TECHNOLOGY INDUSTRY GROUP

AI is Driving Change in Cybersecurity: Pitfalls and Opportunities

The rising prominence of artificial intelligence (AI) across the cybersecurity software sector has effectively become an arms race between companies using it as a tool to detect and deter threats on one hand and bad actors utilizing it as a threat on the other. It's no wonder cybersecurity software providers are keen to define and refine their approach to incorporating AI and machine learning (ML) into their portfolio strategy.

Key considerations for incorporating AI/ML investments within Cybersecurity software:

- **AI must be contextually relevant:** Understand the various levels of models and apply them in a contextually relevant manner according to their intended use.
- **AI's impact on cybersecurity:** Realize how the cybersecurity software landscape has fundamentally changed due to advancements in AI and ML.
- **Data security and integration:** Customers are cautiously optimistic that next-generation threat detection platforms can be trusted — especially with data privacy — and consider a seamless integration of AI with their existing digital ecosystem to be a crucial criterion when selecting applications.
- **Justifying AI investment:** It's important to qualify the investment in AI and define the use cases for cyber software.

These factors have been gleaned from A&M's experience, through our sector survey, 2024 Cybersecurity Market Study, and a more recent study in November 2024 on the various use cases of AI and ML in cybersecurity.

Key Takeaways

Use-case led: The process of defining an AI strategy should be use-case led to ensure model types are fit-for-purpose and well suited to accommodate data types, size, sources, volume and other criteria.

AI is effective: Applications of GenAI and LLMs to Cybersecurity software have proven effective in accelerating root cause analysis and incident response activities, via virtual assistants.

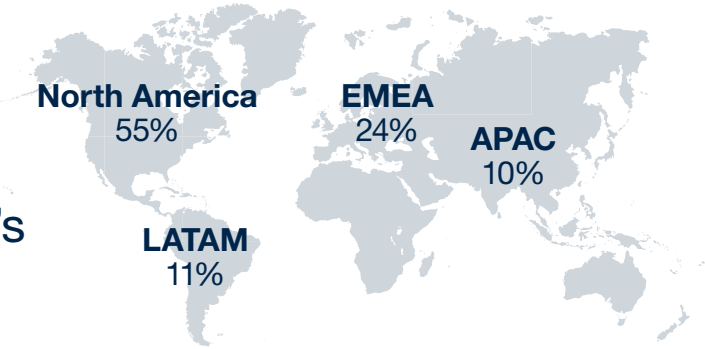
Predictive models are best: A prevention-first approach to managing threats requires detection software with predictive models built on advanced data science and/or computational statistics

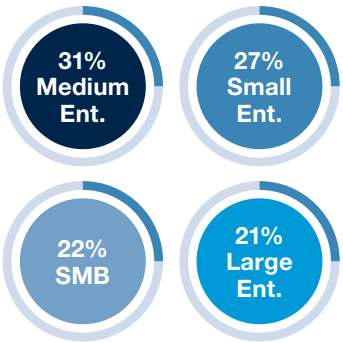
Integration is key: Customer preferences call for cybersecurity software providers who are investing in AI and ML applications to prioritize ease of integration and improved interoperability, data privacy, flexibility in deployment models and post-sales support.

This graphic is a high-level summary of the main survey's findings:

Survey Participants

340+
decision makers for their company's cybersecurity





Key Survey Findings

Growth Rate is Slowing

67% of companies believe they are at the right level of spending for cybersecurity

Revenue growth rates remain positive but have slowed, with an additional 19% of respondents stating they are overspending

R&D Budgets Need to Be Focused

Slowing growth plus steadily increasing average R&D spend reaching 26% of revenue, requires focus on core solutions

21 leading public cybersecurity companies' R&D spend grew with the market and now requires optimization amidst slowing growth rates

Consolidation is Crucial

46% of respondents think there are too many overlapping solutions and too many vendors

Crunchbase estimates ~10k cybersecurity firms, M&A has slowed, and customers want solution consolidation

AI is Impacting The Sector

"It's an arms race"
- Cyber Expert

The impact of AI will be felt from both the threats faced and the solutions used to detect and respond

Leaders and investors in cybersecurity software companies can benefit from the analysis and recommendations below, which are intended help them better incorporate AI and ML in their strategies — first, by demonstrating how the technology evolution requires new responses to address threats at several levels, and ultimately, how companies can best integrate AI and ML and qualify their investment in it.

Applied Forms of AI Must be Contextually Relevant to the Intended Use

The impact of AI in cybersecurity must be understood within the context of how model types should be applied when they are best suited to support a given use case. Since forms of AI and ML are not created equal for uniform application, the intended use cases should inform the type of model applied. The exhibit below summarizes this idea.

