The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2019

The 15 Providers That Matter Most And How They Stack Up

by Josh Zelonis
March 18, 2019

Why Read This Report

In our 11-criterion evaluation of cybersecurity incident response services providers, we identified the 15 most significant ones — Aon, Booz Allen Hamilton, CrowdStrike, Cylance, Deloitte, EY, FireEye, IBM, KPMG, NCC Group, Optiv, PwC, Secureworks, Trustwave, and Verizon — 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

FireEye, Deloitte, CrowdStrike, And IBM Lead The Pack

Forrester's research uncovered a market in which FireEye, Deloitte, CrowdStrike, and IBM are Leaders; Aon, Verizon, Cylance, PwC, Booz Allen Hamilton, and Secureworks are Strong Performers; Optiv, KPMG, EY, and Trustwave are Contenders; and NCC Group is a Challenger.

Cyber Ranges And Actionable Deliverables Are Key Differentiators

Vendors that can provide cyber ranges and actionable deliverables position themselves to successfully deliver strong incident preparation and breach response to their customers.

The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2019

The 15 Providers That Matter Most And How They Stack Up

by Josh Zelonis
with Stephanie Balaouras, Madeline Cyr, and Peggy Dostie
March 18, 2019

Table Of Contents

Related Research Documents

The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q1 2019

The Forrester Wave™: Digital Forensics And Incident Response Service Providers, Q3 2017

Mature Cybersecurity Incident Response Requires Legal Advice

FORRESTER®

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

Preparation Is The Key To Timely Incident Response

In 2019, pragmatic businesses not only accept that they will likely suffer a breach, they plan for it. According to Forrester Analytics 2018 survey data, 50% of global security decision makers reported suffering at least one breach in the past 12 months.[1] While suffering a breach may be inevitable, properly preparing for and responding to a breach is the best way to curtail damage. That's why 59% of global enterprise security decision makers have indicated that they have an incident response as-a-service agreement in place and another 19% are planning to implement one in the next 12 months.[2]

To ensure ultimate breach prep and response, cybersecurity incident response services customers should look for providers that:

- **Have cyber range capabilities.** Immersive training facilities that simulate large-scale cyberattacks are used to help train employees on their cyberplan to ensure a cohesive response in the event of an incident. The vendors that provide these services are filling a growing need for real-world breach training.[3]
- **Can outsource capabilities if an industrial incident escalates beyond the controller.** If you have operating technology (OT) or industrial control systems (ICS), look for vendors that have a team with strong ICS and OT experience or strong partnerships to outsource ICS incidents to vendors such as Belden, Dragos, Nozomi, and Waterfall.
- **Have actionable and thorough deliverables.** Beyond providing a postmortem of the incident and what went wrong, reports need to include a road map for implementing remediations and easily consumable information about the incidents that may be shared with security operations and your threat intelligence teams. The best vendors include appendices of indicators of compromise (IoC) including file hashes to achieve this.

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 does not represent the entire vendor landscape. You'll find more information about this market in our reports on cybersecurity incident response services.[4]

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™: Cybersecurity Incident Response Services, Q1 2019

