The Forrester Wave™: Public Cloud Platform Native Security, Q2 2018

The Seven Providers That Matter Most And How They Stack Up

by Andras Cser
May 22, 2018

Why Read This Report

In our 37-criteria evaluation of public cloud platform native security (PCPNS), we identified the seven most significant ones — Alibaba, Amazon Web Services (AWS), CenturyLink, Google, IBM, Microsoft, and Rackspace — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways

Google And AWS Lead The Pack
Forrester's research uncovered a market in which Google and AWS lead the pack. Microsoft, Alibaba, and IBM offer competitive options. CenturyLink and Rackspace lag behind.

S&R Pros Increasingly Rely On The Native Security Features Of Public Cloud Providers
In the past, S&R pros were anxious about their firms' cloud adoption, but today, many see the native security of public cloud providers as a way to address their top security challenges. Public cloud market growth has increased because S&R pros increasingly trust public cloud providers to act as strategic partners and advise them on top cloud-security decisions.

Improved IAM, Hypervisor Security, And Network Security Are Key Differentiators
Using on-premises security solutions to protect workloads in the cloud has become outdated and ineffective. Improved identity and access management, hypervisor security, and network security features of public cloud platforms will dictate which providers will lead the pack. Vendors that provide these security capabilities with centralized and intuitive configuration are best positioned to successfully deliver comprehensive, easy-to-price, and predictable security.

The Forrester Wave™: Public Cloud Platform Native Security, Q2 2018

The Seven Providers That Matter Most And How They Stack Up

by Andras Cser
with Stephanie Balaouras, Glenn O'Donnell, Madeline Cyr, and Peggy Dostie

May 22, 2018

Table Of Contents

Related Research Documents

Create Your Cloud Security Technology Strategy And Road Map

The Forrester Wave™: Cloud Security Gateways, Q4 2016

The Forrester Wave™: Global Public Cloud Platforms For Enterprise Developers, Q3 2016

FORRESTER®

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

Native Security Accelerates Cloud Adoption, Differentiates Providers

Organizations continue to move workloads to public clouds, and S&R pros must protect the sensitive data and digital identities found in those workloads. Once wary of cloud adoption, many S&R pros now believe that the native security capabilities of large public cloud platforms actually offer more affordable and superior security than what their teams could deliver themselves if the workloads remained on-premises. However, native security capabilities and features vary across public cloud providers. Three key factors can ensure a smooth transition to the cloud and influence public cloud provider selection: breadth and depth of native security features, unified configuration and management, and aggressive road maps.

- **Breadth and depth of native security features can reduce costs.** Forrester's interviewees report that a platform's security certifications and security track record play a great role in vendor selection. Public cloud platform providers with a broader set of built-in public security capabilities cost firms less to secure their sensitive data than cloud platforms lacking these capabilities and which the security team must procure from third-party security vendors. A German insurance company told Forrester that its stakeholders don't want to pay extra for add-on cloud monitoring solutions.
- **Unified configuration and management can reduce breaches and improve posture.** Numerous public cloud breaches resulting from simple misconfiguration have made it clear to S&R professionals that they should seek comprehensive, centrally configured, and audited security services in a cloud platform. In addition, security teams find that centralized security improves not only the tactical, day-to-day security posture of the firm, such as implementing data encryption, key management, and identity management, but it also helps with restructuring the firm's cloud security governance processes.[1]
- **Aggressive road maps can make sure security teams keep pace with cloud evolution.** Cloud platforms are constantly evolving, and S&R pros often find themselves trying to shoot a moving target when it comes to securing workloads. New serverless functions and containerization, together with accelerated DevOps, massive increases in workload volumes, and overall network complexity, present significant challenges for security teams. While the native security features have evolved since the last publication of this Forrester Wave, there are still major gaps in cloud providers' capabilities. S&R pros must evaluate vendors not just on the capabilities they have today but also the ones in development and how quickly they plan to roll them out.

