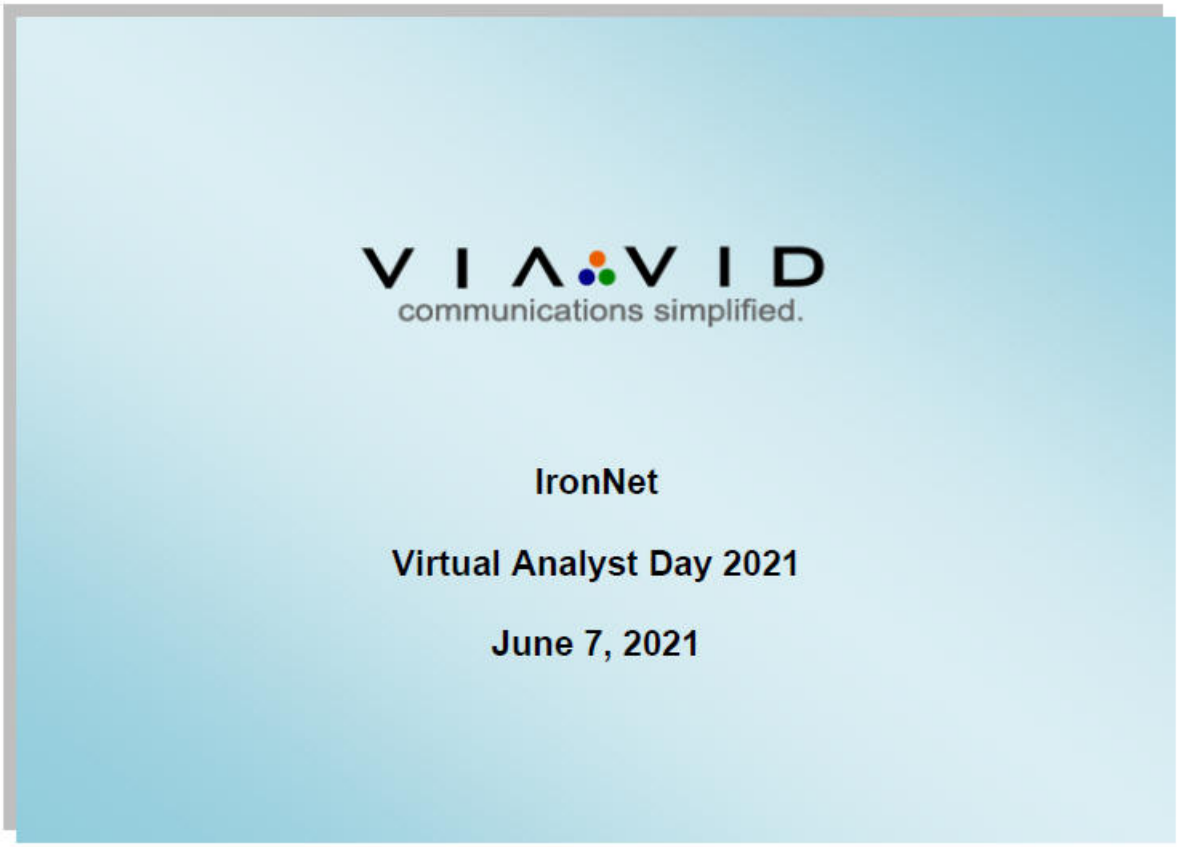
Filed by LGL Systems Acquisition Corp.
pursuant to Rule 425 under the Securities Act of 1933
and deemed filed pursuant to Rule 14a-12
under the Securities Exchange Act of 1934
Subject Company: LGL Systems Acquisition Corp.
Commission File No. 333-256129

The following is a transcript of the virtual analyst day event held by IronNet CyberSecurity, Inc. on June 7, 2021. The video recording of the virtual analyst day presentation is expected to made available on the website of LGL Systems Acquisition Corp.



C O R P O R A T E P A R T I C I P A N T S

Nancy Fazioli, *Vice President, Investor Relations, IronNet*

Rob LaPenta, *Executive Vice President and Chief Financial Officer, LGL Systems Acquisition Corp.*

General (Ret.) Keith Alexander, *Founder, Co-Chief Executive Officer and Chairman, IronNet*

William Welch, *Co-Chief Executive Officer, IronNet*

James Gerber, *Chief Financial Officer, IronNet*

C O N F E R E N C E C A L L P A R T I C I P A N T S

Andrew Nowinski, *D.A. Davidson Research*

Mike Cikos, *Needham & Company*

Jonathan Ho, *William Blair*

Josh Sullivan, *Benchmark Capital*

Imtiaz Koujalgi, *Guggenheim Securities*

Matthew Galinko, *Sidoti*

Nehal Chokshi, *Northland Securities*

Gray Powell, *BTIG Research*

P R E S E N T A T I O N

Nancy Fazioli

Welcome, everyone, and thank you for joining IronNet's Analyst Day. I'm Nancy Fazioli, Vice President of Investor Relations. We have a greatline-up, and we hope you'll find the discussion informative.

Today, you will hear from Rob LaPenta, CFO of LGL Acquisition Corp.; General Keith Alexander, our Founder andCo-CEO; Bill Welch, ourCo-CEO; and Jamie Gerber, our CFO.

We have two videos, Q&A sessions, the first on technical and product, second ongo-to-market, and the third on financial, and some breaks. If you have a question, kindly hold it until one of the designated Q&A sessions or the general Q&A sessions at the end of the presentation. Thank you.

The following presentation contains forward-looking statements. For a description of the factors that could cause actual results to differ from these forward-looking statements, including statements regarding IronNet's projected financial results, please refer to the disclosure under the heading Risk Factors in the Form S-4 filed by LGL Systems Acquisition Corp. on May 14, 2021. The presentation used today will be posted to LGL Systems Acquisition Corp's website.

I'd now like to hand it over to Rob LaPenta of LGL Systems Acquisition Corp. Rob?

Rob LaPenta

Great. Thanks, Nancy, and I'm Rob LaPenta from LGL Systems Acquisition Corp., here to present our announced combination with IronNet Cybersecurity. We thank you for your interest this afternoon.

We're really excited to introduce the IronNet Cybersecurity team, and the presentation, and really, there's a lot going on in cybersecurity. This couldn't be more timely. We think the Company's business model really, really addresses a lot of the challenges that the industry and commercial and government and ecosystems are facing, so we thank you again.

Going on to our next slide, I'm going to get into just some of the transaction points. I'll give you a quick summary of the LGL team, and then we'll get you over to General Alexander and the team.

Our acquisition, this is a pro-forma enterprise value of $927 million. The combination here is that the IronNet team will be rolling over their entire equity —existing equity into this new entity. They'll own 72% of a pro-forma equity. The transaction contemplates $125 million PIPE. The PIPE holders you'll see in the back of the presentation will own 10% of the pro-forma equity and will assume no redemptions. When you combine the $125 million with the $173 million in the LGL cash in trust, we're looking to provide the Company $267 million in cash to the balance sheet at closing. That is net of fees, and that'll assume no redemptions.

The use of proceeds will be continuedbuild-out of the sales and marketing infrastructure that's in place, accelerate R&D and product offerings, and lastly, leave some cash on balance sheet for any M&A opportunities that the team looks to pursue, funded solely by LGL cash in trust after redemptions and proceeds from the PIPE.

Valuation—the $927 million pro-forma EV equates to 17.1 times Fiscal Year '22 and 8.4 times Fiscal Year '23 revenue. Keep in mind, Fiscal Year '23 approximates calendar year '21, and Fiscal Year '23 approximates calendar year '22, just to make it easy for you. This applies a pro-forma equity value of $1.2 billion, and on the last bullet there, I think you can read that, attractive valuation with transformational cybersecurity platform.

The LGL team has evaluated a lot of transactions as part of our work with the SPAC. We have not come across anything as differentiated as, really, the IronNet Cybersecurity team. We think the technology feasibility and behavioral analytics, the model of a Collective Defense model is really timely in the marketplace, and then combined with the exceptional Management team, it's a great package, and we're really excited for you to dig in and do some work on it.

The next slide just shows you a little bit from our team. We have a broad team. It's been very helpful in terms of the sourcing and evaluating transactions. We have folks here that have been allocating capital as corporate stewards. We have portfolio managers, research analysts, a lot of folks with expertise in cybersecurity, folks from private equity, and lastly, teams here that have brought private companies public. We've been working with the IronNet team. We're very excited to continue to help them as they transition from a private Company into a public domain, and I've referenced, we've evaluated a lot of transactions. This was highly differentiated, and, of course, very timely.

Then with that, one of the other things about the IronNet team is the technical (inaudible) be what they are, and the differentiated, I think, approach to the marketplace, but they're a very mission-focused team. That'll come out in the presentation, and that's something that also really, really sets them apart.

With that, if you go to the next snapshot, I usually read a quote from the General, and then there's some payment for doing this, but take a look at that. I think that really, really encapsulate the team and the opportunity, and really, what's going on in the marketplace, so now I'm pleased to introduce you to General Keith Alexander. He's the Founder of IronNet, served our country as a four-star General, former Director of the NSA, Founding Commander of U.S. Cyber Command, widely respected in government and private sector circles for defending our nation against cybersecurity attacks.

With that, it's my pleasure to introduce you to General Keith Alexander. General?

General (Ret.) Keith Alexander

Thanks, Rob. Thanks for that introduction, and for those of you have joined, the inside joke is every time Rob says something nice about me, I have to pay him 20 bucks, and this has been about the 80th time, so I'm into him about $1,600 right now, but other than that, we're on a mission to transform the way we do cybersecurity and address the significant shortfalls that we see in terms of personnel, detection, and malware, knowledge sharing, and crowdsourcing. IronNet has developed a differentiated solution that leverages artificial intelligence-driven behavioral analytics and Collective Defense.

Next slide, please.

I had the privilege and honor of running the National Security Agency for almost nine years, leading our nation's offensive cyber capabilities and establishing the U.S. Cyber Command; two jobs, one paycheck. That's how our government works. I spent 40 years in the military and the intelligence community addressing (inaudible) problems almost entirely associated with networks, computers, and cybersecurity.

Also presenting today are Bill Welch, ourCo-CEO, and our Chief Revenue Officer of Zscaler, former. Bill scaled the business around the Company's novel approach—Zscaler's novel approach that today is the industry standard. He then replicated this as the President of zero-trust leader, Duo Security, and it was purchased by Cisco for $2.35 billion just before they were going public.

Also presenting is our Chief Financial Officer, Jamie Gerber. Jamie has over 25 years experience as a CFO, and tremendous public company experience. Jamie understands metrics, forecasting, and needs of a public company. He has instilled that at IronNet as a metrics and benchmarking-driven operating model for our financial team.

Bill, Jamie, and the team we have assembled has an incredible network of eight players in sales, marketing, engineering, and operations that have enabled us to recruit from high impact and build a great, world-class team. We've assembled a public Company ready Management team and Board.

Highlights from the Board—you can see here we have Ted Schlein from Kleiner Perkins and Don Dixon from ForgePoint, both recognized in the investor community as leaders in cybersecurity.

We also have Mike McConnell and Mike Rogers who served in the government. Mike McConnell was the Director of National Intelligence; Mike Rogers, Chair of the Intel Committee; and Jack Keane, who was Vice Chief of Staff of the Army.

We also have Bridgewater and Temasek, who were first customers, and are now investors in our Company.

Next slide, please.

IronNet at a glance. I want to go back to 2006 in Iraq where our forces were taking increased casualties, in part because our intelligence took too long to get to the combat brigades. Every brigade collected information on the terrorists. It was hard to share all of that information across brigade boundaries. Terrorists and adversaries could easily cross those boundaries without risk of capture. We see the same issue in cyberspace today. In Iraq, we built a system to rewire Iraq, bring all of that information together, cutting the time of collection to operational use from 16 hours to one minute. This included real-time collaboration and sharing across brigade boundaries, a variation of Collective Defense, and the first year of the real-time regional gateway helped us take down 3,950 bad guys, and Dave Petraeus credits this system with breaking the back of the resistance.

When we started IronNet, we faced a very similar issue in cyber; too slow, information (inaudible), adversaries evaded detection, limited knowledge sharing, and the attacks were increasing, and they continue today. That's the problem that IronNet addresses. We're attacking a $25 billion security market, and that market is expanding. Within that market, we have a differentiated technology. Current technology is slow and manual, but most importantly, detects less sophisticated and already known signature-based attacks. We don't just find existing attacks. We use advanced AI-driven behavioral analytics to detect new, non signature-based attacks such as SolarWinds. This market is commonly referred to as network detection and response.

