For Cloud Professionals, part of the On Cloud Podcast

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

Title:	**Security and the cloud: people, process, and other key success factors**
Description:	Join host David Linthicum and guest Lori MacVittie, CTO at F5 Networks, as they discuss security in the cloud. Lori provides her perspective on problems organizations often face with security, and how teamwork plays a more critical role than technology in fixing problems—and making sure they're discovered before they become catastrophic. Lori and David also discuss the future of security in the cloud and what CIOs can do to start moving toward that future right now.
Duration:	**0:25:31**

Operator:
The views, thoughts, and opinions expressed by speakers or guests on this podcast belong solely to them and do not necessarily reflect those of the hosts, the moderators, or Deloitte.

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:
Hey, guys, welcome back to the podcast, and we've got a special guest, Lori MacVittie. Lori has been on the podcast before, and she is a principal technical evangelist with the office of the CTO at F5. Lori has been an applications developer, a systems engineering consultant, a writer, an author, a strategist, and evangelist, special forces, I mean, just one of those people. So application development, application integration, application infrastructure, application delivery, application security, cloud, SDN, and DevOps– so fill in the pieces. What have you been doing? You've been at F5 since I've known you, so – but you focus on lots of different things at F5 in terms of where the ball is going to be kicked and, in essence, kind of helping steer the organization in the right direction. So fill in the missing pieces. What do you do day to day, Lori?

Lori MacVittie:

I – wow. I'm still on the whole special forces, skydiving, right? Like, wow, you know? I've got to try those things. So, day to day I read the Internet. I write. I spout opinions randomly on different social media venues and see what sticks and just try to learn. There's a lot to understand about technology and how it impacts F5's business, but also just the market in general. And so I have to spend a lot of time just trying to understand all those things. So I do all of those things: applications, networking, security, DevOps, into the weeds with SDN and different protocols, and you kind of have to have a holistic view of how it all fits together to understand the impacts on one another and where reactions happen, and why, in order to actually formulate a strategy that makes sense. So I spend a lot of time putting pieces together into a big puzzle and then going, "Aha, now I see."

David Linthicum:
Let's talk cloud security, DevOps, DevSecOps, SecOps, and how security meets CloudOps, and how this whole thing is kind of coming together. One of the things I experienced this week is, you know, sitting in meetings, you know, people go through methodologies and approaches and the way in which they focus on cloud computing. And I noticed that really kind of the notion that security is systemic – it's part of the application, part of the way you build the network, part of the way they build the network, even physical security of the cloud systems that you're using, or even the managed service providers, the on premise systems that you use. It's this holistic concept that I think people have a tendency to consider as an afterthought. And now we have DevOps where you have all these things that are coming together, where you're able to be proactive and build these things into the application and do security testing as part of the automated testing routine. So, where are we at with that stuff and what are the challenges going into 2019-2020 we're going to have to wrestle with?

Lori MacVittie:
We're spinning our wheels sometimes. There are a lot of different approaches to this, right? There's the mantra of shift security left into the application development lifecycle, so into that whole continuous integration, continuous test, continuous build. Build in your testing early. Worry about security then. Build it in. So we've got that aspect to it, but we also have people outside that are, right, continuous security in terms of how you deploy, how you manage those things, because not everything is part of the application stack. There are pieces of the security puzzle that developers are responsible for and should be responsible for. There are pieces of security, as you pointed out, that land in the network that NetOps have to be responsible for and should be responsible for. Then there's the security teams who are responsible for overall policy and governance and how that gets settled. And we have to figure out how to make them all work together. We have kind of this, "Let's make all of these pieces work together inside DevOps and inside NetOps, inside SecOps."