PCPNS Evaluation Overview

To assess the state of the PCPNS market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of the native security capabilities of top public cloud platform providers. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 37 criteria, which we grouped into three high-level buckets:

- **Current offering.** We assessed the native security capabilities of public cloud platform providers against the following criteria: 1) data center physical and logical protection; 2) security certifications and attestations; 3) IAM for cloud platform administrators; 4) hypervisor and container security; 5) storage and data security; 6) network security; 7) scalability, auditing, and integration; 8) online help; and 9) navigation and environment integration.
- **Strategy.** We assessed each provider's future development plans for: 1) data center physical security; 2) certification and attestation; 3) identity and access management; 4) hypervisor security; 5) guest operating system security; 6) network security; 7) security logging and auditing; and 8) using machine learning. We also evaluated: 1) customer satisfaction; 2) the vendor's RFP responses; 3) the vendor's ability to run compelling proof of concept (PoC) demonstrations; 4) services and partners; 5) development staffing; 6) sales staffing; 7) support staffing; 8) vendor's financial transparency regarding security offerings; and 9) pricing terms and flexibility.
- **Market presence.** We evaluated vendors using their: 1) total vendor revenue; 2) native security revenue; 3) native security revenue growth; 4) native security direct installed base; 5) native security indirect installed base; and 6) geographical presence.

Evaluated Vendors And Inclusion Criteria

Forrester included seven vendors in the assessment: Alibaba, Amazon Web Service (AWS), CenturyLink, Google, IBM, Microsoft, and Rackspace. Each of these vendors has (see Figure 1):

- **A thought-leading, productized native security portfolio of products and services.** We included infrastructure-as-a-service cloud platform vendors that demonstrated native security thought leadership and native security solution strategy execution by regularly updating and improving their productized product portfolio.
- **Total annual native security revenues of at least $50 million with at least 15% growth.** We included vendors that have at least $50 million in combined revenues from the dedicated native security portfolio (not just the core IaaS cloud platform) solution and at least 15% year-over-year growth in revenues.
- **At least 3,000 paying customer organizations for native security in production.** We included vendors that have an install base of at least 3,000 paying PCPNS customer organizations in production.
- **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 mentioned by other vendors during Forrester briefings as viable and formidable competitors.

FIGURE 1 Evaluated Vendors: Product Information And Inclusion Criteria

Vendor	Product evaluated
Alibaba	Alibaba Cloud
Amazon Web Services	Amazon Web Services
CenturyLink	CenturyLink Cloud
Google	Google Cloud Platform
IBM*	IBM Cloud
Microsoft	Microsoft Azure
Rackspace*	Rackspace Cloud