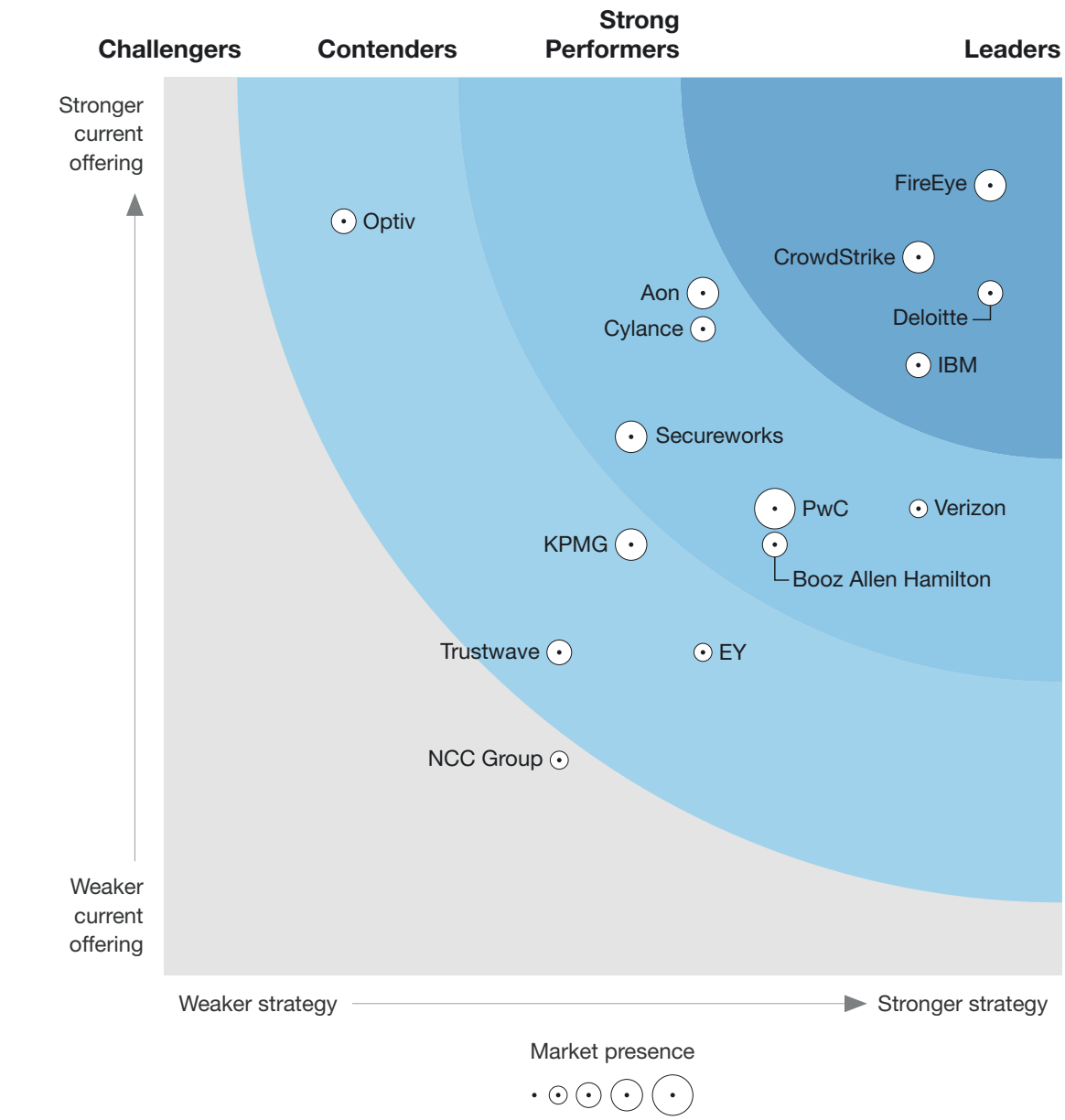

FIGURE 2 Forrester Wave™: Cybersecurity Incident Response Services Scorecard, Q1 2019

	Forrester's weighting	Aon	Booz Allen Hamilton	CrowdStrike	Cylance	Deloitte	EY	FireEye	IBM
Current offering	50%	3.80	2.40	4.00	3.60	3.80	1.80	4.40	3.40
Incident preparation	40%	3.00	1.00	3.00	3.00	5.00	1.00	5.00	5.00
Incident response	20%	3.00	3.00	5.00	5.00	3.00	3.00	5.00	1.00
Post-incident reporting and support	30%	5.00	3.00	5.00	3.00	3.00	1.00	3.00	3.00
Industrial control systems	10%	5.00	5.00	3.00	5.00	3.00	5.00	5.00	3.00
Strategy	50%	3.00	3.40	4.20	3.00	4.60	3.00	4.60	4.20
Incident preparation vision	20%	5.00	5.00	5.00	3.00	5.00	3.00	5.00	3.00
IR retainer vision	20%	3.00	1.00	5.00	3.00	3.00	1.00	3.00	5.00
Supporting products and services	20%	1.00	3.00	3.00	5.00	5.00	3.00	5.00	5.00
Geographic presence (market approach)	20%	3.00	5.00	3.00	1.00	5.00	5.00	5.00	3.00
Talent management	20%	3.00	3.00	5.00	3.00	5.00	3.00	5.00	5.00
Market presence	0%	4.00	3.00	4.00	3.00	3.00	2.00	4.00	3.00
Average hours per response	50%	3.00	1.00	3.00	5.00	3.00	1.00	3.00	5.00
Hours performing incident prep	50%	5.00	5.00	5.00	1.00	3.00	3.00	5.00	1.00

FIGURE 2 Forrester Wave™: Cybersecurity Incident Response Services Scorecard, Q1 2019 (Cont.)

