Daniel Newman: Gary Steele, CEO at Splunk, welcome to the 2022 Six Five Summit.

Gary Steele: Thank you. It's great to be here.

Daniel Newman: It is great. Really appreciate Splunk, the support of the event we've had you over the past few years. New and in charge, new to the helm, so it's great to have you here because I'm sure the market is excited to get your takes and puts on what's going on.

Speaking of puts and takes on what's going on, really interesting market we've actually entered over the past few months. You've come in at a exciting time for tech and also a challenging time for tech. I was trying to find the balance there, Gary, but what's your general perspective on what's going on in the market right now, and how tech is going to deal with a really meaningful change in the economy?

Gary Steele: No, it is very fundamental and I think we've watched the compression of multiples over the course of the last number of weeks and a bigger focus on value and away from the fast growing names. I think, when I looked at the opportunity to come to Splunk, the one thing that I saw was just the importance and strategic nature that Splunk was playing to all of its customers.

Having lived in the cyber world for almost 20 years in my previous role, I really wanted to stay with one foot strongly planted in cyber. Because I think even in this very unpredictable world that we're living in, companies will continue to invest in their cyber posture. They will have no choice.

The world's gotten more complicated and it is so imperative that organizations continue to invest to ensure that they're well protected, and I think Splunk's playing a really critical role in that. While there's a lot of economic turbulence, I think Splunk's really well positioned to endure for the long haul.

Daniel Newman: Yeah, I think that's a great answer, very concise. I've published a handful of op-eds, been all over the television. I keep using this term, deflationary tech, but specifically in the enterprise, my take has been effectively, some discretionary spend might go down. Some people may slow down how quickly they will upgrade an iPhone, or maybe they're not going to buy the newest TV set.

But I said, enterprises have to be looking at things like their data as a vehicle to become faster organizations, more profitable, more streamlined, process oriented. Of course, you guys have a unique position because you're on the observability and the IT operation side.

But you're also on the security side too, which I think a number of the CEOs like yourself at this conference actually have talked about the fact that you can't. In fact, the risks of not continuing to invest in digital transformation, specifically security, are huge.

Gary Steele: No, and I think it's really played out. If you just look at what's happened over the course of the last couple years, whether it's Log4j, the SolarWinds issue, the continued risk around ransomware. The number of things security teams have had to deal with that they frankly just

haven't been fully prepared for really speaks to the fact that there needs to be continued investment on the cyber side.

While we're in this changed economic environment, I do believe that doesn't mean threat actors are going to slow down. I think the reality is, we're going to see just a continued struggle for most organizations to keep up with what threat actors are doing.

I'm super bullish on the fact that Splunk is playing the role that it is, and I look at this broader position extending out beyond security to observability where people trying to keep their applications running, drive resilience in their operations, reduce their overall cost. I think Splunk's playing a really critical role there.

I feel this broad platform supporting what people can creatively do with data really resonates with customers, and I think will be very important from a strategic standpoint with all of our customers over the long haul.

Daniel Newman: Yeah. There's a number of different directions I could take that, and I like that you leaned in a little bit to the observability play because I do think that's going to be a big part of your future. Now, you're helping kick off the security track here at the Six Five Summit. I'm going to lean a little bit in on your 35 plus year's experience in the industry. You've got a huge background in cybersecurity.

We've seen over the course of the pandemic, but really leading up into it, that data's been exponential. The amount of data we are now seeing move through the pipes and also the amount of data that's being collected, it's massive. With all that's going on, all the data, all the need to be able to deliver privacy, security, safety, protect people's assets, what are some of the trends that you're seeing? How are tech priorities changing to meet this growing demand for more secure environments?

Gary Steele: Yeah, I think the world's just gotten more complicated. As digital transformation happened, more apps went to the cloud, but we created a really complicated environment for teams to manage and secure, so attack surface just got bigger. As attack surface got bigger, it became very clear that organizations needed one place they could figure out what the heck's going on in their environment?

That's really the role that Splunk has been playing. Really helping organizations with the inside invisibility that they really need as to what the heck is going on relative to their security posture? I think we're really well positioned to help customers as they've gone into this broader digital transformation world. And they've had this spray of data to really have a single place where they can get the insight and visibility they need to improve their overall security posture.

Daniel Newman: Yeah. I love that you said the surface got bigger. Yeah. What we ended up doing was we ended up taking what, millions of employees, putting them out remotely, putting them on their own devices, having to set up all these different networks, expecting VPNs to operate at a level that was exponential.

Then concurrently try to roll out new infrastructure, software defined infrastructure. Then, of course, everybody was online more doing more, creating all this data, and this was enterprises all the way down to consumers. It was huge. I mean, we're multiple years now, Gary into it, this pandemic, I think we're coming out of it, I hope.

Gary Steele: I hope so.

Daniel Newman: Crossing fingers, I think we're all cautious to ever say it's over.

Gary Steele: Right.

Daniel Newman: The one thing that you alluded to there is the heat is still on, right? It hasn't slowed down. In fact, I would argue it's getting harder. With the fact that it is getting harder, how do you guide and have your team guide security organizations to not fall behind?