I'll give you an analogy of what we're trying to do here using air traffic control. If you think about how radar's working in developing a collective picture of air traffic control so all air traffic controllers and planes are safely operated, we have this great picture that ensures the safety of flight. We don't have a picture in cyberspace. Every company has its own picture of what's hitting that, and only what they know based on those events that they already know about. They don't have a way of sharing the anomalies; the unknown unknowns. We have behavioral analytics that allow us to do that, and so by sharing that information among companies, we can create a picture that, with anonymized data, can not only be shared to protect collectively those companies, and we'll talk about that, but it can also be shared with the government, and that's where the Collective Defense goes.

Today, you're seeing a lot of questions, are we going into a cyber war? It's up in the press today, and the question is, I think we're going to see increased cyber engagements, and this is what we have to fix as a nation and what our allies have to fix; how we defend in this space. Our cloud-based scalable platform incorporates two main layers: IronDefense, which ingests about two trillion data flows a year, analyze, correlates that data using AI and machine learning, and produces relevant threat data. We layer on top of that IronDome, our Collective Defense platform, which brings in the concept of Collective Defense that I was just talking about, and shares that information and intelligence across organizations, sectors, and governments, knowledge sharing and crowdsourcing.

Our cornerstone customer gives us fundamentally new business model, and Bill's going to go into that in detail. Our unique team, our world-class trained cyber hunters and experience has allowed us to create a deep, competitive moat; get access to large, cornerstone companies; retain and expand them; and execute this at scale as a fast-growing, public Company.

Next slide, please.

We understand well the problems in cybersecurity today. If we step back, here are the biggest problems (inaudible) and their team faces. This is what is bothering them. These are the issues. This is the problem. The threats are constantly growing and getting worse. It is impossible to keep up with the evolving attack techniques. Many are from nations like China, Russia, and Iran, but most of today's cybersecurity solutions are point solutions that only look at one thing; for example, a, endpoint, a web gateway, or a firewall. No company is looking across all that to get all the attacks together, and as a consequence, we are losing the forest for looking at the trees.

As you know, every company has a security operations center to defend against attacks. The stock analysts can see the threats that their own company faces, but are completely blind to different attacks happening to other companies around them. Making the problem worse, there's a massive talent gap to hire enough qualified stock analysts. This is only making matters worse.

To summarize, there is a need for a complete solution that can stay ahead of the attackers, provide full visibility into the enterprise, and be intelligent enough to make up for the lack of security analysts.

Next slide.

Why did we start IronNet? In 2008, the Defense Department was attacked by Russia in an operation known as Buckshot Yankee. NSA detected the exploit into DoD's classified network and developed and fielded a system to mitigate the compromise in 22 hours. No one else in the world could have done this with all of the encryption, decryption, and other capabilities needed. Secretary Gates realized we had special skills, and told me that he wanted me to stand up U.S. Cyber Command. I looked at Secretary Gates and, of course, said, "Yes, sir," and he said, "We need to defend the nation," and I said, "Absolutely, we have to defend the nation, but we can't see the nation. One major problem, we can only see the attacks in the commercial infrastructure when they tell us about it. You can't see attacks, so you can't defend against it." We built IronNet to address that problem, and I'll talk about that in a future slide coming up, because my successor, General Nakasone, has said the same thing. "We can't see the dots. We can't correlate what we can't see."

Attackers continue to innovate (inaudible) and advance, the game evolves rapidly, and the stakes are higher each year, as the legacy of attacks show. The concept of proactive defense will alter the cybersecurity landscape. Companies no longer will have to defend in isolation, but can and must operate as part of a collective team. IronNet is not just a better mousetrap, but a force multiplier. We strengthen not only the defense of our customers, but make the rest of the security vendors even stronger, and we present an effective solution for new real-time public-private sharing.

Next slide, please.

What does IronNet do? We're a network detection response platform that identifies cyber threats through the use ofAI-driven behavioral analytics to find anomalies and network traffic behavior with a Collective Defense solution. Before I describe our differentiated solution, I'm going to ask Bill to provide context for what NDR is, and why NDR and IronNet are critical parts on the security stack.

Over to you, Bill.

William Welch

Thank you, General.

Team, from my two decades at cybersecurity companies, we know that the security landscape is evolving, but there's one constant that the attacker's always looking to find a way in, and, as the General mentioned, NDR technology, or network detection response, was really developed to determine if the attacker's in your network, what they're doing, and if they are trying to cause you harm. Once we have determined an attacker is in the network, the response part of NDR provide the actions that addresses those threats. These actions are most effective when they're done automatically and at computer speed, so by analyzing that network traffic using AI-driven behavioral analytics, which the General spoke about, IronDefense's NDR can detect sophisticated evasion methods and zero day threats like SolarWinds, which we'll talk about in a moment.

I want to make sure that you all understand a couple of things, though, related to this industry. Customers do not hire IronNet instead of, for example, CrowdStrike, which protects the endpoint, or Zscaler, which I have some knowledge of, which provides a secure web gateway. NDR platforms ingest the data produced by these point solutions and other centers that we have on the network to analyze the data for these behavioral anomalies to identify the threats. NDR is part of the security stack, and provides a complete picture of threats on an enterprise network, so in other words, we're focused inside the network to find bad actors that have gotten past the other point solutions.

SolarWinds, for example, lived in the networks for months before it caused harm. We found SolarWinds on customer systems six months before everyone else did, shutting it down before it could do damage in our customer environments. That is why some have called IronNet the CrowdStrike of the network.

With that, I'm going to transition back over to the General so he can give you more of an understanding of what makes IronNet unique comparable. General?

General (Ret.) Keith Alexander

Thanks, Bill.

On the left here, you see transforming cybersecurity through AI-driven behavioral analytics and Collective Defense. What does that mean exactly? At its core, IronNet does three things to secure a network.

First, we collect data coming in from the entire security stack. That includes partner companies, as Bill mentioned.

Second, we analyze that data to determine if there's any malicious behavior on the network and provide the response that is in IronDefense.

Third, we share that data across companies to defend as a team.

That is Collective Defense, which we call IronDome.

Our solution enhances performance, and is a dramatic force multiplier similar to what we achieved in Iraq, improves threat detection, and uniquely creates an enormous network effect of more data, better analytics, enhanced intel, and more customers, etc.

Next slide, please.

Our mission space is experiencing significant momentum. The administration has issued an executive order and is mandating enhanced cybersecurity measures across public and private enterprises. Majors see change needed in how industries and nations protect themselves in cyberspace is evident here, how they share and how they work together. Page 1 of the May 12 executive order reinforces this. Protecting our nation from malicious cyber actors requires the federal government to partner with the private sector. The partner sector must adapt to the continuously changing threat environment, ensure its products are

built and operate securely, and partner with the federal government to foster a more secure cyberspace. On here you can see the quote from General Nakasone. He said, “I can’t see the dots.” We’re the Company that’s going to help him see those dots. The DarkSide attack, Cyberspace Solarium Commission, and recent comments from the Director of the NSA all underscore the need for public-private cooperation. We feel we are uniquely positioned at the intersection of these paradigm shifts, and our customers stand to greatly benefit from our products.

Next slide.

IronNet sits in the middle of the security stack, working on ingesting not only netflow data, but we also ingest data from the endpoints, as Bill mentioned, like CrowdStrike; from the firewall like Palo Alto networks; from the web security gateway like Zscaler; and other tools, as shown here. As attacks become more advanced, so must your defenses. IronNet is a cloud-based solution, and it allows us to scale significantly. As I mentioned before, our IronDefense platform analyzes and correlates data through behavioral analytics to identify threats. IronNet then shares this intel between companies and industries through our IronDome platform, and I would point out that that information is anonymized. It allows us to share an unlisted stack of 2015. There’s no content communications, no intellectual property, no customer name.

I’ll give you an example why this is important. Imagine 90 mid-sized banks, each with 10 people working as hard as they can to defend their bank. The amount of information that they see every year is doubling. The number of protocols is doubling. The number of devices is doubling. Their world is doubling every year, but they can’t double the number of people, and down the road is another bank with 10 people doing the same job, and another bank and another bank. There’s 90 of them in the mid-sized bank coalition. Think about this, 90 banks with 10 people each, each defending themselves. Now imagine those 90 banks work together in Collective Defense. You now have 900 people working together, share anonymized data about the dots that General Nakasone was talking about, give that to the government, and we now have a process for defending the nation and the finance sector and the healthcare sector and the energy sector.

Our analytics create alerts. Our patented expert system gives us the insights into these alerts. IronDome helps us create these insights. Anyone who has a similar behavior, it’s correlated automatically, and we’ll talk about that in SolarWinds. The power of Collective Defense is that companies can defeat attackers as a team. IronNet is that force multiplier.

Next slide.

SolarWinds/SUNBURST is an example of how the attacks today are not only sophisticated, but have wide-scale impacts on the supply chain, an ability to disrupt, not only the enterprise, but nations based, in this case, the U.S. government. How did an attack like SolarWinds succeed with every one of the 18,000 companies and agencies that were ultimately affected last year? The attack came from a trusted source. The malware spotted the conventional defenses set there to report on it, and removed references to itself from the conventional endpoint and firewall logs that were trying to report on its presence. The recon command and control activity stayed in the noise of regular activity.

IronDefense analytics operate where the attacker cannot see us, and thus, cannot try to turn us off. It can see through these methods in cutting to noise. SolarWinds is a real life example of how we detected as—almost as soon as it appeared in one of our customer networks back on 31 May, 2020, six months earlier than everyone else, as Bill mentioned. Our behavioral analytics detected command and control at network speed and sent it to the cloud. A few days later, another customer was hit with the same thing. When that was sent to the cloud, it was automatically correlated, and others went on as well.

In our Customer Advisory Board meeting, one of our clients, a major global investment fund, said they had up to 90 products in their stack. IronNet was the only one to detect and advance (inaudible). He went on to tell the other participants that our system was six times faster, and he was now determined what he could pull up. After the customer meeting, he went back to his team and said he wanted to expand IronNet considerably throughout their enterprise and their member companies, and he is doing just that.

Some of you may be asked if detect—if we detected the Colonial Pipeline DarkSide attack. The good news is none of our customers were attacked by that. However, had they attacked one of our customers, we were confident that our software would have detected the initial phishing attack. As a precaution, we run something we call prove the negative with a threat defined query in all of our customer networks when we see this to ensure that they are okay and safe, and then we tell them that so they can tell their c-suite and their board should that come up.

I'll now turn it over to Nancy.

Nancy Fazioli

Thanks. We are going to now show a brief video that will highlight the cyber challenges that the private and public sectors are facing, and we'll follow that with some Q&A.

Video Presentation

[A video of the ABC News Program "This Week," that aired on May 30, 2021 was shown. LGL Systems Acquisition Corp. previously filed a transcript of this video with the SEC pursuant to Rule 425 on June 14, 2021.]

Okay. As I mentioned, we're going to now follow to some Q&A session focused on technical and product-related questions, and we'll have a short break thereafter.

I believe we have a couple of questions here. Jonathan Ho, I'd like to give you opportunity to ask a question. I think you're unmuted now.

Jonathan?

Jonathan Ho

Can you hear me?

Nancy Fazioli

Yes, we can hear you.

Jonathan Ho

My first question is how is it that you're able to detect these threats when others are not able to, and how sustainable is this? AI behavioral also has a history of false positives, so how are you able to be six times more accurate than others?

General (Ret.) Keith Alexander

That's a great question. Let me just start with that one, and I think there's two parts that you've asked. How do we detect what others miss? Most start with a signature-based solution. Think of that as Suricata rules or the proofpoint set of rules, and then they grab all the information that comes from those rules and run behavioral analytics over the results of the events that those rules dictate. With that process, you're only going to see what the rules see, and that's the shortfall in the way they do it.

What we do is we actually look at netflow data packet behavior, and extract features on that packet behavior. Think of (inaudible), inter-packet arrival time, (inaudible), all these different—there's about 120 features you can look at a packet and determine what's going on with that packet. You can take that feature data, put that into a—if you will, a database, and run analytics over them at network speed. What that allows us to do is something that nobody else is doing today, and that is to see events that others miss, and the DNS command and control from SolarWinds was a case in point.