Now let's bring them all together and actually make them work in the cloud, which introduces more challenges because now people have teams of – that do just operations for the cloud. So how do they interface with all these other teams? It's a big puzzle that has to be put together, and I don't think we're connecting all those dots. We keep viewing each of these security concerns as something separate when they all play into the challenge of consistently protecting applications across all environments that you might be operating in, which is one of the challenges we hear repeatedly. Three years running it's been the number one answer when we ask global respondents what challenges do you have with cloud, specifically multi-cloud? Consistent security – it's always number one. It's a big, big problem for organizations, and I think part of it stems from there's just not a lack of coordination and an understanding how the pieces fit together yet.

David Linthicum:
Yeah, one of the challenges I'm finding out – it's not the effectiveness of the cloud security systems that we have out there. It's the ability to in essence leverage them effectively in a heterogeneous environment. I'm finding that there's no one-size-fits-all security. People are running different security systems differently, and what scares me to death is not that the security systems are going to fail themselves, but people are just going to stand behind such a complex set of security things that they're dealing with that they're ultimately just going to miss something because of human error. There's a vulnerability that pops out and suddenly it's exploited by a hacker. Am I being paranoid, or is this something we should be concerned with, 2019-2020?

Lori MacVittie:
Oh, absolutely. We used to talk about the patch gap, right, the time that passed between discovering a vulnerability and actually patching it and how that was a problem. And what I'm seeing now is that that is not nearly as bad as the discovery gap, is people not even finding out that they have a vulnerability somewhere until it's too late. And part of that is the sheer volume of applications that we have, and some of it is this diaspora of environments across clouds, is we don't have the right systems in place to be able to do that kind of testing and scanning asset management. Just knowing how many applications you have, and where, is problematic for organizations. So that discovery gap is becoming more critical than even the patch gap, which, thanks to things like DevOps and SecOps and automation, we're starting to close, right? Once we discover it, we can put those things into place and modern application methods that derive from principles of immutability, right? We can pave and nuke, right – nuke and pave everything and restart with a new, non-vulnerable, patched environment. But we have to know that we need to do that first, and that's where we're seeing that there's a real gap growing that we don't even know that we need to do that yet.

David Linthicum:
Okay, and DevOps will save us?

Lori MacVittie:
Sure. DevOps will save us, sure.

David Linthicum:
Well, what are some of the emerging best practices that we're seeing in terms of the ability to integrate, you know, of course Dev, SecOps, the ability to kind of integrate security and (inaudible) operations, become more proactive, and also kind of automate I think a lot of the complexity that's going on in the back end. And so I don't have to think about best practices in terms of security, and I have an automated system that's

actually doing the penetration testing for me, and the white box and the black box testing behind the scenes. So I don't necessarily have to figure out the fact that I'm going to modify an application or modify a database that's going to open exposures in 100 different systems. We have this back-end system that's able to ensure that the correct testing is done, the correct security is in place. Are we there yet?

Lori MacVittie:
No, that is a great theory and a great vision of how it's supposed to be, and I think that's the ideal that everybody wants to get to, but we're not there yet, right? We still – I think we still have a challenge that DevOps is still faltering at the, okay, it's deployed – you know, that operate piece, right, that piece on the bottom side of the infinity circle that we use for DevOps, right, the operate and monitor piece, right, where that information is coming from. We can run the tests. We can do all these things, but we're not doing enough to be able to collect that data and then use it in a meaningful way. So we've got to finish up that whole cycle. We're kind of stopping and faltering and then going back to the beginning and just deploying again.

David Linthicum:
Yeah, I think that we're going to have to iterate our way through, you know, the ability to kind of be good at this. I mean, I've been dealing with cloud complexity really kind of as a concept so that's where my head's at, and the major reason we want to deal with the complexity and heterogeneity of cloud – and the fact of the matter is we can't stop it. And everybody's going to manage by magazine – they're chasing the shiny objects. They're going to go off and use whatever cloud technology they think is going to be the cool stuff at the time and different systems, and now we're building things using cognitive computing and things like that. I'm really concerned that we're going to get things where there are so many moving parts, and so many end points, that it's impossible to think about how we're going to secure all these things. And I think that people do have the perception that DevOps will save them, that if they use some sort of a modern toolset that they can automate their way out of it, and I think the reality is that some of the technology exists; most of it does not.

