IDC MarketScape

IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency Services 2018 Vendor Assessment — Beyond the Big 5 Consultancies

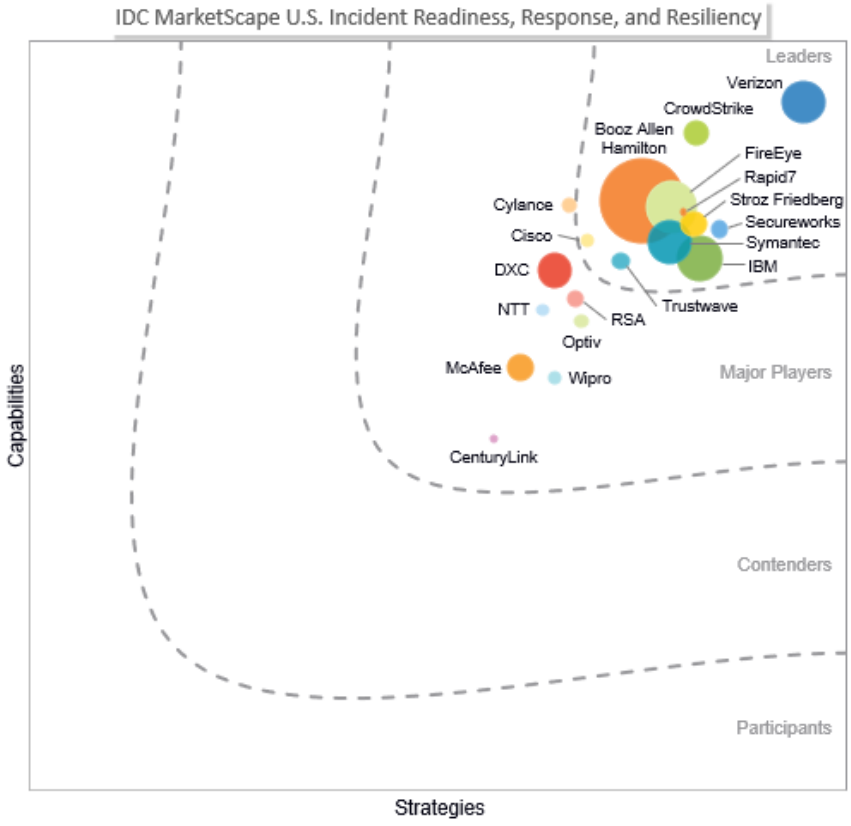
Christina Richmond Pete Lindstrom

THIS IDC MARKETSCAPE EXCERPT FEATURES TRUSTWAVE

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape U.S. Incident Readiness, Response, and Resiliency Vendor Assessment



Source: IDC, 2018

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

September 2018, IDC #US44257117e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency Services 2018 Vendor Assessment — Beyond the Big 5 Consultancies (Doc # US44257117). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Advice for Technology Buyers, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The incident response (IR) services marketplace comprises providers such as the Big 5 consulting firms, start-ups, security services consulting organizations, and managed security services providers (MSSPs). Earlier in 2018, IDC published its first document on incident readiness, response, and resiliency services when it looked at the Big 5 U.S. consulting firms in *IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency 2018 Vendor Assessment — Big 5 Consulting Firms* (IDC #US43588417, March 2018). The current document reviews companies that do not fall under the Big 5 definitions. It includes those providers whose revenue is derived from both the small and the midmarket as well as the large enterprise and government.

While traditional incident response is focused on identifying and containing a security breach or attack, this document broadens the scope to include pre-attack readiness and post-attack resiliency. IDC believes that service providers need to evolve beyond a point-in-time engagement, to both satisfy increasing demand for security consulting and remain competitive and viable.

Enterprises can differentiate their security programs with readiness, response, and resiliency capabilities. Even those with no immediate need for incident response services struggle with ensuring they are ready to respond to a large incident, and fairly routine smaller incidents may turn into larger ones. The experience that IR service providers gain from working on many different incidents at many different companies is an invaluable perspective that enterprises crave for strategic planning purposes.

