ChatGPT

Reimagining Cybersecurity Research Services in the AI Era

The Problem with Traditional Analyst Research

Cybersecurity and technology market research firms (the Gartners, Forresters, etc.) historically deliver insights through static reports – PDFs, lengthy Word docs, slide decks, web articles. These one-size-fits-all documents are **not easily digestible or tailored** to a specific reader's context. Security teams or executives must sift through dense reports to extract the few relevant insights they need, an **inefficient process**. Ironically, the effort required to consume and apply these reports can outweigh their value, leading many customers to under-utilize the research they pay for. This limits the **tangible impact** of analyst research and often caps its adoption within organizations.

Another challenge is **lack of personalization**. The content is generic, written for a broad audience or market segment. Every reader gets the same text, figures, and recommendations, even though each organization's needs differ. There's no straightforward way to filter or reframe the insights for, say, *"a retail industry CISO interested in UK ransomware trends"* or *"a DevSecOps lead at a mid-size company"* without manually parsing the report. Unlike personalized tools in other domains – for example, how developers can get code answers tailored to their exact query – analyst research tends to be static and context-agnostic.

Finally, the rise of **Generative AI** poses an existential competitive threat. Why purchase expensive analyst reports if an AI (via services like Perplexity, ChatGPT, or Claude) can synthesize public information into a handy answer or brief tailored to your question? By 2025, large language models can mimic the format of an analyst's advice, albeit with varying quality. These AI-driven "deep research" tools deliver *on-demand answers* drawn from vast public data, something traditional research firms don't readily offer. Clients are asking: *Why wait weeks for a report or pay for a subscription, when I can query an AI that reads the entire internet?* This shifts the value proposition – **speed and convenience** from AI versus the **trust and depth** of established research. As IDC's CEO observed, *"Information is everywhere — but intelligence you can trust is not… (clients) want speed, but not at the expense of trust"* [1]. In other words, today's buyers demand both instant answers **and** credible, evidence-backed insights.

The Vision: From Static Reports to Interactive, Evidence-Backed Intelligence

To stay relevant, cybersecurity research firms need to **transform how they package and deliver insights**. The future lies in turning their proprietary research into living knowledge bases that are *navigable, queryable, and verifiable* by the consumer. Instead of static text, the content should be represented in **graph structures and linked data**. This means breaking down reports into a **semantic knowledge graph** of facts, statistics, companies, threats, technologies, etc., all inter-connected via defined relationships (ontologies). Such an approach treats information as a *web of nodes and links* – much like how a well-structured database or an encyclopedia works – rather than a linear document.

Why graphs and ontologies? Because they impose **taxonomy and structure on the domain**, which is a key value-add that these firms can provide. Analysts invest significant expertise to categorize things

(e.g. defining what counts as “XDR” vs “SIEM” in security, or mapping how threat actors relate to attack techniques). These **ontologies and taxonomies** are effectively the “schema” of an industry’s knowledge – a *shared map* of how different concepts connect. Creating and curating such maps is hard and time-consuming, which is precisely why it can be a competitive moat. A high-quality ontology simplifies complexity and lets users traverse from one piece of data to related items easily. For example, a knowledge graph could let a user navigate from a statistic about *ransomware attacks in retail* to the underlying *threat groups involved*, then to *techniques used*, and further to *vendors providing defenses*, all via linked nodes. This is far more powerful than burying those links in prose or footnotes on different pages of a PDF.

Equally important is **making evidence and provenance first-class citizens** in research delivery. Tomorrow’s analyst report shouldn’t just *assert* a fact or recommendation – it should *show its work*. Every claim or data point should be traceable (via hyperlink or reference) to its source: whether that’s a primary dataset, a survey result, or a news/article that the analysts used. Essentially, research firms need to adopt a *scientific citation* approach (much like academic papers or investigative journalism). When an analyst states a fact like *“45% of UK retailers experienced a ransomware attack in 2025”*, the client should be able to click and see the source of that statistic (perhaps the firm’s survey or an external breach database). Providing this **transparent evidence chain** builds trust. It allows the consumer to verify and understand the basis for the insight, increasing credibility. In a world flooded with AI-generated text of uncertain accuracy, being able to *trace claims to validated sources* is a distinguishing feature – *“accuracy and credibility win trust”* as Forrester puts it [2].