Gary Steele: Yeah. I 100% agree that it is harder, and why is it harder? Well, we're operating in a world today where the war in Ukraine really represents a big unknown for every organization. Will we see Russian funded state actors target US companies? I don't know, but I think that every organization owes it to themselves to have the right environment that gives them confidence that they're secure and can withstand some form of attack. This is the world we're living in and it's just fundamentally different.

Organizations need to be very focused on how do you respond quickly, remediate quickly, react quickly in a world where what may be coming out of you is going to be different every single time? I think that's been one of our key points of success is this single point of visibility and insight, and it's unique in the industry. As this attack surface has grown and gotten much more complicated, how do you bring it all together so you really understand what the heck is happening in your environment? And Splunk's really at the heart of that.

Daniel Newman: Right. Something you've been suggesting here, and I heard you say it, so I got to dive a little deeper, but you mentioned the word reactive. Would you say that a lot of the CISO, CIOs and leaders, is that their big priority then? Is that the first thing in order to not fall behind is they're actually trying to get out from the reactive to the proactive approach to security?

Gary Steele: Yeah. Well, I think you can just look at what's happened in these big events. Log4j, that was reactive and people were exhausted. People spent months trying to figure out how to identify and then remediate what they needed to do relative to Log4j?

This sort of reactive, I can't tell what's actually happened in my environment and what I need to do, needs to be transformed to how can I be proactive and be out in front of this and have the right capabilities in place where I can see what is going on in my environment, and do I have risk and exposure? If I do, can I take action quickly?

There's some elements there. One, is having a data-centric approach that puts all the data in a single place where you can see it and find it easily. Then two, automate as much as you can

because in a world where it's tough to find great security people, there is so much demand for security professionals today, you've got to make the life of your security teams easier, and you do that through automation so they're not spending, security teams aren't spending time doing things that can be simply automated.

There's just this whole evolution going on in how people think about being proactive, and how do you turn what has been this exhausting beaten down environment to one where you're really ready for what's next? You've got automation so you can simplify things. You've got visibility so that you can take immediate action and actually drive the remediation requirements.

Daniel Newman: Yeah. I'm glad you mentioned the tight labor too because we could have hit that early in the economic conversation we were having. But in some of these fields like security, specialized skills, I mean, through the roof value right now. People that have backgrounds in Splunk or people that have backgrounds in different security technologies, right now the demand is crazy. If you're out there, know your worth.

But I would also say security, Gary, it's a little bit of a culture thing. Earlier, I was talking about all these new surfaces, which you of course can go up and down the stack. We can talk about the surfaces at the semi level, at the software level, kernel. There's all these different surfaces. There's also been this width surface that's been created by having so many more people with access remote with tools.

I'd love to get your take on culture though, because I've talked to CISOs of many organizations over the year. One of the things that constantly comes back to me is that getting that culture of people to buy into security. Because a lot of the breaches, a lot of the risks that are created, they're not necessarily created in these hardened environments. They're created because people are phished out. People pick up random USB drives and stick them in their machines. People get visually hacked and leave their password sitting on stickers on their keyboard and someone gets them in a photo because you posted it on Facebook.

I mean, it's not all these great... It doesn't all look like Mr. Robot. I mean, some of this is actually just culturally driven. What do you think about creating a culture of security to make sure that these easier breaches don't happen in organizations?

Gary Steele: No, I'm a big believer that every organization today needs to raise the visibility and awareness of security, and the role that every single person plays in thinking about it. It's from thoughtful actions taken by every employee, to what developers are doing and how they think about their CICD pipeline, and how you're building security in as you're going through that digital transformation? It really becomes a different way of thinking about a whole enterprise.

It takes time. Those things don't happen overnight. But I do see today, the leading organization is really trying to build it into how everything's being thought through, and it's especially true in the digital transformation world. One of the things that we're seeing is as these new applications are being deployed, building security in. Because at the end of the day, if you have an application outage, is it a application event or is it a security event?

There's such a close tie and that's why strategically, we've extended our product line beyond security to things like observability because they're so related. In a modern world where applications are running, something goes bump in the night. What is it? Is it a security event or is it just some application failure? Being able to untangle that in the middle of the night, and do it quickly, is something that we see super important.

As we raise the awareness and culture around security, we need to be building it into everything we do, including all the new applications that are being deployed.

Daniel Newman: It also makes a huge case for what you mentioned earlier about automation, right? A) Is the bump in the night, is it an application issue? Is it a security issue? And then how can we automate a cure as often as possible, determined first, right? How can we use data, observability to determine the issue? Then what kind of workflows can we automate to reduce the friction, reduce human error or human involvement? There's so many different things to part and parcel there, but you make want to-

Gary Steele: No, I think automation, and everyone I talk to, automation is a key theme because I think everyone will acknowledge the staff shortage. But in reality, even if you could hire, people don't want to work on these things that can be automated. The modern workforce is really like, "Can we just automate that? There's no reason not to." There's so much opportunity there that there's still a lot of low hanging fruit there.

It's really true broadly across how people think about what to do in a security event? It's true also in the world where people are thinking about application restarts. Okay, we had a component fail. We had a failure because we probably have a memory leak. Let's just get the component restarted. Let's go.