	Forrester's weighting	KPMG	NCC Group	Optiv	PwC	Secureworks	Trustwave	Verizon
Current offering	50%	2.40	1.20	4.20	2.60	3.00	1.80	2.60
Incident preparation	40%	3.00	1.00	5.00	3.00	3.00	3.00	1.00
Incident response	20%	3.00	1.00	3.00	1.00	1.00	1.00	5.00
Post-incident reporting and support	30%	1.00	1.00	5.00	3.00	5.00	1.00	3.00
Industrial control systems	10%	3.00	3.00	1.00	3.00	1.00	1.00	3.00
Strategy	50%	2.60	2.20	1.00	3.40	2.60	2.20	4.20
Incident preparation vision	20%	1.00	1.00	1.00	3.00	5.00	1.00	3.00
IR retainer vision	20%	1.00	3.00	1.00	3.00	1.00	1.00	5.00
Supporting products and services	20%	3.00	3.00	1.00	3.00	3.00	5.00	5.00
Geographic presence (market approach)	20%	5.00	1.00	1.00	3.00	3.00	3.00	5.00
Talent management	20%	3.00	3.00	1.00	5.00	1.00	1.00	3.00
Market presence	0%	4.00	2.00	3.00	5.00	4.00	3.00	2.00
Average hours per response	50%	3.00	3.00	5.00	5.00	5.00	3.00	1.00
Hours performing incident prep	50%	5.00	1.00	1.00	5.00	3.00	3.00	3.00

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

Vendor Offerings

Forrester included 15 vendors in this assessment: Aon, Booz Allen Hamilton, CrowdStrike, Cylance, Deloitte, EY, FireEye, IBM, KPMG, NCC Group, Optiv, PwC, Secureworks, Trustwave, and Verizon (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor
Aon
Booz Allen Hamilton
CrowdStrike
Cylance
Deloitte
EY
FireEye
IBM
KPMG
NCC Group
Optiv
PwC
Secureworks
Trustwave
Verizon

Vendor Profiles

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

Leaders

› **FireEye has an intelligence-driven approach to preparation and breach response.** FireEye is a global company with a direct sales approach as well as multiple go-to-market channels through law firms and cyberinsurers. It is focused on providing customers a road map of proactive services to enhance the ability to respond to cybersecurity incidents.

FireEye has a cyber range where it offers training as an intermediary step between tabletop exercises and purple team engagements, to allow live fire exercises in a safe environment. While its retainer offerings are less well defined, its client references were still positive. FireEye would be an excellent partner to improve your ability to respond to incidents.

› **Deloitte enables clients to manage high-impact events with confidence.** Deloitte is a global consultancy with cyberintelligence integrated into its end-to-end services to ensure incident readiness for clients. It has a deep understanding of the requirements for a successful incident response and differentiates in how it articulates these requirements.

Deloitte offers a broad spectrum of services, but client references indicate challenges with communication during incident triage and response. Due to the breadth of services provided by Deloitte, we have observed that in many situations, it is already onsite and ready to begin triage when a breach occurs.

› **CrowdStrike has an advantage in its threat intelligence and response expertise.** CrowdStrike is a global company built on three pillars: threat intelligence, endpoint protection, and incident response. Each of these capabilities not only informs the others but is buttressed by complementary services as well.

CrowdStrike is focused on helping its clients understand how to improve their cybersecurity IR capabilities through the mantra “Am I breached? Am I mature? Am I ready?” While CrowdStrike doesn’t have in-house capabilities for responding in ICS environments, it does have a partnership in place with Dragos to provide this service. Customer references were positive, demonstrating client confidence. CrowdStrike would be an excellent partner for cybersecurity IR, whether you use its endpoint products or not.