In fact, firms that have invested in **rigorous data collection and investigative research** would benefit most from this transparency. It *rewards the good players*: those who *do* have solid evidence will shine, whereas any who were bluffing or spinning opinions will be exposed if they can’t back up their claims. By revealing the evidence, research providers essentially say *“Our insights are as good as our sources – judge for yourself.”* This kind of openness could become a *badge of quality* that sets apart trusted research in the era of AI. It aligns with the concept of **content provenance** that’s being discussed broadly (for instance, in combating misinformation, news outlets and analysts are looking into cryptographic signing or blockchain trails for their content). While still an emerging idea, we can envision a future where an analyst firm not only provides a source link but perhaps a verifiable digital signature on each published fact, so clients know it indeed came from that firm and hasn’t been tampered with.

In summary, the next-gen research service should deliver a **semantic, interlinked knowledge base** rather than a static read. All content should ideally be available in structured, machine-readable forms (e.g. JSON or Markdown with hyperlinks), not just human-readable PDFs. The role of the analyst shifts to curating this knowledge web – defining the ontology, ensuring data quality, interpreting connections – and **the output is the entire knowledge ecosystem**, not just a single write-up. The deliverable to the client, in effect, becomes a *slice of this live knowledge graph*, assembled on-the-fly to answer their question or use-case, with all supporting evidence attached.

Personalization via APIs and AI: Research-On-Demand

To achieve the above vision, **accessibility is key**. Research firms must expose their knowledge assets through flexible interfaces – essentially, they need to provide **APIs (Application Programming Interfaces)** and interactive tools on top of their data. Instead of the PDF being the end product, the *graph/database is the product*, which clients can query and manipulate.

APIs for direct data access: An API allows a client (or their software tools) to retrieve information from the research repository in a structured way. Imagine, for instance, an API endpoint where a client can input a query like *"cyber incident statistics for retail sector in 2025"* and get back a structured answer or data set. Some firms have begun moving this direction. IDC, for example, is **enhancing its APIs to provide more integrated access to IDC data and research**, so that clients can directly integrate IDC's intelligence into their own analytics and workflows [3] [4]. This means a customer could programmatically pull, say, the latest cybersecurity spending figures or risk metrics from IDC's database into their internal dashboard. The research firm in this scenario becomes a **data provider** as much as a publisher – delivering value not only through written analysis but through raw or semi-processed data that clients can plug into their decision-making systems.

This API-centric approach also forces providers to **clean up and structure their internal data**. To serve answers on demand, the underlying research findings, statistics, and taxonomies need to be stored in a well-organized way (ideally as linked data files, databases or a file-system based repository that scales to terabytes of content). Many research firms have decades of proprietary data (market sizes, survey results, tech vendor profiles, etc.) that might currently live in scattered spreadsheets or report appendices. Exposing an API pushes them to consolidate that into a cohesive backend. The better their data management and metadata, the more useful their services will be – it becomes a **competitive advantage** to have deeper, cleaner data. (It's analogous to how Google's search index or Facebook's social graph confers advantage – here the "analyst graph" would be the crown jewel).

AI-driven conversational interfaces: While APIs serve the more technical integration, a huge leap in usability comes from layering **Natural Language interfaces (AI chatbots)** on top of the research graph. This leverages large language models (LLMs) as a friendly front-end to the structured knowledge. Instead of requiring the user to write database queries or know the exact API parameters, they can simply ask questions in plain English (or any language) and get answers formulated from the underlying research content. We're essentially talking about a **domain-specific research assistant** – an AI agent that has read all the proprietary reports and data, and can generate answers or even custom reports upon request.