And really the thinking doesn't exist. I don't see the really kind of focus on the deep security needs within the DevOps crowd, and I think the reason is we have a tendency to silo IT. We have the DevOps folks, we have the security folks, we have the governance folks, we have the Ops folks, and never the two shall meet, even though DevOps is about Ops and Dev working together. But we are missing integration in some of these core parts. There needs to be a cultural change. So I guess what I'm saying is at the end of the day it's a people issue, right? This is not a technological issue. Eventually the technology is going to catch up, but we have to align people, skill sets, organizations sets in order to attack the problem.

Lori MacVittie:
Well, absolutely, right? It's always people and process, right? I mean, the concept of data processing and everything else and computer sciences, right – garbage in, garbage out. If you automate processes that are designed around a siloed IT, you're just going to be siloed faster, right? You're not going to get that integration you need, like you said, that collaboration across all of those different groups. And we still do it, right? Dev and Ops brings developers and Ops together, and NetOps wants to bring network engineers and operators together, and SecOps – right? You've got – you're still just creating new silos, and too often with cloud we see that, too. "Well, we have an Azure group and we have an AWS group," because the operational models are so completely different. Nobody has standardized on one cloud and just that's what they do. They're multi-cloud, so they have multiple groups to deal with all of the operations under that and they're necessarily siloed, just by nature of the languages and tooling that they have to use. So we're just – we're creating more silos.

David Linthicum:
So you're taking over as –

Lori MacVittie:
We're doing it faster.

David Linthicum:
Yeah, we're able to move fast and we're more agile at destroying ourselves in some instances.

Lori MacVittie:
Yes!

David Linthicum:
Okay, and let's say you're a CIO of a billion-dollar company, which in essence is going to be a small business. So you're going to create a net new organization, greenfield, you know, building skill sets, and things like that that's going to be optimal for you leveraging cloud and leveraging security. Tell me how you do that.

Lori MacVittie:
I hire you to consult, right? Isn't that –

David Linthicum:
Well, yeah, obviously that's the optimal way to do it. But the thing is, like, where would you start? Would you start breaking down the silos? Would everybody sit in one big room, no offices? Would it be – I guess what I'm talking about is the organization. They're typically reporting up to a structure and people sit in silos and different organizations are running Sec and Ops and cloud, and then you can break down cloud 20 different ways. We have the cognitive, we have the data, we have providers all those sorts of things. I mean, how do we solve this problem? If we're getting to these very complex environments, people are typically organizing around the technology or the pattern of technology. That's problematic unto itself, so how do we fix it? You're CIO. You can't quit, by the way. You're locked in for the next five years.

Lori MacVittie:
Oh, wow! That's my only option; I have to do this. Wow. I mean, you can't – you have to have specialization, right? But you still have to work together. I mean, your hands can't be exchanged for your feet, right? I mean, it doesn't work. You need them both but they have to work together, so you know, some kind of combined teams that are measured based on the same things. We're all measured based on, you know, the security profile, the performance, and the uptime, right, of the application. We are all accountable for all those things, so that we all work together to achieve that, because there is no piece of this puzzle when you look at the different silos that doesn't somehow impact the security or the performance or the availability. They are all intertwined. So just – you know, your feet don't get the medal for winning the race; the whole body does, right? It's the team that gets it, not the individual pieces that maybe were sometimes more relevant than others. So, I think some sort of a combined team that's measured based on the same things. And maybe that's the important part for if you're trying to do this in something that isn't a greenfield, is first get aligned on what it means to be successful in the first place, right? It isn't just you get measured on this one piece of it and you get measured on this other piece of it. You have to be measured on the same things and take responsibility for that so that you work together. You're more likely to – and to communicate more, to understand the impacts and thus form a more – you know, I guess broader set of expertise across that team to understand. So, if I was going to do it, I think that's how I would do it. It would be like, okay, everybody gets to be, you know – gets to be a piece of this one big thing that we're going to try and build, and you know, it's all or nothing. That's it. We're all either successful or we all either fail. We do this together.

