VISASQ / COLEMAN

CNAPP, AI-driven Security & Automation, and Disinformation Security

Our Expert :
Gary Meshell

Executive Partner – CyberEdge Advisory

About Our Expert:

- Executive Partner – CyberEdge Advisory (January 2025 – present)
- Vice President, Global Alliances – Palo Alto Networks (July 2024 – January 2025)
- Global Leader, Cybersecurity Alliances – AWS (July 2021 – May 2024)

Gary Meshell has over 15 years of experience in the cybersecurity industry, holding senior roles at leading organizations such as Palo Alto Networks, AWS, and IBM. Over the course of his career, he has led global go-to-market efforts and built strategic alliances across system integrators and security-focused technology partners. He currently advises clients on AI security strategy and M&A, while also helping technology providers develop global partner programs that align with market demands and drive competitive advantage.

Moderator:
Max Le Sieur

Founder & Managing Partner at Rosemont Legacy

- MBA, Harvard Business School - 2022
- Investment Banking Associate at BMO Capital Markets (07/2016 – 08/2020)

Expert Insights On:

- Cybersecurity market overview and size
- Key elements of cloud-native security
- Use cases for AI-driven security and automation
- Disinformation security landscape and outlook
- Most pressing cybersecurity threats in 2025
- How the threat landscape has evolved
- Unique security requirements of cloud-native environments
- CNAPP risks and gaps
- The rise of cybersecurity platformization
- Key players across CNAPP, AI-driven security and disinformation security
- M&A and market consolidation in cybersecurity
- Cybersecurity investment risks

Max: Okay, great. So, hi Gary. My name is Max, and I'll be leading this call on behalf of VISASQ/COLEMAN Research today. As you know, the purpose of this discussion is to learn about the cybersecurity market, including key players and trends in the industry. Before we begin, I would like to remind you that we are in no way soliciting any material non-public information, or any information that is confidential and related to any company or organization that you are currently or have ever been affiliated with. If ever you feel as though the answer to any question involves non-public information, please tell me right away and I'll simply take us in a different direction. Any questions for me before we begin?

Gary: I am ready to go. Thank you.

Max: Awesome. Just to kick things off here, can you please provide just a short overview of your background and experience as it relates to the cybersecurity market?

Gary: Sure. I've held executive leadership positions in cyber for the last 15 years. I was general manager of IBM software security business for 2016 to 2020. I subsequently went on to AWS, spent four years at AWS, where I was responsible for security go-to market, as well as our security ecosystem partners. While I was there I established a joint venture with 15 cybersecurity companies to build a series of next-gen AI software products and security. Spent a year on a special project with Palo Alto working for the CEO and the board, advising them on M&A and their AI security strategy. And for the last eight months I have been working with a number of private equity firms and venture capital firms, advising them on investments in the cybersecurity space.

Max: Awesome, thank you very much. Gary, I'm going to move us through these four broad agenda topics today. The first of which is an overview and an outlook of the market. And so, that's where I'd like to start. How big is the cybersecurity market today, and how would you define cybersecurity broadly?

Gary: There's a lot to unpack there. I think if you look at all things cyber and you pack them all together, we're somewhere around 110 to 120 billion in total addressable market. My outlook for the next five years is we're probably going to grow incrementally somewhere between 18 to 20% CAGR per year, and we're probably looking at a total addressable market by 2026. I'd say somewhere around one to $1.2 trillion. Cybersecurity definition, boy, that opens a big can of worms, doesn't it? I think if you look at cybersecurity definition today and the way most people think about cybersecurity, I think they view it as more of a "detection and prevention," and I give it sort of a definition of it's a practice, it protects systems, it protects networks, it protects applications, and it protects data. And if I unpack that a little bit, I think the objective of cyber is first and foremost confidentiality, integrity and availability. Where it gets really interesting is defining the overall scope. Typically, when I talk to folks around what cybersecurity today includes, it includes network, end point, cloud security, identity and access management, application security, data protection, and then security operations. That's sort of the way I see it today.

Max: Awesome. That's helpful. There are three sub themes that I'd like to focus today's discussion on. The first is cloud-native security, so CNAPP, AI-driven security and automation, and then disinformation security. Do you mind just briefly explaining what each of those three sub themes means?