Your second part of that was what about the false positives? False positives is a big issue for all behavioral analytics, and ours included, so what did we do about that? We created an expert system with machine learning and AI, and what that does is it takes all of the information from endpoints, from the SIM, from all these other things, plus what our experts in that analytic would look at to understand is this a real DNS command and control issue, is it malicious, is it suspicious, or is it benign, and it would grade it, so you'll see we grade—everyone is graded by the machine, so we're not just serving that to the customer, here's a bunch of data. Good luck with it. We actually grade everything and say, these are known malicious. Look at these. These are in a high category, suspicious, and then these are ones we don't think you need to worry about, so we grade everything in that way, and that allows us to drive down false positives.

There's yet another area that comes into this, though. When you think about the number of events that people are looking at, knowledge sharing and crowdsourcing are now part of that future, so if I say it's bad, automatically everybody who has that same behavior benefits from that knowledge sharing and crowdsourcing, so we get two sets of benefits here; the machine learning and AI that we have with our expert system, and the crowdsourcing and knowledge sharing that we have with our IronDome IronDefense.

Jonathan Ho

Thank you for that explanation. Just one clarification. When you say that you're able to look at the netflow data, a lot of the firewalls out there, and perhaps, Zscaler, are looking at north-south traffic that's going into and out of networks or into and out of the cloud, but my understanding is that with netflow, you can also look at east-west traffic inside of the network. Is that an important differentiator for your solution, and does that allow you to catch things that have gotten past the perimeter already?

General (Ret.) Keith Alexander

Yes, so it's both. It's both of those, Jonathan, and you hit a key point, so you can look at both the north-south and the east-west. The east-west gives you insights for lateral movement and other things like that. On the north-south, though, on the many—just look at a few subsets of the features, Zscaler included. Great company and a great partner, but they're looking at a different part of their web gateway. We're looking at all the behaviors associated with packets that go through, so we see things in more detail than they're going to see with what they're doing. I think that's hugely important.

Does that help?

Nancy Fazioli

Thanks, Jonathan.

We'll go to the next question with Mike Cikos at Needham. Mike?

Mike Cikos

Hey, guys. Thanks for taking the question here. I did have a question on the ingesting of data. Can you just further hash out all these different sources of data you're pulling in and tying together, where is that—how does that process take place, and where are you guys doing this analysis and correlation with respect to your customers' IT environments?

General (Ret.) Keith Alexander

Yes, so what we do is we set up two parts of the environment. Great question, Mike.

First, we have a sensor that sits in their traffic. We have both a virtual and a physical sensor depending on how they want to operate. With that, we can also store on their site pcap data so that they can go back and look at something that's of interest, and then we send that data the—if you take the metadata from our flow extraction, so we extract features from that flow data and we send it into a database, and from that database on their network, we run that in their environment, and we generate alerts. Those alerts then go through an expert system that looks at each alert individually and adds to it information from the firewall, from the endpoint, from the SIM, plus a number of different enrichment things like is this a frequently-used website? What are the things that we want to understand about? What would an analyst go do manually to determine if that alert is important to them? They do research.

What we do, because there are false positives, we say, why waste an analyst's time when the machine can do all that, so we actually run all that through our machine, and then we list out the results, so when an analyst clicks on it, they don't have to go through all that. If they're interested in that, they can see everything that's happened, what the expert system has done, and if another analyst has looked at it and it's in the dome, they get the benefit of that knowledge as well.

Does that help, Mike?

Mike Cikos

It does. It does. Thank you for that, and then the follow-up, with all these alerts being pushed, and we're talking about the analyst going through the data, but I'm trying to think about it in the context of this community defense. Is that being automatically pushed to all your customers, and is that automatically —is that defense automatically taking shape for them, or is there some manpower resources required to adopt those?

General (Ret.) Keith Alexander

That's a great question. No, that's great, Mike. You're hitting exactly on where this is, where—what we do, and why this differentiates itself.

If I see something, let's say I'm a really good DNS command and control guy, and I've got really good knowledge on that, and I say, whoa, this is bad. I say it's malicious. Everybody who has that event or that type of event is automatically notified at network state. It goes out to their entire system. You've got a bad thing, heads up, so think of it as a fire alarm. You've got one and everybody knows, and then when you look at it, you can now have a discussion and say, well, here's what I see. I don't understand why you're saying it's bad. Can you help me? I'm not familiar with domain name server command and control. Why is that? Well, we look down three domain levels, which we actually did in the SolarWinds. Most people stop at the first subdomain level. We found some things in the third subdomain level that were very important. We listed that out. The expert system laid out what it saw in all that.

That's the type of help that I think is needed, so what you're doing is you're doing what a machine can do very good. It can grab all that data source, it can lay it out, it can grade every event, so you can have a million events, it's going to grade them all, and the good part is a human didn't have to look at that yet. Then it's going to rank order them. Here's the ones that are above a 900. Here's the ones above 800. Here's above 700. Here's the ones we don't think you should worry about. Now, we put the ones you don't think we should worry about. We don't throw them away. We say, that's odd, but we don't see anything bad to that right now. Then if something were to occur that makes us think it's bad, so now I think you have a DNS command and control. We're waiting for a response, and if the response in the SolarWinds was like a Cobalt Strike Beacon that comes back, then those two would be paired together and you'd know you have something really important. We do that as well.

Does that help, Mike?

Nancy Fazioli

Thanks, Mike.

I'm going to turn next to Josh Sullivan of Benchmark Capital. Josh?

Josh Sullivan

Good afternoon.

General (Ret.) Keith Alexander

Hey, Josh.

Josh Sullivan

Can you just go over, what is the main incentives for those other players in the cybersecurity stack to work with IronNet on new attack vectors? Is this information that just isn't valuable to them for their individual tools, or do you need the customer to say, hey, listen, IronNet's got a great product. It's very valuable to us. Please provide them with the information they need.

General (Ret.) Keith Alexander

It's really the latter. Customers are coming in and saying, hey, we want to CrowdStrike you guys, Palo Alto. Work with IronNet and what they're doing. It helps both of us, and to be honest, the cybersecurity companies are saying, look, the better we partner together, the better we're going to support companies, and we all want to do that, and so it's actually—I think you're seeing a conversion, so many of these companies now working together for the good of the companies they support. The better we work together, the better it helps our customers and the more they appreciate it, so that's like a double bonus.

We get that from all of our customers, especially in the energy sector, the CISOs (phon) said, yes, can you also work with this, so you saw publicly, we talked about Dragos, and looking at OT. How do you build IT and OT, so those are things that bringing those together helps the energy sector, and I think that's part of the future; working together. I think that's got to be where we go, not only as a Company, but where sectors, states, and nations are going to go.

Does that help, Josh?

Josh Sullivan

It does. It does. Thank you.

Maybe just one more, just how resilient are the behaviors? You're looking at the packet level. Are these pretty static behaviors, or are these updated continuously? Just what's the differentiating factor there?

General (Ret.) Keith Alexander

Yes, it's updated continuously, and it's an evolving area, and when I say that, think about this. It's actually, with machine learning and AI, there are things that we can do that we're patenting that allows us to see events that others cannot see by the way we cluster events around known malware that is not a signature, but a close association with a signature. You can't do that any other way than what we're doing, so that gives us a great opportunity and a great advantage. I think what that really does is it says to companies, in the future, where are we going? We're going to go to this type of system which integrates with others, exchanges data with the endpoint, with the firewall, with the SIM, and allows us to begin to use this machine learning, AI expert system to help defend networks and share that across companies. That's what I think is the future of cybersecurity. We have to do that. There is no other way to see the unknown unknowns, and that's what's kicking everybody's butt.

If you look at all the stuff that's happened over the last six months, nobody knew about SolarWinds. Nobody saw the Microsoft hack. Nobody saw Colonial, if you look at all, and the reason is they're looking for what they know and the bad guys are changing it to something they don't know, so you have to go to this part. It is harder. We spent seven years creating it. It's like the seven-year itch, and it's not been easy. That's why we brought in Bill who has great experience in building companies here and helping us take this to a commercially viable Company. We have great technology, and then I think it's patented, both this and what we call IronNet 2.0, so thanks for that question.

Nancy Fazioli

Thanks, Josh. Next to Taz Koujalgi from Guggenheim Securities. Taz?

General (Ret.) Keith Alexander

You may be on mute, Taz.

Imtiaz Koujalgi

Sorry about that. Can you guys hear me now?

Nancy Fazioli

We can hear you.

Imtiaz Koujalgi

Perfect. Hey, guys.

I have a couple of questions. Number one is who else does what you guys do? Can you talk about the competitive landscape, who you guys compete with, when customers buy you guys, who do they (inaudible) IronNet against; and number two is can you talk a little bit about the deployment model, your form factor? Are you guys on-prem? Are you guys in the cloud? Is it a SaaS model versus anon-prem license model, so those two questions?

General (Ret.) Keith Alexander

Okay, so real quick, we normally get compared with—Darktrace is probably the biggest one, Vectra and ExtraHop. Those are the ones that people see in the—what we call behavioral analytics. There is a big differentiation there. Most of them start with Suricata-based rules to actually create their events. That's a shortfall that they have that means they will not see some of the stuff that we see, and we can prove that with our cyber threat emulations. More importantly, you're not sharing the known knowns and correlating that data. That's another value that they need, so that's who we compared with. I think Bill brought a great point out earlier when he said think about IronNet. It is a CloudStrike for the net itself, and that's what companies are actually saying about us. I think that's part of it.

Now, our deployment model. We've worked hard over the last few years—Bill can—Bill will smile about going from a refrigerator to virtual capability in the cloud, so we wanted to go—it takes way too long to grow a lot of equipment and do all that. We can now spin up the capability in the cloud in 15 minutes. That's good, and we have virtual sensors as well. Many customers want an on-prem sensor, but each of those, we're talking a day or less to do all that and to set up a customer. That's part of the future, so they get a choice.

Then finally, some are going to say, I don't want to go to the cloud, so we have a (inaudible) ready, Nutanix (phon) version that we can deploy on their infrastructure, and we can spin that up, and we actually demonstrated that on (inaudible) in any environment. You've got that Nutanix. We can fire it up and we can run our system there, so for companies or countries that want their own infrastructure, we can do that as well.

Does that help, Taz?

Imtiaz Koujalgi

Yes, it does, and just surprised how you have customers who are running (inaudible) on Azure so people who are on the cloud, you can still deploy IronNet sensors and your (inaudible) core—your core back end on the—on public clouds as well?

General (Ret.) Keith Alexander

That's correct. That's correct. In fact, we have a great partnership with them, and it's growing.

Nancy Fazioli

Great. Thanks, Taz.

I'll move next to Gray Powell from BTIG. Gray?

Gray Powell

Great. Thanks. Can you hear me okay?

General (Ret.) Keith Alexander

We can.

Nancy Fazioli

We can hear you. Thanks.

Gray Powell

Cool. Yes, so I had a few questions here, and I think you've pretty much hit on this first one, but yes, as you look at the other vendors in the NDR space like Darktrace and Vectra and ExtraHop, what do you say is the biggest one or two points of differentiation? Is it the data sharing capabilities with IronDome, or is it just the overall effectiveness of your AI detection rates?

General (Ret.) Keith Alexander

Well, the most visual one people come to the fastest is the Collective Defense through IronDome. That differentiates us from all of them. Hidden underneath it is the foundation of the way we do behavioral analytics, so it's those two, actually. The second one, the behavioral analytics and the differentiation there is significant. It means we're going to see things they will not see. The Collective Defense, though, is the important thing for what we're doing to help defend companies, sectors, states, and nations. You need to see the dots. General Nakasone said, "I can't see the dots." We're creating the dots that the private sector can use and working together, knowledge sharing and crowdsourcing, and because they're anonymized, there's no personally identifiable information, no content or communication, no company name, they can be shared with the government and the government can say, wow, why is that happening? Imagine sharing all that on the SolarWinds. The government could have shut this down in June of last year. That's where we should have been. That's part of the future.

Gray Powell

Okay. That's really helpful, and then this is a hopefully not too basic question, but do you bill separately for the detection capability versus the threat intelligence from IronDome? If a customer wanted to, could they just purchase a small—could they just cover a small portion of their assets with the detection piece of your products, but then get all of the crowdsourced benefits from IronDome? I'm just trying to think through that dynamic.

General (Ret.) Keith Alexander

Yes, so they can determine how much they want to do, when, and they can still do that in the Dome and benefit from that. Most companies, though, want to see what's going on throughout their infrastructure, and they go for the whole thing. They find that is the most viable. I would say the vast majority do it all. Some say, I'd like to test it on some, and I think that's where they say, let me test a 10 gig thing over here. I'm going to test this data center in Ohio and let's do it this way, so we start with that, and then they say, wow, okay, I really need to see all my events. I need to see it across my entire enterprise.