Artificial Intelligence: Any technique that enables computer systems or algorithms to solve tasks and imitate intelligence human behavior (e.g., natural language processing, language models, GenAI)

Machine Learning: A subfield of AI that enables machines to learn to perform tasks by analyzing large datasets without being explicitly programmed (e.g., supervised ML, unsupervised ML)

Neural Networks: A subfield of ML with multiple layers, that mimics how neurons in the human brain function, to learn, perform pattern recognition, and make predictions

Deep Learning: A form of ML where multi-layered neural networks can analyze data with logical structures to draw conclusions like a human

Type	Suited For
Natural Language Processing	Sentiment analysis, task automation, search optimization
Language Models	Chatbots, data synthesis, summarization
Generative AI	Content creation from text-based prompts
Supervised ML	Classification and regression
Unsupervised ML	Behavioral analysis, clustering of large datasets
Neural Networks	Classifying data, clustering, predicting, associating
Deep Learning	Explainability, inferencing, computer vision

In many situations, a combination of two or more forms are utilized to achieve desired outcomes. For example, the increasingly common “virtual assistant” typically relies on large language models (LLMs), small language models (SLMs) and deep learning:

- **Large Language Models —** A type of Generative AI (GenAI) that is capable of ingesting and processing enormous amounts of data, querying the datasets based on user-defined parameters and generating a response in natural human language.
- **Small Language Models —** Pared-back versions of LLMs that are designed to be more efficient, compact and resource friendly. These models have fewer parameters and focus on essential skills, like understanding or generating text, offering reduced latency, improving privacy and conserving bandwidth
- **Deep Learning —** A subset of machine learning that can perform tasks like classification and regression for inferencing and explaining to draw conclusions like a human would. These models continually learn from available data and interactions to sharpen outputs.

LLMs have gained immense traction in recent years, primarily driven by the scaled, public release of AI-powered chatbots, such as ChatGPT, Claude, Gemini and others.

Other key growth drivers include the:

- Availability of open-source foundational models and increased effectiveness and versatility resulting from rapid expansion of parameters,
- Ability for models to interact with one another to create a cognitive “mesh,” and
- Evolution of the transformer architecture to incorporate self-attention mechanisms.

These consequential advancements improve performance and capture more context for natural language processing tasks.

While LLMs are well suited to provide conversational, prompt-based interfaces, they are less than ideal for other advanced applications, such as prediction or decision intelligence.

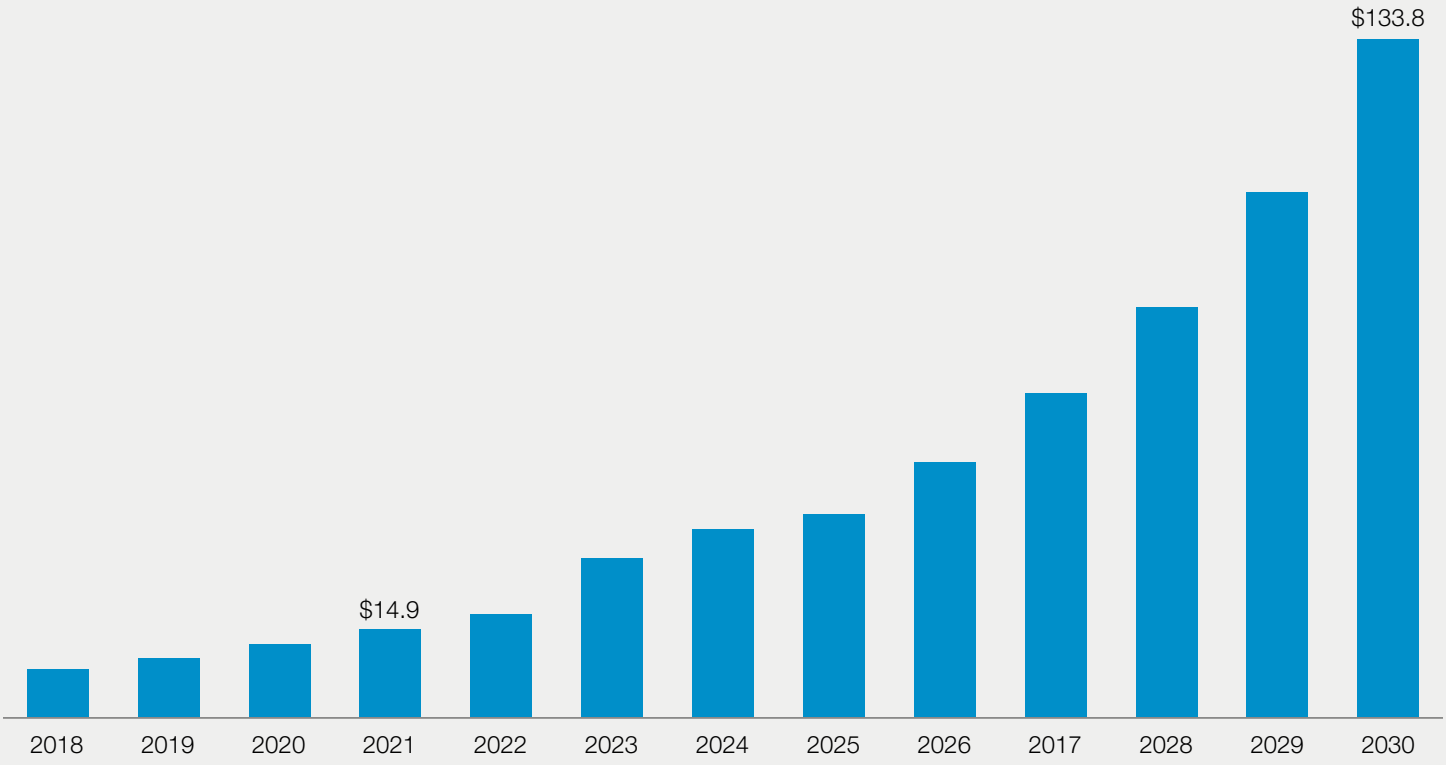
Rather than utilize the data synthesis and summarization capabilities of an LLM, unsupervised ML models with multiple layers like neural networks are better paired with deep learning to support predictive use cases. Unsupervised ML models can be trained on unstructured data without human intervention to discover patterns and relationships. Neural networks expand on this foundation, utilizing multiple layers to mimic how neurons in the human brain function, to provide self-learning capabilities, perform pattern recognition and ultimately make predictions.