Importantly, such an assistant must still **cite its sources and distinguish fact from opinion**. A good design is to have the AI provide *verifiable, personalized answers*. For example, if a CISO asks: *"What are the top threats for the financial industry right now?"*, the assistant might respond with a summary of key threats *with footnotes or hyperlinks* to the firm's reports or data backing each point. (This is already being done in some implementations – as we'll see, Forrester's AI tool provides "traceable links back to validated, original sources" in its responses [5]). By doing so, the service marries the **convenience of AI (natural language Q&A, instant synthesis)** with the **credibility of research (every claim tied to a vetted source)**.

Another aspect of personalization is adjusting to the user's **persona and context**. The same knowledge graph can answer a question differently depending on who asks. A high-level executive might want a brief, strategic answer, while a technical practitioner might need detailed technical data. The output could be customized in tone and depth: e.g., more narrative vs. more data-heavy, more explanatory vs. assumption that the reader has background knowledge. It could also be localized (language, regional data focus) as needed. Modern LLMs are quite capable of style and tone adjustments given instructions, so an analyst firm's AI front-end could take into account user profile metadata (role, industry, etc.) to tailor responses. We already see early signs of this: Forrester's AI service is marketed as *"optimized to provide succinct advice and concise responses"* for business use, and they suggest you can use it to *"create business cases, get strategic advice, summarize reports, track trends, find vendors, and more"* [6] – indicating a range of use cases from executive summaries to vendor lists, all generated on demand.

On-the-fly report generation: The ultimate goal is that a client could essentially *generate a custom report or brief whenever they need*. The "report" might be as simple as an answer to a one-off question (e.g., *"Give me a quick overview of Zero Trust adoption in APAC region"* yields a paragraph answer with data points). Or it could be a more elaborate output: for instance, feeding a set of inputs (industry, company size, top 3 concerns) and having the system produce a tailored slide deck or PDF with the relevant data and recommendations from the knowledge base. In other words, the research firm's deliverable shifts from static documents delivered on a schedule, to a **research-as-a-service model** where the client pulls information as needed, in a format needed. The *value* the firm provides is the accuracy, insight, and curation of that information, not the static packaging.

Notably, this does **not eliminate the analyst's role** – it augments it. Analysts would still create the fundamental building blocks (the ontology, the verified data points, the expert judgments on likely trends). But instead of manually writing each custom report, they let the system assemble and present their insights in a myriad of ways for different users. Human oversight remains crucial: for quality control, for injecting new knowledge into the system, and for handling truly complex or novel questions that AI might not confidently address. The mantra for these next-gen services is *"AI-fueled, human-driven,"* as IDC aptly described its approach [7] – AI handles speed and scale, while humans ensure rigor and deep understanding behind the scenes.

Key Capabilities Checklist for Next-Gen Research Providers

Bringing this vision to life entails a combination of technological and content capabilities. Below is a **checklist of features** and how they map to the value delivered:

- **Semantic Knowledge Graph & Ontologies:** Research content is stored as an interconnected graph of entities (e.g. companies, threats, vulnerabilities, products, trends) and relationships, under a well-defined ontology. This enables dynamic querying and discovery of related information. *(Example: Recorded Future's threat intelligence platform uses an ontology-driven Intelligence Graph that links over 13 billion entities from open web, dark web, internal telemetry, etc., allowing analysts to uncover hidden connections between threat actors, tactics, and targets [8] [9].)*

- **Evidence/Provenance Linking:** Every factual claim or statistic in the knowledge base links to its source. Sources could be the firm's own primary research (surveys, interviews, data trackers) or external references that were vetted. This builds trust by allowing verification. *(Example: Forrester's AI service cites traceable links back to validated, original sources for the answers it generates [6], meaning clients can click through to see the foundation of a statement in a report or dataset.)*

- **Content in Structured, Machine-Readable Formats:** The firm's research outputs are not limited to PDF/HTML. Clients (or their systems) can obtain information in JSON, CSV, or via database query. This makes integration and automation possible – e.g., plugging a data feed of relevant cyber risk metrics directly into a client's risk dashboard. It also means content is more modular (easy to remix into custom reports). *(Example: IDC is moving toward offering direct data access through enhanced APIs, allowing organizations to securely pull IDC's data into their own analytics and AI tools [10].)*

