IDC MarketScape

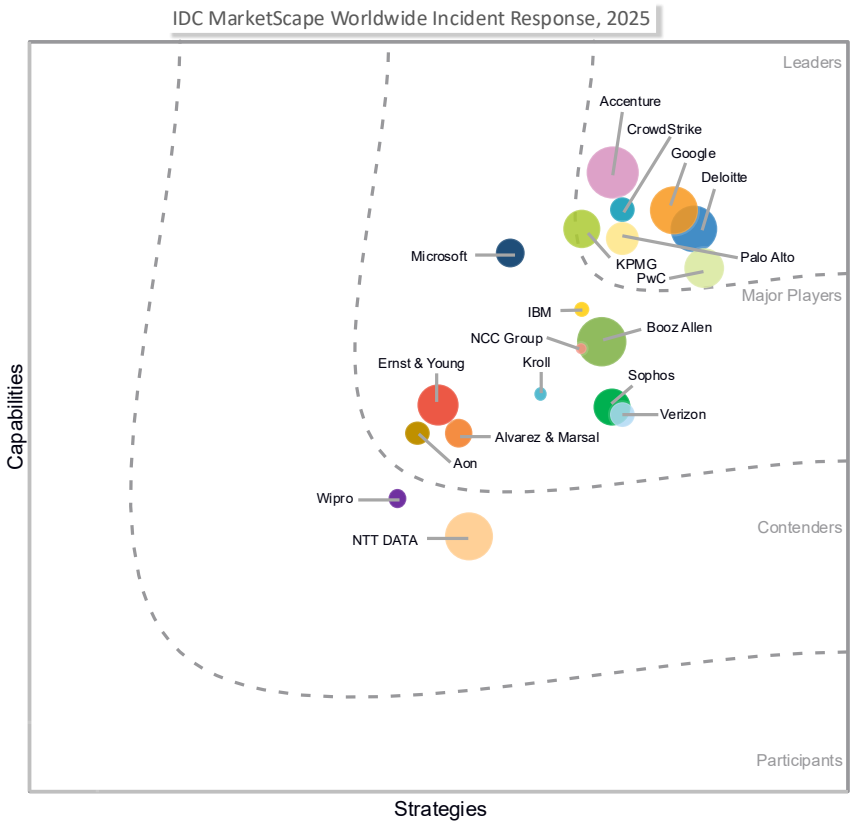
IDC MarketScape: Worldwide Incident Response 2025 Vendor Assessment

Craig Robinson Scott Tiazkun

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Incident Response Vendor Assessment



Source: IDC, 2025

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

August 2025, IDC #US52036825

IDC OPINION

There has been a dramatic sea change by organizations worldwide recognizing the need for incident response (IR) services. Fortunately for CISOs, this bodes well for giving them a chance to establish some tenure rather than the sad prior reality of seeing them being key pieces of helping their firms recover from cyberattacks only to see them forcibly removed at the end of the recovery period.

Simply stated, the threat environment has never been more elevated. The variety of attacks that nation-state actors and other cybercriminal groups can deploy against their targets is increasingly difficult to completely anticipate and stop. The need for incident response services is a matter of when, rather than "if."

IDC sees the following changes as key market movers and new realities in the incident response market:

- **Incident readiness:** As organizations increase the maturity of their cybersecurity capabilities, a strategic part of their defense has been the proactive incident readiness measures that they are utilizing. This IDC MarketScape is largely focused on the reactive pieces of incident response, but a key part of building up the muscle memory of incident response is dependent on what happens before a major attack actually lands.

  Readiness activities such as tabletop exercises help drop departmental barriers as traditional tech bastions like cyber and information technology (IT) work with operations, finance, HR, and communications up and down the chain of command from analysts up to the board to measure and test their capabilities of responding to a variety of potential scenarios. These activities have helped elevate the role of the CISO to be seen as a strategic business partner rather than just being the voice that is only heard and seen in crisis situations.
- **Cyberinsurance and legal firms:** Providers of incident response have traditionally strived to sit on cyberinsurance panels as a way of gaining additional market share. This has essentially flip-flopped. True, many IR providers wish to have business relationships with cyberinsurance providers, but the downward pressure that is placed on the hourly rates that occurs when an IR firm is "on-panel" has seen many IR providers making the strategic decision to choose to be "off-panel." Being off-panel means fewer automatic referrals, but it can offer more control, higher margins, and stronger client relationships — especially for firms with a strong brand or niche expertise.

  The new preferred route for many IR firms to gain additional engagements is now through legal firms. Getting on their short (but growing) list of preferred IR firms helps retain their preferred rates. Some of this activity can occur more

organically in the U.S. market as invoking "privilege" is very common, with less use of legal privilege occurs in EMEA and even less in Asia/Pacific.

- **Artificial intelligence (AI) and generative AI (GenAI) integration into incident response:** Vendors are rapidly embedding AI and generative AI into their IR workflows to enhance speed, accuracy, and scalability. Key applications include:
  - **Threat detection and triage** using machine learning (ML) and anomaly detection
  - **Automated report generation,** timeline reconstruction, and executive summaries
  - **Natural language querying** for log analysis and threat hunting
  - **AI agents** for malware analysis, code interpretation, and adversary behavior prediction
- **Global scale with local expertise:** Most leading vendors now operate with a follow-the-sun model, offering 24 x 7 global IR coverage. Localized support in native languages is very common, with AI assistants available to handle translation needs as necessary.

  Onshoring, nearshoring and offshoring options are more frequent. While not widespread as of yet, IDC believes the number of firms that start offering lower rates for lower-cost areas will change from a handful to a more significant number.
- **Industry-specific solutions:** Vendors are tailoring IR services to specific verticals such as healthcare, financial services, critical infrastructure, and manufacturing. Some firms have developed industry-specific teams for more nuanced needs such as operational technology (OT)/industrial control systems (ICS) environments.

  Locations as unique as nuclear submarines and cruise ships have seen the need for IR services. Expertise in providing IR for operating systems from the 90's, mainframes, and IoT devices were showcased, demonstrating the need for a wide range of disparate technologies.
- **Retainers:** The use of retainers in incident response is not a new phenomenon; the usage of these retainers is what has dramatically changed. It used to be easier to list what different capabilities an IR retainer could be utilized for. Today, it almost seems easier to note what retainers *cannot* be used for.

  Many firms offer different tiers in their retainers, with lower hourly rates and improved service-level agreements (SLAs) tied to higher-priced tiers. One notable innovation is with CrowdStrike's usage of a dedicated retainer management team that helps organizations ensure optimal service planning and provides proactive scheduling.

Many IR retainers also include periodic touch points and threat intelligence briefings that are tailored to the region and industry that the buying firm falls into.

- **Meeting the always growing compliance needs:** IR firms are increasingly tailoring their services to meet the diverse compliance needs of clients across industries and geographies. Many firms, such as Deloitte and PwC, embed regulatory alignment into their incident response planning, offering frameworks that map directly to standards like NIST, GDPR, HIPAA, and Digital Operational Resilience Act (DORA). These firms provide structured severity matrices, escalation protocols, and reporting templates that help clients meet legal obligations during and after incidents.

  KPMG and Google emphasize regulatory intelligence and legal coordination, offering services that include breach notification guidance, litigation support, and integration with legal counsel to preserve privilege. KPMG, for example, leverages its global law network to support clients with cross-border compliance, while Google provides escalation matrices and regulatory reporting timelines tailored to industry and jurisdiction.

  Palo Alto Networks and Microsoft focus on embedding compliance into technical workflows. Palo Alto Networks includes regulator notification tables and escalation diagrams in its IR plans, while Microsoft integrates compliance dashboards into its security tools, helping clients track and meet regulatory requirements in real time.

  Firms like Accenture and NCC Group also offer proactive regulatory monitoring, ensuring that clients' IR plans remain current with evolving laws. These services are often delivered through retainers, which include regular updates, workshops, and scenario planning.

- **Threat intelligence:** Access to deep, real-time threat intelligence is a critical enabler of effective incident response. Leading providers maintain proprietary intelligence platforms, monitor the dark web, and analyze telemetry from thousands of incidents. This intelligence informs investigations, accelerates threat actor identification, and enhances containment strategies. Some providers embed threat analysts directly into response teams, ensuring that every decision is backed by the latest insights. This capability allows organizations to stay ahead of evolving threats and respond with precision.

  Many IR firms show their capabilities around their understanding of threat actors with the reporting that they provide on a regular cadence. Annual reports such as the Verizon Data Breach Investigations Report, commonly known simply as the DBIR, and the IBM X-Force Threat Intelligence Index are two examples of reports that provide comprehensive information that can feed incident readiness and response operations. Other offerings such as Kroll's quarterly Cyber Threat

Landscape and Booz Allen's regular industry-specific threat intelligence reporting help inform the "good guys'" understanding of the ever-changing threat environment on a more frequently updated basis.

- **Ransom negotiations:** The need for a threat intelligence–led capability when negotiating with threat actors during a ransomware/encryption or extortion related attack has resulted in firms leaning into their IR firms for their negotiation skills. It is important to note right away that none of the studied firms in this study said that they will facilitate the actual payment. That is not a surprise, given some of the legal issues that surround the issue of paying ransoms.

  IDC chooses to not divulge the specific strategies that the studied IR firms choose to utilize, but there are three general strategies.

  - **No involvement:** Only one of the studied IR firms directly said that it will not negotiate or refer its clients to a third-party ransom negotiation firm.
  - **Directly negotiate:** A handful of companies noted that they will directly get involved in negotiations. They are able to deploy specialized practitioners with prior relatable experience such as a background in the U.S. Federal Bureau of Investigations (FBI) that they can utilize in the negotiations.
  - **Refer to specialized firms:** This was the most common strategy. IDC knows that the skills required to get to an acceptable outcome are very hard to obtain.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in this 2025 IDC MarketScape for worldwide incident response services, providers had to meet the following criteria:

- **Portfolio of incident management skills:** The provider must be able to provide the following capabilities:
  - Incident readiness capabilities such as incident response plan preparation and testing; tabletop exercises; red, blue, and/or purple team exercises; and contextualization of threat intelligence
  - Incident response functions such as assessing and scoping the impact and applying a severity level, scoping out the resources needed to fully contain and remove the threat actor from the environment, and utilizing a combination of the clients tooling along with the IR providers preferred toolsets to facilitate the incident response functions, follow and advise the client on all required compliance measures throughout the life cycle of the incident, work with and under the communications requirements when

incidents fall under legal privilege, and provide full remediation and recovery skills or be able to lead other firms that provide these capabilities
    - Digital forensic services include functions such as the collection of data to attribute who the attacker is, determining the root causes of the incident, and identifying the people and organizations that need to be notified about any PII or PHI data that might have been divulged
- **Geography:** The provider must operate in a multinational footprint and have customers in more than one region out of the North America, Latin America, EMEA, and APAC regions.
- **Revenue:** The provider must have more than $30 million in incident management revenue for the calendar year 2024.

ADVICE FOR TECHNOLOGY BUYERS

When selecting an IR provider, organizations must look beyond basic technical capabilities and consider a wide range of strategic, operational, and regulatory factors. The right IR partner not only helps contain and remediate cyberincidents but also strengthens an organization's overall resilience, compliance posture, and long-term security strategy.

That last note around long-term strategy was brought up by several firms in their presentations to IDC. Several firms noted that they see IR as a vehicle for better aligning their customers' cybersecurity posture and maturity in post-incident engagements. Further:

- **Technical expertise and threat coverage:** At the core, an IR provider must demonstrate deep technical proficiency across a wide range of threats — ransomware, business email compromise (BEC), insider threats, nation-state attacks, and supply chain compromises. Look for providers with:
    - Proven experience across diverse threat vectors
    - Capabilities in cloud, hybrid, and on-prem environments
    - Specialized knowledge in operational technology and industrial control systems, and a variety of operating systems that might not necessarily be widely known or supported any longer by their OEM, if applicable
    - Use of advanced tools for malware analysis, memory forensics, and endpoint telemetry
    - Capabilities in not only ingesting telemetry from your infrastructure but also the capability of natively operating your "detection and response" systems (EDR, XDR, NDR) in those crucial early hours prior to their deployment of their tooling, if needed

- **Speed and scalability of response:** Time is critical during a cyberincident. Buyers should assess:
  - Average time to triage and scope an incident
  - Global coverage and 24 x 7 availability
  - Ability to scale response teams quickly for large or multi-region incidents
  - Use of follow-the-sun models and regional staffing (onshore, nearshore, offshore)

  IDC noted in its discussions that almost all firms are quite capable of easily beating their stated initial response times. When negotiating an IR retainer, garnering better SLAs, especially for initial response/hands-on-keyboards metrics, is not a difficult ask.
- **AI and automation capabilities:** Modern IR providers are increasingly leveraging AI and automation to accelerate investigations, reduce analyst workload, and improve accuracy. Buyers should look for:
  - Use of AI for malware analysis, log triage, and threat detection
  - Agentic AI or LLM-based assistants for report generation and timeline reconstruction
  - Integration of AI into proprietary platforms or third-party tools
- **Compliance and regulatory alignment:** IR engagements often involve sensitive data and regulatory scrutiny. Buyers should prioritize providers that:
  - Offer pre-built severity matrices and escalation protocols.
  - Understand and support compliance with GDPR, HIPAA, DORA, SEC rules, and other frameworks.
  - Provide regulator-ready documentation and breach notification guidance.
  - Work under attorney-client privilege and coordinate with legal counsel.
- **Industry-specific experience:** Different industries face unique threats and compliance requirements. Buyers should seek providers with:
  - Tailored services for sectors like healthcare, financial services, energy, manufacturing, and government
  - Sector-specific playbooks, threat intelligence, and response frameworks
  - Experience with critical infrastructure and OT/ICS environments
- **Proactive services and retainer value:** A strong IR provider should offer more than just reactive support. Look for:
  - Retainers that include proactive services like tabletop exercises, compromise assessments, and IR plan reviews
  - Flexible use of retainer hours across readiness, response, and recovery

    - Regular threat briefings, regulatory updates, and scenario planning
    - Expanded ability to roll over unused retainer hours and/or funds at the end of the term (Many firms have standard terms that state the limitations at best, or no rollover allowed at worst, for unused retainer funds. This is another opportunity to get an up-front agreement that allows for more of a rollover allowance than what is in their standard policies.)