David Linthicum:
Congratulations. I think you just nailed it. I mean, I hear all kinds of different responses. "We're going to go to, you know, a training and even get a corporate psychologist," and all these sorts of things. But I do think it is going to be shared metrics, you know, shared wins or losses, and the ability to kind of get people coordinated around the same set of goals. So maybe we should hire CIOs by just drafting people, so they have no choice. They just get – sorry, man, you've got to be CIO. You've got to be CIO of this company for the next five years. "I don't want to do that." Doesn't matter. Doesn't matter. You've got to do it. We found you competent. But it is – I think the challenge would be, and I think a lot of the listeners who are listening to this podcast always think of, like, how they would do this in their corporate environment. And we have a tendency to lead with technology, and I think that's going to continue going forward. This typically isn't going to be about changing tools. This is going to be about changing orgs. And you and I are both technologists, and so I have experience in changing orgs, but I'm probably like you; I'm not comfortable doing it as a profession. So what would be the way in which we should think about the org in terms of technology? Where are we looking to go? And you wrote about – or you've been researching this. We talked about this before the show, with some of the stuff you've been doing on security. So what's your take on all this in terms of how it meets technology?

Lori MacVittie:
Wow. I actually don't know how to answer that. I mean, security is – there are so many different pieces to it, and it's – I mean, there are different technical ways – I mean, there are different answers in technology to the same problem, right? There's – you can do – to address something like an application vulnerability let's say, you can do continual testing. And when I mean continual testing, I mean like every day. Like every single day you are testing for those vulnerabilities to find them and then patch them. That's one way to address it, and that's your entire strategy. There's another way that says, "Well, I can put a web app firewall in front of it and just stop that potential attack from ever getting to the app, so if it is vulnerable, it's okay. I'm covered." Right? And then, you know, there's still another way. That might be identifying these attacks as coming from certain IP addresses or identities or devices and just blocking them. There's a lot of different ways to approach the same problem when it comes to security. And you know, you have to find the right approach for your business model, for your teams, for what you're capable of. I mean, no matter how much automation you use, no matter how many different team structures you have and you've restructured the org and it's all working great, no matter how many different things you use, it still comes back to, you know, overall is this application secure? It's less about how did I do it, but did I do it in a way that makes sense for my organization given the resources, the expertise, and the budget that I have?

David Linthicum:
So –

Lori MacVittie:
If that makes sense.

David Linthicum:
No, it does make sense, and I think it's a good answer. So what would be – if you're in the elevator ride with the CIO who's facing these issues, what would be the top three things he or she should be looking at in 2019 to start moving in the right direction?

Lori MacVittie:
Well, so one, I think they have to look at what the business goals are, right, and try and figure that out first. Is it to deliver apps more frequently? Do you have an idea about how many times a year you want to make these releases happen and things like that? We say more frequently, we say we want to do it faster, but what does that really mean? Because that has an impact then on the kinds of technology and the ways that you're going to integrate, you know, your security into those processes, because some are more laborious than others. I mean, that's just a fact of – the way it is. You know, we've got – internally we have millions and millions of lines of code. Doing static analysis on that from a security perspective takes time. You cannot release in an hour. It's not going to happen. So you have to be able to balance how often do we want to get applications out and aligned with the business and keep them happy but still stay secure, right? So maybe there's another solution or another option, right, that's going to help us achieve those goals. And, you know, look at balancing everything without sacrificing security, because security is always the most important thing we have to do. And it's always the first thing we sacrifice when anything else gets in the way, like getting to market or performance, which is just – you know, it's amazing to watch. It's most important, but we'll get rid of it at the drop of a hat. So finding a way to, like, realistically balance that, and you know, if you're a business leader looking at that perspective of how technology's going to fit in, you know, be aware that you can't – maybe you have to give. Maybe you can't release something every two weeks, but it's going to be every three weeks, in