- **Open APIs and Integration Endpoints:** There are documented APIs or endpoints through which clients can query the knowledge base, ask questions, or retrieve updates. This could range from simple RESTful APIs for numeric data to GraphQL endpoints or even SPARQL for graph data. API access also implies the firm may offer SDKs or support to help clients build on top of

their intelligence. *(Example: Recorded Future's Intelligence Graph is accessible via API, powering integrations that embed its threat intelligence into other security products [11]. In the market research realm, IDC's upcoming platform similarly emphasizes API access to expand use of their intelligence across client workflows [10].)*

- **AI-Powered Query and Chat Interface:** A user-facing assistant (chatbot or search assistant) that allows natural language queries over the content. This should handle follow-up questions (conversational context) and deliver answers or summaries, complete with source attributions. Ideally, it has no or high limits on queries so that users truly rely on it as an everyday tool. *(Example: Forrester's Izola tool, launched in 2023, was one of the first in the industry – it lets clients ask any question and generates answers drawing from all of Forrester's research corpus, with no query limits and with citations to the relevant reports/blogs [12] [13]. It's now used daily by thousands of clients to get fast advice [14].)*

- **Personalized and Contextual Outputs:** The system can tailor its responses based on the user's role, industry, region, or even based on an input scenario. This might involve pre-defined templates (e.g., "summary for executive" vs "detailed technical explainer") or dynamic adjustment of tone and detail. It also could incorporate the client's own data/context if provided (for example, ingesting some internal documents to combine with the research). *(While no firm publicly details persona-based output yet, Forrester hints that AI Access can be used to "find vendors" or "create business cases" [6] – implying it can produce output for specific needs, and Frost & Sullivan's AI coach is intended to help tailor strategies for a client's specific growth questions [15].)*

- **Fact vs. Opinion Labeling:** The content delivery differentiates between raw facts (data points, what happened, how many, etc.), and analyst opinions or hypotheses (interpretations, predictions, recommendations). Both are valuable, but marking them helps the user know what is evidence vs. an analytic judgment. This could be as simple as tagging sentences or having separate sections in outputs. *(For instance, a response might list factual findings with sources, followed by an "Analyst's perspective" section. While this practice is not yet standard, it aligns with the push for transparency. None of the major firms have explicitly advertised this feature yet, but it could be a future improvement to build trust.)*

- **Real-Time or Frequent Updates:** Instead of annual or quarterly static reports, the knowledge graph is continuously updated with new information (new threats, latest survey data, news events, etc.). This ensures that the answers or custom reports generated are always using the most up-to-date intelligence. Many cybersecurity topics evolve quickly, so this is crucial. *(Example: Recorded Future's system continuously ingests data in real-time from a million sources [16], so the intelligence is always current. Analyst firms are also starting to issue more frequent "alerts" or use feed-like delivery alongside big reports – the shift to a platform makes it easier to push incremental updates.)*

- **Workflow Integration and Partnerships:** Recognizing that clients might want to consume intelligence within their existing tools, leading firms may offer integrations or partnerships to embed their insights into popular platforms. For instance, integrating with a SIEM for threat intel, or with a business intelligence tool like PowerBI for market forecasts. IDC explicitly mentions plans to *"embed IDC insights directly into the applications and tools where business decisions happen"* via strategic partnerships [17]. This way, the research doesn't live in a silo; it surfaces at the point of need (e.g., while a CISO is working in a risk management software, they see relevant IDC risk benchmarks right there).

- **Analyst Validation and Human-in-the-Loop:** Even with AI and automation, the best services will still involve human expert oversight for quality. For critical or high-stakes queries, some workflows might route the AI-generated answer to a human analyst for review or augmentation before delivery. Or an analyst might proactively curate "research digests" that the AI can draw from for accuracy. The end result is that the client gets a trustworthy answer fast, and knows that behind the scenes a domain expert's methodology backs it up (if not their real-time intervention, at least their prior vetting of the content). This might not be visible as a feature, but it's part of the service promise of being "human-driven" in insight even if "AI-fueled" in speed [7].