Does that make sense?

Nancy Fazioli

Yes. Thank you very much, Gray, and we're going to move to Andrew Nowinski of D.A. Davidson. Andrew?

Andrew Nowinski

Great. Thank you very much. This is very interesting. Thank you for the presentation, General.

I just had a high-level question. Maybe if you go back to the first mega breaches of Target and Home Depot back in 2013, there's always been an obvious need to share information with other entities to prevent those same types of attacks from happening again, yet it's never happened, and breach activity has continued unabated for the last 10 years, so how willing do you think are government agencies, particularly the intelligence agencies, to share data with IronDome, and then similarly, what has changed now that enterprises will—are now willing to share their data with their potential competitors?

General (Ret.) Keith Alexander

Yes, that's a great question, and in complete candor, not all companies yet have bought into sharing their data, but 90%-plus are moving down that road very quickly. The energy sector en masse is going down that road, and we're seeing that across the defense industrial base. We're seeing that in healthcare. We're seeing that in some of the finance sector, and in some of the hedge fund community, so I believe—this is an area that I've lived my whole life, and I've worked both the offense and the defense, and if you want to defend in this space, you've got to do essentially what we're talking about here. It's the only way we could think of to defend our nation.

Now, with respect to are they willing to share? Absolutely. I've talked to the intelligence community and the Defense Department. They want to share. They need a vehicle to share. It's one thing everybody wants them to share what's going to go with my software? That's something they may not see and others may see, but what they can do is they can say, oh, I—you're seeing A, I think A is bad, and here's what I can do, and they don't need to say, oh, it's coming from intelligence agency one, two, three, or four. They just can say it's the U.S. government. This is bad. Everybody benefits from that knowledge sharing and crowdsourcing. More importantly, Andrew, what they can do is the intelligence community, and my old place, NSA and Cyber Command, can say, now, what the heck are they up to?

Re-imagine SolarWinds. We are detecting that now in May of 2020. June, we're seeing what's going on. We can be blocking that at the same time our offensive teams are looking at what's the SVR doing to our country and why are they doing it? Let's send them a message right now, just take down part of their network or do whatever they've got to do, and look, they get the message. That ends there. That's where we need to be. That's what we have to do, and it requires, as you point out, the government sharing, the private sector sharing, we've got to work this together. I think that will come, and I think that will be good for all of us.

Andrew Nowinski

Thank you, and then what kind of vetting do you do of companies that want to participate in IronDome? There could be, certainly, some companies who are nefarious organizations. How do you give at those—that 10% of enterprises that are unwilling, so far, to share that—to give them the confidence that their data is secure and that this is the right community to share data with?

General (Ret.) Keith Alexander

Yes, a great point. There's a couple of tests that we can do on that. So far, it has been easily—easy for us to regulate and go through, and the second part would be there are things that we can do to test to see the efficacy of some of the people that we're doing. Work to be done in that area, for sure. It's a great question, Andrew. Now, the nice part is they don't know how the events and the alerts are actually correlated and they don't see all that, so an adversary that comes into this, this is going to be part of the give-and-take of cybersecurity is understanding who's trying to penetrate what. There are things that we can do to hide and do that that will evolve as we go forward.

Great question, and things that we're working on. Thanks.

Nancy Fazioli

Great. Thanks, Andrew, and thanks to all of you for your questions. We're going to move to a short five-minute break here, so we'll start again at 1:05, and let you take that short break. Thank you again, and if you had additional questions, we will have a general question session at the end. Thanks.

General (Ret.) Keith Alexander

Okay. Welcome back, everyone.

I'll now let Bill, who has deep experience in scaling businesses at both Zscaler and Duo, walk through our plans for how we plan to replicate his prior success and do it here at IronNet. Over to you, Bill.

William Welch

Thanks, General.

As the General shared with you, I have seen the security industry evolve from legacy providers such as Symantec. I worked at Symantec, and I saw the evolution from the inside of next generation security providers like Zscaler and Duo. Point solutions are providing point protection, not comprehensive protection like the General and all of us have been talking about today, so no existing vendor in the market, to our knowledge, is approaching cybersecurity like IronNet, so after I helped Zscaler become the industry standard for cloud security, I then went to Duo where I was part of the next generation two-factor authentication of that company. I was pursuing the next category-defining company, which is why I chose IronNet. See, I've seen how cloud adoption has evolved over the past few years, and I believe that Collective Defense and knowledge sharing will be the new way for cybersecurity.

This slide tells you a couple of things that I want you to take away.

Number one is many of the companies represented here were not considered household names by all of us in the security world five years ago. Now we consider them as next generation security leaders. These companies identified security industry pivot points very early. They delivered on the innovation of value curve better and faster than anyone else. The companies helped customers do this, and the investors who backed these companies, as you all know, saw great rewards.

IronNet has identified a security pivot point. We're the only Company, to our knowledge, that takes this Collective Defense approach, so let me repeat that. We're the only Company that allows a customer to move from security in isolation to security in teams, and we believe that, due to our product capabilities and our unique business model with Collective Defense, that we're going to be part of the next generation leaders that investors will come to know as defining and transforming cybersecurity.

Next slide.

We go after multiple segments similar to what Zscaler and CloudStrike did. I can speak from my Zscaler experience when we sold a secure web gateway, but we set the vision for cloud security. IronNet's doing the same thing. We're starting with an addressable market serving the network traffic analysis, or NTA, and network detection and response, which is the NDR space. We're dominating in that space. It's

growing because of everything you're seeing in the news from SolarWinds to Colonial Pipeline to Microsoft, and all these other similar attacks. In this market, Gartner lists our competitors as Darktrace, Vectra, and ExtraHop. However, there's a larger global TAM that we have the opportunity to grow into, including endpoint, web security, MSS DDoS prevention as identified by our customers.

Our platform for innovation is the vision to expand in the global, as well as the U.S. markets. We've already had great success in EMEA and APJ, which I'll talk about later on. In addition, our total addressable market, or TAM, as you all know, is growing with the advent of 5G, IoT, and increased Internet usage, expanding the need for IronNet and this concept of Collective Defense. You might have noticed recently in your readings that CrowdStrike recently increased their TAM, which we completely agree with. We've kept our TAM conservative, but we believe that it's similarly expanding across the cybersecurity space.

Next slide.

This is the first Company I've been at where we have this concept of a network effect, and I know you've seen network effects like Facebook and Twitter drive expansion and increase usage. It expands the marginal return for each new party that joins, as well as the cost of leading that platform. Let's talk about on the technical side. On the technical network effect, IronNet, at its core, as the General described, is an advanced, AI-driven behavioral analytics platform. We leverage our artificial intelligence and machine learning algorithms to deliver these high-fidelity analytics required to detect these unknown threats, as we've described today. In addition, we provide advanced enrichment techniques via our expert system to ensure great levels of low false positive rates and great visibility, all of it done at network speed and cloud scale.

On the customer network effect, a flywheel is created as more customers join the IronNet Collective Defense. This creates a customer flywheel based around a cornerstone customer. You'll hear that term a couple of times today, cornerstone customers and community customers, who then help us as a result of getting a cornerstone customer to recruit community customers. These cornerstone and community customers strengthen the technical behavioral analytics platform that I described on the technical network effect. By gaining a cornerstone customer, and then having this cornerstone adding community customers, it's better than doing 50 individual sales calls.

IronNet has the ability to convene CEOs and leaders within an entire industry. Example we've already given you—the energy dome. We've been able to convene the top energy companies across the United States and make sure that they're working together in this Collective Defense to defend critical infrastructure.

Some other examples—New York Power Authority where we're bridging and building New York municipalities, the munis and co-ops; Berkshire Hathaway, bringing in their portfolio of companies; and Southern (phon) Company, bringing along their supply chain members, and including other examples like the defense industrial base, so we sell to enterprises and governments.

We first wanted to ensure that we secured enterprise customers first. Then we're expanding in the government. That has been our plan since the origination of the Company.

Next slide.

We describe our go-to-market as land and expand with network effect. Our goal is to land at the top with a cornerstone customer, and then expand out into their respective communities, so as the community grows, the value of our platform grows to each of these customers both technically and commercially. A good way of thinking about our go-to-market is that we're expanding horizontally with our cornerstone and vertically with our community, so once we have a community customer, we have the opportunity to make them into a cornerstone customer, and then expand from there.

Just so you know how we define a cornerstone customer, it's a customer who's a leader of a recognized industry, nation, state, or vertical, so the two examples of this land, expand, and multiply here in the United States, with a U.S.—with the U.S. government with the defense industrial base where we have a large systems integrator, along with a branch of the military, securing their thousands of supply chain members with Collective Defense.

Another example—a large APJ global investment fund that the General mentioned was a customer, and now is an investor, that we expanded from a single portfolio to multiple portfolios, and the goal is to expand in their 600-plus portfolio companies.

Next slide.

Previously, you heard the General describe a full year of data for us in 2020 around what we ingested. We ingested almost two trillion pieces of information and data, and we—that resulted in over 2,000 indicators of compromise for our customers, and what you see on this page is that more and more customers, as they adopt our products, the value to our customers grows, and switching costs will rapidly begin to grow, so one thing I would highlight, it's the same thing that Apple does where people buy iPads, iPhones, and Apple Watch, and use many Apple apps. Over time, it becomes nearly impossible for someone to leave the ecosystem or leave Collective Defense because they would have to start all over again on another platform. At IronNet, we believe that with more customers, our customers will receive an even better product. This will lead to upsell, cross-sell, great pricing dynamics, which, in turn, will help ARR accretion, and in the future, we're going to analyze net retention rate not only on a whole Company basis, but also at a community level basis.

Next slide.

We sell into all elements of the supply chain; companies, sectors, industries, nations, governments. A key insight that General Alexander brought to IronNet was that the leading companies in any industry are in it together whether they like it or not. The weakest link, as some of you have referenced in your questions, can bring down the strongest, and as a result, everyone must work together and be a part of Collective Defense, so we've identified tens of thousands of cornerstone customers, hundreds of thousands of community customers. Of these, we're targeting over a thousand cornerstone customers already with an expected penetration of 40% to get us to our FY '25 numbers. Eight-hundred-and-fifty of those, along with their community customers, will help us achieve $1 billion in revenue. We expect the number of community customers will be far larger than the number of cornerstone, with a ratio of about 13.5 by the end of FY '25.

We have great examples of our go-to-market approach that have already been brought to light; our energy dome, our U.K. healthcare dome, the APJ global investment dome. There are many familiar logos and household names that we've already incorporated into the domes that you see on this page, and companies are beginning to collectively purchase their security out of efficiency and effectiveness. The scale of this is critical, and so we're able to send back insights into thousands of customers at once so everyone in our domes are operating at scale at once.

I'd like to have the General now expand on the user interface that you see on the slide, and how actually this is being done inside of our customer environments. General?

General (Ret.) Keith Alexander

Yes. Thanks, Bill.

We talked about the events that are created by our analytics and that go through our expert system. On the left, you can see an enterprise looking at the whole suite of events that have been created over a one-week period. On the inner circle, you see the red events. Those are ones that are deemed malicious either by the customer or by the expert system itself. The orange are ones that are suspicious, and the bluer ones that were of lesser value, but are out there, and what we do with those is we look across, in this case, it's an energy sector company. They can see other companies in the energy sector in a consolidated view, and in the oil and gas sector by looking at events that they have in common.

If you look at the top event there, it has a red line coming from the enterprise. That company has already determined that to be malicious. The energy sector has one or more companies with that same issue. We'd know the number of companies. It would come up in the numbers, and they see it as suspicious, so they benefit from that knowledge sharing. The next three events that are suspicious, that enterprise has not yet looked at. They gain from that knowledge sharing and crowdsourcing by someone already determining they're suspicious, so that helps everybody work together.

What we're seeing is we add in companies. The number of events that automatically correlated are increasing significantly. This is a huge benefit for knowledge sharing and crowdsourcing. What it will get to is eventually, companies have to look at a fraction of the events that are going on in their environment because others are looking at them and already grading them, that knowledge sharing and crowdsourcing is how we leverage those 900 people in the banking sector to work together. That's part of the future.

This is an area where you can actually play it over time. You could take that one event and you could show when it hit the enterprise and when it hit the energy sector, when it hit the oil and gas sector, you could actually play it over time, you could sweep it back and forth and you can help people understand what's going on and where it's happening.

This is a great opportunity that can actually look at it from a recon perspective, from a command and control, they can look at all the different aspects and parse the analytic and the threat environment and the picture that they're looking at for only those things that they're really interested in. We think it's a great opportunity and a great user interface.