Daniel Newman: Yeah. Well, when labor's as tight as it is, automation becomes a really exciting prospect for most organizations. Of course, it should be anyways, because part of our responsibility as business leaders is to be upskilling and to be getting more and more of what machines can't do out of our teams.

I've written books about this. It's easier said than done. You've hit on the culture aspect. There's a lot of things that make that happen, but I think right now is one of these "moments" for automation because I think companies realize they have to move faster to automate because there's just too many processes, too much that can't get done and not enough people. Not enough security analysts, not enough IT network architects. There just aren't enough of them out there. Automation is a big part of the way.

I'd like you to talk a little bit about that through the lens of Splunk. You've mentioned things like proactive versus reactive. You've mentioned automation, you've mentioned culture, you've mentioned growing security concerns. But even in your own research, you did a state of security report. It showed that 59% of security teams are spending probably too much of their time, it's a third, but at least a third of their time, responding to crises rather than preparing for a

"advanced attacks." With that in mind, what are you doing? What does Splunk do to help companies overcome that exact hurdle?

Gary Steele: Yeah, I think one of the key components of our overall offering, there's a store offering where we provide automation, where we make it easy to automate those redundant things, make it very quick to do remediations, and also set people up where the skills required to do that automation continues to go down. Simple point and click, drive automation through, no code environments.

I think, we're really trying to lower the barrier every single day so it's easier to drive that automation across everything people have to do. That's a journey, but I think we're making really good progress there. You couple that rich automation with a data set that really shows you exactly what's happening broadly across your environment. That's how you set yourself up to be very proactive in your approach, and you have the visibility you need to make the decisions you need to make, whether it's in the middle of the night or anytime that some event happens.

Daniel Newman: Yeah, absolutely. This is the money shot right here, Gary. New in the helm, running the show, out in front of customers, talking to markets. Clearly, you know this need and demand for security. It's not slowing anytime soon. It's a real challenge.

What are you advising to when you're talking to your biggest customers and, of course, when you're talking to your teams and getting them in front of your customers, what are the key steps that Splunk is advising with all the technology in the world, what should they be doing?

Gary Steele: Yeah, I think it's a really great question. I think first, it's really getting your environment set up that's capturing all that relevant data. So, build that rich data set that puts you in a position where you can truly be proactive.

One of the actions that we took as a company a couple years ago, way before I joined, was moving away from a pricing model that inhibited people from wanting to put all their data in. We really want to give people access and opportunity to look at all their data and not have pricing inhibit that.

That's a critical thing, and we think about that data in a way where you can leave it where it is. You can do federated search, so you can look across your multi-cloud environment or your hybrid environment where part of your data's in the cloud and part of your data's on prem, and being able to do that without necessarily having to back all that data across clouds or across data centers.

We've made a lot of leaps in terms of enabling organizations to bring together all the data that ultimately makes them have the visibility they need. So, that's the first step. Two, is automate everything you can. That's second step. That's a critical part of it, and even if you take those two steps, I think you're in a very good position to be much more proactive than you have traditionally been, and you can get out of that reactive environment that so many organizations have struggled with.

Daniel Newman: Yeah, and I think another thing if I could just add, and maybe something that I'll let you tell me if you agree or not. But I also think there's too many tools and it creates too much complexity. I think for a lot of companies, right, the IT environment has just gotten massive. You look at whether it's the ERP stack all the way to different SAS and tools that are used up and down to having too many collaboration tools and certainly having too many security tools.

Now, again, it's not too many for the sake of too many. It's the fact is that getting the right tools and then leaning into them and becoming extremely good at using them, I think that's important because I think we've done... There's a little too much trial going on at times.

Gary Steele: No, and I think you're exactly right. If you look across the security industry, I don't know, there's probably 8,500 security companies. It's not uncommon to see 50, 60, 70, 100 different security tools getting used in environments. With that, you oftentimes have this fragmented view of what's actually happening? That fragmented view meaning, are you really going to go to 75 different dashboards to figure out what the heck's going on in your environment?

I think one of the things that we see is you've got to bring it all together to have a single view. Single view really is taking the data from those different systems, standardizing it on a platform and getting the right level of insight coming from your standard platform, and that's really where Splunk plays a role.

While all those security tools can play a role, you really need a single way to look at your environment and not be confused because 50 dashboards, 75 dashboards just don't cut it.

Daniel Newman: That's a great way to end this, Gary. Too many tools does not work. You got to get the right tools. You got to commit to them and, of course, you got to get the right data.

Gary Steele: Right.

Daniel Newman: In a world where no matter how much the economy is growing or not, security is going to play a huge role and opportunity, it's great to have you here to talk about just that. It'll be fascinating to watch how you're going to lead this company forward. It's been great to track so far. I do believe Splunk has a role to play. Thank you so much for joining us at this year's summit, Gary. I hope to have you back really soon.

Gary Steele: Sounds great. Really appreciate the time today.

Daniel Newman: See you soon.

Gary Steele: Take care.

Daniel Newman: See you at Comp.

Gary Steele: Yes, definitely.


The Six Five
SUMMIT