Early Movers: Which Firms Are Adopting this Approach?

The transition from traditional reports to interactive, AI-enabled research services is underway. Some analyst firms and cybersecurity intelligence companies have started to build these capabilities:

- **Forrester Research** – *Forrester* has been a front-runner in this space. In 2023 they launched **Izola**, one of the industry's first generative AI research assistants, *"years ahead of industry peers"* [18]. Izola (now part of the **Forrester AI Access** service) allows Forrester clients to ask questions and get answers synthesized from the firm's extensive repository of reports, data, and analyst insights. Crucially, the answers come with **traceable citations**: Forrester highlights that the service provides *"presentation-ready insights… with traceable links back to validated, original sources providing credibility, context, and confidence."* [19] This means a user can not only get a quick answer but also click through to the original report or chart from which that answer was derived. Forrester's AI Access is designed to serve everyone from senior execs to front-line practitioners with *trusted, quick advice* [20]. It's even available on mobile, indicating the intent for it to be a daily tool [21]. While Forrester still produces traditional written reports, it has effectively made its entire research knowledge base accessible in a conversational manner. (Forrester has not publicly advertised a raw data API for clients, focusing more on the Q&A interface; however, the underlying platform likely could provide data exports on request. The key takeaway is their **shift to an AI-first delivery** model for research, setting a template that others are now trying to follow.)

- **IDC (International Data Corp)** – *IDC* is in the process of a significant transformation toward AI-powered delivery. In a November 2025 announcement, IDC's CEO described a *"year-long effort to rethink products and how we deliver"* research, culminating in a new **AI intelligence platform** [22]. This platform aims to combine *"the speed of AI with the depth and credibility of IDC intelligence"*, making their vast library of data (11.5+ billion data points, 115k publications) **"conversational, contextual, and workflow-ready."** [23] [3] ***In practical terms, IDC is building a chat/assistant interface so users can move*** **"from question to decision faster"*** [24] **by querying IDC's knowledge. Alongside this, IDC is rolling out** direct API access **for customers –** ***"enhanced APIs and AI usage rights"*** **to** ***"integrate our intelligence directly into your… AI tools and workflows."*** [25] **This explicitly addresses the need for integration: clients will be able to pull IDC's data into their internal dashboards or even use it to fine-tune their own AI models (with proper licensing). IDC is also pursuing partnerships to embed their insights into other popular platforms where clients work** [17] **(for example, one could speculate integrations into tools like Salesforce, or strategic planning software). All these steps point to IDC not just publishing research, but providing it as a** service accessible anywhere**. They emphasize that this is done without compromising their** ***"time-tested rigor or quality,"*** **i.e., keeping analysts in the loop to ensure the AI outputs remain reliable** [26] [7]**. The full unveil of IDC's new AI platform is slated for Q1 2026** [27]**, but the direction is clear:** conversational AI + APIs + partnerships** to meet users where they are. IDC's approach

underscores that trust is still the differentiator – they acknowledge the trade-off between speed and credibility and are striving to offer both [1].

- **Frost & Sullivan** – This global consulting and research firm (known for market "Frost Radars" and growth strategy reports) launched its own AI-based assistant in 2024. Called the **Frost AI Growth Coach**, it's essentially an AI that *"incorporates the company's institutional knowledge across industries"* [28] to support client decision-making. The Growth Coach provides *"on-demand access to actionable insights,"* converting Frost's research findings into clear answers and recommendations for clients [15]. It leverages Frost & Sullivan's internal **Growth Opportunity Analytics (GOA)** library as its knowledge base [29]. In practice, a client could ask the Growth Coach a question about, say, entering a new market or adopting a particular technology, and the AI will draw from Frost's decades of research to guide strategy – effectively acting as a digital consultant. The assistant *"automates data interpretation and presents data in natural language"* [30], making the insights easily digestible. Frost's leadership has framed this as blending AI with *"over six decades of research expertise"* [31] – again highlighting that human knowledge is at the core, with AI as the delivery mechanism. While details on whether it provides source citations or how much can be customized are scant, the move itself shows Frost & Sullivan aligning with the trend: using AI to *personalize and streamline* the client's access to research. They also mention additional AI offerings (AI Engine, Growth Vector, HiDiAI) [32], suggesting a broader strategy of embedding AI in their services. This indicates even traditional management consulting-oriented firms see the need to evolve their research delivery in similar ways.