Gary: Sure. Let's start with cloud security. If I give you a definition of cloud security, it really comes down to cloud-native security practices, their tools, their architecture. And I think to think about it, it really starts with protecting cloud-native environments. And if you think about cloud-native environments, it's things like containers, it's Kubernetes, it's microservices. And I think it's also important to think about, it's just not securing things in the cloud. A lot of people have a misnomer that it's securing things in the cloud. It's more about embedding security into the overall ecosystem of things that are cloud-native applications. And we're talking from development through runtime, so I think that's really, really important.

Then if you talk about the key characteristics of cloud-native security, I think there's a number of things we should think about and unpack. One is visibility and posture management. What you do there, you want to identify things like misconfigurations, policy violations, and then you've got another pillar, which is identity and access control. There what you want to do is you want to focus on monitoring and servicing your accounts. You want to provide permissioning in the cloud. Then you've got CWPP or Cloud Workload Protection. That's more about detecting and responding the threats in containers, Kubernetes. There's a shift left that's also happening within the cloud towards DevOps, and this is important, especially as you see more and more cloud-native applications being built. You want to be able to detect security breaches and issues, not only at runtime, but when you're building them. And then I think you have to think about that traditional security can't handle the more cloud-native workloads, and that's why CNAPP is really essential when you start thinking about security innovation that happens at the speed of DevOps.

Max: Got it. Super helpful. What about this sub-theme of AI-driven security automation tools?

Gary: Man, we could spend 100 hours talking about that. First of all, it's new, it's morphous, it's emerging, and it opens so many different avenues of thinking, different avenues of what it means. I think there's two key definitions that's worth talking about. One, there's a definition where you're using AI and machine learning to detect, prevent, investigate, respond to cyber threats more effectively, greater scale than traditional systems. There's a second optic that gets lost in translation, and it pains me, which is you need to focus on securing AI itself, the large language models, the inference models, the government, the governance. There's sort of a big black hole right now of folks who are not spending enough time thinking about securing AI itself.

But if you want to stick to the theme of AI-driven security, it focuses on, I think a number of key things. One, it's all about real time. Second, and I think an emerging unbelievable opportunity is you're not only going after emerging threats, but you're going after unknown threats. And those threats could be repetitive. It gets heavily used in cloud-heavy in high-volumes environments, and I think there's five use cases that are beginning to emerge. You've got threat detection where you're using AI to detect anomalies, behavior-based attacks. You've got triage and prioritization, and this is important, because when there's a breach, you've got to think about what alerts you want to be chasing and what alerts you don't want to be chasing. I think you're getting a lot of good automatic scoring based on context and risk that come from AI. You've got automated response, you're remediating low-list threats without human intervention, and that's key given the labor shortage and the skill shortage that we have.

There's a huge emerging area of threat intelligence. We're looking at massive volumes of threat data. And you're thinking about how to generate insights, how do you generate analytics? And then there's the AI model itself, which I think is the black hole where I actually for me feel there's the most risk. You got to think about how you're going to look at the model itself. Is someone hallucinating your model, or is someone injecting prompts into your model? I got to tell you, that is probably the biggest risk. And I think if you look at AI systems, what they're really doing is they're looking at supervised learning. They're training on a known threat, whether it's malware, whether it's phishing. Then there's unsupervised learning, what you're there, you're detecting an anomaly without labeling the data. There's new attack patterns emerging and you're trying to figure out what it means.

There's a lot of natural language processing that goes on in things like AI copilots, incident summarization, but it's not without challenges and risks. There's way, way, way too many false positives right now. So, poorly tuned models can misclassify something that's benign, or it could miss malicious activity. There's a operational risk that a lot of the security teams that I talked to, they don't trust it. They view it to some degree as black box, and they're fearful of a black box.

There's potentially a over-reliance on automation. Automation can lead to a missed signal. It could lead to a unsafe remediation. And then I think another thing that we're going to have to get our hands wrapped around is data quality. Keep in mind that AI is only as good as the telemetry and the labels it's using. If I try and bring this back, I think AI does matter now. I think the scale and the speed exceed human behavior, they exceed human detection capabilities. It fills the talent gap, for sure. I don't think it's a buzzword anymore. I think it's becoming somewhat foundational, but it's important to call out that the real value is combining that AI with transparency, with context, and the ability to be automated ready. And you just can't layer models on top of legacy tools, if that makes sense to you?

Max: Yeah, yeah. Okay, that's super helpful. I do want to move us on, because it does sound like there's a lot to unpack there, but just the third sub theme is disinformation detection. Can you talk a little bit about that? What is that?