Using the IDC MarketScape model for this study, IDC has compared 19 U.S. firms whose revenue is derived from small, midmarket, and large enterprises or government and that offer IR services. Through in-depth interviews with the service providers and their customers, IDC evaluated the vendors in this study of comprehensive IR services and, through granular evaluation, IDC found that each provider possesses certain strengths and weaknesses when compared with a peer group. The differences appear in both current capabilities and future strategies.

Some of the service provider capabilities that were reviewed during the study are:

- Breadth and depth of core and complementary offerings, encompassing readiness, response, and resiliency
- IR services delivery methods (remote, onsite, private cloud, public cloud)
- Methodology, including approach to analyzing, scoping, and validating incidents for purposes of prioritizing IR activities
- Customer communication strategy
- Incident checklists and documentation
- Investigation and case management tools
- Threat intelligence and big data/analytics capabilities

- Service-level agreements (SLAs), retainers, and onboarding processes
- Bench strength and skills of IR personnel
- Talent acquisition, retention, and education/reskilling

IDC believes there are several service provider capabilities that will drive growth and maturity in the IR marketplace, and allow service providers to sharpen and differentiate their value propositions. These are described in the Appendix section of this report.

For this IDC MarketScape study and evaluation series, IDC grouped the service providers into the following categories:

- Big 5 firms that often sell more strategic services that are acquired through a CFO's office
- Service providers that fall outside the "Big 5 consultancy" definition and have the resources and experience levels to be able to assist in major incidents

Please refer to *IDC MarketScape: U.S. Incident Readiness, Response, and Resiliency 2018 Vendor Assessment – Big 5 Consulting Firms* (IDC #US43588417, March 2018) for insight into the Big 5 capabilities.

Cautionary note: Do not read this document by scanning only the Leader quadrant. All participants in this study have been selected because they are strong providers and each participant differentiates itself uniquely. It is entirely possible that the best IR service provider for your company is a Major Player and not a Leader. Also use caution in equating the size of the marker in Figure 1 with the most experienced and appropriate provider to your business. As noted in the Appendix, the size of the individual vendor markers in the IDC MarketScape represents the *relative* market share of each individual vendor within the specific market segment being assessed. Many up and coming, newer providers are experiencing rapid year-over-year growth because of new technologies and approaches and should be considered.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 19 IR service providers as part of this IDC MarketScape. IDC narrowed the field of providers for this study based on the following criteria:

- **Standalone service capability across the incident readiness, response, and resiliency life cycle.** Each service provider was required to possess delivery capabilities in some or all of the incident readiness, response, and resiliency life cycle (see the Appendix for an explanation of incident response).
- **Retainers.** There is a broad range of retainers offered within incident response services. For the Big 5 consulting document, it was a requirement to offer retainers. In this second document, there is more of a variety with some service providers not offering retainers and/or including incident response within managed security services (MSS).
- **Revenue.** While there was no minimum required, each service provider was required to prove 2017 U.S. revenue garnered in the incident response arena.
- **Geographic presence.** Each vendor was required to have IR delivery capability in the United States.
- **Time frame.** The time period studied was 2016-2017, with research ending toward the middle of 2018. It is possible that service providers have enhanced services since that time. Where

possible, IDC notes that changes are expected, but it is incumbent upon the buyer to request a services update from the shortlist of companies you have compiled.

ADVICE FOR TECHNOLOGY BUYERS

Organizations that want to conduct a thorough evaluation of incident response services face a challenging task. The marketplace is heavily fragmented with some providers highlighting certain capabilities like criminal investigations, technical prowess, breach or attack type, or even worldwide presence. They may focus on certain industries like retail or government support, and they may go to market through the CFO or the IT department. As a result, some enterprises choose to have multiple relationships with multiple IR providers for specific services. Enterprises rarely outsource IR services entirely but augment to lesser or greater degree their in-house IT/IR staff, processes, and technology.

