A&M | TECHNOLOGY INDUSTRY GROUP

A&M'S 2025 CYBERSECURTY MARKET STUDY

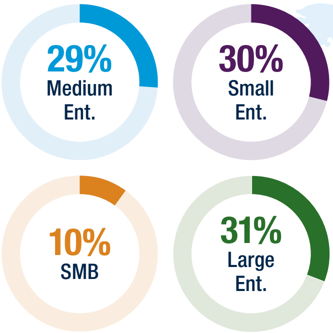
The Ongoing Battle: Balancing Cybersecurity Risks and Budgets

Cybersecurity teams are continuously challenged by emerging threats, including a significant rise in cyberattacks, ransomware, and novel threats leveraging artificial intelligence (AI). The cybersecurity landscape continues to evolve to counter these risks while customers navigate changing needs and seek to balance trade-offs between budgets and security posture.

Based on responses from more than 360 technology and cybersecurity leaders, Alvarez & Marsal's annual Cybersecurity Market Study explores how cybersecurity companies are facing an increasingly competitive marketplace with a key focus on trends involving outsourcing, cloud security, vendor consolidation, and AI. These factors suggest cybersecurity technology providers will need to optimize their product portfolios and realign research and development investments for more targeted use cases.

A&M surveyed **360+ technology and cybersecurity leaders** on their cybersecurity budgeting practices, technology solutions, and cyber related concerns.

Company Segments



Role Representation

98% of respondents are **Executive or Management Level**

All respondents are **decision makers and key influencers in cybersecurity budgeting and solution selection** (Security, IT, Tech, and C-Suite)

Respondents represent companies across **all major industries**

Regional Segments

North America
59%

Europe
26%

APAC
16%

1 Outsourcing

Acceleration of cybersecurity outsourcing

Companies of all sizes are increasingly relying on third-party cybersecurity providers to deliver specialized expertise, scale security frameworks, and provide cost-effective solutions, with 69% outsourcing operations

2 Cloud Security

Increased focus on cloud security

Cloud security has become a strategic priority, with 70% of respondents identifying it as a key concern. This underscores the increasing need to safeguard critical data, ensure regulatory compliance, and maintain business continuity

3 Consolidation

Continued vendor consolidation trends

The majority of firms plan to consolidate vendors over the next two years, with 1 in 5 planning significant consolidation. This points to a more competitive future landscape, where fewer vendors will command a larger market share

4 AI Adoption

Use-case a key driver of AI adoption

While 52% of respondents indicated they are not using AI tools in their cybersecurity tool set, adoption varied greatly across industry, offering type, and geography, suggesting focused use-cases are critical for adoption

1. Acceleration of Cybersecurity Outsourcing

The trend of cybersecurity outsourcing continues with increasing adoption and related expenditures. Companies of all sizes are relying on third-party cybersecurity providers to deliver specialized expertise, scale security frameworks, and provide cost-effective solutions. Compared to last year's 61%, 69% of this year's respondents replied that they were outsourcing operations, with 66% reporting a year-over-year increase in their outsourcing budget. Cloud security has been the most outsourced service according to our survey, reflecting the critical need to protect cloud environments as businesses migrate to the cloud.

Managed Security Service Providers (MSSPs) remain the primary outsourcing provider, with more than three quarters of respondents using MSSPs or similar providers. While nearly 90% of companies in the Asia-Pacific (APAC) region utilize MSSPs—the greatest amount of any region—only about 63% of European companies do so. This is partly due to the rapid development of regulatory frameworks, including data sovereignty laws, which are driving organizations to adopt MSSPs that provide expertise and ensure compliance with evolving laws. In contrast, European companies prefer in-house solutions due to concerns over data privacy and control, influenced by stringent regulations like GDPR.

MSSPs and other providers are not just vendors. They can be strategic partners who fortify and enhance a firm's overarching security strategy, providing specialized skills and tools, scalable solutions, and 24/7 threat monitoring and response. Outsourcing reduces the burden on internal teams while allowing companies to quickly scale and fortify their cybersecurity frameworks, making it attractive for businesses of all sizes. As businesses continue to adopt cloud-based environments, protecting them against threats becomes a top priority. While MSSPs have traditionally focused on security operations center (SOC) and security information and event management (SIEM) offerings, cloud security has now become a top service provided by MSSPs according to our survey, driven by growing demand to fortify cloud environments as cloud-based platforms become the standard.