Vendor inclusion criteria

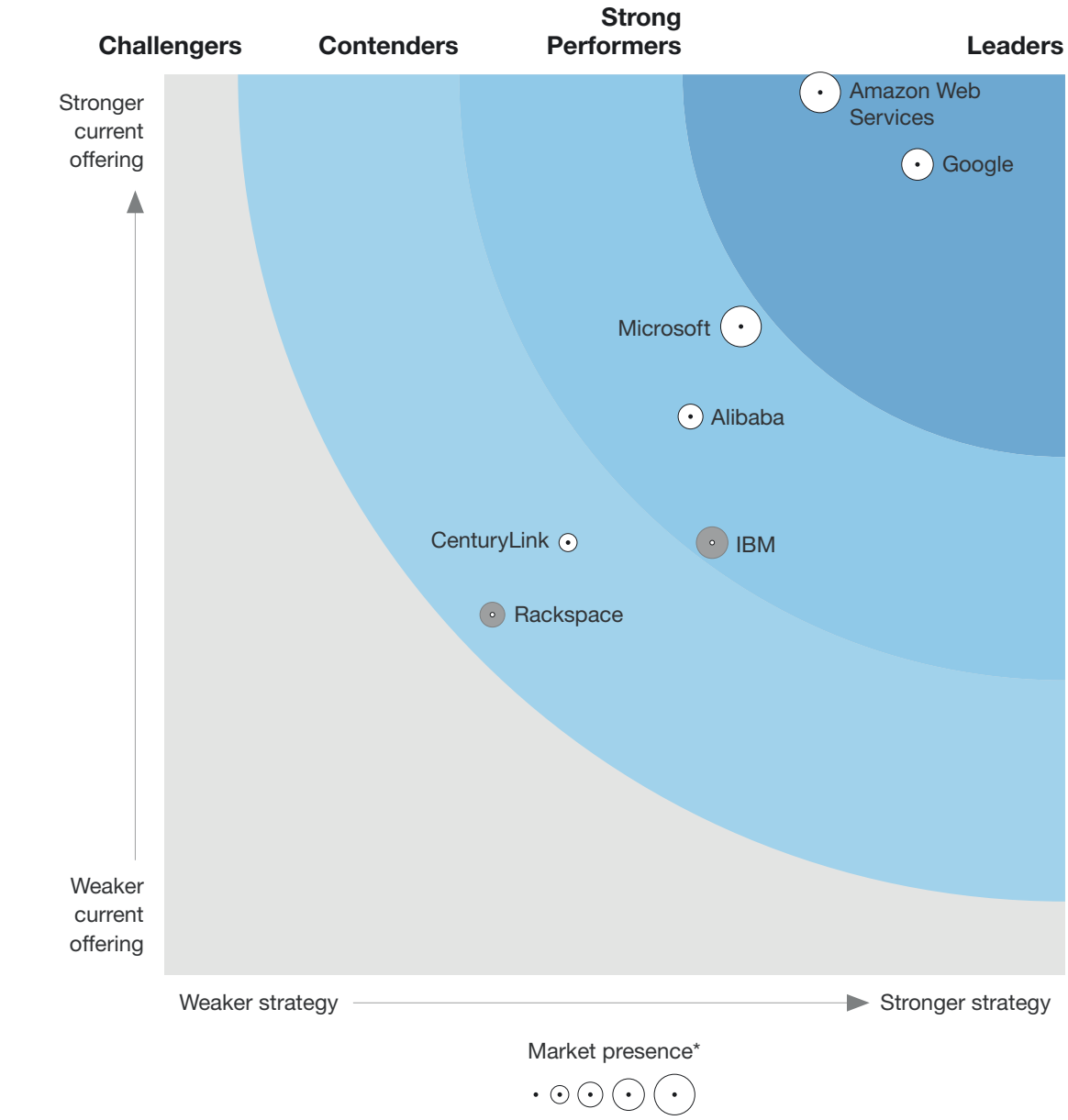
A thought-leading, productized native security portfolio of products and services. We included infrastructure-as-a-service cloud platform vendors that demonstrated native security thought leadership and native security solution strategy execution by regularly updating and improving their productized product portfolio.
Total annual native security revenues of at least $50 million with at least 15% growth. We included vendors that have at least $50 million in combined revenues from the dedicated native security portfolio (not just the core IaaS cloud platform) solution and at least 15% year-over-year growth in revenues.
At least 3,000 paying customer organizations for native security in production. We included vendors that have an install base of at least 3,000 paying PCPNS customer organizations in production.
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 mentioned by other vendors during Forrester briefings as viable and formidable competitors.

*IBM and Rackspace declined to participate in or provide information for our research. Scores are based on Forrester estimates.

Vendor Profiles

This evaluation of the PCPNS market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 2 and see Figure 3). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 2 Forrester Wave™: Public Cloud Platform Native Security, Q2 2018



*A grey marker indicates incomplete participation.

FIGURE 3 Forrester Wave™: Public Cloud Platform Native Security Scorecard, Q2 2018

	Forrester's weighting	Alibaba	Amazon Web Services	CenturyLink	Google	IBM	Microsoft	Rackspace
Current Offering	50%	3.10	4.90	2.40	4.50	2.40	3.60	2.00
Data centers	10%	3.00	5.00	1.00	3.00	3.00	5.00	1.00
Certifications and attestations	10%	3.00	5.00	3.00	5.00	3.00	5.00	1.00
Administrator user management	10%	3.00	5.00	1.00	5.00	3.00	1.00	3.00
Admin entitlements and certification	10%	1.00	5.00	1.00	5.00	3.00	1.00	3.00
Hypervisor security	10%	3.00	5.00	5.00	5.00	1.00	3.00	3.00
OS and container security	10%	3.00	5.00	3.00	5.00	3.00	5.00	1.00
Storage and data security	10%	3.00	5.00	3.00	5.00	1.00	5.00	3.00
Network security	10%	5.00	5.00	1.00	3.00	1.00	5.00	1.00
Scale, auditing, and integration	10%	5.00	5.00	3.00	5.00	3.00	3.00	1.00
Help and documentation	5%	1.00	3.00	1.00	5.00	3.00	3.00	3.00
Navigation and integrated environment	5%	3.00	5.00	5.00	3.00	3.00	3.00	3.00

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

FIGURE 3 Forrester Wave™: Public Cloud Platform Native Security Scorecard, Q2 2018 (Cont.)