› **IBM has an advantage in the people, products, and services it can deliver.** IBM is a global company that is able to deliver local resources to support response efforts. It attaches X-Force threat intelligence analysts to its IR teams to ensure full situational awareness across the investigation.

IBM prides itself on its incident preparation services, including a cyber range where it offers incident responder training as well as war-gaming exercises. While client references were satisfied with provided services, IBM had the lowest satisfaction rating for how it communicates expectations to the client during a response. IBM is a strong choice for training and incident preparation services.

Strong Performers

› **Aon has a plan for the future of cyberinsurance brokerage and the midmarket.** Aon is a global company, and its acquisition of Stroz Friedberg has helped it market its cyberoperations capabilities primarily in North America and EMEA. It also has an ICS lab in Dallas to pursue the regional opportunities with oil and gas companies.

Aon wants to be your partner and advocate, working with clients to assess their cybersecurity posture to help facilitate negotiation of insurance deductibles and premiums. Aon received high marks across the board from client references for its cybersecurity incident response work. It would be a fine choice for organizations wanting a broker that can perform IR services and be their advocate to cyberinsurance issuers.

- **Verizon ensures timely response with well-defined escalation paths, service levels.** Verizon is a global company with forensic labs distributed worldwide and a broad set of security services it brings to the market. It continually reviews legal and regulatory matters to defend its clients from the inevitable litigation that follows a major incident.

  Verizon has an excellent vision for its Rapid Response Retainer Service and has demonstrated expertise in performing digital forensic investigations. Client references were positive, but not outstanding. Verizon would be a strong choice for any organization looking to engage it for its retainer offering.

- **Cylance has well-defined processes and tooling to ensure effective incident response.** Cylance is a global company that will only have greater reach with its recent acquisition by BlackBerry. It has a wide range of products and services, and it has established partnerships with law firms as well as insurance brokers and carriers.

  Cylance has demonstrated incident response expertise including investigating industrial control system (ICS) environments. It's weaker when it comes to compliance reviews, frequently relying on clients to be aware of regulatory issues impacting how it should conduct the investigation. Overall, it receives positive feedback from client references and would be a good all-around choice.

- **Booz Allen transforms its clients' IR program with pre- and post-incident services.** Booz Allen Hamilton is a global company with a strong ICS capability. It differentiates with a broad range of security suites it uses throughout an investigation. It's focused on helping clients not only respond to incidents but build the capabilities they need to combat future issues.

  Booz Allen Hamilton has an excellent vision for incident prep that follows the critical stages of diagnostic measure, management, and maturation. Client references were satisfied with post-incident response services but indicate a lack of engagement around proactive services. Booz Allen would be an excellent choice for ICS-related responses leveraging its global presence outside North America.

- **PwC has a strong vision and road map for the journey to incident preparedness.** PwC is a global consultancy that differentiates with talent management, especially around embracing diversity in its workforce. If you're in a pinch and don't have a cybersecurity incident response firm on retainer, PwC offers a suite of escalation channels and will activate a response in under an hour.

PwC has a strong retainer strategy supported by a standard set of preparatory service offerings if you don't need to use the purchased hours for an investigation. Client references were generally positive, although there was some concern about PwC's ability to make stated SLAs. PwC would be a good choice if you need a reputable, global consultancy that can provide incident response support and help you develop a road map for improving your response capabilities.

› **Secureworks has a strong vision for preparing clients to respond to incidents.** Secureworks is a global company with excellent post-incident reporting and a college program that ensures a steady stream of talent within its ranks. Surprisingly, one-third of the IR engagements are with net-new clients.

Secureworks' ability to communicate a road map for prep services based on customer maturity and need is a key differentiator for it. The SLA attached to its retainers is weak, potentially the source of weak customer references regarding the ability to communicate expectations for triage and escalation during a breach response. Comprehensive post-incident reporting and its incident preparation vision are two reasons to select Secureworks.

Contenders

› **Optiv has a well-stated engagement model and ability to manage diverse product sets.** Optiv is primarily a North American company that performs the majority of its IR work for clients through existing relationships, either as a client's value-added reseller (VAR) or a managed security service provider. Its focus is on serving a broad customer base with a wide variety of needs.