> As cloud adoption grows, cloud security has become a strategic priority and is one of the primary drivers of incremental cybersecurity spend. In fact, 70% of respondents identified it as a key concern.
>
> **A&M 2025 Cybersecurity Market Survey**

This growing emphasis on cloud and network security signals a broader shift toward proactive, cloud-driven strategies within both outsourced MSSPs and internal cybersecurity functions. Additionally, the consistent increase in outsourcing budgets suggests that reliance on third-party providers will continue to grow. There are considerations that cyber technology providers and MSSP businesses can take to enhance their response to increased outsourcing:

Grow the MSSP Channel:
The continuation of outsourcing is increasing the need for MSSP channels for cyber technology providers to bring solutions to market that are best of breed and integrated with other key solutions in the ecosystem. Alternatively, cybersecurity providers can look to become the platform of choice by offering comprehensive solutions that consolidate and simplify cybersecurity management for their MSSP partners.

MSSP Growth:
MSSPs should consider strategically expanding their coverage in critical outsourced areas while maintaining their operational efficiency to protect and improve margins. Adopting solutions from providers that are highly integrated or that provide platform covering requirements across the MSSP offerings, including cloud, can streamline operations and enhance service delivery.

2. Increased Focus on Cloud Security

Cybersecurity remains a high priority for virtually all companies, with nearly all firms reporting that they increased or maintained related expenditures. As cloud adoption grows and bad actors target the cloud environment, cloud security has become a strategic priority and is one of the primary drivers of incremental cybersecurity spend. Companies are shifting toward proactive, automated, and data-driven cloud security measures, with investments in cloud security becoming critical for maintaining business continuity in the face of growing cyber threats.

Respondents indicated that cloud security budgets were increasing or remaining the same in 99% of cases, with over 53% reporting a year-over-year increase in cloud security spending, reflecting its current and growing importance. This underscores the increasing need to safeguard critical data, ensure regulatory compliance, and maintain business continuity.

In fact, 70% of respondents identified cloud security as a key concern when it comes to MSSP offerings, budgetary increases, and emerging threats. Only data loss prevention was a higher reported concern at 71%. Cloud security is the most demanded service from MSSPs, being utilized in 93% of respondents, which underscores its critical role in modern cybersecurity strategies and MSSP product mix.

Threat intelligence and hunting, security information and event management (SIEM), and security orchestration, automation, and response (SOAR) were also areas where the majority of respondents indicated increasing spend. This reflects a strategic shift toward proactive, data-driven, and automated security measures.

Bad actors know valuable data exist within the cloud ecosystem, and leadership must continue to stay ahead of these evolving threats by investing in proper safeguards. As cloud adoption grows, cloud security will remain a primary driver of cybersecurity and related research and development (R&D) spend. Ease of integration is a key purchasing criterion, reflecting the need for seamless deployment of cloud security solutions. There are other considerations technology solution providers need to evaluate as well:

Adapt to Threats

Adapting solutions and services to increase cloud security capabilities is critical as the sophistication of threats in this arena continues to grow. Providers must ensure their solutions are proactive, scalable, and capable of addressing the challenges presented by cloud-based threats.

Develop an MSSP Strategy

As cloud adoption accelerates, technology providers should focus on enabling MSSPs to expand their coverage and expertise in cloud security. Offering tailored solutions that align with MSSPs' needs can help providers capture the growing demand for outsourced cybersecurity services.

Integration and Usability

Cloud security solutions should seamlessly integrate with existing cloud environments, applications, and workflows to enable rapid deployment, minimal disruption, and ease of use. Providers that deliver user-friendly, cloud-native solutions designed to work across multi-cloud and hybrid environments can differentiate themselves and strengthen their value proposition.

