Wave, but they chose not to participate, and we couldn't make enough estimates about their capabilities to include them in the assessment as nonparticipating vendors.

Vendor Profiles

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

Leaders

› **Google continues aggressive investment in its IaaS platform's native security.** Google has been steadily investing in its offering and has added many new security features, including Anthos (a service to manage non-Google public and private clouds) and Security Command Center Premium. The vendor plans to: 1) invest in providing customers with digital sovereignty across data, operations and software in the cloud; 2) expand security for multicloud and cross-cloud environments; and 3) increase support for Zero Trust and identity-based and richer policy creation.

The solution offers good guest OS and container protection, including API-based and OS protections, container runtime vulnerability scanning, and CI/CD pipeline integration. Anthos is ahead of the competition when it comes to managing non-Google, third-party clouds. Data leak prevention (DLP) capabilities, integration support for external hardware security modules (HSMs), and third-party threat intelligence source integration are also nice. However, the solution lags the competition in native firewall configuration flexibility — currently, only firewall rules are available, and firewall policies are planned but not yet supported. Security Command Center (SCC) dashboards offer little customization. Forrester estimates that Google Cloud Platform's (GCP's) infrastructure size and presence remain behind AWS's and Azure's. The solution is a good fit for companies that want to minimize cloud service provider vendor lock-in and manage non-Google clouds from within GCP.

› **Amazon Web Services focuses on best-practice security policy templates.** AWS has been investing in its Security Hub Foundational Security to detect when resource configurations contain vulnerabilities or don't follow security best practices. The vendor has significantly invested in building out multiorganizational hierarchy support for managing identities and policies. AWS plans to: 1) expand Nitro enclaves to support isolated compute environments; 2) provide detection of fraudulent payments online; and 3) offer managed network firewall and in-line packet inspection services.

The solution offers very strong identity and access management capabilities, including single sign-on (SSO) for organizational administrators; protections for bare-metal hypervisors (Nitro); and its own cloud security posture management, which offers extensive detection and remediation features. AWS's included contextual help and documentation are also very strong, and wizards are available for most tasks. However, the solution lacks a single centralized dashboard to view and manage all active IPNS services.[1] It's currently missing malware protection at the guest OS level, hypervisor-level information, and hypervisor event correlation and support for managing hybrid and multicloud environments. Identity and access management (IAM) policy management is broad and powerful, but understanding effective permissions between AWS resources is extremely and unnecessarily complicated. Customers report that AWS's IPNS is more likely than its competitors to lead to vendor lock-in. The solution is a great fit for firms that have strong API cultures and predominantly use AWS public cloud infrastructure services.

Strong Performers

› **Microsoft expands core security and tools across Azure, Azure IaaS, and Office.** As with other areas, Microsoft has been expanding its security event management to monitor third-party systems and clouds. Microsoft plans to: 1) add Application Guard to Office 365 to allow for opening untrusted documents in virtualized containers; 2) offer a compliance score to control complexity and risk; and 3) invest in security posture management in the Azure Security Center.

  The solution's SSO management and multifactor authenticator management for admins are strong, and its multitenancy management is ahead of the competition. It offers resource access policies that are easy to understand and use; robust detection of unauthorized policy changes; and auditing and threat intelligence correlation from its own and third-party sources. However, the solution generally lags in the hypervisor security space; it provides no way to detect and remediate suspicious activity at the CPU level. It doesn't support configuring virtual root-of-trust and measured/secure boot at the hypervisor level but plans to do so. Firewall deployment to enable forced-tunneling support is possible during deployment (build) time but not at runtime.[2] The solution is a great fit for organizations that have extensive Microsoft Cloud deployments and want relatively simple cloud security administration capabilities.

› **IBM invests in network and data security.** IBM designed its Virtual Private Connection (VPC) solution to cover virtual machine (VM)-based compute workloads. The platform also uses keep-your-own-key (KYOK) services, essentially a single-tenant key management system with customer-controlled FIPS-140-4 HSMs. The vendor plans to: 1) invest in security compliance posture and governance; 2) provide additional insights around security threats to improve workload security; and 3) extend data security, including KYOK support for hybrid multicloud environments.

  The solution offers a very nice facility to view logs and provides outstanding productized CI/CD build pipeline integration. Administrators have a flexible way of controlling non-human access to resources. KYOK data protection is a differentiating concept across cloud service providers, and virtualized network controls are easy to use and intuitive. The solution also has a deep integration with VMWare. However, managing federated IAM for administrators is very complex, and there are no traditional admin roles, only user actions. Guest OS protection; traditional network security, including web application firewall (WAF), intrusion detection system (IDS), and distributed denial of service (DDoS) protection capabilities; and threat intel capabilities all lag the competition.[3] Some of these capabilities require admins to use a separate management console. The solution is a good fit for firms with large general-purpose cloud computing needs and companies with extensive SAP infrastructures.