  Retainers are best used when they are, well, used! Items like pen testing, incident response plan testing and, of course, tabletop exercises are items that should have a regular cadence of usage, on top of other uses.
- **Recovery and transformation support:** Post-incident recovery is as critical as containment. Buyers should evaluate:
    - Ability to support secure rebuilds of Active Directory, cloud environments, and critical infrastructure
    - Partnerships with recovery specialists or in-house remediation teams
    - Strategic advisory for long-term transformation and resilience
- **Communication and executive reporting:** Clear communication during a crisis is essential. Buyers should expect:
    - Regular status updates and stakeholder briefings
    - Executive-level reporting tailored for the C-suite and board
    - Support for internal and external communications, including media and regulator messaging
    - Incident response planning and tabletop exercises should have specific callouts and procedures documented when it comes to all communications
- **Pricing transparency and geographic flexibility:** Cost structures should be clear and adaptable. Buyers should look for:
    - Transparent hourly or retainer-based pricing
    - Regional pricing models or discounts for different geographies
    - No hidden fees for tooling or platform use during engagements
- **Cyberinsurance and legal coordination:** Many incidents involve insurance claims and legal oversight. Buyers should ensure providers:
    - Are approved or recognized by major cyberinsurers
    - Can work under privilege and coordinate with breach coaches
    - Provide documentation and support for claims and legal proceedings

VENDOR SUMMARY PROFILES

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 each vendor's strengths and challenges.

Accenture

Accenture is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide incident response services. The firm has significantly evolved from a traditional IR provider into one that is focused on end-to-end cyber-resilience. With a comprehensive portfolio that spans readiness, response, recovery, and transformation, the firm delivers integrated, scalable, and intelligence-driven services to clients across industries and geographies.

A defining strength of Accenture's IR practice is its global delivery model. Operating under a unified command structure, the firm's 24 x 7 follow-the-sun model ensures seamless handoffs and consistent service quality across regions. This global team is not a loose federation of regional units, but a single, integrated organization with standardized playbooks, shared tooling, and centralized oversight. Clients benefit from local expertise backed by global coordination, enabling rapid and effective response to incidents anywhere in the world.

One of the most distinctive aspects of Accenture's offering is its deep expertise in crisis management and business recovery. The firm supports clients through the full life cycle of a cyberevent — from containment and forensics to executive-level decision-making and full-scale recovery. Its ability to mobilize cross-functional teams, including experts in legacy systems, cloud infrastructure, and operational technology, allows it to recover even the most complex environments.

Proactive testing and continuous readiness are central to Accenture's approach. The firm has consolidated all testing services — including red teaming, tabletop exercises, application security, and offensive security — into a single readiness and response group. This enables continuous threat exposure management (CTEM), allowing clients to move beyond point-in-time assessments to ongoing, prioritized testing based on real-world threat actor tactics. The goal is to build measurable cyberconfidence through iterative testing and improvement.

Artificial intelligence plays a pivotal role in enhancing Accenture's IR capabilities. Proprietary tools such as React (for remote forensic acquisition) leverage AI to automate data collection, triage, and threat intelligence. Accenture's tools accelerate

investigations and reduce analyst workload, while generative and agentic AI are used to support report generation, language translation, and even penetration testing.

Clients benefit from a flexible and value-driven retainer model. All retainers are paid engagements, with hours that can be used for both proactive and reactive services. Structured onboarding, quarterly briefings, and access to a global team of experts ensure that clients are prepared before an incident occurs. In select regions, Accenture is piloting enhanced onboarding models that include compromise assessments and tailored readiness plans, further increasing the value of its retainer offerings.

Strategic partnerships with well-known cybersecurity vendors such as CrowdStrike, Google Mandiant, and Rubrik enhance Accenture's ability to deliver comprehensive IR services. These alliances enable joint delivery of incident response, recovery, and transformation services. While vendor-agnostic in approach, the firm's integration capabilities ensure seamless collaboration across partner ecosystems, providing clients with solutions tailored to their environments.

Industry-specific expertise further differentiates Accenture's IR practice. The firm tailors its services to the unique needs of sectors such as healthcare, energy, financial services, and critical infrastructure. It also maintains active participation in global cybersecurity initiatives, including the Joint Cyber Defense Collaborative (JCDC), and holds certifications such as CREST and CBEST. Workforce development efforts, such as the Cyber Response Academy and Cyber Million initiative, ensure a steady pipeline of skilled professionals.

Accenture is also advancing its use of agentic AI to automate complex tasks such as penetration testing and forensic analysis. These AI agents assist human analysts in planning, executing, and documenting engagements, significantly increasing scale and efficiency. Predictive analytics is another area of focus, with the goal of anticipating threat patterns based on geopolitical and industry-specific intelligence.

To support global expansion, Accenture continues to grow its footprint through acquisitions and talent development. Recent acquisitions in Mexico and Spain have strengthened regional capabilities, while internal programs like the Cyber Response Academy and Capture the Flag (CTF) competitions uplevel their staff's cybersecurity skills. The firm is also redefining security operations center (SOC) roles to include AI fluency, data science, and automation engineering.

Strengths

Customers surveyed noted that Accenture is quite accurate in estimating up front in an IR engagement what the total costs and scope will be for its services.

Accenture can offer regional in-market resources in localized languages. Accenture also has branded Cyber Fusion Centers, SOCs, and cyber-ranges across all three markets (Americas, EMEA, and Asia/Pacific)

The company offers tools and capabilities to support all phases of IR and recovery within OT and IT environments including power, oil and gas, utilities, life sciences, maritime, and automotive. To support this, Accenture employs tooling from Nozomi, Claroty, and Splunk for commercial-off-the-shelf (COTS) solutions.

Challenges

Accenture as a global systems integrator (GSI) brings a lot of different capabilities that can be used in services such as incident response. One customer noted that on one occasion their IT/network team did not always have clear communication with the cybersecurity team. The customer did note that this was just a onetime occasion.

Consider Accenture When

Organizations with a global footprint that desire a mature, globally integrated, and innovation-driven approach to incident response should consider Accenture.

Alvarez & Marsal

Alvarez & Marsal (A&M) is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. A&M delivers a business-aligned, forensic-driven IR capability through its Global Cyber Risk Services (GCRS) practice. With a foundation in high-stakes investigations and crisis management, A&M's IR services are designed to help organizations prepare for, respond to, and recover from cyberincidents with speed, precision, and strategic clarity. The firm's credentials, including national-level certifications and global recognition, reflect its credibility and technical depth in the field.

A&M's IR methodology is structured around a full-spectrum response life cycle that includes preparation, detection, analysis, containment, eradication, recovery, and post-incident activities. The firm begins by reviewing an organization's existing incident response plan, identifying gaps, and developing or refining frameworks tailored to the client's business operations, regulatory obligations, and threat landscape. This preparation phase includes cybersimulation exercises, policy and procedure development, and deployment of new security measures to enhance readiness.

When an incident occurs, A&M's global response team can be onsite within hours, offering immediate triage and containment support. The firm's analysts are skilled in identifying indicators of compromise (IoCs), preserving evidence, and conducting forensic investigations to determine the scope and impact of the breach. Their

detection and analysis capabilities are supported by advanced network monitoring, behavioral analytics, and log analysis, enabling rapid identification of anomalous activity and attacker tactics.

Containment and eradication efforts focus on minimizing business disruption while securing the environment. This includes isolating affected systems, deploying patches, reconfiguring security devices, and hardening infrastructure to prevent reinfection. A&M's recovery services involve rebuilding compromised systems, restoring operations, and ensuring that security controls are reinforced to withstand future attacks. Throughout the process, A&M maintains close coordination with legal counsel, regulators, and law enforcement when necessary, ensuring that all actions are defensible and compliant with applicable laws.

Post-incident, A&M conducts a thorough root cause analysis and lessons-learned review. This includes identifying how the breach occurred, assessing the effectiveness of the response, and recommending improvements to policies, procedures, and technologies. The firm also supports clients in preparing regulatory disclosures, communicating with stakeholders, and managing reputational risk. A&M's emphasis on post-incident learning helps organizations build long-term resilience and reduce the likelihood of recurrence.

A&M's IR services are enhanced by its broader cybersecurity and risk advisory capabilities. The firm offers cybersecurity maturity assessments, threat modeling, vulnerability assessments, and third-party risk reviews, all of which inform and strengthen its incident response engagements. A&M's ability to integrate IR with enterprise risk management, legal strategy, and board-level reporting makes it a valuable partner for organizations seeking to align cybersecurity with business objectives.

The firm's experience spans a wide range of industries, including financial services, healthcare, retail, energy, and critical infrastructure. A&M tailors its response strategies to the unique regulatory and operational requirements of each sector, drawing on its deep bench of industry experts and former law enforcement professionals. This sector-specific expertise enables A&M to deliver contextually relevant guidance and ensure compliance with standards such as NIST, ISO, HIPAA, and GDPR.

A&M's IR team is also known for its ability to manage complex, multi-jurisdictional incidents. The firm's global footprint and multilingual capabilities allow it to coordinate response efforts across regions, ensuring consistency and speed in high-pressure situations. A&M's cyber–war room model provides a centralized command structure for managing large-scale incidents, facilitating real-time decision-making and stakeholder communication.

A&M has revealed where a lot of its future focus lies in its "Seat with an Expert" series of YouTube videos. The series emphasizes integrating advanced technologies like AI and machine learning to improve the speed and accuracy of incident response. A&M indicated its planned use of AI's role in detecting data trends, which likely informs plans to incorporate tools like A&MPLIFY into retainers for faster data triage and anomaly detection. In addition, A&M's adoption of cloud-based platforms like RelativityOne suggests future retainers will leverage scalable, cloud-driven solutions to handle complex, multi-jurisdictional incidents, ensuring rapid response times for clients under SLAs.

A&M's global expansion of cybersecurity expertise is another key focus, likely enhancing IR retainers with region-specific capabilities. A&M's commitment to rapid, defensible responses suggests that retainers will include tailored, proactive services like cyber–war room design and threat simulations. These enhancements aim to ensure clients receive immediate, expert-led support during incidents, with SLAs potentially offering response times measured in hours for critical cases.

Finally, A&M is aligning IR retainers with regulatory demands, as noted in discussions on GDPR, CCPA, and the European Union's (EU's) DORA. This focus ensures retainers support legally defensible responses, particularly for regulated industries. By combining technology, global expertise, and compliance, A&M likely plans to offer more robust, client-specific IR retainers, to maintain their competitiveness in the cybersecurity market.

Alvarez & Marsal was not an active participant in this study. Publicly available information sources and an IDC customer survey with 37 of the 1,118 participants providing insights on Alvarez & Marsal's incident response capabilities were used to provide an assessment for this study.

Strengths

Tabletop exercises are at the top tier of utilization of incident readiness services for most organizations. It gives the opportunity to bring together diverse personas to evaluate how they handle different types of incidents. IR customers surveyed by IDC have a positive perception of Alvarez & Marsal's capabilities reporting that they were "very satisfied" with their tabletop exercises.

Challenges

The same survey indicated that A&M performs in the bottom tier of surveyed IR providers when it comes to reporting to the C-suite or the board during an IR engagement. A&M should consider prioritizing its interactions with groups outside of traditional IT and cybersecurity teams.

Consider Alvarez & Marsal When

Organizations with a need for an IR firm that can manage complex, high-impact incidents with cross-border implications and operational continuity concerns should consider utilizing Alvarez and Marsal.

Aon

Aon is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. Aon's incident response capabilities are deeply rooted in the legacy of Stroz Friedberg, a renowned digital forensics and cyberinvestigations firm that became part of Aon's cyberpractice. This heritage continues to shape Aon's approach to incident response, combining deep investigative expertise with a strategic understanding of cyber-risk, insurance, and regulatory environments. Today, Aon delivers a globally integrated IR service that helps organizations prepare for, respond to, and recover from cyberincidents with speed, precision, and business-aligned insight.

Future development will be impacted by the announcement on June 11 of the pending acquisition of Aon's Stroz Friedberg business unit by LevelBlue. IDC's analysis of Aon's capabilities was done prior to this announcement.

The foundation of Aon's IR services lies in its digital forensics and incident response (DFIR) team, which brings decades of experience in handling complex cyberevents, including ransomware, business email compromise, insider threats, and nation-state attacks. The methodology is grounded in forensic rigor, legal defensibility, and a deep understanding of attacker behavior. Aon's IR engagements are typically initiated through its Cyber Incident Response Retainer, which guarantees clients access to expert responders, legal coordination, and forensic support in the event of a breach.

Aon's IR services are uniquely positioned at the intersection of cybersecurity and cyberinsurance. The firm's ability to align technical response with insurance policy terms and claims processes is a key differentiator. During an incident, Aon's IR team works closely with insurers and legal counsel to ensure that all actions are documented, privileged where necessary, and optimized for potential recovery under cyberinsurance policies. This alignment reduces friction during high stress events and helps clients maximize the value of their insurance coverage.

Aon's proactive services are equally robust. The company offers a suite of readiness solutions, including tabletop exercises, incident response plan development, and compromise assessments. These services are informed by proprietary cybermaturity assessments and benchmarking data, enabling Aon to tailor its recommendations to each client's specific threat landscape, regulatory obligations, and business priorities.

The technical capabilities of Aon's IR team are enhanced by proprietary tools developed through its Stroz Friedberg lineage. These include specialized forensic utilities designed to accelerate investigations and improve visibility into attacker behavior. This kind of tooling reflects Aon's commitment to combining investigative depth with operational efficiency.

Aon's IR engagements are managed through a centralized incident manager who coordinates all aspects of the response, from forensic analysis to legal and regulatory communication. This structure ensures that clients receive consistent, high-quality support throughout the incident's life cycle. Aon also provides post-incident services such as root cause analysis, regulatory reporting support, and strategic recommendations to improve resilience and reduce future risk.

The firm's global footprint and cross-industry expertise further strengthen its IR capabilities. Aon supports clients in sectors such as financial services, healthcare, manufacturing, and critical infrastructure, each with unique regulatory and operational requirements. Its familiarity with frameworks like NIST, ISO, and GDPR enables Aon to provide contextually relevant guidance and ensure compliance with applicable standards. The ability to coordinate multinational response efforts is particularly valuable for global enterprises facing simultaneous threats across jurisdictions.

Aon's integration of cyber-risk quantification into its IR practice is another one of its strengths. By linking incident response data with financial modeling, Aon helps clients understand the business impact of cyberevents and make informed decisions about risk transfer, investment in controls, and board-level reporting. This capability is especially useful for aligning cybersecurity strategy with enterprise risk management goals.

