Deloitte.

For Cloud Professionals
November 2020

For Cloud Professionals, part of the On Cloud Podcast

David Linthicum, Managing Director, Chief Cloud Strategy Officer, Deloitte Consulting LLP

Title: **Solving the modern cloud security conundrum with automation**

Description: Cloud has become so complex, and new technologies are introduced and deployed so quickly, that it's often difficult for companies to keep up with security demands. Savvy companies are turning to SaaS-based, data-driven security-automation platforms for help. In this episode, David Linthicum and guest, Lacework's Scott Ford, discuss how automation is helping companies implement effective security processes in their complex, multi-cloud environments. Scott's take is that it's essential to automate and continuously update the security process, so companies can get the information they need to secure their cloud environments and re-focus their resources on innovation and growing their bottom line.

Duration: **00:21:26**

Operator:
This podcast is produced by Deloitte. The views and opinions expressed by podcast speakers and guests are solely their own and do not reflect the opinions of Deloitte. This podcast provides general information only and is not intended to constitute advice or services of any kind. For additional information about Deloitte, go to Deloitte.com/about. Welcome to On Cloud, the podcast for cloud professionals, where we break down the state of cloud computing today and how you can unleash the power of cloud for your enterprise. Now here is your host David Linthicum.

David Linthicum:
Welcome back to the On Cloud Podcast, your one place to find how to make cloud computing work for your enterprise. This is an objective discussion with industry thought leaders who provide their own unique perspective around the pragmatic use of cloud-based technologies. Today on the show we have Scott Ford and he's the principal at Lacework, a software-as-a-service, data-driven security platform focused on solving challenges of securing models of cloud environments at scale. Scott, welcome to the show. I bet you there's a larger story behind that, so give us the Scott Ford story. How did you get to Lacework? What do you do during the day? I always love to hear the stories behind the strategy of the company.

Scott Ford:
David, thanks very much for having me on. Yeah, so, I'm a principal architect at Lacework. My story is I'm a longtime systems administrator. I cut my teeth in the trenches helping companies really automate large-scale datacenter deployments, back when we used to do a lot more of that, but got really into automation and into the movement that you would call DevOps. I ended up spending six years working at Chef Software, and that was a really unique opportunity to work with brilliant people that were kind of at the forefront of that movement to automate everything. And my last position, the last couple

years were spent in a global position, traveling around the world working with companies and helping them to automate all the things, automate the way that they bring their digital products to market and then also the ways that teams work together to achieve that. So, that was really, really powerful for me and shaped who I am today.

But I came to Lacework because I saw some things out there in the field that were big challenges to companies in their ability to adopt automation at scale. And Lacework, at its core, is built on the hypothesis that cloud breaks traditional security, and that companies can't really keep up with the traditional approach to writing rules for how you secure their environment. So, Lacework was founded by data scientists, really. Our cofounder and CTO, Vikram Kapoor, is a longtime Oracle guy, worked on really big data problems in the Bay Area for a number of years before founding Lacework. And the hypothesis being that modern cloud security is a data problem to solve. You've got all this change that's happening all the time, so how do we, first of all, be able to ingest just tons and tons of data every single day, organize all that data, make sense of it, and raise up relevant information around security so that companies can focus on their ultimate goal, which is shipping products, and then secondarily to that, keeping those products and their customers safe.

David Linthicum:
So, going forward, if we talk about security at scale, and it seems like we talk about everything at scale at this point, but it seems to me the challenges in cloud security are, number one, the complexity that seems to be arising around the using of many technologies, the ability to deal with automation effectively, and the distribution of data that's within multiple platforms, and multiple security environments, and things like that, and the ability to kind of get all these things working and playing well together. Even as security starts to advance moving forward, it seems to be the problem to solve. Am I off somehow?

Scott Ford:
No, I think you're right on. It is a very complex problem. I do think, at its core, all of us, including Lacework – I mean, we're a 100 percent SaaS platform built in the cloud. We operate 100 percent in the cloud. We're in the business of shipping product. The best ideas in the world don't mean anything unless you get those ideas out to your customers, to find out what's working and you can set up that feedback loop. So, that's the number one priority that we are focused on as a company. But all of our customers, too, they're building products in the cloud.

Now when it comes to security, security's, like –traditionally – and, David, you've been in the industry a long time as well. Like security's often sat off to the side in their own silo. The security folks, they come in and they stamp their approval on or push back on whether or not changes go out. But in the new world things have gotten so complex, we're moving so fast, we're adopting new technology, new technologies like Kubernetes and containers that go out there to help us be able to ship those products faster, and security's having to adapt, first and foremost, with the way that they operate. This idea that you can come in and block people's speed just doesn't work anymore.