Back to you, Bill.

William Welch

Thanks, General.

Let's go to the next slide.

We're all encouraged by these entities on the slide that trust our platform, whether it's a large APJ global investment fund, whether it's a top agent mobile phone operator, a global European bank, large investment firms, or as the General mentioned, top energy companies. But we're going beyond the enterprise. Our solution is trusted by nations, DoD branches, U.S. state agencies, state and local governments who have very, very strict and stringent security requirements. We're partnering, as you heard earlier, with Amazon and Microsoft, who trust IronNet for our AI-driven behavioral analytics and our Collective Defense.

But this slide is the confidence slide, as I call it. Why I call it the confidence slide is it represents the reason we have confidence we'll achieve the revenue and billings that we presented to you today. We believe we have the ability to follow a similar growth trajectory that my team was able to achieve at Zscaler. We expect to deliver these results by securing multi-million dollar large, cornerstone customers with long contract values that we've already demonstrated and Jamie will share with you in a moment. In addition, we're securing community customers by leveraging our volunteer sales force with our cornerstone customers and partners which expect to deliver contracts worth hundreds of thousands of dollars, each of them bringing into the IronDome.

We're going to show you a brief video with some of our customers and industry leaders that highlight our value proposition.

Video Presentation

John Allaway, Chief Technology Officer
Temasek Holdings

What we're recognizing in domestic is that no single agency has the war chest, the wherewithal, the ability to get access to talent, tools, technology to put the whole thing together. So, we're calling for collective defense. In line with what IronNet's doing with its Iron Domes.

Tom Wilson, VP and CISO
Southern Company

Look, there's a lot going on from the collaboration standpoint, and that need (phon) and focus has always been there for an industry that really collaborates, and some of that intelligence sharing, working with our energy sector (inaudible) while working with our government. We have daily updates from our security operations centers across the industry talking about what's going on so that the end of the (inaudible) of that broader view which is one of the reasons that we (inaudible) of that situational awareness and get away from anything that (inaudible).

We've seen interesting news on things like we have what's called cyber mutual aid (phon) that many, many. You think about normal mutual aid for our industry to where we can help each other against storms, (inaudible) big ice storm, people will come from all over the country to develop this one service. We are implementing those types of concepts for cyber.

John Allaway, Chief Technology Officer
Temasek Holdings

We have people (inaudible) to us. Silver bullets and many opportunities literally all the time and there's a lot of hype in the market. There's a lot of promises that are broken, etc., I think, in the cyber security space and on some wishful thinking, and for us to who are very analytical people and investors, we like proof of life. We really tangible things that we could see. We put the IronNet capability into our environment, and low and behold, the results were as follows:

The IronNet tools then were six times more accurate than any of the other tools that we had in our defenses in terms of detection.

The other interesting thing was speed. We want network speed in (inaudible) and we want to be able to network that out to others. Our existing tool set was taking days/weeks/months. The IronNet tool set, an average of 15 minutes on these attacks to alert us. That time is so precious because the sooner you know someone's in there, the sooner you can contain it, do triage on it, and start thinking about your remediation.

Arno Robbertse, CEO
ITC Secure

IronNet's Iron Dome and collective defense solution helps us, as a more security service provider, and ultimately our clients, do more with less. We're able to scale our security operations center by having a very sophisticated tool that reduces false positives. Organizations are learning that by learning more about the attacks on their peers, they can protect themselves better and they're able to share their information and learn from their information without compromising any sensitive information or any regulatory information internally. We're able to learn from not only attacks on our own organization, but observations across all other organizations participating in that dome. Therefore, achieving the true collective defence, and not only to defend on our own.

Steve Swick, Chief Security Officer
American Electric Power

We're a top target. Having those partnerships and being able to share valuable actual data at the government level is critical for us because we are getting the attacks. The threats are absolutely out there, and we need to figure out how to be able to take that action and give them the picture that you described so they can actually see where those attacks are and then be able to help us address those threats that are over in those threat countries.

Tom Wilson, VP and CISO
Southern Company

While we are a U.S. only entity, we can't have a U.S.-only mind set. The systems that we are all using across both our sector, the unit cross (phon) sectors (inaudible) the same. The adversaries are all the same, so we have to find ways to work together and to share on our common knowledge and our common (phon) experiences to raise the level of all of us, and I look forward to this as we work with General Alexander and IronNet bringing more international companies into the fold to give us more situational awareness of what is happening around the world.

William Welch

As we pull the presentation up, I just want to echo how thankful I am to our customers and partners who are out there everyday obviously securing and helping us transform cybersecurity through Collective Defense.

If we can go to the next slide, that would be great.

As we've gone through our presentation today, we believe that all the points in this slide are pretty self-evident. Our growth is anchored by world-class benchmarks with a focus on constant innovation. The SUNBURST event and all the other events that you've seen in the news recently really has validated our mission to drive AI-driven behavioral analytics and Collective Defense to the overall security market. We're continuing to invest in our platform. Our focus on expanding the sales force will add thousands of cornerstone customers and then hundreds of thousands of community customers. International expansion is another path to grow our Collective Defense communities for the global enterprises, which we already had great success in. Our platform is also purpose-built to leverage additional security technologies in either a buy or a build posture.

With that, I'm going to hand it over to Nancy. But I will tell you we have a very exciting story. We're just at the beginning of transforming cybersecurity through AI-driven behavioral analytics and Collective Defense.

Nancy Fazioli

Okay. Thanks, Bill. We're going to take 15 minutes of Q&A on thego-to-market and sales strategy, and after that we'll have a short break. When we come back from break we'll then hand it over to Jamie for the financial overview.

With that, let's take a look and queue up your questions.

I'm going to pass it over to Mike Cikos. Mike?

Mike Cikos

Hey guys. Thanks again for taking the questions here. Just wanted to come back to it but can you help me define the cornerstone customers that you're talking about? Then the follow-up question to that is, if I think about let's say the oil and gas industries being a vertical you're expanding into versus healthcare versus financial services, are these domes that you're setting up eventually seeing individualized or industry specific AI engines based on the different requirements for them? Can you help clarify that point as well?

William Welch

Yes, absolutely. Mike, great questions. Let me take them one at a time.

First of all, a cornerstone customer to us is somebody that is that leading in their sector, they're a vertical nation, state. For example, it might be the State of Texas, it might be a very large technology company in Europe, or it might end up being, like I said, a very large APJ global investment fund or some of the examples we gave in the energy company. You saw some of them in the video just now. These are the cornerstone customers. These are the ones that not only are bringing together their peer group, like in the energy sector, bringing in the Southern Companies, the Con Eds, the Avangrids, all the different names, but at the same time they're bringing in their supply chains, they're bringing in those areas that obviously are the most vulnerable and trying to protect them. It's not only just in the United States, but it's, as you've heard in the video, it's going at a global level, because as you know the adversary is testing things overseas. That is how we go after our cornerstone is those that are leaders in those market segments that we just described.

As far as the verticals and industry specific, they all have obviously the ability to have their energy dome or their healthcare dome, but then they feed up to a U.S. dome or a global dome to where information is being shared anonymously between their vertical domes, their GO domes or across the globe so that we can get real-time information over to these domes so that they can take action. The technology is the same, whether you're in an energy dome or whether you're in a financial, healthcare, whatever, and the analytics are the same across those different domes.

Mike Cikos

Thanks for that. Then a quick follow-up. Once you guys have identified these cornerstone customers or the community customers that go alongside that, how is it you're approaching these customers? What is the go-to-market process? How long are the sales cycles? Can you walk me through that process as well?

William Welch
Absolutely. Go-to-market, right now, it's very much a direct model. We have been working very closely with partners also, like Booz Allen and Raytheon and Jacob (phon), some of these you've seen announcements already. But our direct models that go after those targeted cornerstone customers, which we have clearly defined, as I mentioned, and our team is in a direct model going after them to secure them. What happens is once we actually secure a couple of them within that space, we actually leverage them to help go get other members. That's what we had in the energy dome, where we started with a few and then we have many and then it's expanding out from there. You can understand that network effect.

As it relates to the actual interaction with a customer, our sales team will go in and do a cyber threat emulation exercise where we'll actually showcase to them what would happen to them if an adversary actually was targeting them. We will do that cyber threat emulation exercise. Usually it takes a couple of days, nothing extravagant. Then in turn, we'll end up possibly doing a proof of value. That proof of value will last no longer than 30 days. The nice thing is because we've already been in their network, where we might be putting in an AWS instance or an Azure and that information, they can go and deploy on the 31st day after they've seen that information and seen the value of our technology.

Very quick time to value, very quick deployment, very quick results.

Mike Cikos

Sure, thanks for that. Then just two more, if I could real quick building on that. The POV that you do over the course of the 30 days, that is in their environment using their data. You're doing this in real-time through that POV process is the first question. The second follow-up, for that process, who is your, for lack of a better term, cheerleader or buyer? Are you pretty much doing this with a CTO, the CISO? Who are you going to?

William Welch

Yes. You described it perfectly, exactly what happens in the proof of value and as far as the target persona. The good news is that we actually have the ability to go to multiple personas. The security operator is certainly interested in the behavioral analytics and the detection and some of that visualization that we showed you earlier with the General. But then the CIO and CISO is obviously keenly interested in making sure that the security operator is more efficient and can get more work done because, as the General said, they have no lack of amount of things that they need to do. The CIO and CISO is very keenly interested in this whole crowdsourcing and the ability to share the information across companies, sectors, nations and states.

Then, certainly at the CEO level they're very interested and the executive team because they're the ones that are being asked, the question of the board is, are we secure? That's where the General mentioned our ability to go do threat defined queries, so when a Colonial Pipeline happens or some of these other incidents of compromise, our ability to go in there and say, "No. If this had happened, you are already protected. This is what the result set would have been."

Mike Cikos

All right. Thanks, Bill. I'll turn over the mic, guys.

William Welch

Thanks, Mike.

Nancy Fazioli

Thanks. Bill, we have a question in the chat from Jon Ho at William Blair. He wanted to ask if you could please talk a little bit about the channel engagement and how IronNet is rising above the noise from folks like Darktrace and Vectra. That's the first one.

William Welch

Yes. We're very, very encouraged by the traction that we've had already in the channel. You've seen some announcements recently with Jacobs where we're working with them on some of their portfolio captures that they've done not only in the state and local market but also the U.S. government. We also have great, as you saw in the video, partnerships over in EMEA and also in APJ. It's not just here in the United States. What I will tell you is that these partners do a great job of helping us with deployment and the governance and the policy management, making sure that companies are coming together and working in the dome.

Those are just some of the examples that we've seen with our channel.

As far as the competition, I will tell you the differentiator goes very similar to my days at Zscaler is, we would compete on a secure web gateway with the technology companies that Gartner put us with but once we competed in that space we set the vision for cloud security. It's the same thing in IronNet. We will compete head-to-head in an MDR bakeoff, the network detection and response, and we've done that. As a matter of fact, we have an example recently of a very large state here in the Northeast that did a competitive bakeoff we saw an adversary in the network, our competition didn't, they went dark, just a point of phrase there, and what I will tell you is that on an MDR head-to-head, we are beating the competition because we are at a behavior-based while they're still legacy signature.

Then the last thing I will share with you as far as our winning against our competition, is that they love the idea now of not only just absorbing our IronDefense or behavioral analytics, but that Collective Defense to where they can actually get that leveraged network effect of other security operation center experts to help them with these indications of compromise.

Jonathan Ho

Thank you for that, Bill. A follow-up question would be, how much of your customer base value proposition comes from the automated threat detection and the crowdsourcing on versus maybe things like manage threat hunting and response, just having that support sit behind the efforts that a lot of these overwhelmed IT people face?

William Welch

Yes. They're very encouraged by obviously our ability to detect and given the analytics and the network speed and obviously at the cloud scale, but I think the other thing that they're very encouraged by and we've seen this with our CIAC, as we call it, where we actually have some of our hunters that are engaged with their security operation centers. We have a small, very small services part of our business, but where we're actually coming alongside them to show them what is the most effective way to do threat hunting, the most effective way to make sure that they're leveraging the tools.

As you heard in the video, where one of our customers had over 90 different tools, we make sure the efficacy of the technology is leveraged appropriately so that there might have been things that they were missing that they should have had a certain firewall where we could have showcased that to them as a result of our detection and analytics. As a matter of fact, one of our customers we're very grateful for, they're so trusting of not only our detection and analytics and also our hunters, that they automatically take our response and our recommendations, put it into a ServiceNow infrastructure and then immediately send it to their help desk to deploy the remediation that has to happen at the network level.