The Cybersecurity Software Landscape Has Fundamentally Changed Due to Advanced AI and ML

Category	Where it Fits	Model Types	Model Application	Use Cases
End-to-End Cyber Platforms	Broad coverage that's a must have for every organization	Supervised & Unsupervised Machine Learning	File Classification, Behavioral Analysis for Detecting Anomalies	Proactively monitoring environments for potential security threats, detecting incidents, responding to cyberattacks, investigating suspicious activities
Threat Detection & Response Products	Last line of defense for organizations with critically sensitive information within IT environment	Computational Statistics, Unsupervised Machine Learning, Deep Learning Neural Network	Advanced Behavioral Analysis to Predict and Prevent	Prevention-first threat management, pre-execution identification and quarantining of malicious files, securing data stores, critical infrastructure and applications from bad actors
Anti-Virus Products	Legacy software that's isolated to end-user devices	Heuristic Models, Signature Based	Basic Behavioral Analysis	Monitors, identifies and blocks malicious files, scans local hard disks and monitors file access
Virtual Assistant	Chatbot-like capabilities that are commonly built into E2E Cyber Platforms	GenAI, Large-Language Models, Small-Language Models	Prompt-Based User Interface	Assists InfoSec personnel in conducting threat hunting, root cause analysis, incident response and investigative workflows

Most, if not all, cybersecurity software providers have incorporated some form of AI into their product portfolio. Further, market leaders as identified by A&M were early adopters of AI and ML, initiating investment in the technology decades ago. While some of these organizations capitalized on an "early mover advantage," gaining market perception as innovators, **many have struggled to deliver high efficacy solutions** that can effectively prevent security incidents from occurring.

The Global AI-Powered Cyber Market Accounted for ~$15B in 2021, and is Estimated to Reach Market Value of ~$134B by 2030 (Acumen, July 2022)



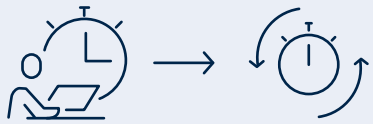
When evaluating the various forms of AI applied to threat detection software, there exist three main categories that can be grouped by generation.

Legacy organizations: First, there are the legacy players who leverage signature-based or heuristic models to perform basic behavioral analysis. These solutions do not utilize AI in core offerings, and as a result, are characterized by relatively low accuracy and high false positive rates. Further, they are often deployed as computer-intensive agents that slow down end-user devices and require frequent software updates. For these reasons, this segment of the threat detection software market has observed a sharp decline in growth over the past decade.

