Bill Murphy: Hello, you were listening to Bill Murphy's RedZone Podcast. I interview leaders who inspire me in the areas of exponential technologies, business innovation, entrepreneurship, thought leadership, enterprise IT security, neuroscience, philosophy, personal development, and more. Welcome to the show.

[00:00:30] Welcome back to the show, everyone. This is Bill Murphy, your host of the RedZone Podcast. My guest today wrote this article that led me to him, and it's called Cloud Security Secrets Your Cloud Provider Doesn't Want You to Know About. I thought, well, what are those secrets? That led me to read the article published by David Linthicum, and I didn't realize how much of a giant David is in the industry, but he's the Chief Cloud [00:01:00] Strategy Officer at Deloitte Consulting. He was named the number one cloud influencer via a major report by Apollo Research. He's a thought leader, executive consultant and author, which I'm going to get to what he's done in that realm. He's been a CTO five times for public and private companies, a CEO twice in the last 25 years. Few individuals have reached David's level of achievement, reputation and leadership, and he's a regular research [00:01:30] analyst for [Gigamon 00:01:31]. He's written for IEEE Computing, TechTarget's SearchCloud, and SearchAWS.

He's been an NPR many times. He's published 13 books, and he has 5,000 published articles and spoken at more than 500 conference presentations. He has a very, very deep and rich history in educating the marketplace about where cloud is going. As you might imagine, Deloitte has often brought in very large companies [00:02:00] to consult. What I love is, if you know where the big, big, big companies are really looking for, if you're in the small to medium enterprise, you can be rest assured, in the next, either now, or coming in the next 12 to 24 months, that you're going to see the impact of some of the things that are happening. I asked him a lot of questions that may apply to you now, but they certainly may not apply now, but they'll definitely going to apply 12 months, 24 months down the road.

It's a great way to look around the corner [00:02:30] of what companies are really asking. We talked about why businesses have a tendency to learn from pain. Now is a time to think independently and question why things are currently being done. Cloud security only improves in a culture that challenges status quo. Another learning element here is there's going to be architectural trade-offs that we have to do that'll challenge what we do pragmatically with the technology that's out there. We talked about how security can hinder performance and cost way money [00:03:00] each month if it's not engineered into applications. We also really talked about, when you hire people, you need to hire people who are going to be continuous learners, autodidacts, which is more than leaning into a specific skillsets, leaning into people who have width and want to be continuous learners.

We get into a lot more than this, but I almost wanted to give you just a bit of a teaser of what is in this interview. [00:03:30] Really, lean back, take lots of notes. We put links to the show notes for you to read through it if you prefer. If you want to go find him on LinkedIn and read some of his material, he's got a wealth of information that we'll put into the show notes. With that, I want to welcome you to my conversation with David Linthicum.

David Linthicum: Well, thank you very much Bill. I appreciate you having me on the show.

Bill Murphy: Well, all of my listeners have just listened to me talk [00:04:00] about your extensive and very prolific background. I'd love for you to talk about the present. You've just written this, I think, a great article on LinkedIn, Cloud Security Secrets Your Cloud Provider Doesn't Want You to Know. Now that we're all working from home, and now that everybody's really taking advantage of all of the resources that have been built through the years through the cloud, what are your thoughts? What are the secrets some of the providers [00:04:30] don't want you to know?

David Linthicum: Yeah, that was a blog I did on InfoWorld. Ultimately, did that last week. The big thing is that we're moving into a multi-cloud world. I think the cloud providers themselves are very interested in their own domain, and so they want to keep security in their own public clouds. They offer some very good identity access management encryption systems, directory services, things that are table stakes for moving into security, but typically don't deal with the multi-cloud [00:05:00] world. When we're moving into a complex heterogeneous solution, which everybody's moving to right now, whether you're against it or not, ultimately, this is something we have to think through.

They're not necessarily instructing you on how to work and play well with other clouds, and so the end users are on their own. They have to think through what the technical solutions are, what the details are, how to make it happen, how to deal with security managers, what tools are out there, things like that. I think [00:05:30] that's really a tougher nut to crack out there. I think enterprises are going to end up making mistakes.

Bill Murphy: Do you think this comes down, when you say a multi-cloud, you're beyond just authentication and identity management in multi-cloud, are you referring more to the backend having multiple systems and moving them between clouds? Or maybe we can clarify for people what we mean by multi-cloud and what layer.