Jonathan Ho

Thank you.

William Welch

Not on mute, Nancy. Are there other questions?

Nancy Fazioli

Sorry. Next, Nehal Chokshi. You may be on mute.

Nehal Chokshi

Now you can hear me, right?

William Welch

Got you.

Nehal Chokshi

All right. I have two questions. One question's on financials, but I assume that we're going to have a financials section so I shouldn't ask the financial question here. Correct?

William Welch

Correct.

Nancy Fazioli

Correct, (inaudible). Thanks.

Nehal Chokshi

The first question then is on—I like the Slide number 10 here. It I think provides the layers of differentiation. I love that you have it in a nice visual here. I think one of the key things here that you're talking about is that you have the cornerstone customers and then you have the community customers. But when you think about large cybersecurity players, they effectively already have this. The rest of this is effectively algorithms that they can potentially replicate. Can you talk to what you believe will be your sustainable differentiation as some of the larger cybersecurity players come in and see what IronNet is doing and saying, "Hey, this is a good idea. We can replicate that." What will stop them from doing that given that they already have effectively the community in place?

William Welch

Yes, actually, I'm going to ask the General to come alongside me on this and explain what we've observed with Palo Alto and CrowdStrike and what they're doing in their own environments versus at a collective layer. General?

General (Ret.) Keith Alexander

Yes, thanks, Bill. What they do is important. They grab all this information and they take that information, they use it to update your analytics. I did get a good clap for that, I think, as that went through. What they're doing is they see an event, they say, okay, I want to now block that, I'm going to create a signature and I go after that.

What we do that's different is we're not taking the knowledge and then changing our solution to just a point; we're sharing that knowledge amongst all our customers. That knowledge sharing and crowdsourcing makes their analysts better. They learn as we learn in a collective group. That's an important differentiation. You don't see that. Although, and I think the world of Palo Alto and their WildFire database and what they're doing and how they're doing it, that's great, but that's what they use, it's not something their customers can easily use to gain knowledge and grow. Does that make sense?

Nehal Chokshi

Yes. Thank you.

General (Ret.) Keith Alexander

Okay.

Nancy Fazioli

Great. Thanks. That is—we're going to take a five minute break now. We'll be back at quarter to two for the financial section. Thanks.

William Welch

Hey Nancy. Are you going to respond to Jonathan's note there that came in the chat?

Nancy Fazioli

Yes, I will do.

William Welch

If you could respond, it was very kind of him, that note he sent. If you could just respond to him. I didn't want to do it.

Nancy Fazioli

Okay.

William Welch

Thank you. Are we ready?

Nancy Fazioli

I think we can go. Jamie?

James Gerber

All right. good. Welcome back, everybody, and thank you, Bill, thank you, Keith.

Our revenues have grown steadily since our first product release in 2016. We made our first moves to the cloud, as you've heard, in 2018, and are excited about the new packaging and scalability that we'll be getting from our updated cloud versions already coming out now in a general release early next year.

This evolution in our product allows us to deploy to customers more rapidly, scale more quickly and drive our revenue growth. Like our comparables, revenue is heavily software product focused with a small layers, as you've heard, of services. Over 80% of our product revenue is from the private sector. That is our focus. but the government market is largely untapped and we're ramping up rapidly there too. Already 35% of our software product revenue is international, whether regional presence, in APJ and EMEA.

Let me elaborate as well on why we're so confident in our revenue increase now with $55 million this year.

We've primed the pump with well over 50% of that revenue coming from customers already under contract. We have an experienced sales force and enablement team already in the field with 24 fully ramped sales reps and more coming on board.

We also have strong KPIs and strong tailwinds behind us that you've been hearing about. IronNet has a strong recurring revenue base with sticky customer relationships. Our average contract length is over three years. For those multiyear contracts, we often receive payment upfront, greatly facilitating cash flow. Our margins are strong and will continue to increase driven by falling compute costs with our latest generation cloud-based platform. We already have built a solid net retention rate over the last several years, which is similar to where CrowdStrike was at its point in its growth. We expect that net retention rate to improve similar to our comparables to 120% by Fiscal '25.

Because our long-term contract terms have less frequent renewals, this is currently a three-year average. So we expect to start to provide quarterly updates on NRR once those frequencies of renewal will increase. In the meantime, and as we initiate our regular reporting, we'll be using the more aggregate ARR measure to show our overall growth performance over time.

Next page, please.

On the financial metrics page, let me orient this for you.

Rob did a great job upfront reminding you that Fiscal '22 is our current fiscal year. It began February 1. Our revenue is expected to be nearly $55 million this year, with over 80% growth going into fiscal '23.

On this slide, we lay out the specifics on our revenue and margin growth that we'll be driving with the additional capital from this raise. From our earlier financial deck you'll see that we have updated Fiscal '21 with actuals, now showing that we exceeded our revenue and gross margin forecasts. We met our objectives on sales and marketing spend, decreased research and development slightly as we reorganized our engineering departments towards our cloud-based and increasingly SaaS delivered software offerings, and except for $1.5 million of one-time charges relating to our response to COVID restrictions and becoming an all virtual company, our G&A would have declined to $19.8 million or 68% of revenues. We like exceeding our expectations here and we're pleased to add in those actuals.

As you can see, from a percentage of revenues perspective, we'll continue to invest, particularly in sales and marketing and R&D, along similar lines as our other high growth comparables, coming down over time on those metrics into the 60%, low 30% and 20% levels, respectively, for our various operating expense categories, while continuing to expand our gross profit margins. Significantly, I want to highlight several factors in that go-forward investment.

We've invested in sales and marketing spending already, starting in calendar 2020 to capture the current market opportunities that General Alexander and Bill described. Take note of the sales and marketing line. We nearly doubled sales and marketing spend in calendar '20, which supports our growth going into this calendar year '21. We plan to use our additional capital to invest more into our sales team and to continue to grow the business.

IronNet's network effects make our business model more efficient than our high growth comparables because our cornerstone customers also drive sales. You've asked some great questions in those areas. Like our high growth security comparables, we're focusing our capital to grow our revenue given the huge TAM and market opportunity in network effects.

On the R&D line, R&D investment will continue to be focused on developing additional features, (inaudible) options, covering of different communications media and sharing functionality. We already cover physical networking and cloud deployed application medians and are already deployed on telecommunications' backbones to detect abnormalities in mobile device traffic. We've already also shown efficacy against ad fraud types of traffic and expect that our ability to detect and to automatically enrich and cross-analyze threat behaviors as the variety of customer communications expand will remain priorities for our R&D teams.

It is that feature set expansion that will not only continue to solidify the leading position that we have as we grow into our expanding TAMs, but also to add to those feature sets the ability to increase expansion and future upsells into our existing customer base to expand the NRR.

Having our cyber operations center embedded within our R&D teams—sorry, with our R&D teams, will assure that our product remains highly informed with techniques and findings developed by our (inaudible) teams and that our customers remain constantly scanned with the most updated analytics and with the latest in specialized threat defined queries to give them confidence that their communications networks, data and operations remain clear of potentially damaging threats.

On the cash flow slide, as we'll cover more extensively on the next slide, upfront payments on our contracts will also to help fund our growth. Given our current level of revenue and expected path to profitability, we expect to reach cash flow breakeven within similar timelines to CrowdStrikes, Zscalers and Cloudflares based on their progression. We also have invested strongly in R&D to continue to upsell our customers, win new customers and outperform other security products.

Our model lends itself to the fact that there is a large TAM out there and a massive opportunity to grab market share in the underpenetrated MDR segment, and like every high growth security name, our focus is going to be on the top line as work ourselves to a cash flow breakeven in the outer years. Our game plans are clear. Based on benchmarks of other high growth security companies that have gone before us in the same growing TAM that we're pursuing, the additional capital we'll be garnering through this de-SPAC combination will be a key accelerator to our growth.

Next slide, please.

In addition to what we've shown in previous decks, we have introduced within ourS-4 both the ARR and billings metrics. We did want to show you what those components of our going forward model were.

We have updated the Fiscal ‘20 and ‘21 bars on these graphs with the actuals from theS-4 that we recently filed. ARR is defined more broadly, that is usually the case, to capture the recurring nature of our contracts, regardless of the subscription or analytic support renewal contract forms. We’ve been standardizing those forms and that is a key element to our scalability, but ARR makes sure that regardless of contract form that we get to show the add-ability to continue to layer on our recurring revenues, one cohort on top of another.

Substantial growth in recurring revenue in Fiscal ‘21 as we completed the transition of contracts fromnon-recurring to recurring revenue is a really important element of that. Leading up to Fiscal ‘21, we did have more non-recurring components to our revenue, but we have completed that transition now and that’s a really significant element in our ARR growth for Fiscal ‘20 to Fiscal ‘21 and coming into Fiscal ‘22.

Until contract renewals develop sufficient frequency for us to present NRRs, I’ve noted, as a regular reporting metric, we’ll be utilizing ARRs as our primary indicator of the annualized run rates of revenues reported and of the ACBO (phon) contract signed during the quarter as an indicator of forward revenue. As we complete our transition to a SaaS-based model, we expect ARR growth to continue to be driven by the three underlying key growth factors: retention and upsell with our current customer base, attraction of new cornerstone customers, and expansion to smaller related companies through the community cornerstone effect.

On the billings metric, again, like many of the high growth security companies in the sector, we’ll continue to have the benefit of payments upfront on our contracts and this will be the metric that will help to show that. As many of our contracts continue to be multiyear, we will often also be paid upfront, as noted, for those multiple years, all upfront instead of just for a single year. Of course, we’d like the multiple year upfront payments as they’re clearly favorable to the cash flows of our business, but what we’ve modeled here is just one year or 12 month annual upfront payments. We do have an opportunity to outperform on this metric as well.

With that, back to you, Bill.

William Welch

Thank you, Jamie.

Let’s go to the next slide.

I just wanted to share with you some of the insights as we think on our operational benchmarking.

We think of IronNet as a transformation security company, but also a data analytics company given the amount of data ingest and the AI capabilities of our platform. On this slide, we’ve done comparables against traditional security companies like Zscaler, CrowdStrike, but also data analytic companies like Palantir (phon) and C3 AI. We compare very favorably with these names on the slide in terms of growth and have similar software gross margins.

As I’ve shared, I started at Zscaler when it was not a household name, much like IronNet today, but as you’ve seen, the customers and shareholders have been rewarded for their confidence in transformational companies, like we are doing with Collective Defense. We believe the market will position IronNet at the unique intersection of security and analytics, both of those sectors exhibiting great opportunity.

I’m going to let Rob now take you through the valuation benchmarking and some other areas.

Rob LaPenta

Thank you, Bill.

I think, from our perspective, and I think you'll share that the Company's core capabilities places it squarely in this ecosystem and sets it up well to be an integral player in the cybersecurity landscape.

I think a couple of points which I think really worth mentioning. We referenced it. The Company's offerings serve as a complement to many of these offerings of some of these very sophisticated cybersecurity solution providers. We're complementing what they bring to the table and also the threat intelligence market, we are also expanding it. We're really in a good place when it comes to the market dynamics.

As an investor, I look at the investor platform. We've got a high growth, hard to replicate business model, the network effect of cornerstone customers, implementation of behavioral analytics versus the traditional signature, and an experienced Management team, which I think is really key in cyber, which is such a, for lack of a better word, dynamic ecosystem. But we're coming to market here at a significant discount and some metrics here, over 50%, a lot of these have been updated from our prior presentation. These are reflecting stock prices and valuations that are more current. There is some discounting here.

If you go to the next slide, I think what this can show is where we are mapped against some other metrics and I think, again, it all comes down to execution. We spent a lot of time with this Management team and we think they are really well positioned with their experience in both commercial, government, building, private, public, to really make up this valuation gap and really create a lot of shareholder value and really create value for everybody involved here.

Really like the set up as an entry point as well. Then the next slide I think just gives you some more color. Again, a very substantial commitment from the existing shareholder base of IronNet, rolling a significant amount of equity, all their equity, will own 72%. You could see on the next slide that the PIPE shareholders own about 10% and then the LGL trustholders about 14%.

I don't know if that's still on this slide to get to the next slide.

William Welch

Yes, it is.

Rob LaPenta

Yes, there it is. That really shows you the EV build and again pro forma equity ownership post deal.

I think that's back to you, Bill or General.

William Welch

Thank you, Rob.