Aon is investing in the modernization of its IR capabilities to address emerging threats and evolving client needs. One strategic priority is the integration of artificial intelligence and automation into its response workflows. Aon is developing AI-driven tools to accelerate triage, enhance forensic analysis, and streamline documentation. These innovations are expected to improve response speed and accuracy while reducing the burden on human analysts.

Aon is also expanding its threat intelligence capabilities to provide clients with more timely and actionable insights. The firm is enhancing its data collection and analysis infrastructure to detect early indicators of systemic risk and sector-specific threats. This intelligence will inform both proactive risk management and real-time response, enabling clients to stay ahead of adversaries in a rapidly evolving threat environment.

Another area of development is the refinement of Aon's cyber-risk quantification models. By integrating real-world incident data with financial impact scenarios, Aon

aims to help clients understand the cost of cyber-risk and optimize their investment in controls and insurance. This capability is particularly valuable for executive teams and boards seeking to make data-informed cybersecurity decisions.

Aon was not an active participant in this study. Publicly available information sources and an IDC customer survey with 48 of the 1,118 participants providing insights on Aon's incident response capabilities were used to provide an assessment for this study.

Strengths

Incident response buyers were asked in an IDC survey about the effectiveness of the tabletop exercises that their IR provider provided. Aon's customers are well satisfied with them in this category.

Challenges

Customers in the same IDC survey of incident response buyers consider Aon as falling short on the red/blue/purple team engagements that they have utilized from Aon.

Consider Aon When

Organizations that desire to work with an enterprise risk–focused IR firm that is as capable of interacting with the C-suite and the board as it is with frontline IT and cybersecurity professionals should consider utilizing Aon.

Booz Allen

Booz Allen Hamilton (Booz Allen) is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. They have emerged as a formidable player in the incident response market, leveraging their deep roots in national security, cyberdefense, and consulting to deliver highly effective and scalable IR services. With a strong presence in both government and commercial sectors, Booz Allen's approach is grounded in operational rigor, intelligence integration, and mission-driven execution.

The firm's IR capabilities span the full life cycle of incident management — from preparation and detection to containment, eradication, and recovery. Booz Allen's teams are structured to respond rapidly and effectively to a wide range of cyberthreats, including ransomware, advanced persistent threats (APTs), and insider incidents. The company's multidisciplinary teams include incident handlers, forensic analysts, malware reverse engineers, and compliance advisors, ensuring comprehensive coverage of both technical and regulatory dimensions.

Booz Allen's IR services are further strengthened by its advanced analytics and detection capabilities. The firm employs behavioral analytics, endpoint detection and

response (EDR) tools, and machine learning to identify anomalies and IoCs across complex environments. These tools are continuously refined through a DevSecOps culture that emphasizes agility, automation, and integration with broader security operations.

Booz Allen has a dedicated OT practice group and lab that has handled approximately 100 industrial control systems/distributed control systems (DCS) related investigations and over 100 operational technology cybersecurity assessments. These efforts are supported by over 200 credentialed OT cyberprofessionals. Booz Allen partners with Microsoft, Claroty, Dragos, Splunk, ForeScout, Armis, TXOne, ZingBox, Nozomi, Digital Immunity, and Medigate to support OT IR efforts.

Clients benefit from a flexible and scalable engagement model. Booz Allen offers both retainer-based and ad hoc IR services, with the ability to surge resources during major incidents. The firm's client-centric approach includes regular briefings, detailed post-incident reports, and tailored recommendations for improving cyber-resilience. Proactive services such as compromise assessments, red teaming, and tabletop exercises are also available to help clients prepare for future threats.

Booz Allen's cross-sector experience is a major asset. The firm supports clients across defense, healthcare, energy, financial services, and critical infrastructure, applying lessons learned from one domain to another. This breadth of experience enhances the firm's ability to tailor solutions to specific industry needs and regulatory environments. Its ability to operate in both classified and unclassified settings further distinguish Booz Allen in the IR space.

Booz Allen operates as a product-agnostic incident response team, leveraging previously existing toolsets of its clients to analyze available evidence, determine root causes, and identify methods of data access/exfiltration in incident response engagements. Although Booz Allen maintains a product-agnostic approach, it subsequently maintains partnerships with many product companies to ensure that it can deploy net-new tooling in the event that a client's existing security stack is unsuccessful in containing, eradicating, and remediating an active threat.

Booz Allen is focused on expanding its IR capabilities through innovation, automation, and market diversification. The firm is investing in and developing AI-driven tools to accelerate incident detection, triage, and response. These tools aim to reduce analyst workload, improve response times, and enable predictive threat modeling. Generative AI is also being explored for real-time documentation and decision support during incidents.

Global expansion is a strategic priority. Booz Allen plans to grow its managed security service offerings and establish new cyberdefense and incident response capabilities to

support 24 x 7 monitoring. These efforts will enhance the firm's ability to serve multinational clients and respond to incidents across time zones and geographies.

The firm is also deepening its collaboration with government agencies, industry consortia, and international partners. These partnerships aim to improve threat intelligence sharing, standardize response protocols, and strengthen collective cyber-resilience. Booz Allen's role in public-private initiatives positions it to influence policy and drive innovation in the broader cybersecurity ecosystem.

Emerging threats are a key focus area. Booz Allen is prioritizing research and development in quantum-safe cryptography, supply chain security, and AI threat detection. These investments will ensure the firm remains at the forefront of defending against next-generation cyberthreats.

Strengths

A key differentiator for Booz Allen is its seamless integration of proprietary and open source threat intelligence into its IR operations. The firm leverages its DarkLabs team and other internal cyberunits to provide enriched context around threat actors, tactics, techniques, and procedures (TTPs). This intelligence-driven approach enhances the speed and precision of incident triage and root cause analysis, enabling clients to make informed decisions under pressure.

Challenges

Booz Allen's revenue mix is disproportionately reliant on government contracts, which may be a strategic risk if diversification into commercial sectors is not accelerated.

Consider Booz Allen When

Organizations that require strong strategic and tactical threat intelligence and forensic capabilities before, during, and after an incident should consider utilizing Booz Allen.

CrowdStrike

CrowdStrike is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide incident response services. CrowdStrike offers a highly integrated, intelligence-driven, and cloud-native approach to cyberdefense. Its IR services are deeply embedded within the broader CrowdStrike Falcon platform, enabling rapid detection, investigation, and remediation of cyberthreats across diverse environments.

At the core of CrowdStrike's IR capabilities is the Falcon platform, a cloud-native endpoint detection and response solution that provides real-time telemetry, threat detection, and automated response. For clients already using Falcon, the IR team can immediately access forensic data, significantly reducing the time required for triage and

containment. This tight integration between the Falcon platform and the company's IR team allows for seamless coordination and faster resolution of incidents.

CrowdStrike has developed a robust onboarding process that ensures readiness and visibility. CrowdStrike offers a dedicated weekend IR team that operates Friday to Monday, which is further supplemented by an on-call surge team. This structure allows CrowdStrike to offer investigative coverage and accelerates analysis during periods that are traditionally limited to on-call support — providing clients with sustained response capability during off-hours. CrowdStrike also employs a follow-the-sun model, leveraging IR resources in the Americas, Europe, META, and APJ regions. This model allows continuous investigative progress and around-the-clock analyst availability.

While onboarding non-Falcon clients requires additional effort, CrowdStrike ensures preparedness by pre-staging access protocols and, when possible, deploying Falcon to a subset of the environment for testing. This flexibility allows CrowdStrike to support a wide range of environments without compromising response effectiveness.

CrowdStrike's IR team is composed of elite professionals with deep expertise in digital forensics, malware analysis, and threat hunting. These teams are structured to support both proactive and reactive engagements, including compromise assessments, tabletop exercises, and full-scale breach response. Their ability to operate across diverse environments and threat scenarios makes them a trusted partner for organizations facing APTs, ransomware, and insider threats.

The firm's global capabilities are further enhanced by its multilingual support and ability to operate across time zones. CrowdStrike leverages AI-driven translation tools to interpret logs and communications in multiple languages, enabling effective response in multinational environments. This global reach ensures that clients receive consistent, high-quality support regardless of location.

Artificial intelligence and automation are central to CrowdStrike's IR strategy. AI tools assist with log normalization, timeline reconstruction, and threat correlation, allowing analysts to focus on high-value investigative tasks. Automation accelerates containment and eradication efforts, particularly in large-scale or multi-vector attacks. These capabilities enhance the speed, accuracy, and consistency of CrowdStrike's response services.

CrowdStrike emphasizes a client-centric engagement model, providing regular updates, detailed findings, and actionable recommendations throughout the IR process. This collaborative approach builds trust and ensures that IR engagements deliver measurable value. CrowdStrike also provides support for internal and external communications, preparing summaries for C-level executives, auditors, and regulators.

CrowdStrike's Pulse consulting services represent a strategic enhancement to its incident response retainer model, offering clients real-time visibility and control during active engagements. Designed to improve transparency and operational efficiency, CrowdStrike's Pulse Services represent a proactive evolution of its consulting capabilities, providing recurring, expert-led micro-engagements that help organizations reduce risk and steadily advance their security maturity. Delivered on a biweekly, monthly, or quarterly cadence, each Pulse engagement is tailored to the customer's current environment, challenges, and goals, whether focused on incident readiness, cloud security, identity protection, or strategic program growth. Powered by real-time Falcon telemetry and guided by threat intelligence, Pulse helps security teams take decisive action on today's most relevant risks, enabling measurable progress without waiting for the next crisis. This capability is especially valuable during high-pressure events, ensuring that CrowdStrike's expertise is both accessible and actionable when it matters most.

CrowdStrike is focused on expanding its IR capabilities through innovation, platform enhancements, and global service delivery. The company's strategic road map reflects a commitment to staying ahead of evolving threats and delivering even greater value to clients.

CrowdStrike is also investing in broader platform interoperability. While Falcon remains central to its strategy, the company is enhancing support for third-party tools to deliver consistent IR outcomes regardless of the client's existing tech stack. This flexibility is critical as organizations increasingly adopt hybrid and multi-vendor security architectures.

The firm is exploring the use of generative AI to further streamline IR workflows. This includes automated report generation, playbook execution, and contextual threat analysis. These innovations aim to reduce response times, improve consistency, and enhance the overall efficiency of IR engagements.

To meet growing international demand, CrowdStrike is expanding its IR team's global footprint and enhancing its multilingual capabilities. This includes hiring regional experts, developing localized response playbooks, and tailoring services to address region-specific threats and compliance requirements.

Strengths

CrowdStrike does not charge clients additional fees for tooling or platform usage during IR engagements. With its focus on proprietary AI tools, CrowdStrike says that these tools do not replace human interaction but instead ensure that any findings during the investigations are validated by their responders.

In addition, Falcon Next-Gen SIEM enables its responders to ingest and subsequently search large amounts of data from central and/or disparate log sources, yielding faster investigations.

Challenges

Some customers noted that the reporting at the end of the IR engagement took a bit longer than they had anticipated.

Consider CrowdStrike When

Multinational organizations, especially in finance, healthcare, and critical infrastructure where compliance and reporting are critical, should consider CrowdStrike.

Deloitte

Deloitte is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide incident response services. Deloitte's incident response capabilities are anchored in its CIR3 framework — Cyber Incident Readiness, Response, and Recovery — offering clients a comprehensive, end-to-end approach to managing cybercrises.

The firm's IR services are delivered through a globally coordinated network of cyberprofessionals, supported by four 24 x 7 cyberoperations centers and a unified global playbook. This structure enables Deloitte to provide consistent, scalable, and rapid response and recovery capabilities across geographies. Their teams are trained to operate under a synchronized model, ensuring seamless transitions between readiness, response, and recovery phases.

Deloitte's incident readiness services are a core strength. These services include tabletop exercises, ransomware assessments, legal and regulatory preparedness, and strategic planning. The firm emphasizes continuous onboarding and relationship-building with retainer clients, ensuring that response teams are familiar with client environments and can act swiftly when incidents occur.

Deloitte's integrated approach to IR engagements is a differentiator. Bringing together talent from diverse domains within incident response (e.g., forensics, data analysis, and containment) and cyberincident response adjacent areas such as legal, regulatory compliance, crisis communications, and business resilience ensures that technical activities such as containment, eradication, and recovery efforts are aligned with legal obligations, stakeholder communications, and broader business priorities.

Deloitte also has very broad alliances with technology providers that enable Deloitte to leverage the latest tools, insights, and best practices to respond to incidents for clients regardless of their technology landscape, existing tools, or solutions.

In the response phase, Deloitte brings a multidisciplinary model that integrates technical forensics, legal privilege management, crisis communications, and third-party coordination. The incident commanders serve as quarterbacks, orchestrating all aspects of the response — from containment and investigation to stakeholder communication and regulatory engagement. Deloitte's legal capabilities are particularly notable, with breach coaching and legal advisory services available across 80 jurisdictions in 57 countries.

The firm's technical investigation capabilities are bolstered by proprietary accelerators and alliances with major technology providers. Deloitte leverages tools like CrowdStrike Falcon and Google SecOps to rapidly deploy endpoint detection, isolate compromised systems, and conduct forensic analysis. The firm's ability to integrate these tools into client environments within hours of engagement is a key differentiator.

Recovery services are a growing focus for Deloitte, reflecting the firm's belief that true resilience extends beyond containment. Its recovery teams work alongside clients to rebuild networks, restore business operations, and validate data integrity. Deloitte's ability to mobilize experts in manufacturing, ERP systems, and operational technology allows the firm to support complex recoveries, particularly in regulated industries like healthcare and life sciences.

The firm's data-driven incident response platform is a differentiator. This internal tool collects over 700 data points per incident, covering legal, technical, communications, and recovery metrics. It enables responders to benchmark performance, identify trends, and generate real-time insights. The platform also includes a co-pilot feature that guides responders through each phase of an incident, offering recommendations based on historical data and best practices.

Deloitte's ecosystem of alliances further enhances its IR capabilities. Strategic partnerships with AWS, CrowdStrike, Google, and others allow the firm to deploy technologies tailored to specific client needs. These alliances are deeply integrated into Deloitte's service delivery model, enabling rapid deployment and seamless coordination during high-stakes incidents.

Client onboarding is treated as an ongoing process rather than a one-time event. Deloitte conducts workshops, collects detailed environmental and business data, and maintains regular touch points with clients to ensure readiness. Retainer hours can be used flexibly across readiness, response, and recovery services, maximizing value and ensuring continuous engagement.