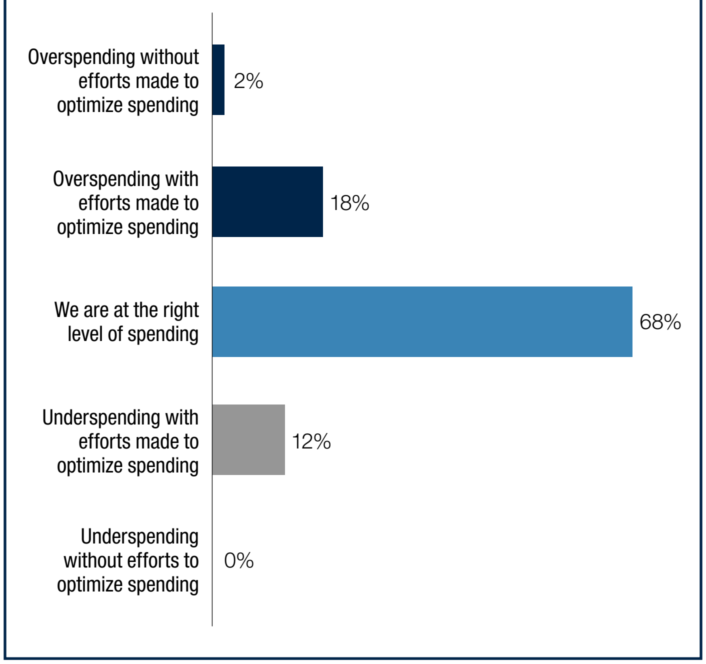
3. Continued Vendor Consolidation Trends

Cybersecurity expenditures and budgets are set to increase in response to the ever-changing threat landscape. Overall sentiment, though, suggests future spend may taper off[1] as firms move toward fewer trusted partners to manage cybersecurity. 19% of respondents are planning major consolidation efforts, signaling a material shift toward fewer, more trusted vendors as a strategic priority.

Last year, 86% of respondents reported they were overspending or at the right level for cybersecurity, which increased to 88% this year. This suggests a persistent and increasing trend, with overall sentiment remaining largely consistent across all revenue buckets and company sizes.

In terms of absolute spend, 53% of all respondents indicated their cybersecurity budget has increased from the prior year—suggesting overspending or comfort in current spend sentiment has not translated to a material reduction in total expenditures. This is further supported by the fact that only 3% of those surveyed reported a decrease in their overall cybersecurity budgets compared to the prior year.

View of Company's Spending for Cybersecurity



However, there has been a shift in focus from the initial approach to cybersecurity, where companies were allocating significant capital to cybersecurity. Now, many firms may feel they are well protected and have moved to focus on cost reduction and optimization to meet more defined needs with a smaller group of trusted partners. As the ever-evolving cyber risk landscape necessitates additional investment in cybersecurity measures, 57% of firms plan to consolidate vendors over the next two years, with one in five respondents planning significant consolidation.

The technology, media, and telecommunications (TMT) industries are leading consolidation efforts, with 66% of technology and 84% of telecommunications and media firms planning vendor consolidation over the next two years—the highest of all industries surveyed. A key driver of this trend is the critical importance of data in these sectors. Consolidating vendors enables TMT companies to streamline and synchronize data across platforms, reducing operational complexity while enhancing control and oversight.

Indications are that while cybersecurity spend trends upwards on paper, the market will become increasingly competitive as vendors compete to be included in an increasingly smaller group of trusted security partners.

According to this year's survey, price was the second most important purchasing criterion, up five times in importance from last year. This rise in emphasis reflects a heightened cost awareness among decision makers. This shift is, in part, driven by a proliferation of vendors offering similar solutions, which has intensified competition for market share and empowered buyers to prioritize both affordability and value.

[1] This is as a percentage of IT budgets, which may be increasing based on percentage of revenue.

These findings point to a more competitive future landscape, where fewer vendors will command a larger market share. Preference is commonly given to existing vendor relationships. Consequently, by emphasizing trust and reliability, cyber technology providers can differentiate themselves from the competition. Further, providers can enhance their positioning by:

Differentiating Solutions

To maintain or grow market share, solution providers need to focus on being a provider of choice while also being able to integrate within existing ecosystems. Ease of integration is a growing concern, with 26% of respondents prioritizing it in their purchasing decisions. Additionally, forming strategic partnerships with other vendors and MSSPs can further enhance value by expanding capabilities, improving interoperability, and addressing the growing demand for comprehensive solutions.