Team, I hope today we've really discussed a lot of these key themes, whether it's a large and rapidly growing TAM, a transformational platform, an experienced and great Leadership team, compelling financial profile and then, most importantly, a cybersecurity company with a mission. We have a founder and chairman of the board that has been mission oriented since he began his career. IronNet is committed to protecting societies through security for global industries, governments and healthcare providers. We're thankful that we have this opportunity to transform cybersecurity through Collective Defense.

I did want to hand it over to the General for some final words before we give it over to Nancy for questions. General, over to you.

General (Ret.) Keith Alexander

Thanks, Bill.

In closing, I want to say that I founded IronNet to fill a national need and opportunity. We brought in Bill and team to help us execute on this vision and I'm with the Company for the long term to build a billion dollar company and beyond.

Thank you, everybody, for your time and participation. Over to you, Nancy, for the next part.

Nancy Fazioli

Great. Thanks, General.

We'll go first to Josh Sullivan. Josh? Might not have—are you able to talk, Josh? Okay, there you go.

Josh Sullivan

Yes. Can you just expand—Jamie, you made a comment about the government end market there. Can you just talk about exposure now and going forward, maybe which agencies or programs are some of the cornerstones in that land and expand strategy? Then maybe, did you see anything in the Biden defense budget request that supports that? Any specific line items that we can look through to call out?

Nancy Fazioli

Bill, do you want to start with that one?

William Welch

Yes. A couple of things. One, we're very excited about the executive order and how it really is talking more and more about the public and private partnerships. I will tell you that we've been very encouraged by what we're seeing also in the defense industrial base within the DoD and the Federal Government. That is the first and most critical area for defense. Obviously, there's a lot of intellectual property, a lot of very important things that we're trying to do as a country. We're seeing some great success there.

We've already had some very good wins within the government, especially within the DoD sector. We are also in the final phases of our Fed ramp status to make sure that we can go across the entire civilian government. Then, more importantly, I will tell you we're seeing a lot of interest at the state and local level in higher ed, whether it's within Texas, whether it's in New Jersey and New York. I can give you example after example of not only customers we've already secured, but even in expansive pipeline in the same local.

I don't know, Jamie or General, if you have anything else you'd like to add.

General (Ret.) Keith Alexander

I would just say that we are seeing, as Bill said, a lot of traction and it's growing. It's interesting that we're seeing the cornerstone and some cornerstones bringing the community along with them. We think that's going to be really part of the future when a big company comes in and says, I need just to secure my supply chain. Can you help me there?"

Great opportunities. Thanks, Bill.

Josh Sullivan

Maybe just as a follow-up, how does IronNet beat out x, y, z government service contractor coming in with low cost, technically acceptable database of cyber tech vectors for communal use? How do you combat that approach to communal defense going forward?

William Welch

Josh, I'm not going to say that we're not going to see that but I will tell you in the early stages right now we're very encouraged by the partnerships that we've seen, like with the likes of Jacobs and Booz Allen, Hamilton and some of these you've already seen in some of our public press releases. We're actually seeing a lot of them coming and approaching us even more of the behavioral analytics and obviously the pedigree of the talent that is at the Company.

They see a great collaboration and partnership that we're working together where they can bring their expertise and their talent with services and people alongside our tech.

Josh Sullivan

Thank you.

Nancy Fazioli

Thanks, Josh. Going next to Taz Koujalgi.

Imtiaz Koujalgi

Hey guys. Can you guys hear me?

Nancy Fazioli

We can hear you.

William Welch

Absolutely.

Imtiaz Koujalgi

A question for Jamie. On the financials, can you give some clarity on the revenue model? You said that most of the revenues are recurring, but are these term licenses that need to be renewed every year? Are these perpetual licenses and maintenance go along with that? Just some clarity on the revenue model would be helpful.

James Gerber

Yes. I made reference to the recurring revenue through a scalable contract form. Almost all are now in the subscription form and most are in multiyear forms of that. We do have some legacy customers that started out years ago with perpetuals, and for them, their contract model, the recurring component is all the analytic upgrades. Even from the beginning of those, that was a very high percentage of the perpetual component. But those have now renewed all completely and are just on that analytical upgrade portion, even for them.

Imtiaz Koujalgi

Got it. Then just one more—two more for me. The NRR, that number's pretty impressive, almost I think 100% over the last few quarters. Is that just renewals or is there an upsell component of that NRR metric included?

James Gerber

Yes. There is some upsell that's in there. We are actually quite gratified to have a nearly 100% at this stage of our growth, with very little upsell actually kicking in quite yet. The form of our product and packaging now really will increasingly lend itself to more upsell opportunities. That's what's really going to drive us here over the next few years.

Imtiaz Koujalgi

Thanks, Jamie. One last one and then I'll cede the floor. Your projections for Fiscal '22, there's a big jump in your revenue growth, almost from 26% last year to 87%. I see that you're investing a lot in sales and marketing, so maybe that's one of the catalysts. But if I go back and look at your sales and marketing growth, that's not changing that much. There's no big inflection there, but you're showing a big inflection in your revenue growth expectation. Is there anything else that's driving the big inflection in revenue growth apart from just sales and marketing?

James Gerber

Yes. I think there's some timing involved there. We made our big investment in the sales and marketing team last year. That's why that big kick-up last year. But that's also while we were seasoning that sales team and getting them into fully ramped status coming into this year.

We're not actually having to add that much in sales and marketing this year to go hit our number. We are adding some more to continue to grow out in the out years, but I think it's really just a little more of timing that we actually started that investment last year.

Imtiaz Koujalgi

Thank you very much.

Nancy Fazioli

Great. Thanks, Taz. Next we'll move to Matthew Galinko from Sidoti. Matthew?

Matthew Galinko

Hey, good afternoon. Can you hear me?

Nancy Fazioli

We can hear you. Thanks.

Matthew Galinko

All right, thanks. One, I was hoping if you could just clarify quickly on the payment cycle on the contracts. I think I heard occasionally upfront on a three years post to annually, but what's the typical cadence there today?

James Gerber

Well, actually, if it's a three-year we almost always get paid all three years upfront. There are some contracts that go multiyear that just go on an annual billing. But that's actually the lesser of the contract payment types in our mix. We most frequently actually get the full amount upfront for however many years it is and we've had some that recently renewed last fall for five years.

Matthew Galinko

Got it, thanks. Maybe going back to the last section for myfollow-up. You touched on expanding TAM through M&A. I was hoping you could go a little bit further into the strategy or philosophy there. Are you thinking that you could be maybe more effective at data collection or more effective at incident response by having maybe an endpoint position, or are you more effective at data collection, drawing into the dome ultimately? If you're in the endpoint, just how do you think about M&A and how it fuels your strategy?

William Welch

Yes. Matthew, certainly it is an area that all companies look at. I will tell you that we're looking at M&A really from two lens. One lens is how it's going to expand our product road map and accelerate that road map and whether that's with getting additional engineers or whether that's, again, moving in our road map modules faster in order to increase our net retention rate and upsell. Then second is, are we going to be able to add some level of accretive ARR?

Those are the two lenses that we will look through and really stay in our space around behavioral analytics and our Collective Defense. We're very thankful for the relationships we have with some of the leading endpoint vendors like CrowdStrike, and we'll continue to maintain them.

Matthew Galinko

Great. Thank you.

Nancy Fazioli

Thanks, Matthew. Next we'll go to Nehal Chokshi.

Nehal Chokshi

Thank you. Hi. Thanks. I had four questions actually. In your net revenue retention rate slide there, you have a big pickup from Fiscal Year '24. I heard 10% to 120% in Fiscal Year '25. What's the rationale for that big pickup there?

James Gerber

Yes. That's actually not at all atypical for our comps. You'll know where our game plan came from for adding those elements of upsell. It is in terms of increasing NRR. It is the blocking and tackling, three yards in a dust of clouds but—cloud of dust, but it is that incremental feature set. It is that expansion from one subsidiary to multiple subsidiaries that is what our customer success team will be doing, just like how this is done, to go ahead and steadily increase that upsell set that drives NRR from that 100% on up. We are blessed with really upper end of the pyramid types of customers. We're not exposed to the kind of churn that some of the companies that focus and sells very heavily on SMB are doing. That's going to be a plus for driving our numbers up. But the key is always just making sure that you're doing that volume and feature set upsell.

Nehal Chokshi

Just to be clear, when you're talking about net revenue retention rate, are you talking about customers that renewed within that year or are you talking about all customers that have an active contract?

James Gerber

Yes. When we start to report that we're going to do it the way it's classically done, which is to focus on customers that are renewing within that period, or upselling within that period and not putting the existing customers in that base if they're not doing anything.

Nehal Chokshi

Got it. Understood. Okay. What is the time to ramp sales and marketing investments to full productivity?

James Gerber

That's a sales rep ramp. Maybe, Bill, you want to cover that one?

William Welch

Yes. Nehal, in the beginning I was seeing about nine months. We have actually moved that down to six months. We're now getting fully ramped reps within six months.

Nehal Chokshi

Got it. Okay. All right. I think you already answered this. Last question is is that for your fiscal '24 and '25 revenue ARR and billings projections here, is there built into that the flexing of pricing power that, Bill, you had discussed that you believe that you will have as these communities build out?

William Welch

Yes. Certainly I think there's a lot of different ways that we can see those dynamics change. Number one is additional modules. As we add additional modules obviously we have additional pricing mechanisms we can add in as they adopt additional technologies as part of the platform. I also believe that as a result of building out these domes, our ability to bring, in one fell swoop, for example, 50 or 100 supply chain members, where either the cornerstone customer may pay for them, or then instead of going out to 50 individual sales calls. There's a bunch of different pricing dynamics that we have the ability to flex on.

Nehal Chokshi

Okay.

James Gerber

I would just say on the model side that we have not been assuming that we're going to be raising our pricing. This is make ourselves efficient for our customer and that's going to continue to be a watch word for us. We have not assumed exerting any pricing pressure in this model in any way.

Nehal Chokshi

Great. Thank you.

Nancy Fazioli

Thanks, Nehal. Moving next to Mike Cikos. Mike?

Mike Cikos

Hey. Thanks again for taking the questions, guys. Just building on that last comment, and I understand the value you are bringing to your supply chain partners on. But do you guys have any examples currently where customers come on board and brought 50 to 100 supply chain partners in one fell swoop?

William Welch

Yes. I'd say we're about to. We're finalizing a contract now exactly like with that model and that's why I referenced it.

Mike Cikos

Awesome. Okay. If I could also just build a couple more questions on the sales and marketing investments you guys have as well. There was mention of 24 fully ramped sales reps and I'm imagining that these are quota carrying reps that you're referencing here.

William Welch

Correct.

Mike Cikos

Is that at the end of Fiscal '21? Can you help us get a sense of how quickly that has ramped, what is that building off a base of, or what are the targets to ramp those reps to by year-end, something like that?

James Gerber

Do you want me to jump in there, Bill?

William Welch

Yes, go ahead, go ahead, Jamie, because I was actually looking for the—I had this all in front of me but go ahead.

James Gerber

I'll let you get in there and add to it. Remember, we weren't coming out from six sales reps coming out of fiscal '20. The 24 was what we came in to this fiscal year with. At the end of '21, which is, say, our fiscal '21, which was back in January, we're coming into this year with 24 fully ramped quota carrying sales reps. Those we are adding to this year and I can go into some of those plans as well. But just to clarify, Bill, (inaudible) for anything he might add, we're coming into this year with that sales rep base already included.

William Welch

That's correct. Mike, what I thought you were asking—and my apologies, I didn't get right to my answer, was I thought you were asking by quarter, because I actually have it here in front of me where we went from three, then added another two, then six, then eight, because by quarter I see how many reps are then fully ramped, and as Jamie said, as we finish the calendar year, we had the entire sales team fully ramped, but as you can understand, based on their hiring, it was a ramp over each quarter, if that makes sense.

Mike Cikos

Yes, it does. I'm also just trying to gauge, so if we have let's say these 24 quota carrying reps coming into the new year, what's the support staff for those reps look like and then there's—sorry, answer that first and then I have another one.

William Welch

Yes, no, so it's really a franchise model that we're incorporating. You have a systems engineer usually at atwo-to-one ratio, and then depending on territory, obviously, over in EMEA and APJ we have to watch the language and that, but what I will tell you, it ends up about two-to-one. Then we have our inside sales and SDRs, our sales development reps, where they're supporting somewheres around three to five reps out in the field. We'll continue to ramp them, those inside sales reps, so we can migrate and mentor them out into the field, and then we run on average at a leadership level about an eight-to-one ratio of sales management to reps.