Deloitte is expanding its data-driven capabilities into readiness and recovery. Inspired by the concept of a "holodeck," Deloitte aims to generate real-time, scenario-based tabletop exercises using historical incident data. This will allow clients to train against

realistic, high-impact scenarios and measure their performance against industry benchmarks.

Trust IQ, Deloitte's proprietary trust-based risk framework, will be integrated into incident response. This tool will help quantify the trust impact of micro-decisions made during an incident, enabling more informed and strategic guidance for clients. The goal is to minimize reputational damage and enhance stakeholder confidence throughout the response life cycle.

Deloitte is also exploring outcome-based billing models to augment traditional hourly rates. Engagement fees can be contingent on the achievement of performance metrics such as mean time to detect, contain, and recover. This model aligns incentives and reflects Deloitte's confidence in its ability to deliver measurable outcomes.

Strengths

Deloitte is investing heavily in AI, automation, and data-driven innovation to redefine the future of incident response. The firm has committed $4 billion through fiscal year 2030 to GenAI initiatives, with over 400 assets already developed. These include agentic AI capabilities that automate investigative tasks and integrate with Deloitte's broader digital workforce.

Crisis communications is an area where Deloitte excels. The firm maintains a global network of communications experts who draft public statements, manage media relations, and conduct sentiment analysis to assess the impact of messaging. Deloitte also operates call centers to handle inquiries from affected individuals, ensuring a comprehensive and empathetic response to data breaches and other high-impact incidents.

Challenges

Customers of Deloitte, based on an IDC survey of incident response buyers, showed lower satisfaction for the post-incident reporting that the company provides.

Consider Deloitte When

Organizations that operate in highly sensitive, regulated, and mission-critical environments should consider utilizing Deloitte for their incident response capabilities.

Ernst & Young

Ernst & Young (EY) is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. EY has a large, global presence in security services, offering robust incident response and readiness services through its Cybersecurity, Privacy, and Forensic & Integrity Services practices. With a

multidisciplinary approach, EY delivers comprehensive IR capabilities, integrating cybersecurity expertise, digital forensics, threat intelligence, and crisis management to help organizations prepare for, respond to, and recover from cyberincidents. EY's global network, advanced technology, and industry-specific experience position it as a trusted partner for managing complex cyberthreats across sectors like industrials and energy, mining, agriculture, government, and public sector.

The firm's IR services are designed to address a wide range of cyberincidents, including ransomware, business email compromises, personal identifiable information (PII) theft, and credit card breaches. Its global Privacy & Cyber Response teams combine cybersecurity and IT forensic expertise with traditional investigative methods, such as interviewing witnesses and analyzing physical and digital evidence, to uncover critical details about breaches. EY's approach emphasizes rapid response, with teams aiming to start work within hours to analyze networks for anomalies, contain threats, and mitigate damage.

EY offers flexible IR retainer agreements, including an annual subscription model that covers fast-reaction emergency response, triage support, initial incident assessment, and event evaluations. These retainers allow clients to repurpose unused hours for additional cyberservices such as cybercompromise assessments or red teaming, enhancing overall resilience. The subscription includes access to EY's cyberthreat intelligence briefs, providing timely insights into threat actor tactics and incident trends. This model ensures clients receive immediate support during incidents while benefiting from proactive readiness services, such as scheduled reviews of critical assets and response playbooks. EY's Singapore-based team, for instance, emphasizes rapid evidence collection and recovery planning to limit damage from malware or ransomware attacks.

With a global network of forensics, incident response, and cybersecurity professionals, EY tailors IR processes to meet regulatory requirements across authorities, addressing challenges in cross-border investigations. The firm's teams collaborate with law enforcement and external legal counsel to ensure compliance with regulations like GDPR and CCPA, as well as industry-specific standards. For example, EY's Privacy & Cyber Response professionals assist clients with regulatory inquiries and litigation following breaches, leveraging their global presence to navigate international legal complexities. This capability is critical for multinational clients ensuring compliance and effective response across diverse regulatory environments.

EY leverages innovative forensic and integrity services technology to enhance IR effectiveness, including tools for data interrogation, evidence preservation, and timeline reconstruction. The firm's services include digital forensics, threat intelligence, discovery and analytics, claims and disputes, transaction forensics, information

governance, and privacy services and crisis management, enabling clients to understand the scope of incidents and recover operations swiftly. The firm's forensic technology also supports complex insurance claims by documenting losses accurately, as highlighted in its resilience services. EY's ability to integrate operational technology expertise further distinguishes its IR offerings, particularly in industries like energy and discrete manufacturing.

The firm's Crisis Management & Incident Response Services offering focuses on preparation through threat identification, playbook development, and regular simulations. These services, led by the EY Forensic & Integrity Services (and forensics managed services) team, help clients anticipate and mitigate risks before incidents occur. EY's four-pillar approach — threat monitoring, playbook development, simulations, and continuous improvement — ensures organizations are ready for crises ranging from hidden to sudden threats. For example, EY collaborates with clients to simulate cyberattacks, testing response and recovery capabilities while building stronger defenses.

EY's cyberthreat management, detection, and response teams offer managed detection and response (MDR) services, data privacy, and digital identity and privileged access management services to monitor and respond to advanced threats. These services include onsite and remote IR support to contain intruders, eradicate threats, and implement enhanced defenses. EY's MDR capabilities are complemented by vulnerability management, penetration testing, and dynamic application testing, ensuring comprehensive protection. 24 x 7 monitoring and IR support across IT and OT environments reduce risk and improve resilience.

EY is poised to enhance its IR capabilities by integrating artificial intelligence and machine learning to improve threat detection and response times. EY's 2025 cybersecurity solutions highlight plans to leverage AI for defense against advanced threats and secure enterprisewide AI adoption, which will enhance IR retainers with automated triage and analytics.

In addition, EY aims to expand its global network of IR professionals, building out its multidisciplinary teams to offer region-specific expertise. Investments in cloud-based forensic platforms and partnerships with technology providers like Microsoft, ServiceNow, and CrowdStrike will further streamline IR processes, enabling faster, scalable responses.

EY's focus on cross-border compliance will also evolve to address emerging regulations like the EU's DORA, ensuring retainers meet future legal requirements. These advancements will strengthen EY's position in delivering rapid, technology-driven IR services and capabilities.

EY was not an active participant in this study. Publicly available information sources and an IDC customer survey with 59 of the 1,118 participants providing insights into EY's incident response capabilities were used to provide an assessment for this study.

Strengths

EY's customers placed EY in the top tier of all the studied IR firms for their proactive red/blue/purple team exercises. In addition, they also gave high marks in their confidence in EY being able to fully eradicate threat actors from their environment.

EY's broad portfolio and global reach allows it to gain perspective and expertise across a broad range of industries. The firm's ability to be able to understand the risk and compliance needs of its customers is a noted strength.

Challenges

Customers in the IDC survey of buyers of incident response services were asked about their IR providers' ability to properly estimate the size and scope of their IR engagement in comparison to the actual costs and scope of work that was done. EY did not stand out in this specific measurement.

Consider Ernst & Young When

Organizations that desire to partner with a global firm that has cyber-resilience as a key part of its offering and that has the industry insights to serve as a business and cybersecurity enabler should consider using EY for their incident response needs.

Google

Google is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide incident response services. Mandiant, now a core part of Google Cloud Security, continues to be one of the most recognized and respected names in incident response. With over two decades of experience, Mandiant has built a reputation for responding to some of the world's most complex and high-impact cyberincidents. As part of Google, Mandiant now benefits from unparalleled access to global infrastructure, engineering resources, and threat intelligence, while maintaining its vendor-agnostic approach and consulting independence.

Mandiant's IR services are built around a "team of teams" model, bringing together specialized groups for forensics, threat intelligence, remediation, and crisis communications. Each engagement is led by a dedicated technical lead and engagement manager, ensuring coordination across all workstreams. This structure allows Mandiant to deliver rapid, scalable, and highly tailored responses to incidents ranging from ransomware and nation-state attacks to supply chain compromises and destructive malware.

A key differentiator is Mandiant's integration with Google's SecOps platform, which enables rapid deployment of investigative capabilities without the need for lengthy software installations. This allows Mandiant to begin triage and scoping within hours, leveraging existing client telemetry and augmenting it with proprietary forensic tools like FACT and Monocle. These tools allow for deep forensic interrogation of endpoints and orchestration of data collection at enterprise scale — capabilities that go beyond what traditional EDR platforms offer.

The firm's crisis communications practice, launched in 2022, is a unique offering in the IR space. Recognizing that cyberincidents are as much about trust and perception as they are about technology, Mandiant provides strategic communications support to help clients manage media inquiries, stakeholder messaging, and align with regulatory frameworks. This includes sentiment analysis and stakeholder-specific messaging. The communications team works closely with client legal and technical teams to ensure consistency and accuracy across all channels.

Mandiant's remediation and recovery capabilities are equally robust. The firm maintains a global team of specialists in identity management, cloud architecture, endpoint security, and cyberdefense. These experts work alongside investigative teams to design and implement containment strategies, rebuild trusted infrastructure, and restore business operations. Mandiant usually leads the entire recovery process, coordinating with third-party vendors only when additional scale is needed.

Mandiant also maintains strong relationships with law firms, insurance providers, and government agencies. With partnerships across 59 law firms and 46 insurers, Mandiant is often the first call when a breach occurs. These relationships streamline engagement, facilitate legal privilege, and ensure alignment with regulatory and contractual obligations.

The firm's commitment to community impact is evident in its victim notification program, which proactively alerts organizations to compromises discovered through Mandiant's investigations or threat intelligence. These notifications are provided pro bono and include actionable data to help victims validate and respond to threats. Mandiant also publishes public threat intelligence reports and playbooks, such as its recent guidance on defending against the Scattered Spider threat group.

Mandiant is focused on expanding its capabilities through AI, automation, and strategic partnerships. As part of Google, Mandiant is deeply integrated into the development of Gemini, Google's AI platform. Gemini is already embedded in SecOps, enabling natural language queries, agentic threat hunting, and contextualized incident analysis. Future enhancements will include multi-agent orchestration, malware analysis, and automated threat intelligence reporting — all designed to accelerate investigations and reduce analyst workload.

Mandiant is also investing in cyber-resilience solutions, including the development of "minimal viable business" recovery environments. These isolated, cloud-based environments are designed to restore critical operations within days of a ransomware attack. Mandiant is working with partners to make these solutions more repeatable and cost effective, aiming to reduce recovery timelines from weeks to hours.

The firm is expanding its AI governance services, helping clients align AI use with organizational goals, protect sensitive data, and meet regulatory requirements. Mandiant is also contributing to Google's Cyber Shield initiative, which supports nation-states and large enterprises in building end-to-end cybersecurity capabilities — from infrastructure to operations.

Finally, Mandiant plans to make its internal IR platform more accessible to clients, enabling them to view incident timelines, benchmark performance, and access threat intelligence directly. This move toward transparency and client empowerment reflects Mandiant's broader mission: to make every organization more secure through shared knowledge, rapid response, and continuous innovation.

Strengths

Mandiant's threat intelligence is a cornerstone of its IR practice. Now branded as Google Threat Intelligence, it combines Mandiant's frontline insights with data from VirusTotal, Chrome Safe Browsing, Gmail, and other Google services. This intelligence is embedded into every IR engagement, enabling Mandiant to identify threat actors, tactics, and indicators of compromise with speed and accuracy. Each IR case is supported by a dedicated threat intelligence analyst, ensuring that findings are contextualized and actionable.

The combination of Google and Mandiant now has a large global presence with cybersecurity experts in 28 countries and supports over 30 languages. The global incident response network includes consultants and responders across regions to provide localized support, and the combined company has responded to incidents in over 50 countries.

Challenges

One customer noted that the firm needs to do a better job at setting expectations for business executives at the beginning of an IR engagement.

Consider Google When

Organizations that seek to work with a globally capable IR firm with strong threat intelligence capabilities and that utilizes a holistic approach to incident response that goes beyond the technical portions should consider Google.

IBM

IBM is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. IBM's X-Force Incident Response (X-Force IR) team delivers a globally integrated, intelligence-driven, and highly scalable incident response service. Operating within IBM Consulting's cybersecurity services division, X-Force IR supports both proactive and reactive engagements across IBM's global client base. With a strong emphasis on technical excellence, global coordination, and innovation, IBM is steadily reinforcing its position as a trusted partner for large enterprises facing complex cyberthreats.

X-Force IR's global footprint is a core strength. The team operates across six regions — North America, Latin America, EU, MEA (Middle East and Africa), APAC, and Japan — with regional leads who manage localized teams and client relationships. IBM's follow-the-sun hotline model ensures that clients always speak directly to an experienced IR consultant rather than a call center intermediary. This model is supported by automation tools like PagerDuty and Slack integrations, enabling seamless handoffs and real-time collaboration across time zones.

The team's multilingual capabilities further enhance IBM's global reach. X-Force IR supports engagements in a wide range of languages, including French, German, Portuguese, Spanish, and Japanese. This linguistic diversity, combined with IBM's market-focused structure, allows the team to deliver culturally and regionally tailored services, particularly in Europe, Latin America, and Asia.

IBM takes not only a vendor-agnostic approach but also a "let's work with what our clients have" approach. X-Force IR leverages technologies that clients already have in place to do analysis where it is possible to do so. This positions IBM to help clients avoid deployment of new software where possible.

IBM's IR engagements are enriched by the broader X-Force ecosystem. Every incident response includes a dedicated threat intelligence analyst from IBM's X-Force Threat Intelligence team, ensuring real-time access to global threat data. The team also collaborates closely with IBM's red team, cyber-range, and managed services units. Notably, IBM's cyber-ranges in Boston; Washington, D.C.; Ottawa; and Bangalore provide immersive training and simulation environments for executive-level tabletop exercises and live-fire scenarios.

The firm's retainer model is mature and flexible, offering three standard tiers (tiers 1, 2, and 3) plus region-specific options like the Essentials Retainer for cost-sensitive markets. Tier 3 includes quarterly dark web monitoring while all tiers include quarterly threat briefings and a dedicated engagement lead. IBM's proactive services portfolio is extensive, covering Active Directory reviews, cybercrisis playbooks, tabletop exercises,

and more. These services are delivered by both the IR team and other X-Force units, ensuring depth and specialization. IBM also offers multilingual delivery of its cyber-range exercises.