Gary: Here's what it is, and it's new, it's confusing, and it's complex. It's all about intentional, false, misleading content. It tends to get very much amplified through digital platforms, and it's meant to cause harm. That harm could be political, it could be reputational, it could be economic. Deepfake is a huge example of this. Fake press releases, phishing mails, compromised websites. There's some scary use cases in financial services, fake news to influence prices. I'm seeing a scary amount of things happening in healthcare around vaccine misinformation. You don't need to be in a bunker to know that we've had major incidents of election interference in the government.
Corporate is really concerning. You're seeing brand sabotage. You're seeing fake CEO statements around deepfakes. And critical infrastructure is probably the scariest part of this, because you're going to start eroding trust in the grids, hospitals, supply chains. The tactics that you see, everywhere fake personas or avatars. Spend a day on Twitter or LinkedIn, you've got synthetic content, deepfakes, manipulated audio. You've got false attribution. You blame attacks on third parties. One of the things that's scary about all this on the dark web is you've got fabricated documents being created in hacker forums, that's really disconcerting. And there's some implications when it comes to cyber. I think it blurs the line between cybercrime and information warfare. It mimics some phishing and social engineering tactics. If you look at it from a detection point of view, you've got threat intelligence platforms starting to work in this space. You've got social media monitoring tools, you've got AI emerging as content verification. There's a lot of policy stuff that's going on. The EU has created the Digital Services Act on disinformation. In the U.S. we have `, C-I-S-A, and they're working on private coordination for misinformation. At the end of the day, I think there's three things we can take away from this. It's a cyber problem, it's not a PR problem. It blurs the boundaries between information security and psychological torture. You need cross-functional defenses, right? It's cyber, it's comms, it's threat intel, it's legal. And it really raises the bar around enterprise risk for things like elections, geopolitical stuff, or major world crises.

Max: Got it. Okay, that's super helpful. I do want to move us on, but just maybe very briefly, which one of these three sub-themes represents the largest TAM, and which one the smallest TAM in your opinion?

Gary: CNAPP is by the largest TAM, and it's a TAM that's addressable now. I think AI is an emerging TAM. It's not ready for prime time. It's going to have hyper growth really from 26 through 28. I think disinformation, it's a blurry line of how this is all going to come together and where the investable dollars are going to be sent. So I think for now it's the smallest segment and it's probably a subsegment of the overall cyber market.

Max: Got it. That's super helpful. And do you see these three trends convert? I've described them so far as distinct sub themes, but would you agree with that characterization? Are they really independent markets or do you see them kind of converging?

Gary: So, there is an absolute convergence, it's happening as we speak. I think convergence and AI and cyber are going to start coming together. I think you're going to see tools that begin to become part of cybersecurity platforms that address these on a more integrated manner. I think AI is going to be a force multiplier, and I think any CNAPP and any detect and response system, AI will be deeply embedded. I don't think frankly, the disinformation defense is going to remain an absolute category. I think it's going to be blended and folded into cybersecurity.

Max: Got it. Super helpful. Okay, I want to move us on to today's cybersecurity risks. We're in 2025, what in your opinion, are the most pressing cybersecurity threats?

Gary: Could you repeat that? I heard the second part, it was just a little bit of static.

Max: Sure. Just the most pressing cybersecurity threats in your opinion in 2025.

Gary: I think it's a mix. I think there's technical attacks. I think there's AI-driven deception, and if I began to break it down, I would start with AI-powered attacks, deepfakes, synthetic voice fraud, AI-generated phishing, clearly top of the food chain. There's this concept that's evolving called ransomware as a service, which is really scary. It involves double triple extortion where you're doing encryption, data theft, denial of service. They're targeting backup infrastructure and cloud-native environments, which really disconcerting. You've got more and more attacks moving towards the supply chain. Things like SolarWind, 3CX where you're seeing disruption at the CI/CD pipeline. You're getting malicious code put in open source libraries. Identity and access continues to be a disconcerting concern around compromised credentials. If you look at the number one cause of breaches, I would say that abused privilege access is still the number one cause. Then you get into cloud and SaaS misconfigurations, there's a lot of problems with multi-cloud gaps. There's a lot of problems with multi-cloud identity access management, misconfigured clusters are all causing concerns. Then you've got a big emerging area around OT security, energy, manufacturing, health care.

Max: What's OT, Gary? What's OT, Gary, when you say OT.

Gary: Operational technology.

Max: Got it.