End-to-end cybersecurity platforms: The second evolution of providers is also the largest, offering reactive threat detection capabilities. The underlying detection engines in these end-to-end cybersecurity software platforms are typically constructed on supervised and unsupervised ML. Used to perform behavioral analysis with incrementally higher efficacy than what is possible with signature-based or heuristic models, the platforms have captured and retained significant market share but have been met with several key challenges in recent years including:

- **Missed threat alerts:** These models have innate limitations in the ability to fine tune model sensitivity that often result in what's considered "noisy alerting" — the generation of a high number of alerts that may not indicate real threats. These high-volume "false positives" can be exacerbated when paired with the broader talent shortage of experienced information security (InfoSec) professionals, meaning an active threat can go unseen for hours or days before being investigated. Cisco estimates as much as 42 percent of companies are affected by alert fatigue, or apathy to proactively defend against cyberattacks.
- **The human element:** Traditional ML models require upfront, manual interactions to define what a threat looks like across attack vectors. This dependency on human knowledge, expertise and time essentially limits the value of the tool because it's based on the availability and skillsets of personnel.

Resource Intensive Feature Engineering



InfoSec personnel are required to stay current on vulnerabilities and their respective threat vectors to manually define rules for detection

Noisy Alerting Environments

Alert fatigue plagues most InfoSec teams, increasing the risk a bad actor has gained access to the environment and remains undetected

- **Low data ingest volumes:** Traditional ML models are fundamentally limited in their ability to ingest and process vast amounts of information, typically hitting a ceiling around 2 percent to 5 percent of available raw data.
- **Zero-day threat detection:** These models are incapable of identifying unknown or zero-day threats. Bad actors utilizing AI-powered adversarial maneuvers can rapidly create mutations and obfuscations of known threats to bypass detection tools. While zero-day incidents make up only about 3 percent of total vulnerabilities, they have gained notoriety due to wide-scale attacks, such as the MOVEit attacks in 2023 and the Follina Spring4Shell malicious code in 2022, both of which represent a continued threat since initially showing up in 2015.

Predictive engines: The third generation of threat detection software is the most differentiated, characterized by the ability to identify zero-day security events. These platforms leverage computational statistics like Bayesian models and dynamical systems or advanced data science, such as deep learning neural networks, to offer predictive capabilities. Predictive engines represent the most sophisticated form of behavioral analysis, providing end-users with the ability to detect and ultimately prevent a vulnerability from being exploited pre-execution. These innovative solutions offer several key advantages over prior generations of threat detection platforms.

Unlike traditional machine learning,[1] many predictive engines do not require customer data to train generic models. Rather, they are trained on a wide variety of file types, both benign and malicious, using multiple hyper-parameters to develop pattern recognition abilities. This is especially impactful for customers with high sensitivity data environments or in highly regulated industries with stringent compliance obligations, like healthcare and financial institutions.

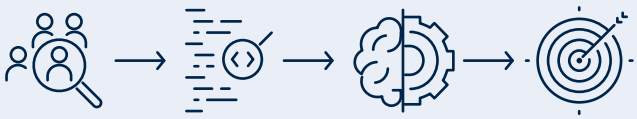
Customer interviews conducted by A&M revealed these organizations place significant value in their ability to deploy threat detection software with assurance their integrations are secure and their data will not leave their footprint.

The innate self-learning nature of some model types allows end-users to forego manual model feature engineering, lowering total cost of ownership and enabling InfoSec personnel to focus on what matters.

Finally, depending on model type, these platforms are capable of ingesting and processing 100 percent of available raw data from customer environments. Applying these advanced models to the entirety of the attack exposure supports a proactive approach to identifying and preventing known and unknown threats from executing.

Both current and next-generation solution providers are applying LLMs and GenAI to materially accelerate incident response and root cause analysis exercises. GenAI is fit-for-purpose to perform security operation center analyst-level malware analysis, generate detailed reports that can go beyond compromise indicators and develop visual representations of how events are correlated. By providing InfoSec teams with an assistant or chatbot interface that's embedded within the detection or prediction platform makes finding the "needle in the haystack" simpler and faster than ever before.

AI Virtual Assistants for Threat Intelligence



Prompt-based interfaces powered by LLMs / GenAI provide InfoSec teams the ability to expedite incident response and / or root cause analysis

1. Traditional Machine Learning refers to unsupervised and/or supervised ML models, which utilize algorithms like decision trees, linear regression, frequent pattern growth or principal component analysis

Customers are Cautiously Optimistic Next-Gen Threat Detection Platforms can be Trusted

Sophisticated InfoSec teams in the enterprise segment and managed security service providers targeting small- and medium-sized businesses are adopting next-gen threat detection and response software platforms, but not without a healthy mistrust in the solution providers' marketing claims. As rapid advancements in AI and cybersecurity are made to offer these predictive or preventative capabilities, chief information security officers and managed security service providers are also getting smarter.