X-Force IR's innovation engine is driven by X-Force Labs, an internal R&D initiative that allows consultants to dedicate up to 20% of their time to research. Labs projects include report automation, AI playbooks, threat hunting orchestration, and recommendation mapping to IBM's broader services portfolio. These efforts are designed to enhance delivery efficiency, improve client outcomes, and foster technical eminence.

IBM's Predictive Threat Intelligence (PTI) platform is a noted innovation. PTI aggregates threat feeds, client asset data, and behavioral indicators to generate tailored threat hunting campaigns. It integrates with IBM's ATOM platform to enable rapid detection and response. PTI is being combined with IBM's Active Threat Assessment service to deliver forensic-at-scale capabilities, allowing clients to identify historical compromises and respond proactively.

IBM is focused on expanding its use of AI and automation to transform incident response. The firm is investing in AI-driven orchestration tools that will allow consultants to query data using natural language and receive automated analysis and recommendations. These capabilities will be powered by watsonx and integrated into IBM's IR workflows, enabling faster, more scalable investigations.

IBM also plans to extend PTI's capabilities, integrating it more deeply with proactive services and enabling real-time threat hunting across client environments. The goal is to reduce detection and response times from hours to minutes, leveraging AI and automation to accelerate decision-making.

Regionally, IBM is developing cost-optimized retainer models for Canada, APAC, and Latin America, using local talent to deliver services at competitive rates. This strategy is designed to expand IBM's footprint in emerging markets while maintaining service quality and global coordination.

The firm is also exploring new go-to-market channels, including partnerships with law firms and large enterprise resellers. While IBM does not currently participate in cyberinsurance panels, it is working with clients and brokers to gain pre-approval status with insurers, enabling smoother engagement during insured incidents.

The creation of an internal advisory board and continued investment in global training and standardization reflect IBM's commitment to delivery excellence and global synergy.

Strengths

The firm's integration with IBM's broader technology and consulting ecosystem is another major advantage. X-Force IR can tap into IBM's deep bench of subject matter experts in areas like SAP, mainframes, and connected vehicles. This access enables IBM to support incidents involving legacy systems, OT environments, and specialized enterprise applications. The team also benefits from IBM's AI and automation platforms, including watsonx and the ATOM threat detection engine used by IBM's managed services.

Challenges

IBM's specific decision to not be on cyberinsurance panels is a mixed bag. It does benefit the firm by not being tied to lower-priced engagements, but it does limit some of the firm's growth opportunities that being "on-panel" can provide.

Consider IBM When

Larger organizations with a diverse IT infrastructure that desire to partner with an IR firm with strong AI capabilities in and beyond the SOC should consider utilizing IBM for their IR services.

KPMG

KPMG is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide incident response services. KPMG's Cyber Response Services practice delivers a globally integrated, multidisciplinary incident response capability that is distinguished by its deep regulatory expertise, sector-specific alignment, and commitment to long-term client transformation. Rather than focusing on high-volume transactional engagements, KPMG positions itself as a strategic partner, guiding clients through the full life cycle of cybercrises — from detection and containment to recovery, regulatory response, and long-term resilience.

KPMG's IR methodology is built around a comprehensive, end-to-end framework that integrates digital forensics, crisis management, legal and regulatory advisory, ediscovery, and recovery services. This approach is supported by a global network of professionals across more than 140 countries, including specialized teams in India, Bulgaria, and Malta that provide scalable, cost-effective support. KPMG's global reach is not just geographic — it is operational, with the ability to deploy teams to remote and high-risk environments, including prior deployments to offshore locations and assets such as oil platforms and cruise ships.

A key differentiator is KPMG's ability to deliver complex recovery services in-house. In 98% of cases, KPMG manages recovery directly, leveraging its global delivery network

and cloud engineering capabilities. This includes rapid deployment of clean environments, business continuity planning, and IT/OT restoration. In rare cases requiring niche expertise or classified access, KPMG may engage vetted third parties, but the firm's preference is to maintain control and consistency through internal resources.

KPMG's IR engagements are often initiated through legal counsel. The firm works closely with a broad network of law firms globally, both as a referral channel and as a collaborative partner during investigations. KPMG also offers legal advisory services through its own law firm entity in select jurisdictions, enabling it to provide regulatory and compliance guidance before, during, and after incidents.

The firm's Digital Responder platform is a cornerstone of its forensic capability. This in-house, cloud-based tool automates evidence processing and standardizes analysis across global teams. It enables KPMG to deliver consistent, high-quality results regardless of geography or analyst experience. Digital Responder also supports fixed-fee pricing models, allowing KPMG to offer predictable costs for common scenarios like business email compromise investigations and ediscovery.

KPMG's case management platform further enhances consistency and quality. It standardizes workflows across regions, ensuring that a BEC in Germany is handled the same way as one in the United States. This platform also facilitates cross-border collaboration and threat intelligence sharing, reinforcing KPMG's commitment to global coordination.

Strategic partnerships play a critical role in KPMG's IR delivery. The firm maintains deep relationships with Microsoft, CrowdStrike, SentinelOne, and others. Notably, KPMG has a unique partnership with Microsoft that allows it to deploy the full E5 suite — including Defender for Endpoint — on a trial basis during incidents. This relationship also provides direct access to Microsoft's IR team and threat intelligence, enabling faster containment and remediation. KPMG's product-agnostic stance ensures that it can work with whatever tools a client has in place or recommend alternatives when needed.

KPMG's IR services are tightly integrated with its broader cyber- and risk advisory capabilities. This includes regulatory mapping (e.g., DORA, NIS2, SEC), crisis communications, and business continuity planning. The firm's multidisciplinary teams help clients not only recover from incidents but also transform their security posture.

The firm's sector-specific alignment is another strength. KPMG assigns professionals to industry verticals such as healthcare, manufacturing, and financial services, enabling them to understand sector-specific risks, regulatory requirements, and operational

nuances. This alignment enhances the quality of advice and accelerates response times during incidents.

KPMG is focused on transforming its IR services through AI, automation, and deeper sector integration. The firm is investing heavily in agentic AI to enhance forensic analysis, automate hypothesis testing, and streamline reporting. Use cases include natural language query generation, knowledge base retrieval, and logic-driven analysis using frameworks like LangChain and Haystack. These capabilities are embedded into Digital Responder and other internal platforms to fundamentally change how analysts interact with data.

KPMG is also expanding its fixed-fee and outcome-based pricing models. These models are particularly attractive to clients that are referred through insurance channels, where cost predictability is critical. The firm is exploring new ways to bundle services into retainers and offer pre-priced packages for common scenarios.

Finally, KPMG is doubling down on talent development. The firm's Future Leaders program, global boot camps, and innovation funding initiatives are designed to attract and retain top talent. By empowering professionals to lead innovation and build long-term careers at KPMG, the firm ensures continuity, quality, and a culture of excellence.

Strengths

Because KPMG's legacy is a risk consulting service provider, its IR services do not focus solely on technology. The KPMG IR service focuses not only on understanding the technical digital forensics and "solving the case" but also on executive stakeholder management, organizational change, and post-incident transformation.

KPMG is the only Big Four firm with an integrated global law arm, enabling it to provide clients with unified support across technical response, regulatory obligations, litigation defense, and strategic communication.

Challenges

As a public accounting firm bound by rigorous professional standards and regulations like the Sarbanes-Oxley Act, KPMG's growth in IR is somewhat limited as the company is required to decline engagements due to potential conflicts of interest.

Consider KPMG When

Organizations desiring to work with a firm that has a global footprint, with professionals in over 140 countries and the ability to deploy to remote or sensitive environments (e.g., oil platforms, cruise ships) should consider utilizing KPMG for their IR services.

Kroll

Kroll is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. Kroll delivers a globally integrated, practitioner-led incident response service that combines deep forensic expertise with a broad portfolio of adjacent capabilities, including ediscovery, breach notification, and litigation support, and separately offers up a managed detection and response service. With a presence in 19 countries and a team of over 650 professionals, Kroll is positioned to support clients across the full incident life cycle — from detection and containment to recovery, regulatory response, and long-term transformation.

Kroll's IR services are structured within its broader Risk Advisory business. This structure enables seamless collaboration across cyber-, legal, regulatory, and physical security domains. The firm's IR engagements are led by experienced digital forensics and incident response professionals, many of whom have backgrounds in law enforcement, intelligence, and enterprise security. Kroll's engagement model emphasizes continuity, with the same DFIR manager guiding the client from initial scoping through resolution.

Kroll's IR services are available through a flexible retainer model that spans the entire Risk Advisory portfolio. Clients can use retainer hours not only for cyber-related services but also for physical security assessments, VIP monitoring, and financial advisory work. Unused hours can be rolled over (up to 20%), and clients that initially engage Kroll through insurance channels can retain those discounted rates if they later convert to a direct relationship. This flexibility has driven strong adoption, particularly among private equity firms and multinational corporations.

Kroll maintains strong relationships with over 85 insurance carriers and is a preferred provider for breach counsel and legal firms. Approximately 80–90% of Kroll's IR cases are conducted under attorney-client privilege, particularly in the United States and the United Kingdom. The firm also supports tri-party agreements with insurers and legal counsel, ensuring a streamlined and defensible response process.

Kroll's technology stack is both proprietary and partner driven. The firm is well known for its open source forensic tool KAPE, which is widely used in the industry and continues to be actively developed. For endpoint visibility, Kroll primarily deploys SentinelOne and CrowdStrike, with Microsoft Defender and Obsidian used for identity and SaaS investigations.

Kroll's IR engagements are supported by a mature automation and orchestration framework that enables rapid deployment of sensors, secure file transfer, and telemetry ingestion. The firm's MDR team works closely with IR consultants to ensure seamless integration of detection and response capabilities. Kroll also offers 45 days of

identity monitoring following phishing or BEC incidents, providing early warning of credential misuse.

The firm's compromise assessment offerings have expanded significantly, particularly in the M&A space. These assessments now include identity hygiene, cloud and SaaS posture, and exposure management, often leveraging tools like CrowdStrike Falcon and Obsidian. Kroll's analysts also assess conditions that could lead to future attacks, such as legacy authentication or unpatched systems, and provide actionable recommendations.

Kroll's IR services are known for speed and accuracy. The firm typically engages within 15–30 minutes of notification and maintains an 86% rate of staying within initial budget estimates. Scoping calls are conducted within an hour, and statements of work are issued rapidly. This responsiveness, combined with a practitioner-led model and global reach, makes Kroll a trusted partner for both SMBs and large enterprises.

Kroll is investing heavily in innovation, particularly in the areas of data strategy, generative AI, and identity-centric security. The firm's unified data platform, built on Azure Databricks, enables federated access to structured and unstructured data across its cyber- and risk advisory practices. This platform supports advanced analytics, threat intelligence mining, and closed-loop feedback into detection engineering and threat modeling.

A key initiative is the use of generative AI and natural language processing (NLP) to extract insights from casework. Kroll has developed tools to automatically map incident data to MITRE ATT&CK frameworks, generate threat actor profiles, and support regulatory assessments like DORA. These insights are shared internally through a "data marketplace" and externally through enhanced reporting and advisory services.

Kroll collects intelligence from 1,000+ IR cases managed per year that are fed into the Kroll threat intelligence platform. Kroll also claims it discovers novel threats on average 10–14 days before mainstream intelligence communities and structures threat intelligence data to fuel detection-as-code. Kroll also has strong capabilities in identifying and investigating insider threats relating to intellectual property theft, fraud, corruption, money laundering and embezzlement to help its clients identify wrongdoers, recover assets, and seek legal remedies.

Kroll plans to expand its identity threat detection and response (ITDR) capabilities, deepen its integration with partners like CrowdStrike and Obsidian, and continue building sector-specific offerings for private equity, healthcare, and critical infrastructure. The firm's strategic vision is to deliver not only world-class incident response but also long-term resilience and transformation through a unified, data-driven approach.

Kroll is also developing AI-powered copilots to assist analysts with KQL queries, report writing, and investigation workflows. These tools are designed to improve efficiency, reduce cognitive load, and ensure consistency across engagements. The firm is exploring the use of generative AI for copyediting and quality assurance, helping standardize tone and structure in client deliverables.

Strengths

An IDC survey of buyers of incident response showed that Kroll performed well in reducing the amount paid out versus the initial ransomware payment demand by the threat actors.

Kroll also supports expert witness services and has experience in high-stakes intellectual property theft and insider threat cases.

Challenges

Kroll's customers that responded to an IDC survey of buyers of incident response are not that satisfied with Kroll's ability to attribute who was responsible for cyberattacks.

Consider Kroll When

Organizations of all sizes facing complex legal or reputational risks and that appreciate extensive ediscovery, breach notification, litigation support, and regulatory compliance capabilities in their IR provider should consider Kroll.

Microsoft

Microsoft is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. Microsoft's IR, formerly known as DART (Detection and Response Team), delivers a highly specialized, enterprise-grade incident response service that leverages the full breadth of Microsoft's global threat intelligence, cloud infrastructure, and security product ecosystem.

Microsoft IR is deeply embedded within the company's broader Customer Success Unit, which includes nearly 1,000 professionals across architecture, deployment, and security operations. This integration enables Microsoft to deliver a seamless experience from incident detection through containment, recovery, and long-term transformation. The team operates on a global, 24 x 7 "follow-the-sun" model, with incident responders, threat hunters, and recovery specialists located across the Americas, EMEA, and Asia/Pacific.

The IR team handles approximately 2,500 engagements annually. Around 80% of these are resolved within hours through Microsoft's frontline support and triage teams, often involving non-privileged user incidents or misconfigurations. The remaining 20% —

typically involving nation-state actors, ransomware, or advanced persistent threats — are escalated to Microsoft IR for full-scale investigation and containment. These engagements often involve large-scale enterprise environments, with 75% of Microsoft IR's work focused on organizations with over 5,000 employees.

Microsoft's IR methodology is built around a multidisciplinary team model. Depending on the nature of the incident, Microsoft deploys tailored teams that may include threat hunters, identity and infrastructure specialists, forensic analysts, and recovery engineers. These teams are supported by dedicated threat intelligence analysts from the Microsoft Threat Intelligence Center, who provide real-time insights into threat actor behavior, TTPs, and global campaign activity. This actor-centric intelligence model enables Microsoft to move quickly and decisively, often identifying and attributing threat actors within hours of engagement.