Gary: Things like power, the grid water, you've got massive amounts of attacks around OT devices in the medical industry. Every day I'm getting a call around ransomware targeting hospital equipment, and then I have in what I call a honorable mention category. You've got a real growing concern around insider threat. I think remote work has kind of opened us up. You've got the concept of zero-day vulnerabilities, which is like you don't even have time to respond, because somebody's turning off the air traffic control system. They're turning off a nuclear power. And then AI model poisoning. It's early, but man alive. It's really concerning when you think about all the models. The fact that you and I can download deepseek, ChatGPT, start building my own inference models. Poisoning those models is going to be a real important thing we got to start thinking about.

Max: Super helpful. It sounds like most of what you just described will have microservices or CNAPP-type services to address them. Is that fair? Is it fair to characterize CNAPP as being there today and a collection of tools and companies that are driven to address the challenges you described?

Gary: Rephrase the question on the microservices. I got the CNAPP. Maybe you could just quickly rephrase and I can-

Max: Well, let's just stick to CNAPP. Is it fair to think about CNAPP as a collection of companies and tools to address the problems you just described?

Gary: Yes and no. I think the more and more that CNAPP can become a unified security framework, we can get there. I think the problem with CNAPP today, there's lots of different components that don't necessarily all come together. You've got cloud security, posture management, you've got cloud workload protection, you've got entitlement management, you've got container scanning. All that stuff to some degree hasn't yet all come together. But what it's doing, it's causing a clear need from enterprises that want to consolidate all their various tools. And platformization is one of the keyest investable areas in the market. You've got a public cloud-native stack that's growing and growing and they're going to need full stack visibility. And I think the way to think about it's SIM plus EDR plus SIM, cloud native apps, but built for purpose. And there's a lot of emerging companies, right? Look what's happened with Wiz, my old employer, Palo Orica. Everyone is going there, but there's some fine blurry lines, like there's lots of overlaps with XDR and microservices I think is going to become the architecture for all this, especially for things like Kubernetes.

Max: Got it. That's super helpful. I want to double click on some of what you just said, but a little bit later in the conversation. Just can you describe how the threat landscape has evolved in recent years, kind of the last one to three, and what are driving those evolution trends?

Gary: Now, just for me, so I answer your question, how's that different than what I gave you in terms of the sort of emerging top threats? Can you just delineate for me the difference between that first question?

Max: Is it because the technology has continued to improve? Is it because what are the trends driving the reason why the attack services are what they are today? You mentioned work from home, that's an interesting one. So people can't get authenticated going into the office, everything being cloud or the technology changing with AI. What are some of the key things that are happening that are the reason why?

Gary: Okay, thank you for clarifying that for me. I think there's a number of things. I'm going to break this into some timelines for you. One is there's a shift from what I call opportunistic attacks to targeted attacks. If you look at, I'd say up to 2023, these things were widespread. And I'm going to use some of my own taxonomy here, so if it doesn't make sense, I'll explain it. You had the concept of spray and pray ransomware. You just throw enough things out there and hope that some of them caused damage. Malware was not yet widely being used from a distribution point of view. And I think now what you've got is highly targeted intrusions. You've got deep fakes everywhere. Ransomware is becoming precision or against critical infrastructure, supply chain attacks and zero day exploitation of very clear victims is being more and more concerning. And I think attacks are customized. They'll look at your stack to look at your geography.

The good and the bad news about cloud and SAS is they're becoming the top attack surface. You've got lots of misconfigurations, you've got lots of identity abuse. One of things we got to get under control. There's way too many IAM products out there. It's like sprawl city. You've got attacks coming against SAS. A lot of companies haven't figured out third-party integrations and this lateral movement around shared service. Clearly we've talked about the rise of AI in both offense and defense.

I think what's also changed now is identity is the new perimeter. 80% of breaches are going to involve credential compromises. There's lots of identity fatigue. There's token theft. Sessions are being hijacked. Another thing that's changed is that ransomware is really moved from file encryption to data theft and extortion. I've witnessed in work that I'm doing over $20 million in the last two months in payments around ransomware. And you've got this sort of triple extortion threat where what you're doing now, you're focusing on your backup. And that's a key point. We used to go attack the production system. They're getting smarter and smarter being able to go after the backup. Cloud is becoming more and more of the target for ransomware. And then I think the last one, and in the category of Dr. Obvious is the geopolitical and nation-state activity rising.

Max: Super helpful. Thank you for that. You mentioned something earlier around CNAPP that I want to double click on. What are legacy tools, and what are the specific risks that cloud-native environments introduce that cannot be covered by legacy tools?