David Linthicum: Yeah, sure. I probably should have stated that first. Multi-cloud is going to be plural public clouds [00:06:00] typically, and it may or may not have a private cloud, which is bolted onto it, which is also multi-cloud. But if a private cloud is paired with a public cloud, that's called a hybrid cloud, according to Nest. We're moving to these environments where we're dealing with many traditional systems and applications that are participating and communicating with many systems that are occurring in the public clouds. Those are typically the big providers, AWS, Microsoft, Google, things like that. Then we have application workloads [00:06:30] that are running on those systems. We have data storage that's running on those systems. We have perhaps specialized systems such as AI technology, IoT technology, they're running on those systems. What we're trying to do is come up with a general common security service that goes across all of these systems, at least that's the objective of where we're looking to move to going forward.

That's becoming a bit of a difficult thing to do. At a point, we're moving into multi-cloud without necessarily the understanding [00:07:00] in how to do the proper security and leveraging the right mechanisms. It's really getting into the mindset that we're going to leverage common services across clouds. Even though people are implementing cloud native security systems today on the different cloud providers, I don't think that's going to scale. It's going to basically cause too much complexity. We're not going to have people around who are able to maintain all three security systems because it's different skillsets, and that's going to end up raising the vulnerabilities in how these [00:07:30] things work.

Bill Murphy: That is such a big issue that I'm quite vocal about, is stripping complexity out of this. I think that we're at a point where we're well beyond humans. If we don't figure this out now, I think, from an architecture perspective, then I don't know if we're going to be able to dig out of the complexity, unless we're really thoughtful about the strategy of how we're going to handle this.

David Linthicum: Yeah, I'm passionate about it. One of the things I've done at Deloitte, and [00:08:00] with a great team here, is create a cloud complexity management methodology, and approach to either fix complexity, as we find it, or avoid complexity as we start moving into the cloud. I think that it's something that should be on one of the top priorities of the different enterprises out there. As we're going through this crisis, and I think one of the things that could be a negative outcome is companies moving too quickly to tactical decisions around security and governance, things [00:08:30] like that, that ultimately lead to so much complexity that you can't operationalize the systems. We saw that in the last year or so. In other words, enterprises will build these very complex heterogeneous multi-cloud environments because that's what the cool kids are doing, and they'll roll it out, and then ultimately, they throw it to operations and operations just doesn't have the resources or skills or the tooling to operationalize stuff.

Then gets kicked back to the developers and the migration systems, and they end up normalizing or, and basically [00:09:00] migrating twice to fix problems with complexity. We can proactively avoid it. However, I'm not a big fan these days of wagging my finger at people who've made mistakes, but we can actually fix the thing once it's been deployed and do so with a minimum amount of work.

Bill Murphy: We have this moving car and we're trying to change the tires in a moving car. Potentially, there's multiple moving cars if there's multiple clouds. I think the authentication, the IAM tools, [00:09:30] I guess thinking of RSA, Microsoft, Okta, Duo, and the list goes on, are you seeing complexity that side of the fence with some of these decisions?

David Linthicum: I am, if they're using multiple tools without a good reason for using multiple tools. In many instances, you'd find out that they're using heterogeneous security managers because something has maybe 5% of the capabilities that they're looking for. To me, that's not a good reason. I'd rather see them [00:10:00] standardize on one tool and do the custom integrations to put it under one abstraction layer, versus multiple abstraction layers. I think that's where people run into problems. Of course, even if you have the people around to maintain a very complex environment, I think ultimately, you're going to find that it's going to raise the risk of breaches just because of the complexity that's there. You can calculate that. The cost of risk is something that consultants had figured out for years and how to do it.

Then the more technology [00:10:30] you have that layers into the systems, even if it has a specific niche-based role, the more complexity that comes in, and the weaker your security system's going to come in. In other words, you can have one security system that's much better than three security systems, even though that one security system doesn't cover every feature and function that you need. People need to consider the trade-offs there. Even staying with traditional security for now in certain instances where you can't incorporate legacy or traditional technology under the security blankets, [00:11:00] different ways of dealing with compliance, things like that. Really, we need to consider these trade-offs. We have a tendency to kind of be kids in a candy store. Since cloud computing is almost instantaneous satisfaction, we can go ahead and add these things in a very short period of time, even some of the on-premises systems, we can download them in a very short period of time. We need to ask ourselves, it's not that we can, it's really, should we? I think that's the question that's not being asked.