	Forrester's weighting	Alibaba	Amazon Web Services	CenturyLink	Google	IBM	Microsoft	Rackspace
Strategy	50%	2.92	3.64	2.24	4.18	3.04	3.20	1.82
Physical security plans	7%	3.00	1.00	1.00	5.00	3.00	3.00	3.00
Certification and attestation plans	3%	3.00	3.00	3.00	5.00	1.00	3.00	3.00
IAM plans	7%	3.00	5.00	1.00	3.00	5.00	5.00	1.00
Hypervisor security plans	7%	3.00	3.00	1.00	5.00	1.00	1.00	3.00
Guest OS workload security plans	3%	5.00	3.00	1.00	5.00	3.00	3.00	3.00
Network security plans	7%	5.00	5.00	1.00	5.00	3.00	3.00	3.00
Security logging and auditing plans	6%	3.00	3.00	5.00	3.00	1.00	3.00	1.00
Machine learning plans	7%	3.00	3.00	3.00	5.00	5.00	3.00	1.00
Customer satisfaction	15%	3.00	3.00	1.00	5.00	3.00	3.00	1.00
Vendor's RFP response	7%	5.00	3.00	3.00	5.00	1.00	1.00	1.00
Vendor's PoC and demonstration	4%	1.00	5.00	3.00	3.00	1.00	3.00	1.00
Services and partners	4%	1.00	5.00	1.00	5.00	5.00	3.00	3.00
Development staffing	4%	3.00	5.00	1.00	5.00	5.00	5.00	1.00
Sales staffing	7%	1.00	5.00	3.00	3.00	5.00	5.00	1.00
Support staffing	7%	1.00	5.00	5.00	1.00	3.00	5.00	3.00
Vendor transparency	3%	5.00	1.00	5.00	3.00	3.00	1.00	3.00
Pricing terms and flexibility	2%	1.00	5.00	3.00	5.00	3.00	5.00	1.00

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

FIGURE 3 Forrester Wave™: Public Cloud Platform Native Security Scorecard, Q2 2018 (Cont.)

	Forrester's weighting	Alibaba	Amazon Web Services	CenturyLink	Google	IBM	Microsoft	Rackspace
Market Presence	0%	2.60	4.20	1.40	3.80	3.40	4.60	2.40
Total vendor revenue	10%	1.00	5.00	1.00	5.00	3.00	5.00	3.00
PCPNS revenue	20%	3.00	5.00	1.00	3.00	3.00	5.00	1.00
PCPNS revenue growth	10%	5.00	3.00	1.00	5.00	3.00	5.00	1.00
PCPNS direct installed base	10%	5.00	5.00	1.00	3.00	3.00	5.00	1.00
PCPNS indirect installed base	10%	1.00	5.00	1.00	3.00	3.00	5.00	3.00
Canada and United States presence	10%	1.00	3.00	5.00	5.00	5.00	3.00	5.00
Central and South America presence	10%	1.00	3.00	1.00	3.00	5.00	5.00	5.00
EMEA presence	10%	1.00	3.00	1.00	5.00	3.00	5.00	3.00
Asia Pacific presence	10%	5.00	5.00	1.00	3.00	3.00	3.00	1.00

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

Leaders

- **Google is continuing to invest in PCPNS.** The platform's security configuration policies are very granular in the admin console as well as in APIs. The platform has a large number of security certifications and broad partner ecosystem, offers deep native support for guest operating systems and Kubernetes containers, and supports autoscaling (GPUs can be added to instances). Role-based access controls can be very complex, and some users may find active directory (AD) sync hard to configure. The solution does not yet offer hardware security modules, but this is planned for 2H 2018. The vendor plans to: 1) provide ongoing security improvements to the admin console using device trust, location, etc.; 2) implement hardware-backed encryption key management; and 3) improve visibility into the platform by launching a unified risk dashboard.
- **AWS shows strong use of APIs across PCPNS.** Across vendors evaluated, AWS shows high degrees of security thinking at IaaS platform design time. The admin console has very flexible and configurable IAM roles, while Inspector provides valuable security features for guest operating systems (OSes). Amazon VPC is robust for network separation, while Macie allows for discovery and classification of data in workloads. AWS keeps all its security revenue and customer install base numbers under tight wrap — which may hinder customers' ability to adequately judge AWS' adoption and fit. KMS is harder to use than competitors, and dashboards are not very configurable.