A key differentiator is Microsoft's ability to integrate its proprietary tools and security products into IR engagements. Customers who are not already licensed for Microsoft Defender or other E5 capabilities are granted 90-day trial access, allowing Microsoft to rapidly deploy tools like Defender for Endpoint and Defender for Identity within hours. These tools are supplemented by Microsoft's own custom-built triage and hunting tools — such as Fennec and Fox — designed to rapidly collect and analyze telemetry across large environments. Microsoft's ability to ingest and process massive volumes of data (e.g., 400,000 endpoints in under two hours) is a testament to its cloud-native scale and engineering maturity.

Microsoft IR also excels in containment and recovery. Unlike some other providers, Microsoft does not outsource these functions. Its in-house experts — many of whom have authored foundational white papers on credential hygiene and identity security — execute containment and rebuild strategies directly. This includes rapid isolation of compromised systems, credential resets, removal of persistence mechanisms, and restoration of identity infrastructure.

Proactive services are a growing focus for Microsoft IR. Approximately half of the team's time is now spent on proactive engagements, including compromise assessments, tabletop exercises, threat briefings, and incident readiness planning. These services are delivered using the same team as the incident response work on prepurchased contracts with customers or as part of Microsoft's broader customer success engagements. Microsoft's compromise assessments use the same methodology as reactive IR, with a strong emphasis on anomaly detection and TTP hunting. These assessments are increasingly used in M&A scenarios, annual health checks, and in response to sector-specific threats.

Microsoft's IR team also provides detailed investigative timelines, IOC lists, and KQL queries to customers, along with executive summaries tailored for board-level

audiences. The team is actively exploring the use of natural language processing and generative AI to assist with report writing and streamline communication while maintaining analyst accountability for accuracy and clarity.

Microsoft's partnerships with law firms, breach coaches, and cyberinsurers is another strength. The IR team is rapidly gaining panel status with major insurers and is already considered "pre-approved" by many. Microsoft does not offer breach coaching, crisis communications, or ransomware payment processing, but works closely with partners to deliver a comprehensive response ecosystem.

Microsoft is investing heavily in expanding its proactive services and scaling its IR capabilities to meet growing demand. The team plans to double in size over the next 12 months, with a goal of supporting over 1,000 retainer customers by year-end. New offerings in development include dedicated M&A compromise assessments, incident response plan development and testing, and advisory services for board-level engagement and threat readiness.

Microsoft is also deepening its integration with the Secure Future Initiative, a multibillion-dollar investment in security engineering, threat intelligence, and product hardening. This includes continued development of AI-powered tools like Security Copilot, which is being A/B tested by the IR team to accelerate investigations and improve detection fidelity. Microsoft is also exploring ways to share compromise assessment results with insurers to support more accurate risk underwriting and potentially influence cyberinsurance pricing models.

Strengths

IDC evaluated the quantity and quality of threat intelligence, governmental regulatory bodies, law enforcement, and advisory boards that IR firms interact with. Microsoft is a major contributor and has significant relationships established with these groups.

Microsoft Security has global scale with representation in nearly every country, and many of its 10,000+ architects, researchers, and engineers assist customers proactively and stand ready to assist during an incident.

Challenges

Microsoft's ability to continue being a go-to IR provider has largely been limited by the relative size of its IR portfolio in contrast to the rest of the Microsoft platform. Increased investments in marketing and IR thought leadership would really be beneficial.

Buyers of Microsoft's IR services that were surveyed in an IDC incident response survey felt the vendor is lacking in its ability to accurately size the scope and estimated costs for incidents at the beginning of the engagement.

Consider Microsoft When

Organizations that seek to work with an IR firm that has access to threat intel and security research teams that can inform investigation and recovery efforts, driving a faster return to business as usual, should consider utilizing Microsoft for their incident response services.

NCC Group

NCC Group is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. NCC Group has developed a mature and multifaceted incident response and readiness capability that serves both public sector and private sector clients across multiple geographies. The firm's approach is grounded in decades of experience, a strong foundation in government and law enforcement, and a commitment to technical excellence and strategic advisory.

A defining feature of NCC Group's IR practice is its emphasis on executive engagement and board-level preparedness. The company conducts extensive board advisory training, including scenario-based tabletop exercises that simulate the emotional and operational stress of a real incident. These sessions are designed to provoke critical thinking among leadership, prompting them to identify their most vital systems and designate alternative deputies to ensure continuity. This proactive approach helps organizations internalize the urgency and complexity of cyberincidents, fostering a culture of readiness inclusive of the C-suite.

NCC Group's global footprint is particularly strong in the United Kingdom, Benelux, and Australia, with the United Kingdom and the Netherlands governmental bodies regularly engaging with the company. NCC Group targets its services efficiently to deliver consistent support across diverse client environments. In sectors like retail, for example, the company tailors its business continuity planning to reflect industry-specific priorities, such as prioritizing sales systems over payroll during disruptions.

Their service delivery is structured around a tiered retainer model — Bronze, Silver, and Gold — that provides scalable support for proactive and reactive incident response. These retainers are designed to be comprehensive, covering both IT and OT environments. The DFIR team serves as the initial point of engagement, with the ability to integrate seamlessly with NCC Group's broader managed security services and professional security services. This integrated model ensures that clients receive

holistic support throughout the incident life cycle, from detection and containment to recovery and post-incident analysis.

NCC Group maintains a technology-agnostic approach, leveraging a wide array of industry-standard tools to support its investigations and developing and releasing its own investigations framework and tool Dissect as an open source offering. The firm's commercial toolkit includes AXIOM and Cellebrite for mobile forensics, CrowdStrike and SentinelOne for endpoint detection and response, and Thor for threat hunting. This flexibility allows the company to adapt to client environments and integrate with existing security infrastructure. The company emphasizes the importance of using multiple tools to ensure comprehensive coverage and maintain best practices in forensic and response operations.

A key strength of NCC Group's IR practice is its integration with legal and insurance ecosystems. In the United States and the United Kingdom, the company frequently operates through legal counsel to ensure privileged communications and regulatory compliance. The company collaborates with prominent law firms and works closely with insurance brokers. This model enhances the firm's ability to support clients through complex legal and regulatory landscapes, particularly during high-stakes incidents. While this approach is most prevalent in the United States and the United Kingdom, NCC Group is exploring similar partnerships in other regions to replicate this value-added service model.

The firm's credibility is further reinforced by its status as a founding member of CREST, an international accreditation body for cybersecurity professionals. All members of the firm's IR team undergo rigorous police and government background checks, ensuring a high level of trust and readiness for engagements involving sensitive data or critical infrastructure. This commitment to ethical standards and technical excellence positions NCC Group as a trusted partner for organizations facing sophisticated cyberthreats. This is also recognized by the United Kingdom's National Cyber Security Centre (NCSC) through NCC Group's approval as an "enhanced" level Cyber Incident Response (CIR) supplier — able to support critical national infrastructure sectors against nation-state attacks.

In addition to incident response, NCC Group provides a wide range of readiness services, including policy advisement, business continuity planning, and identity scanning. These services are designed to help clients strengthen their security posture and reduce the likelihood and impact of future incidents. The firm's proactive engagements often serve as a gateway to deeper strategic relationships, enabling the company to support clients across the full spectrum of cybersecurity needs.

NCC Group is focused on enhancing the integration of legal and insurance services into its IR offerings. The company is exploring new retainer models in collaboration with law

firms to provide bundled services that address privacy, data protection, regulatory compliance, and legal privilege. This initiative aims to streamline incident response for clients by reducing friction between technical, legal, and insurance stakeholders, ultimately improving the speed and effectiveness of response efforts.

The company also plans to make identity scanning a standard component of every retainer, helping clients proactively identify and remediate identity-related vulnerabilities. This initiative reflects the firm's broader strategy of embedding proactive security measures into its core service offerings. In addition, NCC Group is investing in the expansion of its unified IT/OT response capabilities. By offering a single retainer that covers both domains, the company aims to address the growing convergence of IT and OT environments, particularly in sectors such as manufacturing, energy, and transportation.

Strengths

NCC Group's IR team is often embedded in high-level decision-making processes, particularly through participation in Gold Team engagements, where the company advises executive leadership during cyberincidents. This strategic involvement is complemented by its DFIR team, which acts as the ambassador for IR, translating technical realities into executive-level insights and actions.

NCC Group has a strategic partnership with Dragos to deliver an operational technology add-on to its IR retainers. This collaboration can enable incident response coverage, spanning both information technology and operational technology environments, addressing the challenges of industrial cybersecurity.

Challenges

NCC Group already collaborates with law firms but will benefit from setting out more specific plans for future partnerships, initiatives, and ways of working to further position it as a trusted partner in the incident response landscape.

Consider NCC Group When

Organizations that require an IR firm that is as comfortable talking to IT, cyber-, and GRC personas as they are in collaboration with the C-suite should consider utilizing NCC Group for their IR needs.

NTT DATA

NTT DATA is positioned in the Contenders category in the 2025 IDC MarketScape for worldwide incident response services. NTT DATA has emerged as a formidable global player in the incident response space, leveraging its expansive IT services heritage, global delivery infrastructure, and deep cybersecurity expertise. With a presence in

over 50 countries and more than 80 delivery centers, NTT DATA supports over 2,000 clients. The firm's IR services are built on a foundation of global scale, local proximity, and a commitment to innovation, making the company a trusted partner for organizations seeking both proactive and reactive cyber-resilience.

At the core of NTT DATA's IR offering is a flexible, tiered retainer model that includes Bronze, Silver, Gold, and Platinum levels. These retainers are structured around blocks of hours that can be allocated to both proactive and reactive services. The onboarding process is tailored to the scope of services purchased, with more extensive onboarding for higher-tier packages. While the onboarding process is standardized to ensure consistency, it is also customized based on the specific services outlined in the statement of work. This ensures that clients receive a clear understanding of engagement protocols, escalation paths, and technical requirements.

NTT DATA's IR services are categorized into three primary engagement types: standard tiered retainers, bespoke packages tailored to RFPs, and ad hoc incident response engagements. The retainers are designed to support both incident response and readiness activities, including compromise assessments, ransomware readiness planning, threat modeling, and forensic investigations.

The company's IR delivery model is remote first, with most engagements conducted virtually. While NTT DATA has historically offered onsite response capabilities, this is currently limited to legacy contracts and select geographies. However, the company is actively considering reintroducing boots-on-the-ground services as part of its strategic road map.

During incidents, NTT DATA follows a structured process that includes preparation, detection and analysis, containment, eradication, recovery, and post-incident reporting. The firm's analysts provide detailed technical and executive-level briefings, ensuring that all stakeholders — from IT teams to legal counsel — are informed and aligned.

NTT DATA's technology stack is a blend of third-party and proprietary tools. The company maintains partnerships with major vendors such as Palo Alto Networks, Microsoft, and CrowdStrike, and is also investing in niche players and emerging technologies. For example, the company has the ability to deploy tools like Cortex XDR and CrowdStrike during investigations and is developing internal capabilities in agentic and generative AI to enhance automation and efficiency in incident response workflows.

NTT DATA's IR services are primarily relationship driven, with most non-retainer engagements initiated through direct client referrals rather than legal or insurance channels. While the company is not currently on many cyberinsurance panels, it recognizes the strategic value of building relationships with legal firms and insurance

providers to expand its reach. The firm's approach emphasizes trust and long-term value, often resulting in referrals to higher-level entities, such as national banks or regulatory bodies, following successful engagements.

The firm's client base is diverse, but a significant portion of IR engagements — approximately 55% — come from midsize organizations with 500 to 5,000 employees. These clients often rely on NTT DATA for full life-cycle support, from detection to recovery. In larger enterprises, NTT DATA typically plays a more specialized role, complementing internal teams or other service providers.

NTT DATA has set an ambitious goal to quadruple its DFIR business within 18 months. This growth strategy includes expanding team capacity, investing in automation and tooling, and enhancing pre-sales enablement across regional sales teams. The company is also consolidating regional IR teams under a unified global structure to improve consistency and scalability.

Strategically, NTT DATA is focused on reintroducing onsite response capabilities, developing regional pricing models, and simplifying its service catalog to make it more accessible to clients and partners. The company is exploring outcome-based pricing models and considering innovative approaches such as endpoint-based retainers to differentiate in a competitive market. In addition, the company is investing in AI-driven capabilities, including agentic AI for SOC operations and deepfake detection technologies, and has established a secure AI lab to test and validate emerging solutions.

NTT DATA's long-term vision is to position itself not just as a cybersecurity provider but as a resilience partner. By framing the firm's IR services within the broader context of enterprise resilience — spanning operational, financial, and supply chain domains — the company aims to align more closely with business leaders and risk stakeholders. This strategic alignment, combined with the firm's global reach and technical depth, positions NTT DATA as a compelling choice for organizations seeking a trusted partner in incident response and cyber-resilience.

Strengths

A key differentiator for NTT DATA is its ability to integrate IR services with broader IT and cybersecurity offerings. In cases where clients already engage NTT DATA for infrastructure or managed services, the IR team collaborates closely with internal teams to support recovery and remediation. For clients without existing partnerships, NTT DATA offers a full suite of recovery services, often leading to expanded post-incident engagements. The firm's ability to pivot from investigation to remediation and long-term support positions the company as a comprehensive partner in the cybersecurity life cycle.

Challenges

One customer noted the lack of local resources that are available to service their onsite needs. As previously noted, NTT DATA is working on adding local onsite capabilities for its IR customers.

Consider NTT DATA When

Midsize organizations that desire to work with an incident response provider with strong cyber- and IT skills, and also one that has resilience as a core pillar of its service offerings, should consider utilizing NTT DATA.

Palo Alto

Palo Alto is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide incident response services. Palo Alto Networks, through its Unit 42 division, has established a strong offering in incident response and cyber-resilience. With a mission-driven approach, Palo Alto Networks is focused not only on helping clients recover from cyberincidents but also on enabling them to emerge stronger and more resilient. The firm's IR services are deeply integrated with Palo Alto Networks' broader cybersecurity ecosystem, offering clients a seamless and intelligence-driven response capability that spans the entire incident life cycle.

At the heart of Palo Alto Networks' IR offering is a robust, globally coordinated team of experts who bring deep technical expertise and real-world experience to every engagement. The firm's services are designed to address the full spectrum of incident response needs, from initial triage and containment to forensic investigation, remediation, and post-incident transformation. Palo Alto Networks' approach is grounded in a clear understanding of the challenges organizations face during a breach — namely, the need for speed, clarity, and confidence in decision-making under pressure.