Continuous Optimization for Competitive Advantage

To maintain competitive positioning, firms should regularly evaluate their processes, resources, and technologies utilized to identify inefficiencies, eliminate redundancies, and address potential gaps in coverage. This approach addresses industry expectations and helps mitigate overarching vulnerabilities thereby enhancing resiliency.

Assessing Pricing

Since last year’s survey, price has risen significantly as a key purchasing criterion, suggesting that providers should consider commercial due diligence activities to assess how their products and pricing compare to industry competitors.

4. Use-Case a Key Driver of AI Adoption

Service providers are facing pressure to differentiate their offerings and are utilizing new features, including AI, to do so. However, respondents also noted AI presents new challenges for which they have no current solution.

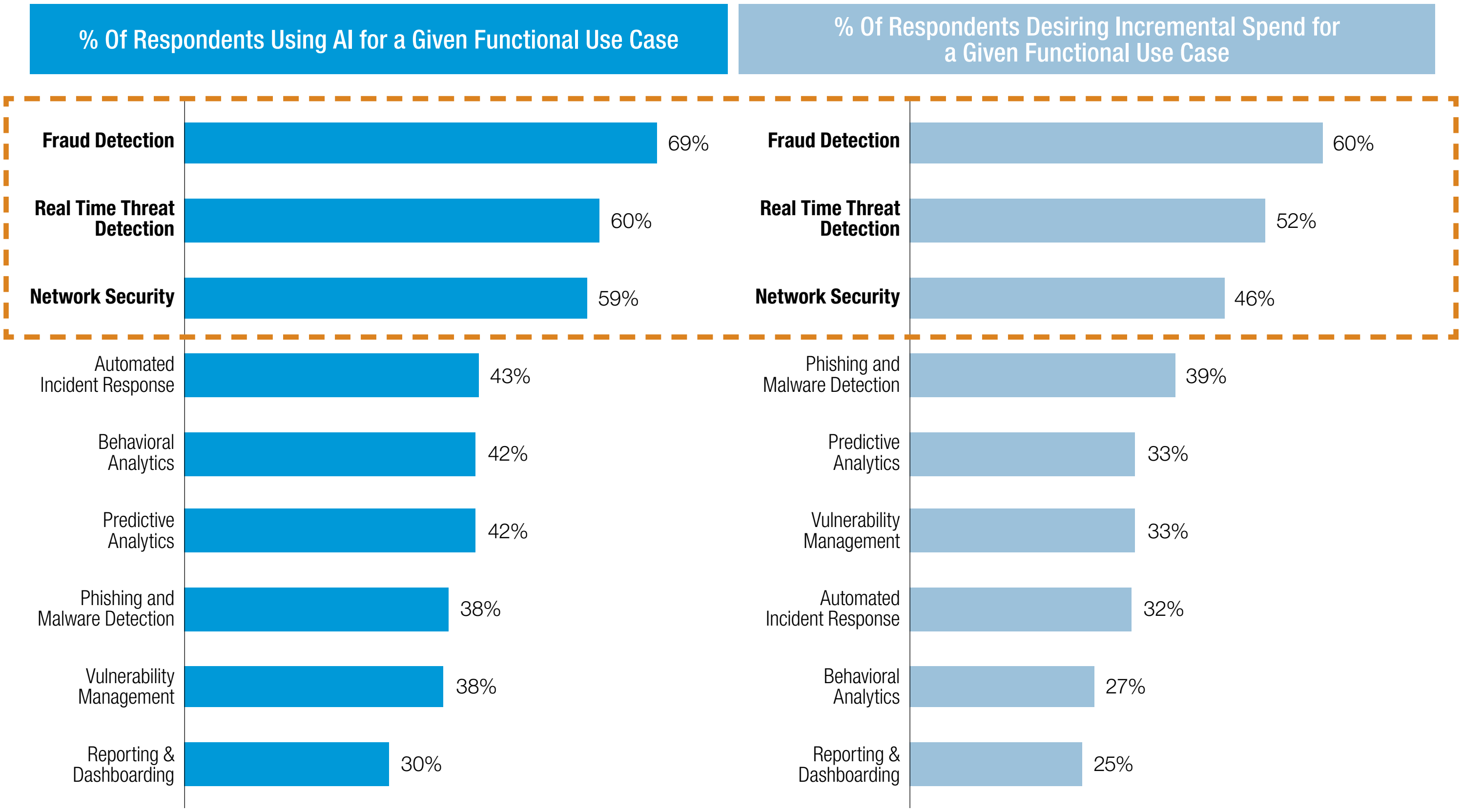
AI adoption has been slower than anticipated amid leadership concerns over reliability, privacy, and implementation complexity. However, companies currently utilizing AI are largely—if not universally—expected to maintain or increase their usage based on survey findings.