Gary: From a definitional point of view, are you talking about existing tools that are out there and what are the risks and what can't they cover as opposed to modern CNAPP?

Max: I think so. I think so. I'll rephrase it in case it's helpful. What are specific risks that cloud-native environments introduce, and why can't they be covered by legacy tools? Why does there have to be this new set of tools?

Gary: Okay, thank you for clarifying that. So, CNAPP, obvious position end-to-end, it's meant to secure cloud-native environments. And there are a lot of legacy tools that it tries to replace, and there's gaps and risks that it can't necessarily cover today. Do you want me to go into some of those?

Max: Sure.

Gary: Okay. Here's some of the risks and gaps that CNAPP can't cover. There's limitations, they're cloud native, so no support for on-prem, no support for legacy VMs, very limited around securing legacy application. Where CNAPP may detect a posture risk or a gap, it's not really good at anomaly detection. And I think one of the key talking points is that CNAPP needs to be integrated as part of your MDR, XDR service. There's limitations around, I mean, they're good at IAS, they're good at containers, but limited visibility into SaaS tools like Salesforce, Slack, they're really weak around API abuse detection. And I think it's important when you think about SaaS especially that you got to have complementary tools. You got to have CASB, you've got to have SaaS Security Posture Management.

I think there's a huge gap you could drive a truck through around CNAPP when it comes to insider threats and disinformation. There's very little visibility into insider behavior. There's little understanding of credential misuse. If you've got an external social engineering campaign, not going to do much there. I think there's a clear need to create identity analytics and user behavior monitoring that's not taking place. And then the last one would be protecting the dev environment. I think if you think of a mental model, CNAPPs tend to be run time forward and a lot of the breaches and a lot of the ransomware and malware is being hit in the DevOps space.

Max: Super interesting. Thank you for clarifying that. The last question here on this agenda item, you mentioned platformization. Can you elaborate on what you mean by that and why it's important?

Gary: Sure. There's a number of things that are taking place in the cyber industry that really are causing the move towards platformization. One, you've got the concept of tool sprawl. There's just way too much stuff coming from way too many vendors. And there's a number of, I guess, economic impacts where CISOs are being really pushed towards eliminating tool sprawl. Second, there's too many point solutions. And when you get into a major breach, if you have 10 identity and access management tools and you have five SIMs, it's not a ticket for a successful outcome of a detect or a response. And I think if you look at it from a market point of view, I think what the market is saying, "We need a strategy that's simplified, it's cost effective, and it has much tighter integration."

And the definition that I use when I advise, I will kind of define platformization. I'm taking a bunch of tools, put it together in somewhat of a unified architecture, and that you're delivering multiple functions. Most importantly, sharing data, policy, analytics. And here's the analogous that I would use. It's really similar to what happened in customer relationship management, like Salesforce. Took all these various CRM tools, brought them together, AWS and cloud. And I can unpack this even further and give you some examples before platform and after platform, if that would be helpful?

Max: Sure, sure, sure.

Gary: Okay. Before platform you had a SIM from one vendor. You had endpoint EDR from another, you had CNAPP from a third, you got vulnerability management from another. If you look at an example of a platform, and the ones I always point to are Palo Alto Prisma, Microsoft Defender, and CrowdStrike Falcon, they offer in a box threat detection, CNAPP identity monitoring, automation. But the most important thing, it has shared telemetry. And that shared telemetry is one of the biggest drivers towards platformization. But there are some challenges. Customers are wary of lock-in. Then you got to get past the psychology of what I call feature parity versus best of breed. And then there's a lot of M&A that's taken place in this space. And there's a concept that I talk about called integration debt. You got to pay the piper for all these vendors that are buying disparate tools. They've got to think about how they're going to get them all integrated, and that's a cause for concern.

Max: Super helpful, really interesting. I suspect we're going to come back to platformization when we talk about investment risks and opportunities, but I do want to move us along. Key players in the space. I'd love to hear you riff for a few minutes on leaders and challengers within some of the sub-themes we've talked about. So CNAPP, AI-driven tools and disinformation.

Gary: We could talk for hours. Guide me where you want to spend more time. You want to start in CNAPP and go from there?

Max: Let's spend a little bit more time in CNAPP, because it sounds like that's the most directly addressable market today. Let's spend a little bit more time in CNAPP, but we'd love to just have you comment on names you're familiar with or seem to be doing interesting things in the other two.