Enterprise approaches to evaluation and selection of IR service providers vary widely — another indication of marketplace turbulence. Vendor selection criteria were discussed during customer interviews, and they include multiple factors — the most highly rated of which are outlined here:

- Reputation and previously existing relationships
- Global response capability
- Nature of breach
- Response times
- Depth of experience, technical competence, and forensics capabilities
- Industry-specific experience

Additional but less significant factors included market positioning, full service versus component offerings, pricing, flexibility with pricing and terms and conditions, performance in a trial event, resource availability, location and certifications, references, breadth of tools, customer service, and infrastructure support and collaboration.

The main reasons to choose a provider is their technical acumen, reputation for security technology, security operational management, and threat visibility. These firms have other attributes, strengths, and weaknesses that may be evaluated and compared with other IR responders as indicated:

- Select a strategic provider as your key readiness, response, and resilience firm prior to any incident occurring. Consider a retainer, or at least work with the applicable provider, to ensure you understand its methods and it is familiar with your organization.
- Use smaller breach readiness projects such as penetration testing, tabletop exercises, and red teaming to test the capabilities of your strategic provider. Ensure it is providing key insights and management oversight, as well as demonstrating its communication skills.
- Ensure that providers have the resources available to address the business, technical, and communication needs of your organization. Constantly reassess these resources as consultants come and go from the providers.
- Fill provider gaps based on circumstances when situations arise. One provider may not be able to provide all the services necessary. When the time comes, this strategic provider should be able and willing to assist in identifying key services that will be more pertinent to the situation. If the provider can't recognize its own gaps and assist in filling them, it should not be a strategic partner.

- Ensure that your IR provider has standard methods and timing for pertinent communications during an incident, and that it is building an incident portfolio that includes details as addressed in reference architectures that avoid ambiguities in certain reference name expressions (such as a "ref1..ref2" format) along the way. The key guiding criteria should be whether someone reviewing the information in three years (such as trial lawyers) will be able to understand exactly what occurred.
- Be wary of technical lock-in. Evaluate any tools that may be required independently for strategic portfolio fit within the organization. If a provider requires technology that must be purchased but isn't a strategic solution, consider other options.

As part of the broader decision process, organizations should bear in mind the following considerations and recommendations:

- **Breadth of offerings, including core and complementary services.** Identify the types of services that are offered by each service provider you evaluate. You may need to make a decision about whether to acquire all the needed services from a single provider or from two or more providers.
- **Incident response plan testing.** No matter how good a plan is, you don't want to be putting it and your playbook into action for the first time during an actual cyberattack. Testing approaches include:
  - Simulation/cyber range/war gaming immersive simulations of a breach beyond tabletop exercises, which include all stakeholders that would be included in a real incident: C-suite executives, legal, corporate communication, the board of directors, the crisis team, the systems organization, and the IT organization
  - Desktop/tabletop exercises involving key stakeholders and the IT organization
  - Red/blue/purple team penetration testing and corresponding practice drills involving key IT organization personnel
- **Scope of delivery methods.** Match up your requirements with providers' ability to deliver services remotely and at onsite locations worldwide.
- **Types of attacks.** Not all service providers respond to all types of attacks. Some specialize in malware-related and other technical attacks, while others may address spear phishing and criminal investigations.
- **Policy and plans.** Providers discussed in this study offer all or most of the policy and plan creation elements included in NIST 2.3 (NIST A [2012] **nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**). Some go beyond NIST to align with other industry standards by including additional or optional supplemental services. Be sure that policies and plans are integrated across business units, departments, locations, and so forth. Responsibilities, decision-making paths, and prescribed actions should be clear to all who are involved in incident detection and response.
- **Partner versus vendor delivery.** If the providers you are evaluating engage delivery partners in some capacity, be clear about who is providing what, as well as the lines of responsibility and accountability. Some partnerships are formed for purposes of the PCI Forensic Investigator Program because this type of investigation may present a conflict of interest depending on a provider's overall business offerings. Other partnerships may be to extend resource capacity during a surge of events.
- **IDC's recommendation: a published standard (e.g., NIST, ISO, or SANS Institute) should be the foundation of a participant's offering.** Review the methodology of service providers so that you feel comfortable with their approach. While every attacker and breach are different, the

methodology should be a proven process that undergoes continual improvement based on postmortems and lessons learned. A service provider should be able to explain its methodology in detail, provide or show sample deliverables, and discuss IR team roles and responsibilities and how and why they may change over the course of an engagement. It may be helpful to review the methodology against one or two scenarios that are plausible for your organization.