While 52% of respondents indicated they are not using AI tools in their cybersecurity tool set, adoption varied greatly across industry, offering type, and geography, suggesting focused use cases are critical for adoption. The highest AI cybersecurity use was reported in the technology and IT, manufacturing, and financial services and insurance industries. Large enterprises, those with more than 5,000 staff, were the only group where over half of respondents are currently using AI for cybersecurity. AI adoption varies significantly not only across company sizes but also across industries and regions, suggesting the need for tailored solutions to address specific challenges in regulatory compliance and threat types.

Only 48% of companies are using AI in cybersecurity despite 79% having no reservations around using AI for this purpose, with respondents indicating integration challenges and reliability issues are some of the key barriers to adoption. The survey also found current AI offerings fall short of expectations, with usage largely outpacing demand for incremental investment across the categories surveyed. This suggests that early AI adoption has not resulted in satisfactory results where users would demand additional investment in these new solutions.

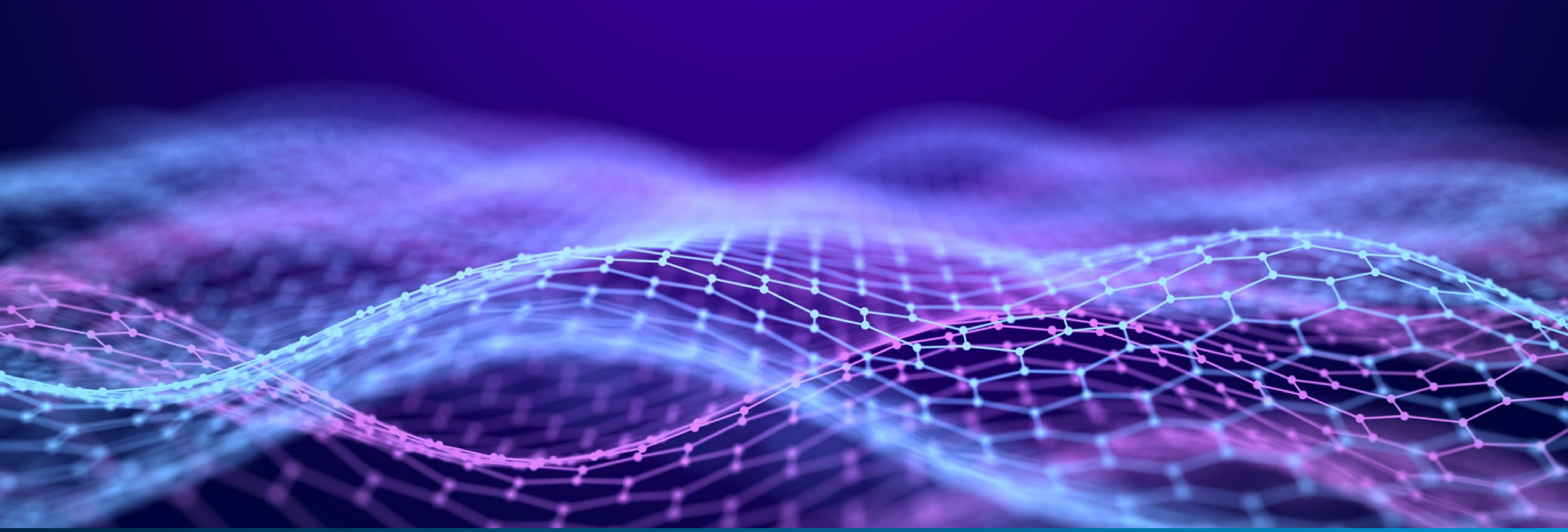
When comparing specific functional use cases, significant variance was observed, with clear leaders emerging. Fraud Detection, Real-Time Detection, and Network Security stood out, maintaining a substantial lead over other functional use cases in both current usage and desired incremental spending by survey respondents, indicating that while the market demonstrates strong confidence in AI's ability to detect cybersecurity anomalies, it remains hesitant to trust AI for response actions.