- **Recorded Future** – This company is not a classic "market analyst firm"; it's a cybersecurity threat intelligence provider. However, it exemplifies many of the principles discussed, applied in the threat research domain. Recorded Future has built an extensive **Intelligence Graph®** – essentially a massive knowledge graph of threats and cyber intelligence. For over a decade, they've been *"indexing, structuring, and analyzing threat data from every corner of the internet"* [33]. Their platform ingests over 1 million sources including open web, dark web, technical feeds, malware analyses, etc., in real-time [34]. This data is organized in an ontology linking entities like threat actors, IP addresses, vulnerabilities, targets, and events. The result is an always-updated, machine-readable **knowledge base of threats**. Clients interact with it not through static reports (though they do have analyst-written reports too from their Insikt research group), but primarily through search queries, alerts, and an API. In fact, the Intelligence Graph is **accessible via API and powers multiple specialized products** (for different needs like vulnerability intelligence, brand monitoring, etc.) [11]. When an analyst uses Recorded Future, they can pivot through data points (e.g., from an indicator to all threat actors associated with it, then to their state sponsors, and so on) – a graph exploration experience. And importantly, the platform often links to original source evidence: for example, if a leaked credential or a Dark Web post is referenced, the user can often view the snippet or source of that information, establishing provenance. This approach has proven the value of structured, linked knowledge in cybersecurity: users gain speed (automated data collection and linking saves *"thousands of manual hours"* [8]) *and* confidence (the system's ontology-driven analysis reduces false positives by ~95% by providing rich context [9]). Recorded Future's success has likely inspired others in the industry – it shows that **interactive graphs + real-time data + source transparency** can indeed replace a traditional report in many cases, or at least complement human analysts by handling the heavy data lifting. While Recorded Future is productizing threat data, one could imagine a similar model for *market* data or *technology trend* data in the analyst world.

- **Gartner** – As the biggest name in tech research, one might expect Gartner to lead such innovations, but publicly they have been more cautious. As of 2025, Gartner's primary

deliverables are still the familiar ones: research articles on their portal, Magic Quadrant PDFs, Toolkits, etc., delivered via their online client portal. There isn't an announced Gartner-branded generative AI assistant for research yet, nor an open API for clients to pull data directly. (Gartner does operate **Peer Insights** – a platform of user reviews with APIs – but that's user-contributed content, not Gartner's own research output). It's very likely Gartner is developing AI-based offerings behind the scenes (they certainly are publishing about AI impacts and advising others to use AI), but nothing akin to Forrester's Izola or IDC's announced platform has been revealed at this time. Gartner analysts do heavily use taxonomy (their IT market segment definitions, hype cycle categories, etc.), so the firm has rich ontologies internally; however, they haven't made those navigable to customers except through the traditional report format. Gartner's relatively slow public response could be due to its large installed base and concern over cannibalizing existing product lines. Nonetheless, given market pressure, we can expect them to introduce more AI-enhanced research delivery soon. (Indeed, Forrester's statement that Izola was launched "ahead of industry peers" [18] implicitly includes Gartner in those peers – suggesting Gartner was not first to this, but will need to catch up.)