- **Service-level agreements and retainers.** A retainer agreement details the terms, conditions, and timing of incident response.

  The most common arrangement is a retainer to which SLAs are attached, and these may be tiered. Customers pay an up-front fee to have the service provider "on call" for future assistance. Onboarding approaches vary from provider to provider as is the time required to complete the paperwork.

  Be sure your service provider allows you to apply unused retainer dollars toward other services (see Table 1).

- **Documentation.** It is worthwhile to compare the standard items or issues tracked by service providers during an IR engagement. Some service providers augment the list described in NIST 3.2.5 (NIST A [2012] **nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**).
- **Communications.** IDC believes the optimal approach to communications during an incident response engagement is for the provider to use some standard templates and some ad hoc communications tailored to the specifics of the client and investigation. Ideally, written communications supplement interactive communications such as daily briefings, but the cadence of all communications should be agreed upon by the provider and the customer.
- **Containment strategy.** Ask service providers to describe the criteria they have established to help them choose and recommend a containment strategy. IDC believes the most important criterion is operational impact — that is, keeping the business running.
- **Pricing models for incident response services.** Assume that pricing models are negotiable, at least to some extent. Models include retainer, per hour, per day, per week, and discounts on multiple services. Retainers are typically set up on an annual basis. Some providers have developed variations such as:
  - A fixed price offering with a set number of hours for emergency response
  - Tiers of hours attached to retainers
  - Ad hoc services negotiated with blocks of time
  - Flexible pricing based on scope of work
  - Zero-dollar retainers
- **Security talent.** While certifications were generally viewed by end customers as important but not critical, they can be an indicator of a provider's investment in its people, along with mentorship, training, and systems for sharing information among first responders. Evaluation of talent without firsthand experience is difficult, so it may be helpful to understand how the provider forms IR teams and matches team member skills to customer requirements. Should you require incident response in multiple locations, you may want to compare the qualifications, experience, and skills of the potential or assigned teams that could be involved. And, if top requirements include skills, such as management/board-level presentations, or expertise in specific areas, such as risk or compliance, understand how these resources are incorporated into the provider's team.

- **Customer service.** Find out whether your potential service provider has a formal customer experience program if this is important to your organization. If it is, you may want to delve into the specifics. For example, understanding how customer satisfaction is determined and how planned service improvements are validated with customers. A dedicated account manager can be essential to the delivery of consistent customer service, but processes should be in place to ensure that the service level isn't dependent on a single person.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of the vendor's strengths and challenges.

Trustwave

Trustwave is positioned as a Leader in the 2018 IDC MarketScape for U.S. incident readiness, response, and resiliency services — beyond the Big 5 consultancies.

Trustwave is a cybersecurity and managed security services provider that has a strong history and foothold in the compliance market. Through the cloud-based TrustKeeper platform, which boasts more than three million enrollees, Trustwave offers automated and cost-effective data protection, risk management, and threat intelligence to its customers. Customers range from small to midsize companies as well as distributed enterprises that need to be in compliance with various regulations.

Trustwave's incident response and readiness program (IRRP) provides 24 x 7 global expert response with flexible hours, IR assessment to determine current incident response maturity level, and risk assessments to identify the client's ideal state. Typically, multiyear strategic plans are developed to help the client achieve a 4-hour remote and 24-hour onsite SLA, if required. Training, plans, and playbooks are all customized to individual client requirements.