Mike Cikos

Understood. Just the last question for you. Thanks again for the time. The question is around the productivity inefficiency. I know that you guys have discussed being able to compress that time to reaching productivity. We went from nine months down to six months now. Just to ensure that you guys are still maintaining those productivity levels. Can you just discuss how you're building this in so it's in a repeatable fashion and something that you guys continue to execute on?

William Welch

Yes. Jamie, I'll let you comment on what you see as far as some of the productivity numbers, how they've been ramping over the years. But the one thing that we're most encouraged by is that we're seeing very, very, as Jamie has said, large multiyear contracts. We actually do reward our sales team to paying them a multiyear contract. While they are compensated and quoted on one year ACB numbers, we are actually also compensating them from an additional bonus for years two and three. That's also helping us with our productivity.

Jamie, any other comments?

James Gerber

Yes, I'd just say you all will be familiar with sales rep productivity in this space, so you won't be surprised that that's a 1.2 plus per year type of quota carrying that goes with that, with those reps. That does of course vary by territory and you know where that goes as well.

I would just note that in addition to sales development reps and the sales engineers, we do have a really solid sales support team that's also out there facilitating the sales team with sales enablement. We've really built this out with a group of real pros that know how to do this, marketing well tied in on messaging and lead gen and customer success really focusing on that quick time to value.

It is a team effort, beginning to end, and the quota carrying reps, the tip of that spear, but it's that really whole team that's driving it.

I hope that gives you a little more color.

Mike Cikos

It does. Very helpful. Thank you, guys.

Nancy Fazioli

Thanks, Mike. Next to Gray Powell. Gray?

Oh, Jonathan, go ahead. I think...

William Welch

Jonathan jumped in front of him.

Nancy Fazioli

Somehow it's my error. Sorry.

Jonathan Ho

I'll just go ahead. Gray, my apologies for somehow getting bumped up. Just in terms of when we look at the five-year potential growth rate, is there a way for you to unpack or maybe help us understand how much is driven by maybe factors like adding new customers versus penetration of your existing customers versus potentially selling new products? Can you just maybe weigh that out in terms of the top three or four things and how that potentially drives that accelerating growth rate?

William Welch

Jamie, I think you're on mute.

James Gerber

It is working—or it was. Okay. Yes, I think the primary vector for growth here for us in our model to really get to the super core is that attracting the cornerstone customer. That's the thing that we have established really strong line of sight towards. As Bill mentioned, we already have in our ABM model the thousand cornerstone customers globally that we're going after. It's a little bit over 400 of those that we built to by our Fiscal '25 number to get there. Now they bring along community and that ratio will continue to expand as we go, but that's going to be—there will be probably in our model be about 8 to 8.5 community customers for every one of those cornerstone customers. I think that's vector number two.

Then vector number three is that increase in NRR, which is, I think, we take comfort in the fact that in the way we've built our revenue model here that that is number three. That, however, really can be a really important driver in and of itself. We'd like to think that that's going to be a nice component of upsell—sorry, upside to where we can drive that. I think doing quite a bit more with the government sector customers than what we've built into the model as well is probably another underweighted component.

Does that also give you a little sense of where the key drivers for revenue are coming from?

Jonathan Ho

It does. That (inaudible) is always helpful from a (inaudible) perspective. Just onefollow-up on—your spending on R&D is significantly higher even in the out years than some of your (inaudible) competitors. Why do you need to spend more and do you see most of the opportunities to leverage that investment to maybe further widen the gap or is this unique functionality that your customers are asking for today? Just want to get a sense of how mature the product and the platform are.

William Welch

Yes. General, you can go first and I'll come alongside you.

General (Ret.) Keith Alexander

Okay. That's a great question, Jonathan. I think talking to some of our peers and CEOs in the market, some of them said they underinvested in this area and they're paying for it now, because they don't have the team ready to go in the next generation product. Add to that the fact that machine learning and AI is really making a strong jump in presence in what we're doing specialty. We believe that this investment in research and engineering is going to pay off. We're seeing we have some tremendous opportunities coming in, what we call our IronNet 2.0 and other things coming down the line.

I think it's really good. Bill and I both talk to some of these and our friends that are out there and they say, "Yes, we kind of screwed that up. We went with a great sales force and now we're stuck with a product that's outdated."

Over to you, Bill.

William Welch

Yes. I would actually—and I think I'd rather be accused of spending too much than too little. I know my competition has that in spades, where they spend not enough in R&D. What I will tell you is that we are an innovation engine company. We are constantly looking for innovating the platform. I don't think it's a matter of shortcomings. I think it's a matter of seeing what's around the corner. I learned that valuable lesson from my Zscaler days is, what is the next two or three modules that we are investing in in market segments?

We will continue to put money into that area.

James Gerber

I think—if I could just come alongside, Mike, to go see (inaudible). I think the invest in R&D model that's most relevant for us here is CrowdStrike. CrowdStrike was at the 46% of revenue level as they were passing through $100 million in revenues, and we're forecasting and built our investment rate at about that level as we go through $100 million ourselves.

I think they have been well rewarded for not only staying out in front of the investment and sales and marketing but also their R&D. I think you'd probably look more to how they've been attacking that continued investment in R&D just from a comparable reference basis.

Jonathan Ho

If I can just have one last question. Bill, you joined the Company relatively recently. I just wanted to understand what opportunities you saw to mature the sales process and help drive this accelerated growth. What were some of the low hanging fruit that you saw and that you've been able to execute through in that timeframe? Thank you.

William Welch

Yes. Jon, that's a great question. I will tell you, this reminded me so much as far as where it was on its maturity model of when I joined Zscaler, when I joined two years ago and saw that—when I joined IronNet, I saw the trajectory, but I also was most encouraged by the mission. This is an opportunity really to transform cybersecurity. I've been selling cybersecurity technology for more years than I want to admit on this call, and I will tell you, even with all that great technology that I've been able to be fortunate to be a part of, we're still not as secure as we should be. The nice thing about it is when I see people like the Colonial Pipeline and companies like that, these are not—they didn't do anything wrong, they are victims, and this was something—this is an opportunity for us to really come alongside these companies because there's no company out there that can compete against an adversary of the likes of Russia or China or some of the other ones that you're seeing.

This is an opportunity for us really to think differently, which is what I was excited about joining IronNet, number one. As far as the transformation of the Company, it's all about making sure everything is visible, predictable and repeatable, which is what we've been doing. Number two, it's about making sure that we are benchmarking ourselves. Opinions are great, but I want to benchmark ourselves against everybody out there from a world-class what you can see, and not only have we done our models, but how we've built out the Company in every single department.

Hopefully that answers your question.

Jonathan Ho

Yes, thank you.

Nancy Fazioli

Thanks, Jonathan. Thanks for nimble there. Gray, we'd like to turn to you now.

Gray Powell

All right, great. Thanks. Thanks for working me in. Can you hear me okay?

Nancy Fazioli

Yes, we can hear you.

Gray Powell

All right. Thanks. Yes, so maybe back on the ARR ramp, how should we think of the linearity in ARR for Fiscal '22? Can you give us a sense as to where you were at Q1? Then how much of that ramp do you have visibility on with the pipeline today versus what you have to go out and win over the next eight months?

William Welch

Jamie, go ahead.

James Gerber

Yes. We'll be putting out our quarterly numbers here before too long and theS-4s. I hope I can get—have you be a little patient for that as we do our next releases on that.

We continue to have—be blessed with some really large opportunities that are getting bigger right at the moment. I think what we're focused on is that ARR built through the year and we like the momentum we're seeing here.

Gray Powell

Okay. Thank you.

Nancy Fazioli

Great. I'll give it a second to see if there's any additional questions.

I think that wraps it up. Thank you, all, again, for your time and participation today. That concludes our Analyst Day, and have a good afternoon. Thanks again.

William Welch

Thanks, everybody.

Important Information and Where to Find It

This transcript relates to a proposed transaction between LGL Systems Acquisition Corp. ("LGL") and IronNet. LGL has filed with the Securities and Exchange Commission ("SEC") a registration statement on Form S-4 (the "Registration Statement") that includes a proxy statement to be distributed to LGL's stockholders in connection with LGL's solicitation of proxies for the vote by LGL's stockholders in connection with the proposed business combination and other transactions described in the Registration Statement, as well as a preliminary prospectus relating to the offer of LGL's securities to be issued to IronNet's stockholders in connection with the completion of the proposed business combination described in the Registration Statement. After the Registration Statement is declared effective, LGL will mail the definitive proxy statement/prospectus to stockholders of LGL as of a record date to be established for voting on the proposed business combination. LGL also will file other relevant documents from time to time regarding the proposed transaction with the SEC. INVESTORS AND SECURITY HOLDERS OF LGL ARE URGED TO READ THE PRELIMINARY PROXY STATEMENT/PROSPECTUS AND, ONCE AVAILABLE, THE DEFINITIVE PROXY STATEMENT/PROSPECTUS AND OTHER RELEVANT DOCUMENTS THAT HAVE BEEN OR WILL BE FILED BY LGL FROM TIME TO TIME WITH THE SEC

CAREFULLY AND IN THEIR ENTIRETY WHEN THEY BECOME AVAILABLE BECAUSE THEY CONTAIN OR WILL CONTAIN IMPORTANT INFORMATION ABOUT THE PROPOSED TRANSACTION. Investors and security holders will be able to obtain free copies of the proxy statement/prospectus and other documents containing important information about LGL and IronNet once such documents are filed with the SEC, through the website maintained by the SEC at http://www.sec.gov. Copies of the documents filed with the SEC by LGL when and if available, can be obtained free of charge on LGL's website at https://www.dfns.ai or by directing a written request to LGL Systems Acquisition Corp., 165 Liberty St., Suite 220, Reno, NV 89501 or to info@dfnsi.ai.

Participants in the Solicitation

LGL and IronNet and their respective directors and executive officers, under SEC rules, may be deemed to be participants in the solicitation of proxies of LGL's stockholders in connection with the proposed transactions. Information regarding the persons who may, under SEC rules, be deemed to be participants in the solicitation of proxies from LGL's stockholders in connection with the proposed transactions described in the Registration Statement and the interests that such persons have in the proposed business combination are set forth in the proxy statement/prospectus included in the Registration Statement.

No Offer or Solicitation

This communication shall neither constitute an offer to sell or the solicitation of an offer to buy any securities, nor shall there be any sale of securities in any jurisdiction in which the offer, solicitation or sale would be unlawful prior to the registration or qualification under the securities laws of any such jurisdiction.

Forward Looking Statements

This transcript includes "forward looking statements" within the meaning of the "safe harbor" provisions of the United States Private Securities Litigation Reform Act of 1995, including, without limitation, statements regarding IronNet's business combination with LGL. When used in this transcript, the words "estimates," "projected," "expects," "anticipates," "forecasts," "plans," "intends," "believes," "seeks," "may," "will," "should," "future," "propose" and variations of these words or similar expressions (or the negative versions of such words or expressions) are intended to identify forward-looking statements, including statements relating to IronNet's future financial performance. These forward-looking statements are not guarantees of future performance, conditions or results, and involve a number of known and unknown risks, uncertainties, assumptions and other important factors, many of which are outside LGL's or IronNet's management's control, that could cause actual results or outcomes to differ materially from those discussed in the forward-looking statements. Important factors, among others, that may affect actual results or outcomes include: the inability to complete the transactions contemplated by the proposed business combination; the inability to recognize the anticipated benefits of the proposed business combination, which may be affected by, among other things, the amount of cash available following any redemptions by LGL stockholders; the ability to meet the NYSE's listing standards following the consummation of the transactions contemplated by the proposed business combination; costs related to the proposed business combination; IronNet's ability to execute on its plans to develop and market new products and the timing of these development programs; IronNet's estimates of the size of the markets for its products; the rate and degree of market acceptance of IronNet's products; the success of other competing technologies that may become available; IronNet's ability to identify and integrate acquisitions; the performance of IronNet's products; potential litigation involving LGL or IronNet; and general economic and market conditions impacting demand for IronNet's products. Other factors include the possibility that the proposed transaction does not close, including due to the failure to receive required security holder approvals, or the failure of other closing conditions. The foregoing list of factors is not exhaustive. You should carefully consider the foregoing factors and the other risks and uncertainties described under the heading "Risk Factors" in the Registration Statement, and other documents filed by LGL from time to time with the SEC. These filings identify and address other important risks and uncertainties that could cause

actual events and results to differ materially from those contained in the forward-looking statements. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and neither LGL nor IronNet undertake any obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise, except as required by law.