- **Other Analyst Firms:** Many mid-sized and boutique research firms (Omdia, KuppingerCole, Enterprise Strategy Group, 451 Research/S&P Global Market Intelligence, etc.) are observing these trends, though few have made major public moves to implement AI-driven research delivery. Most of these firms still deliver insights as written reports or PDFs behind subscription portals. Some offer *partial* interactivity – e.g., interactive charts on a portal, or the ability to download datasets from surveys – but not a full conversational AI or API access to all content. We can, however, cite a general shift: *TechTarget's Enterprise Strategy Group (ESG)*, for instance, has integrated its research with an online portal that is part of a larger IT community site (TechTarget) – which means users can search ESG research and get some tailored content recommendations. And S&P Global (which owns 451 Research) has been integrating tech research into its **Market Intelligence** platform, which is queryable (primarily oriented around financial and market data, accessible via their GUI or Excel add-ins/API). So, there is movement toward treating research as data. But these firms haven't showcased dedicated AI assistants or the kind of rich graph approach yet. It's likely a matter of time – the **pressure from clients and competition will push even smaller players to at least partner with AI tools** or offer more modular content. We might soon see, for example, Omdia or others partner with platforms like AlphaSense (a search engine for business research that already uses AI to summarize documents) so that their reports can be auto-summarized or queried in new ways. If they lack resources to build their own Izola or Intelligence Graph, partnering could be a way to not fall behind.

- **Industry Consortia and Open Data:** Outside of for-profit firms, it's worth noting initiatives like the **MITRE ATT&CK** framework in cybersecurity. This is an open, community-driven knowledge base (managed by MITRE, a nonprofit) mapping threat actor tactics and techniques in a structured way. It's essentially an ontology of adversary behaviors and is published in machine-readable formats (STIX, TAXII) for anyone to use. Many tools and vendors integrate ATT&CK because it provides a common language and structure for threats. Similarly, standards like **CVE (Common Vulnerabilities and Exposures)** and **CWE (Common Weakness Enumeration)** provide taxonomies for vulnerabilities and weakness types. These aren't "analyst research reports", but they exemplify how **structured, linked information** is incredibly useful in cybersecurity. Analyst firms could take a cue from this success: part of their value could be publishing and maintaining such taxonomies for emerging areas (for example, a taxonomy of "cloud security controls" or "AI risk categories" that everyone can reference). By doing so, they become more *embedded* in the ecosystem's day-to-day operations (and could even license access or charge for advanced versions).

In summary, a few leading organizations have started to implement the components of next-gen research delivery – **Forrester, IDC, Frost & Sullivan** among analyst firms, with Forrester being the earliest to market with a true AI Q&A service, and IDC close behind with a comprehensive vision. **Recorded Future** demonstrates these principles in the threat intel arena, and undoubtedly other threat intel companies (e.g., Mandiant, IBM Security's X-Force, etc.) are also using AI to sift data and could expose that via APIs. **Gartner and others** have the pieces (vast data and domain expertise) but have not yet productized them into a client-facing AI or open data offering as of 2025. We expect a cascading effect: no firm will want to be the laggard once clients see the convenience and power of these new services elsewhere.

Conclusion: The Road Ahead for Research Firms

The landscape of cybersecurity research and advisory services is poised to change dramatically. The traditional model – expert analysts producing static periodic reports – is giving way to a model where the **core product is insight-as-a-service**: living knowledge that clients can query, integrate, and trust in real-time. This transformation is driven partly by technology (the rise of LLMs, knowledge graphs, and cloud APIs) and partly by necessity (clients demanding more value, more personalization, and faster answers, without sacrificing credibility).

For research companies, embracing this model is not just about adding a new feature, but about rethinking their value proposition and business model. They will need to invest in data infrastructure, AI capabilities, and perhaps new skill sets (ontologists, data curators, AI trainers, etc.). They also may need to find new revenue models – for example, charging for API access or per-query usage, or licensing their ontologies to others – in addition to selling subscriptions the old way. There's even a potential for **micro-transaction models** (as the user hinted in the conversation, envisioning revenue streams back to individual analysts): if the content is modular and trackable, could an ecosystem emerge where third parties pay to pull specific pieces of insight, and the original researcher gets a cut? This is speculative, but not impossible in a future where content is granular and provenance is clear.

The good news for these firms is that their fundamental assets – **expertise, rigorous methodologies, and trusted brand reputation** – become even more valuable in an AI-flooded world. Clients will gravitate to sources that can prove their assertions and filter signal from noise. As one industry leader put it, *"faster answers don't always mean better ones"* [35] – anyone can get a quick answer from the internet, but getting the **right** answer with confidence is the hard part. By doubling down on evidence-based analysis and marrying it with modern delivery, research firms can offer the best of both worlds.