Gary: All aside to my former employer, I think Wiz jumps out at top of the food chain. They're to some degree changing the game, because they're going towards agentless deployment. Their ability to look at multi-cloud configurations, vulnerabilities, I think is second to none. Their agentless deployment, second to none. I think they've really figured out really well what they need to do from a partner integration point of view. One of their weaknesses, they've got limited runtime protection. And then the big, big 800-pound gorilla in the room is what's going to happen should the Google acquisition take place. Will they maintain their independence? Will they still be a multi-cloud CNAPP provider, or are they going to be integrated into Google Chronicle?
Next one would be my alumni, Palo Alto Networks. I think they've got the broadest CNET feature set. I think they're the closest to platformization. I think they're as good as it gets when it comes to XDR and sort integration. There's some things they don't do well. It's really difficult to implement and manage. It's professional services heavy. There's total cost of ownership, they tend to be a higher cost.
Next one would be Microsoft Defender. If you are a native Azure environment best in class, they're also moving much more now towards multi-cloud support. It's incredibly, it's like a no-brainer if you're a Microsoft ecosystem. I think they've got the best identity risk management in the industry. They've got a couple of gaps in containerization. They're a little bit weak on third-party integration. The next one that I talk about is Orca. I describe Orca as the first cousin to Wiz. They are as good as it gets, also in agentless scanning of workloads, containers, cloud assets. Their ability, what I call time the value is second to none, because they're really lightweight when it comes to deployment. And then the last one I'll call out is Lacework. They're really, really strong in anomaly detection. What I think they're doing better than anyone, they're focusing on machine learning. They're really trying to attack behavioral analytics, but it's got, I'd say, less capability than a Wiz. And then there's a couple of, I'd say emerging vendors to put on your radar. One is Sysdig, one is Aqua, and the other would be Tenable.

Max: Super helpful. Can you talk just very briefly on what some of these startups or challengers or emerging players are doing well?

Gary: In CNAPP?

Max: Yeah.

Gary: I think there's a few things. Agentless models is clearly top of the food chain. I think DevOps-centric is really, really a differentiator. I think the agentless top of the food chain runtime detection, the ability to do, I guess codeless container security and scanning. And the ability to not only do cyber security monitoring, but do network security monitoring as well.

Max: Super helpful. Very briefly, AI-driven threat detection and security, any key players there? And then disinformation and narrative integrity key players there?

Gary: The ones that for me jump out of me, one is Lacework. I think they've got the first, what I would call lie detector test-ready platform for anomaly detection and behavioral monitoring. SentinelOne bought two companies. One is called PingSafe and the other is called Attivo, leading Edge behavioral AI. Another good one, another one I'm working with actually is a company called Vectra AI. They play really well in complementing CNAPP, especially for hybrid cloud and lateral movement detection. Darktrace. They're doing self-learning AI to detect threats in real time. A couple of others that are just jumping out there. One is called HiddenLayer. HiddenLayer is best of breed in protecting the model itself. Remember we talked earlier, there were gaps in protecting the model. So, they're coming at it first and foremost, we got to protect the model from model theft poisoning, adversarial attacks. Then you've got a company called Protect AI. They're going right after the supply chain security, so they scan the AI pipelines really, really well.
And then the last one that hits my radar is a company called Robust Intelligence. What they're doing more and more is really going after Cloud native where you've got inference models being designed in an AWS environment and a Google environment. They're going after protecting those inference pipelines.

Max: Super helpful, super helpful. Gary, you alluded to the Google acquisition of Wiz, so I want to broaden this question a little bit. This trend of Platformization, how much of that is going to be M&A driven? How important? So just to comment on the impact of M&A in this space generally, right? So how much of this platformization trend do you think is going to be M&A driven? Does that suggest your view is that there'll be an increase in M&A activity over the next 12 to 18 months? And then why specifically is the Google Wiz acquisition of the elephant in the room?