And then on top of that is just the complexity of what's happening, the way that we actually look at environments, whether it's hosts or whether it's containers. We're treating things ephemerally. Things scale up. They scale down. They scale out horizontally. They scale back. And the challenges right there in, like, the traditional approach of, "I'm going to write a rule that says these two IP addresses can talk to each other on these ports and this protocol." How do you do that? How do you do that today if that doesn't apply? How could you possibly write rules for this? And so, these are, like, a challenge, right, that we're faced with, and then plus all the complexities of the compliance frameworks that we're having to adhere to and prove out that we're compliant all the time. There's compliance in auditing and visibility that goes into the entire change process from left to right. So, this is really – I feel is the challenge that security folks are faced with today, and it's immense.

David Linthicum:
It is immense. So, you guys are, in essence, developers for developers. Is that a good way to describe it? I mean, a typical client would be someone who's actually building something, where actually you're building products for people who build products? Or building services for people who build products and services? Is that a good way to describe it? What's a typical Lacework customer?

Scott Ford:
That's great. I've never said it quite like that before but I do think that that sums it up quite well, David. Our customers – our ideal customer profile, they're building products, they're cloud-first, and they're shipping digital products. And, yeah, so yeah, our ideal customer is really that digital-first customer, and their main focus is getting these new features and capabilities out to their customers. And so, we built Lacework so that they can focus on that main problem and allow us to automate the security process for them, so automating the threat detection, the compliance assessments, container vulnerability assessments, host vulnerability assessments. All of that are capabilities of the Lacework platform.

David Linthicum:
Yeah, I wish you guys were around ten years ago. I was doing consulting and actually doing SaaSification of existing enterprise stuff, and the reality is we had to make up security as we went along. And everything, in essence, existed internally to whatever SaaS platform we were looking to build out. And it seems like this is the way to go, the ability to kind of put security into a domain, the ability to have other people who are maintaining it going forward. Since you're software-as-a-service I assume that you're updating and operationalizing the system, you're making sure that the current threats are known, the current attack vectors that people are leveraging are going to be known, and you have responses to those. Is that kind of the way it's working?

Scott Ford:
Yeah, that is one of the main benefits of a SaaS platform. When we update and when we release a new capability, we release that to the platform and our customers get that. So, as an example, just a few weeks ago we moved and announced our new host-vulnerability assessment capability of the platform. So, that is for our customers that are still deploying their applications out on hosts. We will do continuous vulnerability assessments for all the hosts, either at run time or as well at build time, too, where our customers can assess vulnerabilities before they actually build their base images and deploy them out. We do this assessment for them, and that was released and our customers just get it. It's just turned on to the platform.
Now as well as your point with the threat assessments, that is something we have our own internal threat research team that we're continuously updating and providing up-to-date information about threats that exist out there. But, the other thing that's very unique about our platform just in itself is the way that we do threat detection. Our host intrusion detection – the models that we create are unique per environment for deployment. So, if you imagine this, David, our customers, for example, they don't have one AWS environment. They have hundreds of them. And this is not unique to Lacework customers.

This is how you – in my experience, that most companies design. You don't put your production AWS environment and your development AWS environment in the same account. You separate those out. And so, you start to get this big accounts bubble. Each one of those accounts has its own unique footprint, its own unique behaviors in the way that it operates, and Lacework was built to understand that. We understand the difference between your dev environment and your QA environment, your staging environment, or this business unit's environment versus another business unit's environment. Our models are trained to understand what you look like day to day, from environment to environment, and that's across any of the public clouds or your on-prem deployments.

David Linthicum:
What's being conflated with security going forward is the ability to, in essence, leverage compliance and the ability to put policies around how we're going to leverage compliance. And this is something new. I mean, really, the ability to kind of automate some of the guardrails that sit around your existing uses of data, things like that, PII information, the ability not to let information out of the country, because you have a data sovereignty issue, things like that. So, you guys tackle that as well?

Scott Ford:
So, we do continuous configuration and assessments for your cloud resources, and with that we have continuous compliance assessments for frameworks like CIS for the public clouds – AWS, Azure, GCP. We do PCI, SOC, ISO, NIST, HIPAA compliance. And so those are things, too, that as soon as you integrate your cloud environments with Lacework, we will continuously provide those assessments for you across all of your cloud resources.

David Linthicum:
Yeah, that's the, I think, 800-pound gorilla in the room and kind of the advantage of leveraging guys like yourself, the ability to kind of put volatility into a domain, and not only into a domain, but into a domain that other people have to deal with. And so, you guys deal with that as a service, as well as the security stuff?