Strong Performers

- **Microsoft security integrates with PowerShell.** Much of the security functionality in the Azure management console is available in PowerShell scripting — a benefit for seasoned Windows systems administrators. The solution offers versatile access reviews for privileged users, a robust encryption key vault management, IDS/IPS investigation, and firewall configuration. MFA and RBA setup in the console is difficult. Navigation in the console is hard (confusing icons on the left hand side), and online, built-in help is not helpful. The vendor plans to: 1) implement passwordless authentication and conditional access; 2) improve developer integration using Microsoft Graph; and 3) provide workload security baselines out of the box.
- **Alibaba offers high SLAs and simple guest VM encryption.** Forrester's customers find Alibaba's RFP responses easy to evaluate. The solution provides simple and effective guest OS encryption, has its own key management system, and offers DDoS and firewalling with deep learning capabilities and strong dashboarding. The solution is not yet ISO 270017/19 certified and lacks an extensive security partner ecosystem. It has no native support for containerization and lacks English admin UIs for about 30% of total PCPNS functionality. The vendor plans to: 1) improve its data security to cover the entire data life cycle; 2) improve automated product security life cycle (code review, penetration testing, and response); and 3) offer certified cloud migration paths.
- **IBM blends its security portfolio into its cloud platform.** IBM was a nonparticipating vendor in this Forrester Wave. IBM merged its SoftLayer, Bluemix, and PaaS capabilities into IBM Cloud. The solution has an impressive set of regulatory compliance certifications and a broad implementation partner ecosystem. Customers mention Security Analytics (QRadar) integration with IBM Cloud as a viable offering. However, pricing and market presence information is hard to come by, and RBAC and hypervisor security are not exposed. Marketplaces are behind other cloud platforms. The vendor plans to: 1) imbue machine learning into its configuration management; 2) offer bring-your-own security to its customers; and 3) support containers and DevOps tool integration.

Contenders

- **CenturyLink offers a compact but comprehensive security pane to VMware.** In the background, CenturyLink is a web-based management platform for managing a VMware ESX-based public cloud platform. Customers report that the vendor's RFP responses are easy to evaluate. The solution offers a solid Ansible integration support strategy. IAM features in the console (AD integration and user bulk import), storage encryption, container support, and guest OS security (file integrity monitoring, antimalware, etc.) features lag behind, but the vendor plans to: 1) implement a vulnerability scanning service; 2) capture NetFlow information for forensic analysis to prevent network attacks, data exfiltration, and viruses; and 3) manage and enforce centralized authorization in the Control Portal (management console of the solution).

› **Rackspace offers its own Carina container management.** Rackspace was a nonparticipating vendor in this Forrester Wave. The solution supports its own Carina container management system and has hooks for linking into Azure IAM management. The policy management APIs and scalability of the platform are noteworthy. Cloud HSM PCPNS policy setup and management are hard. The vendor's RFP responses are difficult to evaluate, and the vendor does not easily share future road map plans with its customers.

Supplemental Material

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at the beginning of this report on Forrester.com to download the tool.

Data Sources Used In This Forrester Wave

Forrester used a combination of four data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by December 31, 2017.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with three of each vendor's current customers.
- **Unsupervised demonstration environment usage.** We asked vendors to provide us with uninterrupted and unsupervised access to the demonstration environments in which we could test the products' features and recreate the product demos at will.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate or contributed only partially to the evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, please visit The Forrester Wave™ Methodology Guide on our website.

Integrity Policy

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

Endnotes

[1] For a sample description of the shared responsibility model between the cloud platform provider and the customer organization, visit the following website. Source: "Shared Responsibility Model," Amazon Web Services (AWS) (https://aws.amazon.com/compliance/shared-responsibility-model/).

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.