Gary: So, 80% of the work that I'm doing right now is in M&A private equity. And as a entrepreneur consultant, I always look at key trends and where I'm getting paid. So, 80% of the work that I'm doing right now is in the M&A space. There's a lot of drivers of that. You've got platformization that we talked about. CNAPP is driving market consolidation. Buyers want fewer vendors. You are going to have a wave of AI-driven native security startups are going to get bought before they even launch. And there's companies that I always talk about like Vectra AI. There's a company called Harfang out of the EU. There's a company called Grip Security. I don't even think they're going to launch before they get bought. That's how much work is going to happen. If I unpack it for you, if I look at the CNAPP space, I think if you and I are having this discussion in 18 months, I think Oracle, Sysdig and Aqua are gone.
I think there's going to be massive consolidation in M&A at the threat intelligence level. Companies like Flashpoint, Intel 471. And then I think the trends that you should think about in your research, there's going to be CNAPP overload. There's only going to be room, in my opinion, for four to five platforms. The others are going to get absorbed. AI-native tools are going to accelerate dramatically. You're going to have this massive convergent between threat Intel and cloud native. And if you ask me who's going to do the vast majority of the acquisitions, it's going to be CrowdStrike, it's going to be Palo Alto, it's going to be Zscaler. And don't diminish the impact that the Wiz acquisition from Google is going to have in causing a wake-up call in the rest of the CSP market, especially for AWS, who I would argue is lagging miles behind in this space.

Max: Awesome. Super, super interesting. More technical question here on the Google acquisition of Wiz or potential acquisition of Wiz. Does it set the benchmark a little bit from a valuation perspective? Is there some sort of you trigger or does that serve as a catalyst or not really? It's interesting for strategic reasons. The valuation is just the valuation and it's kind of a separate topic.

Gary: So look, at the end of the day they overpaid, but they overpaid with good intentions. One, when you've got billions and billions and billions and billions of dollars of cash sitting around, it's really easy to pay 80 billion to buy a company. But when you start thinking about valuation, you've got to bounce that out with the cost to buy versus the cost to engineer. There's a engineering cost that winds up being saved. I think it matters a lot to Google, because it's going to fortify their cloud stack, especially in the AI era, and they're going to be able to take Microsoft on really, really well. Don't dismiss the fact that that final price, you're probably looking at a current ARR run rate for Wiz of about 1.4 billion. I do think what Google did paying 32 billion when in May, May 24 they offered 12.
They raised the bar, you're going to see a new benchmark for cyber M&A. Not only are you going to see further acquisition, but I think the price that people pay, I mean, we bought at Palo Alto a company in AI about a month ago. Hasn't even generated the first dollar of revenue, and I think the final negotiating price was $800 million in stock. It's going to drive an inflated valuation and it's going to drive sort of a ultimate race to play what I call cyber security whack-a-mo as these companies stick their heads up. These startups are going to need lots of capital. They're going to need lots of investment. You're not going to see a lot of net new cyber companies go public. I think we've kind of exhausted the public market in cyber security. So, that leads you to one conclusion, lots of M&A.

Max: Awesome. Really interesting perspective there. Okay, I want to move us on, Gary to the final topic of today's discussion is investment risks and opportunities. And I actually want to ask a pretty specific question. So you started, you mentioned Platformization as a key kind of investable area or trend in the space, and you also described how, in your opinion, there's room for four or five platforms. So-

Gary: Correct-

Max: I don't want to put words in your mouth, but allow me to describe what we've talked about a little bit. Then I want you to challenge it and elaborate and make sure it corresponds with your view. So there'll be four or five platforms. So, there's a race there to become those platforms and establish as those platforms. But then the four or five platforms create a really interesting investable opportunity for all of the companies that are going to get acquired by those platforms. And so, is the opportunity to try to be top three in your sub category so that one of the platforms will end up buying you? How do you think about, just double clicking on the investable opportunity. Do you need to be the platform or do you need to be a top within a specific category such that one of the platforms will eventually acquire you?

Gary: In my opinion there is no investable opportunity to from the ground up become the platform. There's just too much that's already happened. There's too much investment that's already happened. It's really clear to me that this is sort of a four to five horse race. Don't confuse my four to five who's in the race with necessarily the ones that are going to win. I think you need to look at it a little bit differently. Where I would go, if I was running a cybersecurity venture fund, I would look at making sure that I'm investing in potential areas that can become best of breed so they can become one, part of the platform, or two, become investable. And there's so many nascent areas, excuse me guys, so much nascent areas that are still growing and I'll run them to you quickly. If I had the money, I'd invest in six or seven areas, I'd look at clearly identity, access, security. Why would I go there? It's the primary attack surface.