Trustwave goes through a 10-point plan in its IRP:

- IR assessment to assess the infrastructure and processes against security incident readiness
- Development of computer security incident response plans, playbooks, templates, and procedures
- Security fundamentals, incident response, and advanced forensics/malware analysis training
- Team development and analysis of the roles of IR team
- First-incident responder advanced technical training for IR team
- Tabletop exercises for decision making and to build procedural exercises in order to digest the IR plan and review the processes
- Attack simulations/purple teaming scenarios that simulate real attacks or run live-fire exercises to test people, technology, and procedure readiness under real incidents
- Project close/review and deliverables to customer
- Annual repeated review of tabletop exercises and existing plan
- IR Retainer at reduced rate for any incident that may arise during the contract, if no incident hours may be substituted for other services

Strengths

The Trustwave project update report provides clear update and very clear insight into the number of hours remaining in the retainer. One customer stated that it, "couldn't speak higher of [Trustwave personnel] and of the speed with which Trustwave responded." This customer rated Trustwave highly because it'd "never had a provider respond so quickly and their technical expertise was incredible."

Another customer mentioned that "account management has been fantastic and Trustwave is very communicative. They do a great job of listening to your needs. Any time we've used their services they are extremely responsive. They want to solve the problem and are not just watching the clock."

Challenges

A customer stated that Trustwave's "tabletop exercises are about average compared to others in the marketplace." Trustwave does not have plans for offering integration into customer response management systems. This appears to be a growing trend which Trustwave might wish to consider.

Consider Trustwave When

Small to midsize companies and distributed enterprises that have tight compliance restrictions should look at partnering with a company such as Trustwave.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the relative market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to

provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Breach or incident response planning aims to help organizations prepare to act in the case of security breach or attack by putting in place organized procedures to manage the effect of a breach in the event of such a security incident. The objective is to limit the damage of the security incident and reduce recovery time and costs through the prompt identification, isolation, and eradication of the problem. Incident response readiness or planning sets policies that define what is considered as an attack and also puts in place a well-defined, step-by-step process to be followed in case of an incident. Incident resiliency aims to continue the improvement trajectory set out during readiness and response.

LEARN MORE

Related Research

- *IDC's Worldwide Security Products Taxonomy, 2018* (IDC #US43535614, February 2018)
- *Worldwide Data Loss Prevention and Classification Market Shares, 2016: Cloud Disruption Ahead* (IDC #US43408717, January 2018)
- *Meltdown, Spectre Attack Dangers Require Careful Risk Analysis, Thorough Patch Testing* (IDC #IcUS43470218, January 2018)
- *Worldwide Security as a Service Forecast, 2017-2021* (IDC #US43234517, December 2017)
- *IDC FutureScape: Worldwide Security Products and Services 2018 Predictions* (IDC #US43286117, December 2017)
- *Worldwide Threat Intelligence Security Services Forecast, 2017-2021* (IDC #US43149317, November 2017)
- *Pursue Patch Independence: Latest WannaCry Event Prompts Need for Risk-Based Defenses* (IDC #US42570717, May 2017)

Other Resources

- Community emergency response teams (CERTs)
- Computer security incident response teams (CSIRTs)
- Forum for Incident Response and Security Teams (FIRST)
- Carnegie Mellon University, *Handbook for Computer Security Incident Response Teams* (**resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf**)
- ISO/IEC 27035:2011, *Information technology – Security techniques – Information* security incident management (**www.iso.org/iso/catalogue_detail?csnumber=44379**)
- NIST, *Computer Security Incident Handling Guide (800-61 Revision 2)* (**nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**)

Synopsis

This IDC study presents through the IDC MarketScape model a vendor assessment of providers offering incident response services. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for incident response services. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving short- and long-term success in the incident response marketplace.

"With the relentless onslaught of sophisticated cyberattacks, enterprises must be proactive about incident readiness, response, and resiliency. In-house solutions are challenging to fund and maintain at the required level, so organizations increasingly are turning to service providers for assistance. As more providers enter this rapidly growing marketplace, buyers have more choice but also more complexity related to evaluation and selection. Thorough vetting takes time and attention to the providers' people, processes, and technology. Enterprises should make this endeavor a priority." – Christina Richmond, IDC program vice president, Worldwide Security Services.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2018 IDC. Reproduction is forbidden unless authorized. All rights reserved.