order to stay secure, right? I mean, there has to be give and take on both sides. One of the things I see that's frustrating right now is that everything is kind of sacrificed on the altar of business getting to market faster, and there's no talk about, hey, business, you've got to give, too. So I think in 2019 trying to find a balance between meeting goals and how you go about doing that, using different technology and maybe getting an inventory of what resources you have, what expertise you already have and how you can leverage that into that process would be a good place to start.

David Linthicum:
Yeah, I believe that's a good answer, and also – you get three for three on this podcast. I mean, good thing we're recording it.

Lori MacVittie:
Yeah, yeah. Well, I hope this one takes.

David Linthicum:
Yeah, this time. I don't know if you know, audience, we had a great show a couple weeks ago and absolutely – my voice was all garbled, so we had to redo it, so – we're talking about a different topic, though, so that makes it kind of fresh and nice. So what would your – what kind of things should Dev-SecOps focus on in terms of emerging technology over the next few years? What do you see on the horizon? Which is really going to be a game-changer or just kind of a tactical game-changer, or something that's kind of nice to have that we probably haven't done well in adopting within the enterprise and leveraged?

Lori MacVittie:
Well, if I don't say container security I'm wrong, right? I mean, it's like – right, number one. And it is, right? Containers are pretty much growing at a pace that is set to – I don't know, consume cloud, right? It's just going to eat it up and be mostly container. So container security is a not-well-understood area in terms of both what the possible vulnerabilities are, as well as how to address them. So that's going to be something in the next few years that security folks really want to look at, because some of it is pretty standard, you know, we've already dealt with this. But a lot of it is going to be new and so we need to be familiar with that technology and how it kind of interoperates with everything else. I think zero trust is going to start becoming more of a thing that organizations want and push for. And, so, Dev-SecOps is going to have to understand how that impacts the policies that they're creating and what they're doing and how they view just security in general.

We have a tendency to focus on the network in security, especially in traditional security silos because that's generally where we've had the most opportunity to deploy solutions for security. We put them in the network. We just block stuff. It works really great, until you move to the cloud and you don't have that anymore. So things like zero trust that are looking more at identifying, in some way, a user on every request and making them verify, "Yes, this is me," every time is going to become more common. And that's going to have an impact on security policies because you're going to rely on different technology, but also a different way of looking at security. So understanding zero trust is probably a good place to go for Dev-SecOps in the next couple of years.

If I need one more – let's see. What else should they learn about? APIs – APIs are also very not understood, specifically more from a security perspective because they're very programmatic. It kind of – you know, they're not a technology in and of themselves, right? They're more a thing. It's an interface. And it's kind of hard for a lot of InfoSec professionals to really understand APIs and security, because they are so tightly coupled to the concept of applications and application architectures and integration, all those "I" words in the AppDev world. So getting more familiar with API security, APIs in general API gateways, what provides each of the different functions, would be a good place to go as well, because the more containers and micro-services, the more mobile apps, the more we move away from LAMP and towards MEAN we're getting more APIs, and that's going to be a critical component to secure in the next few years. And it's going to require Dev-SecOps, because it's very tightly-coupled to the application.

Lori MacVittie:
So where can we find your blog?

Lori MacVittie:
You can find it on F5.com, and you can also find it on DevCentral.F5.com.

David Linthicum:
Make sure you get a chance to read Lori's stuff. It's always game-changing. She has a tendency to write very thoughtful, deep pieces, which is unusual out there these days. Lori, it's great to have you on the podcast. Sorry about last time when we did the misfire, but I think this was a better show, so I'm looking forward to listening to it.

Lori MacVittie:
So am I. Thanks for having me back.

David Linthicum:
You got it. Take care, guys, and we'll talk to you in seven days. You be good. '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