Optiv is the rare company in a Wave that has an excellent current offering but comes up short in detailing its overall strategy. It has a well-stated engagement model, and its postmortem deliverables include remediation road maps to help clients avoid repeat occurrences, and its client references were positive across the board. Optiv would be a good choice from incident preparation through remediation.

› **KPMG strives to understand client needs to deliver tech-enabled solutions.** KPMG is a global company that delegates regional responsibilities to member firms to ensure investigations comply with applicable local laws. Unique across the major consultancies is its focus on developing internal solutions to allow it to deliver better results to clients.

KPMG leverages flying squads that have regional responsibilities and, as a result, is versed in local laws. It received positive feedback across the board from client references. If you need a global consultancy with regional expertise, KPMG would be a strong choice.

› **EY views cybersecurity IR as an ongoing cycle of proactive readiness and response.** EY is a global company that performs the majority of its IR work for current clients. By integrating a zero-dollar retainer into many of its master services agreements (MSAs), it enables delivery of cybersecurity incident response services on-demand for these clients.

EY has a lot of expertise working in ICS environments, including having the ability to perform bespoke work and leverage experts from the manufacturers themselves as necessary. Client references were generally positive, although on the lower end of vendors in this evaluation. EY is a good choice for organizations requiring a global consultancy with unique skillsets.

› **Trustwave has a client-first approach to supporting services and packaged solutions.** Trustwave is a largely global company with gaps in Africa and mainland Asia. It differentiates by scoping projects and determining compliance requirements as part of retainer onboarding to ensure parity with client needs.

Trustwave postmortem deliverables are extremely technical, even including malware disassembly, but it conspicuously leaves out the types of indicators of compromise that would be actionable by the inheriting organization. While client references generally gave positive feedback for Trustwave, they indicated some concern about its ability to meet SLAs. Trustwave would be a good choice for an organization looking for capable expertise combined with a managed security service offering.

Challengers

› **NCC Group focuses on metrics and quantification to facilitate board-level discussion.** NCC Group has limited global presence, primarily focused in EMEA with some North American and Australian presence. One of its key focus areas is helping prepare clients for board and C-level conversations.

NCC Group strives to make preparatory engagements as realistic as possible by leveraging recent incidents as material for tabletop exercises. Client references appear satisfied with the delivered capabilities and were generally positive across the board. NCC Group is a good choice for organizations looking for an alternative to the Big Four.

Evaluation Overview

We evaluated vendors against 11 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: incident preparation, incident response, post-incident reporting and support, and industrial control systems.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated: incident preparation vision, IR retainer vision, supporting products and services, geographic presence (market approach), and talent management.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's average hours per response and hours performing incident prep.

Vendor Inclusion Criteria

Forrester 15 vendors in the assessment: Aon, Booz Allen Hamilton, CrowdStrike, Cylance, Deloitte, EY, FireEye, IBM, KPMG, NCC Group, Optiv, PwC, Secureworks, Trustwave, and Verizon. Each of these vendors:

- **Has supported over 120 incidents in the last 12 months.** We included vendors that have claimed to work on at least 120 cybersecurity incidents and breaches in the last 12 months. This allowed us to focus not only on the most significant providers but also the providers that have the scale and the expertise to handle complex enterprise requirements.
- **Has assisted in over 20 tabletop exercises.** Strong incident preparedness work such as conducting tabletop exercises before a breach is critical to success. We selected vendors that had done at least 20 table top exercises in the last 12 months.
- **Has significant interest from Forrester customers.** When selecting vendors for inclusion, we also took into account how frequently they are mentioned in our client inquiries.

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 January 22, 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] Source: Forrester Analytics Global Business Technographics® Security Survey, 2018.

[2] Source: Forrester Analytics Global Business Technographics Security Survey, 2018.

[3] See the Forrester report "The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q1 2019."

[4] See the Forrester report "The Forrester Wave™: Digital Forensics And Incident Response Service Providers, Q3 2017" and see the Forrester report "Mature Cybersecurity Incident Response Requires Legal Advice."

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.