AI for Cybersecurity Usage against Desired Incremental Spend



% Of Respondents Using AI for a Given Functional Use Case

% Of Respondents Desiring Incremental Spend for a Given Functional Use Case



> For those who are leveraging AI in their tool set, 65% reported an increase in year-over-year usage—with none of them reporting a decrease in use. Additionally, 56% of respondents reportedly want to see more AI functionality in their cybersecurity framework. However, 65% of respondents did not want to see more investment in AI.

This suggests that users want to see more functionality from what they are already using and are not satisfied with current offerings. The cybersecurity industry faces a constant battle to stay ahead of threats, especially as AI provides new tools—and new challenges. As the landscape continues to evolve, providers will need to be able to do more with the tools already at their disposal.

Increased AI usage is an inevitability, but these solutions need to become more reliable with easier integration into existing systems before broader adoption can take place. Providers will need to:

Address Existing Challenges

AI solutions need to provide value and address the challenges that companies are actively facing. This can be achieved through the lens of targeted use cases that shape the often amorphous AI tools into a more targeted solution that has a defined and tangible benefit to the end user.

Build Safeguards

As surveyed leadership showed considerable fear over AI “hallucinations” and other reliability concerns, providers of AI cybersecurity solutions should focus on implementations that protect customer data and provide safeguards to control and manage responses. Customer privacy is critical, and exposure of private data to an unsecured or vulnerable AI solution, or one that could inadvertently leak data, is a fear that could result in a material negative impact. A lack of trust in AI solutions and their ability to function autonomously is currently weakening adoption, and introducing tangible safeguards could ease the concerns of interested parties.

Drive Adoption

Research indicates that AI adoption increases when there is a significant pain point, sufficient data exists to train the model, and risk is mitigated to reduce the likelihood of a high-cost failure that could result in reputational or legal issues. Providers should work to identify common pain points, find solutions to address data gaps, and prioritize critical safeguards. Additionally, company policies hinder adoption due to conflicts with security posture, suggesting that solutions should address these common barriers to be considered for implementation.

How to Succeed in the Evolving Cybersecurity Market

Cyber threats continue to rise, and the cybersecurity market has grown to combat these risks with expanded offerings. Now, tens of thousands of companies, including many small players, offer some form of cybersecurity technology services. Cybersecurity budgets, however, are facing increasing scrutiny as businesses place sharper focus on optimizing spend, which has led to the consolidation of their vendors and platforms.

To remain competitive in the market, cybersecurity providers must navigate the needs of their clients and differentiate themselves through their pricing, AI offerings, and cloud services, keeping in mind the following:

Position Services Competitively

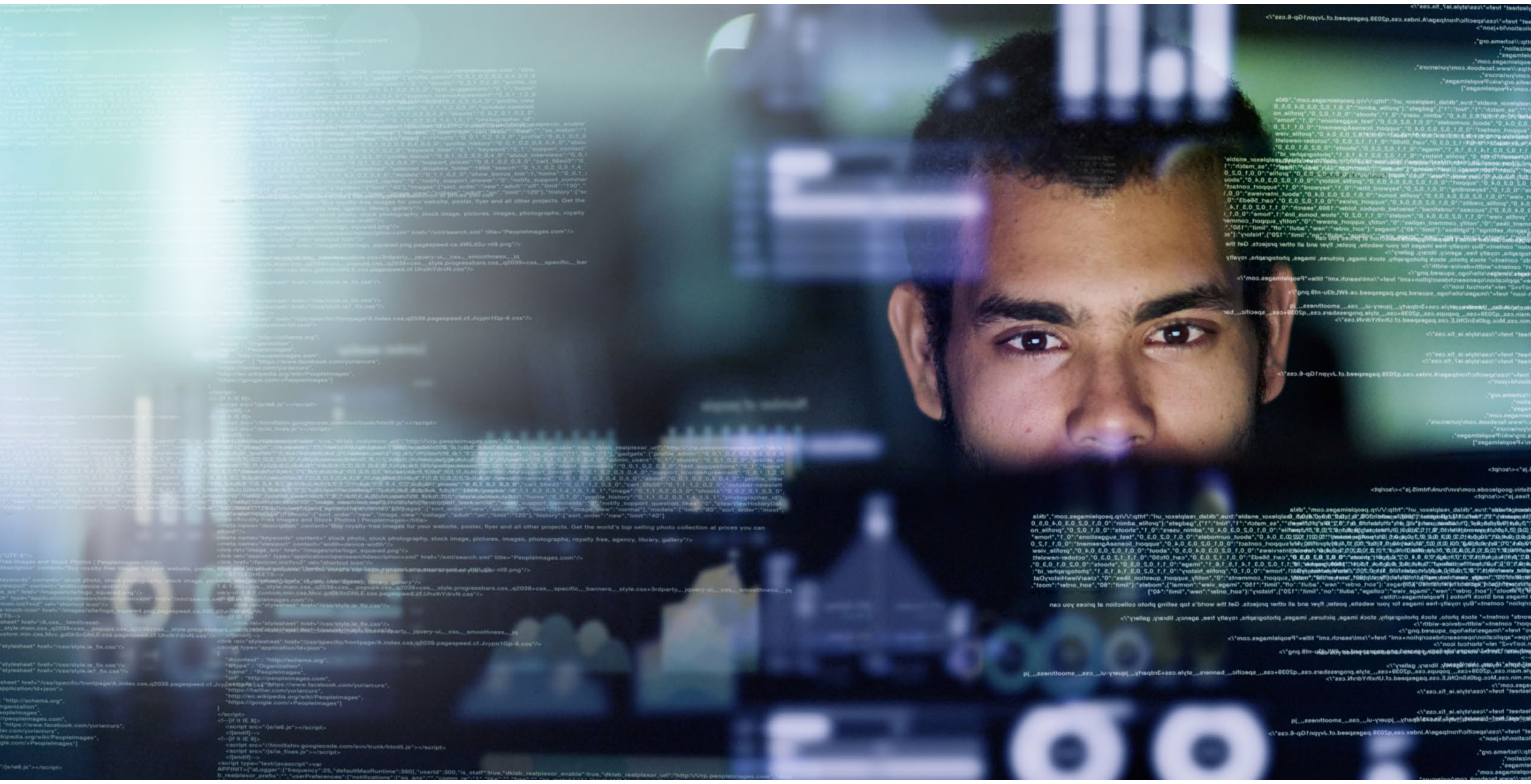
The continuation of outsourcing is increasing the need for MSSPs and other providers to provide best-of-breed solutions that are easily integrated with other key solutions in the ecosystem.

Provide Cost and Scalability Benefits

Outsourcing provides a scalable and cost-effective solution for accessing advanced tools and resources that can be utilized by companies of all sizes.

Drive AI Adoption

Trust is a key factor in driving AI adoption. Mitigating risks like “hallucinations,” highlighting proven success cases, and implementing robust safeguards can enhance confidence and accelerate usage. Further, addressing key pain points with targeted use cases can help remove the uncertainty businesses face with AI implementation and promote adoption through a more tailored approach.



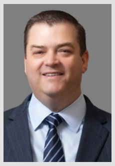
How A&M Can Help

As cybersecurity revenue growth rates slow, R&D investments are squeezed, consolidation opportunities present themselves, and AI evolves, cybersecurity companies have opportunities—and challenges—they must address to succeed in the market.

Alvarez & Marsal's Technology Industry Group within the Private Equity Performance Improvement practice has hands-on experience in the cybersecurity sector with a deep understanding of evolving industry trends. Our experience includes expertise in commercial due diligence efforts, operational improvements, product strategy, platform consolidation, go-to-market approach, buy- and sell-side M&A support, and real-world leadership in navigating major transformational challenges.

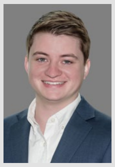
CONTACTS:

Scott Jones
Managing Director
scott.jones@alvarezandmarsal.com



Ian Ross
Senior Director
iross@alvarezandmarsal.com

Michael Slusser
Manager
mslusser@alvarezandmarsal.com



Will Sheehan
Senior Associate
wsheehan@alvarezandmarsal.com

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 worldwide 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

Follow A&M on: