Deloitte.

For Cloud Professionals
October 2021

For Cloud Professionals, part of the On Cloud Podcast

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

Title: **Cloud managed services: a great way to do cloud security**

Description: Cloud security issues are a serious—and growing—problem. Most companies don't have the resources or expertise in-house to effectively manage security in a constantly-changing cloud ecosystem. In this podcast, David Linthicum talks with Ntirety's President and CEO, Emil Sayegh, about how cloud managed services providers (MSPs) can help. For Emil, it's simple: MSPs provide companies with the security expertise and resiliency they need—24/7/365—to reduce their cloud security risk.

Duration: **00:24:00**

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 out 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 technology. Today on the show we are joined by Emil Sayegh, and he is the CEO and president of Ntirety, formerly Hostway and Hosting, I knew it back then as well. Ntirety was formed as a merger of Hostway and Hosting.com in January 2019, with Sayegh at the helm, and he merged the company as a leader in secure and compliant managed-

cloud services. Its team of engineers in North America and Europe deliver secure, compliant, and scalable private and hybrid cloud hosting solutions in 14 geographically diverse datacenters. Wow, that's a lot. So, how you doing, by the way?

Emil Sayegh:
Doing great. Thank you for having me on the show, very excited.

David Linthicum:
Oh, I'm very excited to have you here. So, tell us about this story. How'd you get involved with the firm?

Emil Sayegh:
Yeah, sure. So, as you may or may not know, I was at some point the VP of products at Rackspace, and then I was the GM of the cloud business. I started the OpenStack project over there, then moved on to be the VP of cloud services at HP. Then I became the CEO of a company called Codero for about five years and turned that company around and got it back into growth and whatnot. And then about—after we sold that company to a group of telcos, there was interest from the owners of Hostway for basically the same turnaround to happen at Hostway. So, they brought me in about five years ago exactly, September of 2016, and then very quickly we got Hostway back on the growth track.

And then two and a half years later we merged with Hosting.com, and I became the CEO of the merged company, so both companies together. And then we rebranded to Ntirety about a year and a half ago. So, just the public name became Ntirety of the merged entity instead of Hostway and Hosting and dash marks and hyphens and all that good stuff.

So, that's kind of how I got involved. It's been a great ride for five years. Now Ntirety is focused on managing the entire security stack for customers, and in addition to kind of building on our heritage of managed services and managing the entire IT infrastructure and applications from the ground up.

David Linthicum:
So, you're from Rackspace, so you're physically located in San Antonio, or did you move out of that area? Or were you ever in that area?

Emil Sayegh:
No, I've lived in Austin, Texas since 1986, David. So, I've been in Austin for a long time. And I commuted for many years to San Antonio, and I actually had an apartment down there, and I would go in on Monday and stay there for most of the week while I was heading product and then later the GM of the cloud business. But yeah—no, it was quite the commute.

David Linthicum:
Yeah, Austin's one of my favorite places in the world. Love the barbecue there, love the scene. Everybody's just in a good mood, it seems, when you go to Austin. Is that the case?

Emil Sayegh:
Absolutely, 100 percent, and we'd love to host you if your travels make it that way. We'd love to host you. I've been there since 1986, and I consider myself an expert of the city, so…

David Linthicum:
Yeah, I may take you up on that. I'll take you down to la Barbecue and we'll have some barbecue.

Emil Sayegh:
Absolutely.

David Linthicum:
So one of the things about managed-services providers and managed services, and certainly ones that focus on security, which is an important thing—I guess that's a good way to frame you guys—is that people don't understand that there's not a binary choice between traditional on-premise private datacenters and public clouds, that you have the ability to leverage managed-services providers which provide this intermediate—which provides hosting for different applications and different kinds of workloads. So, those—and a lot of people are doing this right now. They're shutting down their private datacenters, they're moving out to co-los, and they're moving to the public cloud.

But one of the huge options and huge, I think, underserved benefits that we don't really understand in the industry is the value of managed-services providers and the fact that they're able to provide very similar hosting services that provide managed services for you, and therefore provide an alternative to you leveraging a co-lo or, in essence, you're renting the space, but you still have to maintain the computers and hardware and software, or you're giving up complete control and moving into the public cloud. What would you describe the benefits of managed-services providers? And also tell us about the security attributes you guys are able to provide.

Emil Sayegh:
Yeah—no, that's a fantastic question. Look here's one of the biggest advantages that I always tell our customers or people considering a managed service, is that for a company to be legitimately secure or legitimately manage their infrastructure and applications, they're going to need support 24/7. They're going to need support. They're going to need sys admins. They're going to need people that understand their applications. And that's not just 24/7 during the workweek—holidays so on and so forth.

The advantage of a managed-services provider is they've productized essentially all that stack of services, all the way from patching, to stuff that sys admins do to monitoring, to managed backup, to disaster recovery to managing databases, as well as encapsulating all this in some kind of a 100 percent 24/7, 365 days a year monitored security type of a scenario, right, and protocols. And, so, whereas an enterprise may have one or two people that are experts in security, one or two people that are experts in MySQL so on—you get my drift. A managed-services provider has an entire staff that's available 24/7, 365 days a year, and this is all they do.

So, the best analogy that I could give is if, God forbid, one of us needed brain surgery, we want to go to the brain surgeon that's doing these surgeries every single day, not somebody that does them once a year, once a quarter, or even once a month, right? And these experts that work at managed-services providers they're doing these types of mitigations on an hourly basis, right? For our company, we block over half a million attacks a month, half a million attacks a month on our 1,200 customers. You're not going to find that kind of expertise if you're just an enterprise, midmarket enterprise, trying to kind of have that kind of staff onsite.

David Linthicum:
What about access to security services? You know, public clouds have identity access management. They have encryption services, compliance services. Assuming you have analogs of those and you're a managed-services provider in how you deal with security, which is managed by people, so what would the difference be? How would you explain the difference between a public cloud security service that you're kind of—it's kind of DIY yourself versus a managed-services provider where you're doing a lot of the servicing on the back end?

Emil Sayegh:
Sure. I mean, for us, we're agnostic in terms of using public cloud or our internal datacenters or even on-prem with our customers. You know, we see our value being added is in that stack of services that sit on top. So, absolutely, we manage hybrid environments all the time. Actually, most of our customers, the vast majority of our customers, at least the ones that have been coming in over the last three years, have a hybrid type of infrastructure. And in that case, we're using the services that are available through public cloud in terms of IAM and whatnot and incorporating all of that into a comprehensive security solution. And the secret sauce is really the sauce, as well as the automation that kind of pulls everything together, so that whether things are with AWS, Azure, Google, in our datacenters or the customer's datacenters, the customer is secure and they know that they have a single neck to choke when it comes to compliance security.

David Linthicum:
So, say I want to be an Ntirety customer and I am looking at the difference between a managed-services provider, which also incorporates cloud and some of the security services they offer, some other stuff—automation, knowledge, and expertise—versus a pure cloud deployment. What would some of the top three advantages be for leveraging a managed-services provider in dealing with security versus exclusively in a public cloud?

Emil Sayegh:
Yeah. In my humble opinion, there are applications that don't work well in the public cloud. Let's face it. I've been, just like you, in the public cloud space for a very long time, one of the early people, like yourself, that have been involved with public cloud, so I'm a big fan. But, also, we know the warts. We know that there are certain applications that don't work in the public cloud, yet you want to be able to have one security posture that secures the applications that are cloud native as well the applications that don't work very well in the cloud.

And if I'm a CIO, I don't want to have three, four, five different security postures in my company. I would want a single posture that would make sure that all my infrastructure is up to date, all my infrastructure is secure, all my infrastructure is being monitored the same way. And then there's the disaster recovery for every one of those elements. So, if I go cloud-only, I'm ignoring a good portion of my infrastructure and really kind of having two sets of books, right? A set of books, a set of protocols for the applications that sit in the public cloud, and a set of rules for the stuff that I have on-prem. I would say a single neck to choke and a single security posture is one of the first advantages.

Number two, I think, in the case of all the advances that you have in the public cloud from an IAM standpoint and SecDevOps and so on and so forth, you can actually have the agility to set that up and move and transition with time to a public cloud if this is the destination. And a managed-services provider, a company like Ntirety, can help you throughout that journey, right? So, this is not an either/or; you have, again, a single neck to choke to kind of help you with that migration and with that journey, so I would say that's the second thing.

And then the third thing is resiliency and not putting all your eggs in one basket. Having a multicloud solution and multi-infrastructure solution is very advantageous. It gives you an opportunity to leverage costs, to leverage your position as an enterprise between different vendors, and so on and so forth. And dealing with a managed-services provider that's agnostic in terms of infrastructure will actually enable a better cost profile and pricing profile for the end customer.

David Linthicum:
Yeah, sometimes I get confused why managed-services providers are not considered more, certainly with organizations that may not have the resources to maintain and do CloudOps to the level of security and governance that they need to make that happen. And I understand how technology progresses, and also there's a lot more marketing dollars chasing different kinds of technologies out there. But obviously the growth of the managed-services provider that happened during the pandemic will continue on. But it seems to me it should be a little bit more inflective right now in terms of we're using cloud, we're moving to cloud, we're going from 20 percent to 40 percent workloads in the cloud. Managed-services providers are going to be the path of least resistance, and in many cases—and it all includes cloud. We're still using cloud but doing so in a different way. In many cases, it's going to lower the risk, it's going to increase the cost benefit, and it's going to provide a better secure solution. Obviously you agree with that, but put some light around that.

Emil Sayegh:
Yeah, I 100 percent agree with that. The issue that you have is—look, a lot of the new graduates and a lot of the new IT and developers that are coming into the market, right, all they know is cloud, and their natural instinct is to go quickly to cloud and build it and do it themselves. And they've grown up with it, and they know what they're doing, and so on and so forth.

The problem is—and this is partly who we target in terms of our customers—but I'll get back to that first group, to the group of newcomers into the space that are putting everything in the cloud and thinking that this is going to be like that forever. The customers that we generally target are customers—are companies, midmarket companies that have been around for ten years or longer, because guess what? They have a bit of a mess of an IT on their hands. You know, it's not all monolithic. It's not all in the public cloud. It's not all Microsoft. It's a combination of Microsoft and Linux and VMware and some of it is on-prem, some of it's off-prem, some of it's co-lo.

So, they kind of have a little bit of a mess, and then they need help in rationalizing, in migrating, in transforming their organization, but most importantly in securing and managing all these disparate types of installations that have grown over the years. They've done an acquisition here—you get my drift. So, those folks are the ones that need absolute help right now in securing and managing their infrastructure, as well as helping them rationalize that migration to a more what I would say cloud-ready state.

Now the newcomers that are joining, and this is where all the publicity comes in and a lot of the media—it's all in the cloud, and we use this service from AWS and all of a sudden, we're golden. Well, guess what? This works for a few years, but what happens when they do an acquisition? What happens when they get acquired? What happens when they're all in on AWS and they get merged with a company that uses Google or Azure or has some on-prem? They're back in that same—they're going to need help from a managed-services provider that is agnostic in terms of infrastructure and that's going to allow them to kind of have one security posture across all these different infrastructures. So, that's kind of my color commentary on that point.

David Linthicum:
Yeah, and I was just thinking about this. In essence, what we're doing is putting volatility into a domain. And, so, in other words, if we're dealing with multiple public cloud providers, and even niche cloud providers, maybe dealing with SOX compliance, or tax processing, or all the other services that are out there—and there's a lot more out there than just the larger infrastructure as a service public cloud providers, certainly the SaaS services as well. If we're leveraging a managed-services provider, we're, in essence, abstracting ourselves away from that complexity. We're allowing them to manage those things on our behalf, including looking out for security vulnerabilities. And, therefore, that becomes kind of a core value point as well, the ability to deliver services in such a way that, if things change and services start to switch around and security systems update or disappear—like as you just mentioned, companies go out of business sometimes or get acquired—you have an organization that sits between you and that kind of volatility. Am I off base?

Emil Sayegh:
You're absolutely right. And look one of the other things that we didn't talk about is the zero-day threats. That's—I mean, you're absolutely right. Add to what you said the zero-day threats. You know, a managed-services provider is dealing with thousands and thousands of threats that are coming from disparate parts of the world, attacking different types of—as an example, we have a couple thousand customers that are being managed by us. We see threats. If we see a threat that is coming that is unknown to us before, well, we mitigate it, but then we apply that same fix to the other 2,000 customers that we have under our management, right?

So—and I think that kind of almost crowdsourcing of the fix to the threats is something that a customer of a managed-services provider can benefit from tremendously, because these threats are coming in novel ways, right? They're coming in through e-mail. They're coming in through monitoring systems. We've seen them come in through managed-services provider systems. So, that was something that was super novel that spread very quickly to key installations.

So, I think what you gain from working with a managed-services provider is really that collective knowledge about the security scene of what's going on with different industries and different customers. And through working with somebody like Ntirety, a comprehensive security approach that starts all the way down, from patching, monitoring, disaster recovery, and spans that entire spectrum.

David Linthicum:
So, why would a customer say no, and why would a customer say yes? And, so, as you're out there selling it—and I know all CEOs sell. I used to be a CEO a few times. You know, selling's a large part of the job, and you're communicating the value proposition, which you do very well, to prospective customers that are looking at managed-services providers. Some of them are going to bypass managed-services providers and go directly to the cloud. Some of them are going to leverage them. Why would they say no, and why would they say yes?

Emil Sayegh:
Yeah, so at the C-level, you have certain groups that there are internal groups that they've invested in. And I always say a lot of times the alternative is for companies to try to do it internally. But what you are seeing now is a lot more pushback from boards, and from CEOs to their CIOs and CTOs, of really mitigating the internal risk by hiring an external entity like Ntirety and others to do the work. So, where there's engagement by other C levels—I would include the CFO as well. So, CEOs, CFOs, and boards are getting more and more involved, and they're putting pressure on their IT teams to essentially figure out how to mitigate the risk by engaging external entities, because they understand intuitively that there's no way they're going to be able to staff up for all these risks, right?

Because when we're talking security, it's not just about securing the environment. The way I talk about security, it starts at the detection. So, the first question is to an IT organization—and I would always ask that to the C-levels. It's like, "Hey, does your team do repetitive, or hire repetitive, investigations of the threats that are incoming? And once they do that, are they securing comprehensively against these threats? And if, God forbid again, you get a breach, do you have a disaster recovery option that you can invoke at a moment's notice to recover so that your business doesn't stop. And most midsize enterprises can't afford to do that. And then after you've done all that, do you have an insurance program that is continuously looking at your infrastructure and making sure that it's compliant, making sure that it's secure, that all the advancements in security are there?" And if you say no to any of those four vectors, you're going to fall prey.

And usually that's essentially when they say yes. They look at this and they say, "Oh, my goodness, this is overwhelming. There's no way my IT organization is going to be able to do all these four vectors at the same time." And if they fail in one, that could be a company—a brand-damaging type of an event.

David Linthicum:
What's funny, your response I think was very profound. People say no for the same reasons that they say no to cloud. "We have an existing expertise. We've already invested in a private datacenter. We just spent $10 million on hardware that we have to amortize over the next five years, or else we're going to take a huge tax loss," and lots of reasons that may not go to why we're dealing with the solution at hand. We're just dealing with some of the business events. And I can see that as a reason to kind of continue on the way you're going, even if you're going to have to figure out how to move off of it at some point. But there may be a compelling business reason why you're remaining on your current trajectory, just kind of based on the fact that we've gotten ourselves into a certain sunk cost. We have people around, we have equipment around, whatever, and we have to live with it and get the value, or as much value as we can, out of that stuff. It may not be the right decision, but I understand why they're getting to a no.

So, anything else we should know about the company and about the technology? And what kind of homework would you give to the listeners in going out and understanding more about managed-services providers?

Emil Sayegh:
Yeah. I mean, about the company and we're a global company, and three SOCs in the United States, all based in the United States, with multiple datacenters around the world, with deep expertise in Azure, AWS, and now a burgeoning expertise in Google. We have both professional services and managed services; they kind of go hand-in-hand. Our professional services are there to do assessments and whatnot so that we can help customers kind of understand what the landscape looks like and what the threat factors are, and then kind of help them deciding on a path to go.

But again, our approach is that of comprehensive security. We don't believe in point products. We don't believe, oh, a firewall is going to fix it, or an IDS solution or IPS solution is going to fix it. We believe that all these technologies kind of go hand and hand, and it starts with patching, which is the most essential part, being up to date. You know, you won't believe, David, how many times we go into a customer or prospect, and then we find out that they're only 60 percent patched up, their servers. You know, and then what's worse is that we do a discovery, and then we find out that they don't know that they even have 500 devices in their infrastructure or some number of devices, right? It's actually quite concerning. That happens in most verticals that we serve. So, from our perspective, comprehensive security is key. Everything we do is security first. So, we do the entire stack of managed services, but it's with security in mind. And all these things kind of fit like a puzzle in the way that we serve customers.

David Linthicum:
Cool. Plug your website.

Emil Sayegh:
It's www.Ntirety.com, and Ntirety is spelled N-T-I-R-E-T-Y, entirety as in the whole thing, but it's spelled with a capital N.

David Linthicum:
So, keep in mind as you're doing architecture out there and you're considering different solutions, you have to consider holistically what's going on. And at the end of the day, we're trying to find the least cost, best optimized solution that's going to provide you with the best security optimization and governance optimization, application optimization, performance optimization, all these sorts of things. So, collectively you need to consider all solutions out there, and certainly managed-services providers are part of it. And, sometimes co-los and sometimes we keep things on private datacenters, not as much as we'd like to in many cases, or in public clouds, and we're abstracting the complexity of the public clouds through managed-services providers or different automation layers. All these things need to be considered if you're going to get to the optimal solution.

So, if you enjoyed this podcast, make sure to like and subscribe on iTunes or wherever you get your podcasts. Also don't forget to rate us. Also check out our past episodes including the On Cloud Podcast hosted by my good friend Mike Kavis and his show Architecting the Cloud and book by the same name. If you'd like to learn more about Deloitte's cloud capabilities, check out DeloitteCloudPodcast.com. If you'd like to contact me directly, you can reach me at DLinthicum@Deloitte.com. That's L-I-N-T-H-I-C-U-M. So, until next time, best of luck building those cloud projects. We'll talk again real soon. Good luck to you guys. Stay safe.

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.