Bill Murphy: Well, I think this potential, and again, I think the [00:11:30] markets are going to rebound, I know you share that opinion, but I do believe that, regardless of whether the markets rebound or not, businesses want speed, and that is speed in defense. I call it offense and defense. The offense desires for the organization are moving and they're moving fast. One of the questions is how do you structure your defense so that it is mobile and can move fast and keep pace? Because I think businesses are going to keep requiring [00:12:00] more testing, more innovative approaches. They're going to not want the ... Also, because of the potential economic environment, they're going to need to do more with less. That seems like that hand is going to be forced for security.

David Linthicum: Yeah, it is. I think the biggest advice I would give is put complexity and put volatility into a single domain that you can configure. You think about it, we're building security systems. If we do that properly, they should be able to change fairly quickly to adjust to the needs of the organization. If they don't, [00:12:30] then they're going to have value for the first six months, then cease to have value after that. I'd rather see us put the time and effort into creating a security domain that deals with volatility and is able to put volatility into a specific domain that we can configure and change versus these big monolithic systems that are tightly coupled to all the application workloads and all the data workloads and all the systems out there and whatever level it is.

If we change them, we have to decouple them, and it's three or four months of different coding [00:13:00] and developing to merge them into something else. That's just too slow. Number one, it's going to cost us more money. What you just said, we're probably not going to have the budgets going forward we had for the last five years. Number two, we need to move fast if we're going to move into a product line or take advantage of a market movement, things like that. I think that companies that aren't able to take advantage of that are going to end up falling by the wayside, which is a shame. We're going to see this thing that I wrote about a year ago called the Brand Apocalypse, where the [00:13:30] larger brands and the more cumbersome companies that really don't get the ability to leverage technology as a force multiplier and the ability to deal with a running and gunning environment and the ability to deal with a very agile environment, where we're rewarding those kind behaviors are just going to end up going away.

That doesn't mean they're going to go away completely. They're going to get bought by different people. Then, we're going to see a lot of brands just disappear, which is a shame.

Bill Murphy: I think one of the challenges that I know a lot of the decision [00:14:00] makers I run into or I see them unconsciously facing, is when you have different workloads in AWS or Azure and still having legacy systems on-prem, that they're now, they think they're fighting three different solution sets, or potentially three different solution sets, or using the clouds native security to secure them. Instead of using a third party that they can integrate across all three. I'm curious, are you running into similar [00:14:30] situations with Deloitte, that the simple decisions are adding complexity when they need you to simplify on one tool that can scale across the whole?

David Linthicum: Yeah, ultimately, that's really the crux of the issue out there. I think going forward, and people, as they deploy things today, they have a tendency to get certain religious beliefs around the particular cloud provider. You get into some of these enterprises and you have the AWS folks, you have the Google folks, you have the Microsoft [00:15:00] folks. They think everything that's native to their particular cloud of choice is going to be the right solution, including security. So, they end up deploying three different security solutions, when really, we should look at one common solution that goes across the clouds, and that's a tougher road, because number one, you have to have the political will to get into those different groups and sell them on why that needs to occur. Number two, you need to find a mechanism to make that happen, and they're emerging, but they're few and far between right now. In some instances, we have to knit together [00:15:30] a couple of tools to make that happen.

Then number three, you have to figure out some an operational playbook. In other words, hey, you got to run this thing in longer term, and that's where people have a tendency to fall down. If they do build these three different security layers and they don't have common directory services, they don't have common abstraction layers in terms of how you're dealing with security, common encryption frameworks, things like that, they roll it out, then ultimately, it runs into the operational challenges, where they really can't make this thing work [00:16:00] in a safe way for a long period of time. In fact, one of the things that I look for within organizations that are making this mistake, I look at their job postings. If I see cloud ops jobs list and list and list, I can tell they have a morale problem because they operationalize something that probably wasn't prepared to get operationalized, and the cloud ops folks think they're being set up for failure and they're moving out of the company.

I think that's a shame. I think we need to think long and hard and put the money and the talent and the observation [00:16:30] to the common architecture. We're missing that, I think, largely.

Bill Murphy: It's interesting that job description. I often find the job descriptions that ... It's funny, you're working with big, big, big enterprises. I tend to work with more mid-market and big small, which is funny, they're still pretty big companies, but they're certainly not super small. It's interesting that the job postings, they're looking for a savant, and I've yet to see a savant exist [00:17:00] in this world of cloud, because it's, by definition, you're not pulling on someone with 30, 40, 50 years experience. Most of them can't afford that type of a talent. To your point, I don't think that they've really thought through what they want from the outcome, so they ask for everything.