Scott Ford:
Yeah, absolutely. And this is also something from – you know, I had a lot of experience within my previous role. We worked on compliance as code at my previous company. There's a great program called InSpec out of the company Chef Software that allowed you to codify your compliance standards into tests that you could run continuously. And it's brilliant in the way that it's adopted the SDLC, the software development lifecycle into – having those configurations, you can check them in along with the applications that you're pushing out. So, you can continuously test for compliance right from the developer's laptop all the way through.

The challenge with it is that somebody has to always write it and somebody has to always maintain it, and it becomes a huge burden on the company to maintain all that. With Lacework, we have a centralized SaaS platform for you that you can roll that out across any of your environments and know, that as soon as a new environment comes up online, or a new resource is spun up in your public cloud, that we're going to immediately start testing it without having to, say, roll that out or update servers internally for you. It's just handled from the platform in itself.

David Linthicum:
So, obviously we're moving into a new world where we're dealing with multiple cloud brands, call it multi-cloud, hybrid cloud, but basically we're dealing with on-premise systems, maybe private clouds around, and definitely two to three public cloud brands, and then any number of smaller brands. And the ability to kind of make all these things work and play well together is a challenge unto itself, but in dealing with security and compliance it seems to be something that people are breaking their pick on moving forward. The more complex these environments get, the more moving parts they have to deal with, the more complex the cloud solutions are. And as you move into complex cloud solutions around security, that, in essence, raises the risk of breaches within security systems, so how are you guys dealing with that?

Scott Ford:
Well, so this also something that we're seeing. Now each one of the public clouds, they're investing heavily in security and they have some amazing products internally across the board. But the challenge is, in this shared security model it's on the customer, too, to know how to configure those solutions that the cloud providers release and support. And if you're going into a multi-cloud world, which most of our customers are – most of them are deployed across multiple clouds – that is a big burden. That's a big weight on them to be able to understand every single time a new feature comes out. You have different teams with different levels of expertise.

Security teams are getting smaller in everything I've seen over the last few years. They're not getting bigger. And so, imagining that they're going to be able – you've got teams that are experts across both Amazon security services as well as GCP's security services and Azure's security services, that's a big, big ask. And so really what Lacework is, is that – our approach to it is that to be a – the single solution for our customers across any of those multi-clouds to provide these same capabilities, the best-in-class host intrusion detection system, best-in-class configuration resource assessments, compliance assessments across the multi-cloud, and things like vulnerability FIM in all their environments. So, they know that when they deploy out with Lacework that we're going to cover you in any one of those public clouds.

David Linthicum:
So, moving forward do you think the multi-clouds are going to become more complex? And if they're going to become more complex and we're, in essence, trying to put security complexity into a single domain, the ability to conflate security with compliance, the ability to deal with governance, the ability to deal with management and monitoring and the integration of these tools, understanding that in many instances a management and monitoring tool may identify an attack factor, because suddenly the performance goes up and saturating some sort of an IO system – it kind of all drives together, ultimately, and that seems to be the missing piece. So, what are your plans going forward in kind of integrating all these various tools, integrating all these various pieces of information? And is it an information problem, the ability to kind of understand all these multiple factors of things that are going on at the same time, you'll understand them in real time, understand the history, understand the ability to kind of analyze the information as to what's really happening, things like that? Is that kind of getting to it or am I overcomplicating things?

Scott Ford:

No. I think the one thing we can be absolutely assured of is that it is going to continue to be more complex and change is going to be constant. And we see that with our customers, every single year AWS as an example releases all kinds of new services, whether they be – Fargate is the latest example that we're seeing from our customers that are adopting Fargate now as a new option for deploying out their containers, these managed tasks inside of AWS. And with that is how do you secure it? What kind of visibility do we need into it? And this gets back to our core hypothesis.

If this is a data problem to solve, we need to be able to understand that when you deploy out a service into Fargate, or whether it's a serverless deployment, what communication is happening between the services that you're deploying out there? Who's talking to them? What are they talking to? And that's where our real strength is going to be. Like, we see this. This is not really up for debate that there are going to be new services that our customers are going to want to deploy to, and with each one we're committed to using that same power of the data platform to ingest the data from our customers' environments, understand what's going on, and be able to raise up relevant security information for them to be able to focus in on what matters.