I would look at AI security and AI model protection. Why? No one's doing it. Attackers and defenders are leveraging it. And there's new categories. I think it's really important that so many new categories that are going to become investable haven't even begun to be thought through. Model integrity, inference protection, AI threat protection. I'm working on a fascinating project right now in quantum cybersecurity. Jensen Wan last night, he's been a little bit schizophrenic in talking about where quantum is and now he believes that quantum is ready for prime time. If we get to a point in the next 12 to 24 months, which I think we will, where quantum can become a huge cryptography risk, it could become a huge risk to cryptocurrencies. That is going to be incredibly investable. And I think it's to some degree under scope and under invested. And I think you're going to see a whole bunch of smart money start coming into that space.

And then the last one for me, there's two last ones. One is OT, and I think we talked about the reality of attacks on critical infrastructure, highly under invested right now. Then the last one that I'm interested in is the concept of integrating cyber insurance and risk quantification. It's one thing to get insurance after the fact. It's another thing to better measure and ensure, you know what your cyber risk, there's going to be a whole bunch of money that gets invested in doing things like analytics-driven underwriting, cyber risk quantification platforms. You're actually creating a cyber actuarial capability.

And then the last one that I'm starting to think about, I can't go into enough of it yet, because I haven't formed a premise. There's going to be this massive, massive integration of physical security and cybersecurity. Smart cities, smart glasses, smart devices, home security powered by smart devices. One of the intriguing things I'm working on now for a major cloud provider that I can't talk to you about is they are very intentionally putting together a investment strategy of how they will merge their physical security and their cybersecurity together. Because they view the convergence around AI and devices, and campus security is ultimately coming together. You're going to see a lot of investable opportunities in that integration of physical and cyber.

Max: Yeah, that's super interesting. Thank you for sharing those. That's exactly the insight we were after. Okay, so that's great. So there's going to be, there's this platformization trend and then there's the opportunity to invest in strong players such that the outcome or the exit or the liquidity for some of these companies is going to be absorption into the platforms. So, that creates a nice investment landscape or investable landscape. What about the risks? What about the risks? If someone, you gave this hypothetical example of if you were running your own cybersecurity VC firm, that's what you'd be looking at. And then what are the big risks to avoid? Are there elements, are there segments where it's too capital intensive, where the technology changes too quickly, the length of the sales cycle? What would you are the biggest risks if someone were to pursue that strategy?

Gary: Overhype market and feature inflation. Everybody's hyping and overstating capabilities. There's a huge risk that all these categories that you and I have been talking about, they're highly dependent on telemetry, like the quality of the data. There's risks that are yet to be determined around what the regulatory and ethical landmines are going to be. You're going to have all sorts of regulations that are going to impose stricter rules on a lot of the technology that we talked about. The big, big, big 800-pound gorilla is big tech competition. Can you really take on Microsoft, Google, Palo, CrowdStrike and AWS? And at the end of the day, I think too much hype. There's concerned about lack of technical depth. Can you build something that doesn't wind up getting obsoleted before you even bring it to market? And then the platform threat.

Max: Right. Super interesting. Thanks for describing those. So Gary, look, we're coming up on time here. We've covered a lot today. Is there anything related to cybersecurity and the three subsegments we've talked about that we didn't touch on today that you think is really important or that you come across frequently?

Gary: Yeah, I would guide you to really double click on quantum. It's got a total addressable market that by 2028 I believe will be about 40 to 50 billion. It's probably, you got to sit in the confidential meetings that I get to sit in, the number one thing that make executives nervous is they don't really know what quantum means to the attack surface and what the implications are. Think about if you break the current cryptography. Think about that.

Max: Yeah.

Gary: All hell breaks loose. So, I would clearly guide you there.

Max: Super helpful. Great way to end the discussion. Quantum as a big open question, an overhang on the entire cybersecurity security space. Well, Gary, thank you.

Gary: I got another meeting. I really hope I helped you guys. I hope this was informative.

Max: This is exactly the kind of insight we were after. Thank you so much for taking the time today. We really appreciate it. Enjoy the rest of your day.

This Transcript is accompanied by Coleman Research's comprehensive attestation completed by the Expert following the Hosted Event conference call (the "Attestation"). The Attestation requires the Expert to re - confirm, inter alia, their qualification to consult with CRG in accordance with: 1) Coleman Research's Expert Terms & Conditions, 2) any duties, agreements or contracts in connection the expert's employment, or otherwise, 3) the absence of any disqualifying events in the Expert's personal or professional life, 4) Coleman Research's Seminars restriction against employment by or prohibited relationships with any company with publicly traded securities or government entities. Finally, the Attestation requires the Expert to re-confirm that they did not discuss any information of a confidential nature or provide information constituting material non-public information as circumscribed by applicable securities laws.