Enterprise IT environments are increasingly becoming heterogenous, leveraging best-of-breed technology solutions across the application suite, infrastructure tooling and security stack. **A threat detection and response software platform's ability to integrate with the existing ecosystem was identified as a critically important variable in customer's selection criteria.** Customers don't want to maintain bespoke integrations and highly value secure, bidirectional data transfer. Solution providers should consider the existing and planned research and development investment required to develop an open application programming interface (API) strategy with secure, off-the-shelf connectors to commonly integrated technologies, such as Security Information and Event Management, Security Orchestration, Automation, and Response or Endpoint Detection and Response systems.

Software providers applying AI and ML across sectors and segments have observed increased scrutiny in recent years from customers on data privacy, with increasing concerns on what data is being accessed and what it's used for. IT leaders are largely taking the stance they will not consent to their organization's information being used to develop and train generic models. **Solution providers in the earlier stages of defining use cases for AI in their product portfolio have a unique advantage here, given they can and should invest in developing capabilities that do not require customer data for model training.** Providers with well-established AI capabilities should consider exploring deployment models that would allow for self-contained instances of their software platforms.

Consumers of cybersecurity software often leverage proof of concept testing, requiring solution providers to prove their attested advantages to demonstrate such qualities as higher efficacy or noise reduction. Vendors with mature, sophisticated platforms should focus on refining post-sales methodologies to reduce friction across onboarding, implementation, customer success, service and support and ensure the trial period is a positive experience. Platforms requiring a more hands-on, resource-intensive implementation should ensure sales personnel and go-to-market materials relay the importance of appropriately tuning models for individual environments and guidance on doing so. Developing an onboarding playbook is strongly advised, with dedicated content for setting up integrations, managing configurations, deploying policies and fine-tuning underlying models.

Qualifying the Investment and Defining Use Cases for Cyber Software

Given the time- and resource-intensive nature of developing AI capabilities, it is imperative the use cases for models being developed are well defined and data inputs are classified by type, size, volume and source. Cyber software providers preparing or in the process of incorporating AI and ML into their portfolio strategy should first consider the following questions:

- Are there more critical business objectives to prioritize that may address customer churn?
- Is the existing software architecture modular enough to develop AI capabilities that will scale in a cost-efficient manner?
- Does my organization have the requisite skills to design, develop, maintain and evolve an AI capability?
- Are the appropriate pipelines in place to facilitate bi-directional data flow? Is data hygiene maintained across the required data sets?

These questions can assist in determining whether the organization is mature enough to start down the path of incorporating AI and if the data lifecycle management posture is commensurate in supporting the investment.

With these questions answered, consider the following when defining use cases:

- What tasks associated with deploying, configuring or maintaining the software platforms are impacting efficiency or satisfaction in the post-sales or onboarding process?
- Are end-users effectively utilizing features and functionality as intended?
- Which value propositions within the portfolio rely on performance or accuracy?
- Do customers routinely perform manual tasks that can be automated?

With the investment qualified, and use cases defined, consider the following when designing your solution architecture:

- What foundational, open-source models can be utilized to address the need?
- How will the deployment model in customer environments need to be adjusted?
- Which external customer systems will the AI capability rely on?
- Can the solution be designed to train models without customer data?

How Can A&M help?

Whether your organization is in the early stages of defining an AI strategy, in the midst of a modernization or re-platforming effort that contemplates incorporating AI, or have deployed AI across your software portfolio, A&M's Technology Industry Group can augment your end-to-end product strategy process to support the identification, definition, development and refinement of AI across the software portfolio.

Featured Experts:

Scott Jones
Managing Director
scott.jones@alvarezandmarsal.com

Ian Ross
Senior Director
iross@alvarezandmarsal.com

Paul Chakraborty
Manager
paul.chakraborty@alvarezandmarsal.com

Follow A&M on:

ABOUT ALVAREZ & MARSAL

Founded in 1983, Alvarez & Marsal is a leading global professional services firm. Renowned for its leadership, action and results, Alvarez & Marsal provides advisory, business performance improvement and turnaround management services, delivering practical solutions to address clients' unique challenges. With a world-wide network of experienced operators, world-class consultants, former regulators and industry authorities, Alvarez & Marsal helps corporates, boards, private equity firms, law firms and government agencies drive transformation, mitigate risk and unlock value at every stage of growth.

To learn more, visit: AlvarezandMarsal.com

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.℠