David Linthicum:
So, everybody who's deploying multi-cloud environments and building net new applications or even migrating and refactoring applications is leveraging some sort of new enabling technology. In some instances, it's serverless, some instances it's containers and Kubernetes. In many instances it's both. And the ability to kind of look at this new technology in terms of how we're going to provide security and governance seems also to be a stopping point as people are starting to move forward. And there's lots of different solutions to consider, but the ability to kind of deal like this holistically where you're able to automate things and basically remove human beings – because I agree with you 100 percent. We're reducing the amount of security teams, reducing the amount of operation teams moving forward. At least that's what cloud computing should provide. So, what are the new needs of containers and Kubernetes in terms of security and compliance?

Scott Ford:
I think the real need is the ability to raise up relevant information. What are the things that we're going to focus on? So, let's imagine, David, you and I walk in tomorrow to an environment and we're told that we own security. Like, where do you even start? If you're in a multi-cloud environment, you've got many different AWS accounts, GCP organizations, GCP projects, you've got different Azure tenants – where do you start? And for me it's going to boil down to how can I get at the data for what's most relevant to my environment? So, that's really – the need I think – what our customers are telling us and what we've been seeing is the need for high-fidelity information, high-fidelity alerts.

Alert fatigue is a real thing. This is from a guy that, like, I cut my teeth deploying massive-scale Nagios deployments across a global datacenter. And one of the first things that I learned is that you can generate all these alerts, but the first thing the people who are receiving it are going to do is set up the Outlook rules or the Gmail rules to send those alerts off to some other folder where they're not going to deal with it. At the point that you have a thousand alerts a day, you effectively have zero alerts, right? So, what we need to focus on, the need of our customers today, is high-fidelity information. Show me what really matters so that I can focus in with the limited people and the limited time I have in a day to go after what really matters.

David Linthicum:
So, the difference between monitoring and observability, the ability, to have information at your fingertips that you can act upon immediately, the ability to have massive amounts of data which is conflated into certain actions that need to take place, and even tying those to automation so these actions can automatically take place, the ability, for example, to block an IP address that seems to be attacking your systems, that's where we're heading?

Scott Ford:
Yes, that as well – so observability, the people that are responsible for that day to day, but also for the business leaders, too, this is also a data question for them. They want to be able to look at that data in a different way. Like, if I'm the CISO of an organization, I don't necessarily care about the minutiae of every – show me a list of every single S3 bucket that's out of compliance, or show me every single vulnerability I have in my environments from day to day. I might want to look at that data in a different way. Like, show me over time, are we progressing as an organization in security? Are we shipping products fast, but are we also at the same time driving down the number of critical vulnerabilities that we release out into an environment or driving down the number of resources that we release that are out of compliance? And so, I think in both cases, right, you want – for the people that are responsible for it day to day, we're headed in a world, like, we need the high-fidelity information to act upon this fast. And for the business leaders that are driving the business, we need to be able to look at that data in a different way and say, "Are we meeting our SLAs? Are we headed in the right direction and becoming a more secure company over time?"

David Linthicum:
This all sounds great. And where can our listeners go to learn more about Lacework as well as the security and compliance and also about yourself?

Scott Ford:
Well, thanks very much, David. Yeah, so Lacework.com is our site. We're releasing all the time new updates. We've got a blog up there where we're keeping our customers up-to-date about all of our new, exciting releases out there. I'm on LinkedIn myself, so Scott Ford – ScottFord-IO is my LinkedIn space there. And yeah, that's the main two places that you can find out more about what we're doing.

David Linthicum:
It's exciting stuff and I think it's important as we move forward that we have these kinds of technologies that are able to take care of a problem that's absolutely systemic and is a hindrance to productivity and a hindrance to success as we move through these more complex environments. So, if you enjoyed this podcast make sure to like and subscribe on iTunes or wherever you get your podcasts. Don't forget to rate us. Also check out our past episodes including the On Cloud Podcast hosted by Mike Kavis, my good friend, and his show Architecting the Cloud. And if you'd like to learn more about Deloitte's cloud capabilities, check out DeloitteCloudPodcast.com, all one word. And if you'd like to contact me directly you can reach me at DLinthicum@Deloitte.com, L-I-N-T-H-I-C-U-M. So, until next time, best of luck with your cloud computing projects. We'll talk real soon and you guys stay real safe. Bye-bye.

Operator:

Thank you for listening to On Cloud for Cloud Professionals with David Linthicum. Connect with David on Twitter and LinkedIn and visit the Deloitte On Cloud blog at www.deloitte.com/us/deloitte-on-cloud-blog. Be sure to rate and review the show on your favorite podcast app.

Visit the On Cloud library

www.deloitte.com/us/cloud-podcast