Contenders

- **Oracle grows its cloud security footprint and certification.** Oracle Cloud Infrastructure (OCI) currently has 26 live and 12 planned regions worldwide. The vendor has increased its security certifications to offer ISO 27001, SOC 1, 2, and 3, and GDPR compliance, among others, to be on par with competitors.[4] Oracle plans to: 1) provide a unified umbrella for all its identity-related policies and operations; 2) check OCI configurations against security best practices, including CSA and CMU; and 3) offer secure and measured boot capabilities to ensure hypervisor security.

  Storage-level data encryption is on by default, making data protection easier. Managing access for customers with large, complex multitenant organizational structures is very intuitive and functional. Oracle uses its CSG/CASB solution for user and entity behavioral analytics. However, OCI doesn't support review campaigns to assess the access rights of admin users and provides no predefined role-based access control templates. Oracle provides no intellectual property HSM service of its own, and there's no way to integrate logs from non-Oracle clouds.[5] DevOps integration, dashboarding, and machine learning were lacking at the time of this evaluation but are areas of planned investment.[6] The solution is a good fit for companies with large footprints of Oracle databases and business applications that they're migrating to the cloud.

- **Alibaba introduces hybrid cloud, native WAF, and DDoS proxy protection.** The vendor has added Zero Trust IAM, allowing for multifactor authentication for administrators and risk-scoring admin activities. Ransomware protection for compute instances, vulnerability remediation, and container security are also improved. The vendor plans to: 1) improve user-access risk-scoring capabilities using behavioral and device context, 2) embed security features into its core cloud computing services (e.g., add WAF to its load balancers); and 3) implement a Zero Trust edge network architecture.

  The solution provides a capable, agent-based, and API-based (agentless) guest OS plus container security features such as guest OS behavior-anomaly detection and remediation, privilege escalation detection, and vulnerability scanning. Network security, especially firewall and WAF policy configurations, is outstanding. However, the IPNS solution still isn't entirely localized to English — some functionality is available only in Chinese. Role-based access control for admin users, cloud security posture management, configuration management for non-Alibaba clouds, serverless security, and contextual help and documentation are lagging. The management interface is rather nonintuitive. The solution is a great fit for clients with Chinese-speaking cloud security staff who don't mind working with Chinese-language-only interfaces.

- **Huawei offers a maturing IPNS portfolio.** Huawei is relatively new to monetizing its IPNS portfolio; the company has made significant efforts to make the management console available in English. Investments in data security (including HSM support) are starting to bear fruit. The vendor plans to: 1) improve its resource access authorization policy; 2) provide access analysis for IAM objects; and 3) perform formal verification of permission policies.

  The solution provides capable storage and data security; key management is particularly impressive. It offers its own HSM, which can also support non-Huawei clouds as well as customers using their own HSMs against the Huawei IPNS infrastructure. DLP capabilities are versatile. However, the solution's administration is very complex and nonintuitive. In general, resource-to-resource access policies are missing or very hard to configure. Its risk-based authentication, firewall, and IDS/IPS lag the competition. Standards-based identity federation also lags, and bulk-user CSV file imports are missing. Active Directory (managed by Huawei), cloud security posture management, workload segmentation, serverless security, and integration with third-party logging or threat intelligence system systems all lag competitors. The solution is a good fit for firms supporting China-based operations with cloud infrastructure.

Evaluation Overview

We evaluated vendors against 29 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 include global data centers; IAM; policy change and posture management; hardware and hypervisor security; guest OS and container protection; storage and data security; network security; auditing, threat intel, and integration; solution delivery; navigation and integrated environment; and static and contextual documentation.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated execution roadmap, market approach, staffing for development and sales, R&D spending, planned enhancements in current offerings, staffing for professional services support, breadth of the partner ecosystem, and the IPNS solution's commercial model.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's IPNS revenue and revenue growth.

Vendor Inclusion Criteria

Forrester included seven vendors in the assessment: Alibaba, Amazon Web Services, Google, Huawei, IBM, Microsoft, and Oracle. Each of these vendors has:

- **A thought-leading, productized portfolio of products and services.** We included cloud platform provider vendors that demonstrate thought leadership and solution strategy execution by regularly updating and improving their productized IPNS product portfolios. Customers of vendors reported that the solutions have native, purpose-built security features.

- **Annual IPNS revenues of at least $75 million, with at least 14% growth.** We included vendors that have at least $75 million in combined revenues from IPNS components and at least 14% year-over-year growth in IPNS revenues.
- **Mindshare with Forrester's end-user customers.** The vendors we evaluated are frequently mentioned in Forrester end-user client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.
- **Mindshare with vendors.** The vendors we evaluated are frequently mentioned by other 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 October 20, 2020, 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™ and New 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] Tags are an inconvenient workaround for listing all IPNS services that a company uses.

[2] Other firewall configurations are available at runtime as well.

[3] CI/CD build pipeline integration for WAF and IDS is there, though. Guest OS encryption is supported.

[4] GDPR is the European Union General Data Protection Regulation.

[5] Oracle, however, allows clients to purchase a private vault, managed through the KMS service.

[6] Since our cutoff date, Oracle has introduced CloudGuard, Security Zones, and auditing services.

FORRESTER®

forrester.com

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

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.