Palo Alto Networks' IR capabilities are built around a flexible retainer model that allows clients to engage proactively or reactively. These retainers are structured to provide rapid access to Palo Alto Networks' experts, with service-level agreements that prioritize fast response times and clear communication. The onboarding process is streamlined yet thorough, ensuring that Palo Alto Networks understands the client's environment, escalation paths, and key stakeholders before an incident occurs. This preparation enables faster and more effective response when time is critical.

A key differentiator for Palo Alto Networks is its integration with Palo Alto Networks' technology stack, including Cortex XDR, Cortex XSOAR, and the broader Palo Alto Networks portfolio. This integration allows Palo Alto Networks to leverage telemetry and analytics from across the client's environment, enabling faster detection, deeper

investigation, and more precise containment. The firm's use of automation and AI-driven analytics enhances the speed and accuracy of response, reducing dwell time and limiting the impact of attacks.

Palo Alto Networks also brings a strong emphasis on threat intelligence to its IR engagements. Drawing from Palo Alto Networks' global threat research and telemetry, Palo Alto Networks consultants are equipped with up-to-date insights into attacker TTPs. This intelligence-driven approach allows the firm to quickly identify indicators of compromise, attribute attacks to known threat actors, and recommend targeted remediation strategies. The firm's ability to contextualize incidents within the broader threat landscape adds significant value for clients seeking to understand not just what happened but why and how to prevent recurrence.

In addition to technical response, Palo Alto Networks provides strategic advisory services that help organizations improve their overall security posture. This includes post-incident reviews, executive briefings, and board-level reporting that translate technical findings into business-relevant insights. The firm's consultants work closely with clients to develop and refine incident response plans, conduct tabletop exercises, and build organizational resilience through training and simulation.

Palo Alto Networks' client base spans industries and geographies, with a strong presence in highly regulated sectors such as financial services, healthcare, and critical infrastructure. The firm's global reach and ability to deliver services remotely or onsite (as needed) make it a trusted partner for organizations of all sizes. While its IR services are often delivered remotely, Palo Alto Networks maintains the capability to deploy experts onsite when required, particularly for high-impact or sensitive engagements.

The team's commitment to continuous improvement and client success is evident in their collaborative approach. Palo Alto Networks emphasizes partnership and transparency, working side by side with client teams throughout the incident life cycle. Their goal is not just to resolve the immediate issue but to leave the client in a stronger position than before the incident occurred.

Palo Alto Networks is investing in expanding Unit 42's capabilities to meet the evolving needs of the threat landscape. One key area of focus is enhancing its AI and automation capabilities to further accelerate response times and reduce consultant workload. The company is also exploring new service models that integrate IR more deeply with proactive threat hunting and managed detection and response offerings, creating a more unified and continuous security experience for clients.

Another strategic priority is expanding Palo Alto Networks' global footprint and partnerships. This includes building stronger relationships with legal and insurance ecosystems to support clients navigating regulatory and compliance challenges during

incidents. Palo Alto Networks is also focused on increasing its visibility and accessibility to midmarket organizations, recognizing the growing demand for enterprise-grade IR services in this segment.

Finally, Palo Alto Networks is committed to thought leadership and innovation in the IR space. Unit 42 continues to publish high-impact threat research, contribute to industry standards, and engage with the broader cybersecurity community to share insights and best practices. The firm's vision is to redefine what it means to be an IR partner — not just a responder but a catalyst for long-term resilience and transformation.

Strengths

Palo Alto Networks' threat intelligence is gathered from multiple proprietary sources such as Unit 42 IR engagements, MDR, managed threat hunting services, and threat telemetry from 70,000 Palo Alto customers worldwide. In every IR engagement, Unit 42 presents findings that align with the client's chosen frameworks (MITRE ATT&CK, NIST, CIS, etc.) and identify control or capability gaps that resulted in the incident.

Palo Alto Networks clients that were surveyed in the IDC survey of incident response buyers gave the firm's IR team good marks for confidence that it was able to completely contain and remove the cyberattackers from their environment. They were also very satisfied in the tooling that was installed for their incident response needs.

Challenges

One of the firm's customers noted that the post incident report lacked specificity in the recommendations for them to consider.

Consider Palo Alto When

Organizations of any size that desire a strong intelligence-led incident response service should consider using Palo Alto Networks for their incident response needs.

PwC

PwC is positioned in the Leaders category in the 2025 IDC MarketScape for worldwide incident response services. PwC's offering in the global incident response and readiness market combines technical depth, operational agility, and a business-aligned approach. Its IR services are not treated as a transactional offering but are instead integrated into a broader framework of cybertransformation and resilience. This philosophy is evident in how PwC engages with clients, manages incidents, and supports long-term recovery.

One of PwC's most notable strengths is its global scale paired with local expertise. With a workforce of 364,000 professionals (well beyond the IR domain) across 151 countries,

PwC can rapidly mobilize resources to respond to incidents anywhere in the world. This expansive reach is complemented by deep regional knowledge, allowing teams to tailor responses to the cultural, regulatory, and operational nuances of each location. The ability to conduct IR in numerous languages further enhances communication and coordination, ensuring that language barriers do not impede effective incident management.

PwC typically begins IR engagements with an onsite kickoff and concludes with a formal report delivery. While regional preferences vary, this model helps establish trust and accelerates alignment during the critical early stages of an incident. The firm's scoping process is designed to be transparent and efficient. It includes a rapid assessment of the incident type, identification of required skill sets, and a clear first-week plan with a defined run rate and a "not to exceed" cap. This approach helps clients manage expectations and budget while maintaining flexibility.

The firm's technical capabilities span the full spectrum of IR, from investigation to recovery. PwC teams are proficient in a wide range of forensic, endpoint detection and response, and extended detection and response (XDR) platforms. This cross-platform fluency allows the firm to integrate seamlessly into client environments and use the most appropriate tools for each situation. This depth of technology expertise ensures that investigations are both thorough and efficient while also laying the groundwork for long-term resilience.

PwC's response capabilities are designed to scale. Whether managing a small breach or a complex, multi-vector attack, the firm applies a consistent methodology supported by proprietary and industry-standard platforms. Initial triage and breach analytics are followed by structured containment and recovery processes, often enhanced by automation. This scalability allows PwC to adapt quickly to the size and complexity of any incident, minimizing disruption and accelerating resolution.

The firm's end-to-end incident management services are another key strength. PwC supports clients through every phase of the IR life cycle — from initial investigation and containment to eradication, recovery, and post-incident remediation. It conducts impact assessments, ensures compliance with data privacy and regulatory requirements, and provides broader crisis management support. This comprehensive approach helps clients not only recover but also potentially emerge stronger and more resilient.

PwC also brings a business-centric perspective to IR. Its business-aligned Risk and Resilience Advisory services integrate legal, regulatory, privacy, and cyberstrategy expertise to ensure that technical response efforts align with broader organizational goals. This multidisciplinary approach helps clients navigate the business implications of cyberincidents, from continuity and reputational protection to long-term strategic

planning. By embedding IR within the context of business operations, PwC helps organizations make informed decisions that support both immediate recovery and future resilience.

The firm's proprietary triage tool, Breach Indicator Tool, plays a critical role in the early stages of incident response. While not a full-scale platform, Breach Indicator Tool enables rapid assessment and prioritization, helping teams quickly understand the scope and severity of an incident. PwC also partners with external specialists when needed, allowing it to scale and adapt to unique client needs while maintaining control over service quality.

PwC's experience in the cyberinsurance space adds another layer of value. The firm works with insurers as an IR provider, giving it a nuanced understanding of how insurance dynamics affect incident response. The firm's familiarity with claims processes and regulatory expectations allows it to support clients effectively in high-stakes situations. Its pricing is competitive and transparent, reflecting a commitment to delivering value without relying on cross-subsidization from other services.

PwC is investing in the continued development of Breach Indicator Tool, with plans to incorporate advanced analytics and AI-driven threat modeling. These enhancements aim to reduce time to insight and improve decision-making during the most critical phases of an incident. The firm is also expanding its global IR talent pool and strengthening regional coordination through standardized playbooks and centers of excellence. These efforts will support hybrid and remote response models, ensuring consistent service delivery regardless of geography.

Strengths

PwC's incident response and readiness capabilities are grounded in experience and scale, and arguably, the most important factor is the understanding of business risk. This approach was recognized in an IDC survey of buyers of incident response where their customers considered PwC's post-incident reporting as impressive.

Challenges

Customers in the same IDC survey considered PwC lagging behind when asked how accurately the company was able to estimate the scope and costs for incidents at the beginning of the engagement versus what the scope and costs actually ended up being.

Consider PwC When

Large organizations with a desire to integrate broad risk management strategies into their operations by utilizing the firm's resources and solutions to protect assets and enhance readiness should consider utilizing PwC for their incident response needs.

Sophos

Sophos is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. Sophos delivers a highly integrated and agile IR service that reflects its broader cybersecurity philosophy of combining human expertise with advanced technology. Sophos' approach is designed to meet the needs of organizations of all sizes, with a particular emphasis on speed, simplicity, and scalability.

At the core of Sophos' IR offering is its ability to leverage telemetry from its global MDR operations. This integration enables the IR team to act on high-fidelity alerts and contextual threat intelligence, significantly reducing the time required to identify and respond to incidents. The IR team operates with a high degree of coordination across disciplines, including threat hunting, digital forensics, malware analysis, and remediation engineering. This multidisciplinary structure ensures that incidents are addressed holistically, with each phase of the response process informed by real-time intelligence and expert analysis.

Sophos' IR services are available both as part of a retainer model and through ad hoc engagements. The company has seen strong demand for bundled offerings that combine readiness services with MDR, reflecting a market shift toward proactive and continuous protection. This bundling allows clients to benefit from pre-incident planning, such as tabletop exercises and incident response plan development, while also ensuring immediate access to response resources when an incident occurs. The flexibility of this model is particularly attractive to midmarket organizations that may lack in-house security operations capabilities.

A key strength of Sophos' IR practice is its ability to operate within legal and insurance frameworks. The company maintains relationships with a broad network of law firms and cyberinsurance providers, enabling it to support clients under attorney-client privilege and within the parameters of insurance panel requirements. This positioning allows Sophos to engage quickly and compliantly in a wide range of incident scenarios, including ransomware, business email compromise, and data exfiltration.

The IR team's operational model emphasizes collaboration and transparency. During an engagement, clients receive regular updates, clear action plans, and post-incident reporting that includes root cause analysis and recommendations for future risk mitigation. Sophos prioritizes communication and education throughout the incident life cycle, helping clients not only recover from incidents but also improve their long-term security posture. This client-centric approach is a hallmark of Sophos' service delivery and contributes to high levels of customer satisfaction.

Sophos also brings a strong technical foundation to its IR engagements. The team utilizes a suite of proprietary tools and commercial platforms to conduct forensic investigations, analyze malware, and assess the scope of compromise. These tools are tightly integrated with the Sophos Central platform, which provides unified visibility and control across endpoints, servers, firewalls, and cloud environments. This integration streamlines the response process and enables rapid containment actions, such as isolating infected devices or blocking malicious domains.

Sophos' IR capabilities are further enhanced by its threat intelligence operations. The company's threat analysts continuously monitor the global threat landscape and feed insights into both MDR and IR workflows. This intelligence supports proactive threat hunting and enables the IR team to anticipate attacker behavior, identify indicators of compromise, and recommend targeted remediation steps. The integration of threat intelligence into the response process ensures that actions are based on the latest adversary tactics, techniques, and procedures.

Sophos is focused on expanding and evolving its IR capabilities to meet the demands of an increasingly complex threat environment. One of the company's key strategic priorities is the continued integration of artificial intelligence and machine learning into its detection and response workflows. Sophos is investing in AI-driven automation to accelerate triage, improve threat classification, and reduce analyst workload. These enhancements are expected to increase the speed and accuracy of incident response while maintaining a strong human-in-the-loop model.

Sophos is also exploring new service models that further integrate IR with its broader cybersecurity offerings. This includes the development of more comprehensive retainer packages that combine MDR, IR, and proactive consulting services. These packages are designed to provide clients with continuous protection and rapid response capabilities in a single, unified engagement. In addition, Sophos is working to expand its legal and insurance partnerships to ensure broader coverage and faster activation of services in high-pressure situations.

Another area of focus is the enhancement of readiness services. Sophos plans to offer more customized tabletop exercises, sector-specific response playbooks, and executive-level training to help organizations prepare for a wide range of incident scenarios. These initiatives are aimed at improving organizational resilience and ensuring that clients are equipped to respond effectively when incidents occur.

Strengths

Customers in an IDC survey on incident response were asked about the effectiveness of the work that their IR provider did on their incident response plans prior to the need to

use the plans during an incident. Sophos customers placed the firm at the upper tier for their work in the plans.

Challenges

The acquisition of Secureworks by Sophos that closed on February 3, 2025, has the potential to create some operational challenges as the IR capabilities of the two firms are brought together. There is always the possibility of unforeseen challenges. It should be noted that prior Secureworks customers interviewed as part of this research have not seen any operational issues as of yet.

Consider Sophos When

Organizations that seek to work with an IR firm that is widely well regarded within the legal and insurance industries worldwide should consider utilizing Sophos for their IR capabilities.

Verizon

Verizon is positioned in the Major Players category in the 2025 IDC MarketScape for worldwide incident response services. The company delivers a comprehensive suite of capabilities that span the full incident life cycle, including readiness, detection, containment, eradication, and recovery. Verizon's IR operations are structured around a tightly integrated digital forensics and incident response model, which enables seamless coordination between technical disciplines and ensures rapid, effective responses to cyberthreats.

Verizon's IR capabilities are enhanced by its use of threat intelligence to drive decision-making and response strategies. The company leverages a combination of proprietary telemetry, global threat feeds, and insights from its broader cybersecurity ecosystem to contextualize incidents and anticipate attacker behavior. This intelligence-driven approach improves detection accuracy, supports proactive threat hunting, and enables more effective containment and eradication of threats. Clients benefit from Verizon's ability to correlate threat data across industries and geographies, providing a strategic advantage during incident response engagements.

A significant component of Verizon's IR offering is its emphasis on readiness services. These include incident response plan development, tabletop exercises, compromise assessments, and red team simulations. These services are tailored to the specific needs and regulatory environments of each client, helping organizations build resilience and reduce response times. Verizon's proactive approach to readiness ensures that clients are not only prepared to respond to incidents but also capable of continuously improving their security posture.