In the coming years, we can expect to see **wider adoption of AI assistants and data-driven research portals** across the industry. Perhaps Gartner will unveil its own AI advisor; niche firms might specialize their knowledge graphs for sub-domains (e.g., a company might build the definitive knowledge graph for cloud security controls or for data privacy regulations). Collaboration could also occur – maybe multiple firms contribute to a shared ontology to ease clients' comparison of their insights.

From the client perspective (cybersecurity teams, CISOs, technology leaders), this evolution is welcome. It means their paid research subscriptions can finally become **daily tools** rather than shelfware. The research becomes actionable: they can query it during a strategy meeting, integrate it into risk analyses, or have an assistant summarize how a new development (say a major breach or a new technology) impacts their specific environment. In effect, the analyst firm becomes a *virtual member of the team*, available on-demand. This is how research insight can become **mission-critical** to businesses – by being ubiquitous, tailored, and trustworthy.

In conclusion, the firms that succeed will be those that **embrace personalization, interactivity, and transparency** in their services. The old model of PDF reports is hitting its ceiling. The next generation of cybersecurity research will live in knowledge graphs and AI-driven dialogues, not PDF pages – and it will be delivered via APIs and assistants, not just email and webinars. The transition is already visible: from Forrester's Izola to IDC's upcoming platform, and Frost & Sullivan's coach, the race is on. Those who move quickly to provide *consumable, verifiable, and customizable* intelligence will solidify their role in the industry's future. Those who don't risk seeing their PDF reports get outpaced by an AI – and their clients' trust along with it.

Sources:

- IDC (Genevieve Juillard), *"AI-Fueled, Human-Driven: How IDC is Redefining Trusted Tech Intelligence,"* Nov. 19, 2025. Describes IDC's new AI platform, API access strategy, and focus on combining speed of AI with trusted research [3] [25]. Emphasizes need for speed **and** trust in research delivery [35].

- Forrester, *"Forrester AI Access"* service page, 2023. Details the Izola AI tool and how it provides answers with citations from Forrester's proprietary research. Notes it launched in 2023 ahead of peers, and that it offers traceable links to validated sources in responses [36] [6].

- VKTR (Chris Ehrlich), *"Frost & Sullivan Releases AI Assistant,"* Sep. 27, 2024. News about Frost & Sullivan's **AI Growth Coach** launch. Explains that it draws on Frost's institutional knowledge (Growth Opportunity Analytics library) to give clients on-demand insights in natural language, to accelerate data-driven strategy [37] [38].

- Recorded Future, *"Intelligence Graph"* product page, accessed 2025. Explains the concept of Recorded Future's threat intelligence graph that indexes over 1 million sources and connects data via an ontology. Highlights that it's accessible via API and helps uncover connections with speed and context (reducing false positives) [8] [11].

- Forrester AI Access page (continued): Mention of Izola's usage and capabilities [12] [14], and the benefit of providing credible answers with source links to clients (quote: *"presentation-ready insights … with traceable links back to validated sources"*) [39].

---

[1] [3] [4] [7] [10] [17] [22] [23] [24] [25] [26] [27] [35] IDC - AI-Fueled, Human-Driven: How IDC is Redefining Trusted Tech Intelligence
https://www.idc.com/resource-center/blog/ai-fueled-human-driven-how-idc-is-redefining-trusted-tech-intelligence/

[2] [5] [6] [12] [13] [14] [18] [19] [20] [21] [36] [39] Forrester AI Access
https://www.forrester.com/research/ai-access/

[8] [9] [11] [16] [33] [34] Intelligence Graph | Recorded Future
https://www.recordedfuture.com/platform/intelligence-graph

[15] [28] [29] [30] [31] [32] [37] [38] Frost & Sullivan Releases AI Assistant | VKTR
https://www.vktr.com/ai-news/frost-sullivan-releases-ai-assistant/