Verizon supports clients across a wide range of industries, including financial services, healthcare, manufacturing, and government. This cross-industry experience enables the IR team to navigate complex regulatory landscapes and tailor response strategies to sector-specific requirements. The company's familiarity with frameworks such as NIST, ISO, HIPAA, and GDPR allows it to provide both technical remediation and compliance-aligned guidance, which is particularly valuable for organizations operating in highly regulated environments.

Client engagement is a core strength of Verizon's IR services. The company emphasizes collaboration, transparency, and knowledge transfer throughout the incident life cycle. During an engagement, the IR team maintains frequent communication with client stakeholders, providing real-time updates, strategic recommendations, and post-incident reviews. This approach fosters trust and empowers clients to make informed decisions under pressure. Verizon also supports post-incident learning through detailed after-action reports and lessons-learned sessions, helping clients strengthen their defenses and refine their response strategies.

Verizon employs a robust suite of proprietary and commercial tools to support its IR operations. These include endpoint detection and response platforms, forensic imaging tools, malware sandboxes, and automated analysis pipelines. The company's investment in automation and orchestration reduces manual effort, improves consistency, and accelerates time to resolution. Verizon's ability to integrate these tools into client environments enhances visibility and enables faster containment and eradication of threats.

Tactically, Verizon has teams based in the Americas, APAC, and EMEA that can provide independent responses for IR engagements or work as a team, handing off engagements for "follow-the-sun" capabilities. In addition, Verizon has six worldwide full-scale, cybersecurity labs designed to support customers through malware/log analysis, mobile forensics, traditional forensics, offensive security attack platforms, and litigation assistance among other capabilities.

Verizon's IR services are also supported by a strong foundation in digital forensics. The company's forensic analysts are equipped to perform in-depth investigations across a wide range of environments, including on-premises infrastructure, cloud platforms, and hybrid networks. These capabilities enable Verizon to uncover the root cause of incidents, identify indicators of compromise, and support legal or regulatory proceedings when necessary. The forensic function is tightly integrated with the broader IR process, ensuring that investigative findings directly inform containment and remediation efforts.

Verizon is actively investing in the evolution of its IR capabilities to address emerging threats and meet evolving client expectations. One of the company's primary areas of

focus is the integration of artificial intelligence and machine learning into its IR workflows. Verizon is developing AI-driven tools to assist with incident triage, threat hunting, and report generation. These capabilities are expected to enhance analyst productivity, reduce response times, and improve the overall quality of incident investigations.

Verizon is also expanding its managed detection and response offerings to include more tightly coupled IR services. This convergence will enable faster handoffs between detection and response teams, reducing mean time to respond (MTTR) and improving incident containment. In addition, the company is developing industry-specific IR playbooks and response frameworks to address the unique needs of verticals such as critical infrastructure, retail, and education. These tailored solutions will provide clients with more relevant and actionable guidance during incidents.

Verizon is also working to increase transparency around its IR metrics and service delivery models. The company is developing more granular reporting on service composition and role allocation, which will support clients and industry analysts in benchmarking IR capabilities and making more informed decisions about service selection and investment.

Strengths

Verizon has gravitas in the incident response market via its well-respected DBIR. It is considered one of the go-to annual reports that provides insight into threat actors, attack patterns, vulnerabilities, and industry-specific risks that have emerged over the prior year. The insights and efforts that Verizon goes through to produce this report helps facilitate and accelerate its threat intelligence–led incident response and readiness capabilities. In addition, Verizon's network provides perspective into sources and nature of attacks, allowing Verizon to investigate, contain, and deal with threats.

Challenges

One of Verizon's customers noted that a monthly report that they receive is overly technical and not really suited for legal or other line-of-business groups to be able to readily comprehend or utilize.

Consider Verizon When

Organizations in highly regulated industries that place a high priority on forensics and actionable threat intelligence should consider utilizing Verizon for their incident response services.

Wipro

Wipro is positioned in the Contenders category in the 2025 IDC MarketScape for worldwide incident response services. Wipro, a global player in information technology, consulting, and business process services, delivers robust IR services through its Cybersecurity and Risk Services (CRS) practice. With a presence in over 110 countries and a team of more than 9,000 cybersecurity professionals, Wipro provides comprehensive IR solutions that integrate advanced technology, threat intelligence, and industry-specific expertise. Its services address cyberthreats across sectors like financial services, oil and gas, and utilities, ensuring rapid response and recovery. Wipro's global network, AI-driven tools, and strategic acquisitions position it as a trusted partner for managing complex cyberincidents.

Wipro's IR services form a critical component of its Cybersecurity and Risk Services, offering end-to-end solutions to detect, respond to, and recover from cyberincidents such as ransomware, data breaches, and advanced persistent threats. Operating 24 x 7 x 365 security operations centers globally, Wipro ensures rapid incident response, with teams capable of initiating containment within hours. Its MDR services integrate endpoint detection and response, threat hunting, and digital forensics to provide a holistic approach. For example, Wipro supports financial services clients with real-time threat monitoring, containing incidents like business email compromises to minimize disruption. The firm's IR process includes root cause analysis, threat attribution, and remediation, leveraging standardized methodologies aligned with frameworks like NIST and MITRE ATT&CK to ensure thorough incident resolution.

Wipro's proprietary AI platform, Wipro HOLMES, enhances IR capabilities by automating threat detection and response. HOLMES employs machine learning and predictive analytics to identify threat patterns, score incidents by severity, and accelerate response times. This technology enables Wipro to analyze vast data sets, detect anomalies, and predict attacker behaviors, significantly reducing MTTR. The Cyber Defense Platform integrates security information and event management (SIEM), analytics, and threat intelligence, providing a unified view for managing incidents in complex IT and operational technology environments. For instance, in the oil and gas sector, Wipro deploys AI-driven IR to protect critical infrastructure, ensuring rapid containment of OT-targeted threats like ransomware, which is critical for operational continuity.

With operations spanning 110 countries, its global SOC network — with hubs in regions like the Middle East, Canada, and Australia — delivers localized expertise and compliance with regulations, such as GDPR and CCPA, and sector-specific mandates. Wipro's critical infrastructure protection (CIP) strategy focuses on safeguarding critical assets through tailored IR plans. For example, Wipro collaborates with oil and gas

clients to address nation-state threats, partnering with government bodies and law enforcement to share threat intelligence and ensure regulatory compliance during cross-border incidents.

Wipro emphasizes proactive IR readiness through services like threat simulations, tabletop exercises, and customized incident response planning. These offerings help clients anticipate and mitigate risks before incidents occur. Wipro's IR retainers provide pre-incident preparation, including vulnerability assessments, penetration testing, and playbook development, ensuring organizations are well prepared. For utilities clients, Wipro conducts regular security posture reviews and simulations to strengthen defenses against sector-specific threats. The firm's proactive offerings include disaster recovery and business continuity planning, enabling clients to maintain operations during cybercrises. This proactive approach ensures clients, such as those in critical infrastructure, are equipped to handle incidents efficiently.

Wipro's IR capabilities have been bolstered by strategic acquisitions, including Capco, Ampion, and Edgile in 2021. Edgile's cybersecurity consulting expertise enhances Wipro's ability to deliver business-aligned IR solutions, while Ampion strengthens managed services with DevOps and cybersecurity integration. Partnerships with technology leaders like Microsoft, CrowdStrike, and Palo Alto Networks enable Wipro to incorporate cutting-edge tools into its IR offerings, ensuring compatibility with clients' existing infrastructure. For example, integration with CrowdStrike's EDR solutions enhances Wipro's threat hunting capabilities, providing clients with robust incident containment and recovery options across multicloud environments.

Wipro's IR services prioritize client satisfaction, offering high-quality staff and onsite support. The firm's competency framework ensures continuous training for cybersecurity professionals, maintaining expertise in evolving threat landscapes. Automation, driven by AI/ML and zero trust principles, streamlines IR processes from incident scoping to remediation, reducing response times. Wipro's flexible pricing models, such as pay-per-use and outcome-based options, cater to diverse client needs, making IR services accessible to organizations of varying sizes.

Wipro plans to advance its IR services by deepening AI and ML integration through Wipro HOLMES — aiming to enhance automation for faster threat detection and response, reducing MTTR, and improving predictive threat analysis. Investments in cloud-native security, leveraging acquisitions like Edgile, will allow the firm to strengthen IR for multicloud and hybrid environments, aligning with zero trust architectures to counter sophisticated threats.

Wipro intends to expand its global SOC network, particularly in emerging markets like the Middle East and Asia/Pacific to provide localized, 24 x 7 IR support with region-specific expertise. Strategic partnerships with technology providers like Microsoft and

CrowdStrike will drive innovation, integrating next-generation tools to enhance IR scalability and effectiveness. In addition, Wipro will focus on compliance with emerging regulations, such as the EU's Digital Operational Resilience Act, ensuring IR services meet future legal requirements. These strategies aim to position Wipro's abilities in delivering agile, technology-driven IR solutions — enhancing client resilience and competitiveness in a rapidly evolving cybersecurity landscape.

Wipro was not an active participant in this study. Publicly available information sources and an IDC customer survey with 49 of the 1,118 participants providing insights on Wipro's incident response capabilities were used to provide an assessment for this study.

Strengths

An IDC survey of buyers of incident response shows that Wipro is well regarded when it comes to the effectiveness of the work that Wipro did on their incident response plans prior to these plans being used in an actual IR engagement.

Challenges

The same IDC IR survey revealed that customers raised concerns about Wipro's ability to properly map out the attackers' next steps during the course of an attack. Wipro should consider better aligning its threat intelligence capabilities with its incident response teams.

Consider Wipro When

Organizations in critical industries that seek to work with an incident response provider with strong cloud security skills and a global reach should consider utilizing Wipro for its incident response needs.

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 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

Incident response is an organization's process of reacting to threats such as advanced cyberattacks. The difference between response, aka little "r," and big "R" as defined here, has some graying of the lines. IDC sees the need for incident response instead of more normal response occurs when the confidentiality, integrity, and availability (CIA) of data or systems is seriously impacted, then incident response services are needed.

Some of the key steps involved are detecting the incident, assessing and scoping the impact and applying a severity level, communicating with customers, escalating the incident to the correct responders, delegating incident response roles, utilizing forensics to determine the history of the attack and to potentially identify the attacking group, determining how much (if any) private data has been compromised, resolving the incident, and making appropriate compliance notifications and reports.

Strategies and Capabilities Criteria

Tables 1 and 2 summarize two sets of primary assessment factors that incident response service providers must take into consideration to project success and realize market potential.

TABLE 1

Key Strategy Measures for Success: Worldwide Incident Response

Strategies Criteria	Definition	Weight (%)
Financial strength	Historical growth funds and fuels the likelihood of continued investments in incident response services.	5.0
Growth	The likelihood of current customers to recommend their IR provider, as shown through the Net Promoter Score (NPS), portends the likelihood of future IR revenue.	15.0
GTM	Effective GTM strategies require a detailed plan on how to maximize revenue through the mix of work generated from cyberinsurance providers and law firms. Targeted marketing at the different personas such as the CISO and CIO and different departments like risk, compliance, operations, and finance can influence IR purchasing decisions and interactions.	45.0
Innovation	IR firms need to continue to invest in a variety of different AI technology capabilities to succeed against the growing speed and capabilities of different threat actors.	20.0
Functionality or offering strategy	Strategies to invest in the incident response retainer plans enable customers to get full utilization of the investment in their incident readiness and response capabilities.	10.0
Talent management	IR firms that invest in their team with dedicated time and funding will retain their teams and drive better and faster outcomes for their customers into the future.	5.0
Total		100.0

Source: IDC, 2025

TABLE 2

Key Capability Measures for Success: Worldwide Incident Response

Capabilities Criteria	Definition	Weight (%)
Custom service delivery	▪ Delivery of various proactive incident readiness capabilities are reviewed. ▪ Tabletop exercises is evaluated. ▪ Incident response plan preparation is evaluated. ▪ Red/blue/purple team exercises are evaluated. ▪ Forensic capabilities and methodologies are evaluated. ▪ Balancing the need for speed in cyber-recovery versus forensic data collection is evaluated. ▪ Accuracy shown in initial estimates of the size and scope of the incident response engagement is evaluated. ▪ The tenure of the IR firms' team is evaluated. Longer tenure provides for better team cohesion and likely better outcomes.	45.0
Functionality or offering	▪ Incident response engagements often require the IR firm to have different specialties such as IR managers/commanders, crisis managers, security analysts, forensics, communication/media/public relations, legal counsel, HR, IT, risk, compliance, threat intelligence analysts, and cyberinsurance and cyber-recovery specialists. IR providers were evaluated on the ability to provide these capabilities. ▪ The range of cyber-recovery capabilities a firm is able to deploy has a direct effect on how quickly an organization can return to a normal operating state.	15.0
Partnerships	▪ Membership, contributions, or collaboration in a variety of public and private organizations are evaluated.	20.0
Customer satisfaction	▪ Retainers that feature the fastest response times for the lowest tiered offering provide openings for new business.	10.0
Portfolio benefits	▪ IR providers that can fully operate a broad variety of EDR and XDR platforms — which is crucial in the time period prior to their own tooling being installed — are able to provide a better outcome.	10.0
Total		100.0

Source: IDC, 2025

LEARN MORE

Related Research

- *Cybersecurity 2025 Update: Miscellaneous Musings from IDC's Security and Trust Team* (IDC #US53535825, June 2025)
- *Cyber-Resilience — Turning Every Crisis into an Opportunity to Emerge Stronger* (IDC #US52280524, April 2025)
- *Cyberinsurers — Stepping Up to a Pivotal Role* (IDC #US52697324, November 2024)
- *IDC PlanScape: Cyber-Range Security Services* (IDC #US52544324, September 2024)

Synopsis

This IDC study represents a vendor assessment of incident response services through the IDC MarketScape model. It assesses 19 cybersecurity services vendors offering incident response, incident readiness, and digital forensics services. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for incident response services. The document provides detailed vendor profiles, highlighting their strengths, challenges, and key offerings.

"The 'when,' and not the 'if,' incident response capabilities will be needed for any firm that has IT infrastructure is the question that needs to be asked," says Craig Robinson, research VP, Security and Trust at IDC. "Forward-thinking firms are recognizing the importance of choosing and utilizing an incident response firm that understands their organizational DNA in advance of actually needing their services will have a direct impact on the speed and quality of the recovery effort that will be needed in the aftermath of a crisis situation."

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com