David Linthicum: Yeah, and you can't do that. I think ultimately, when you hire people, you need to hire people who are typically going to be continuous learners, autodidacts, which is more important in specific skillsets. [00:17:30] I think that they're few and far between right now, in people who have every skill. One of the things I recommend that when people hire, whether it's for security, governance, database, whatever, is that they hire people with the ability to move their skills very quickly as things change. One of the things that is a big career booster for me is you got to be prepared for the changes coming down the line, and be able to self-learn as you move forward. When I hire people, I hire people with the same sort of a pattern, because I can do [00:18:00] more with them over time.

If someone has an AWS security certification and I'm going to put them in into a security architect role, eventually, the AWS security stuff's going to change, we're going to move to different layers, we're going to move to different levels, different clouds, things like that. If they can't maneuver with those changes, and then ultimately, they're not going to be much good. I think the enterprises nearly need to think the same way.

Bill Murphy: You had written in this article in InfoWorld about training counts more than technology. [00:18:30] Are you seeing that people are going to be able to make that jump from on-premise skillsets to cloud skillsets, and then once they're into cloud, skillsets not become so dogmatic about one particular cloud provider that they start crying if they have to go learn something different?

David Linthicum: Yeah. I think ultimately the ability for people to understand where this stuff is going, and as we just mentioned, your ability to become a continuous learner is going to be the most effective thing to do. But the thing is, [00:19:00] enterprises need to splurge and provide the availability of training. People who want to go take a video course on Lynda.com or Cloud Guru, or any other place that they teach this kind of stuff, should have the capability of doing that. What I say in the article is that, it's a thousand factor for every dollar you spent. Every dollar you spend on cloud training, you remove a thousand dollars of cost of risk from your system. To me, that's a bargain, that's something that I can make [00:19:30] a tangible value, and you can measure that as well.

Ultimately, you need to provide people with an opportunity to self-train, and you need to provide people with the ability to, in essence, localize the training in what they're doing on a day-to-day basis. You're going to have certain people who have different religious beliefs and things like that, what I call managed by magazine crowd. In other words, they're following the hype. You need to identify that and make sure you break those behaviors, because those aren't necessarily [00:20:00] going to scale and it's going to lead to making bad decisions. As far as moving people who are dealing with traditional technologies, security on premise, things like that, and security in the cloud, completely different beast, but I'm finding that pretty much half the people can make the migration. It used to be thought, well, none of them can. We have to hire new people with new skills and things like that. Reality is that someone who has 30 years experience in IT, and you're moving them into a security architect role, they come with invaluable knowledge [00:20:30] of traditional systems and how to layer security back into those systems.

I think, as we're moving into very complex heterogeneous cloud environments, where we have traditional systems and public clouds and private clouds and IoT and edge-based computing, all these sorts of things, those skills are invaluable because they know how to extend security to a mainframe system. You talk security to someone who's been in the business for the last 10 years, has only dealt with cloud, they're just going to think of cloud-based security, when really it's holistic within the enterprise. In fact, you're going to have [00:21:00] more ability to have value in terms of security system with traditional systems than you will with cloud systems, because that's where everything's still running. Most companies only have 20% to 30% of their assets in cloud. While the rest is running on premise, those things need to be secured. Those security systems need to be updated.

By the way, I think we can use common security layers between the cloud and traditional systems, and thinking through that is a very complex array of technology, a very different way of thinking. That's typically going to be a team of the traditional [00:21:30] players and the new cloud players that make that happen.

Bill Murphy: Have you seen organizations that are successfully bridging their security from on-prem world into this multi-cloud world? Are there some case studies or some wins, and not like a classic case study, but are you seeing people that have really got this figured out and they have got teams that are managing all of these domains and pulling it together quite nicely?

David Linthicum: Few and far between, there's a couple key examples. [00:22:00] Some of the banks that I've worked with over the years have the ability to create common directory services and common identity access management layers, and implementing common security services and common encryption services between traditional systems and the public clouds. They've done that typically through a lot of pain, trial and error and spent a lot of money. Typically, the finance groups, finance organizations have more money to spend on technology than say retail and manufacturing, things like that. For the most [00:22:30] part, the pattern is this, the pattern is they go ahead and move into cloud. Typically, that's two to three public clouds, and they're using one as a primary. 80% of the stuff runs on one cloud and 20% of the stuff runs on the other cloud, but they're still supporting the multiple clouds.

Don't have any clue as to how to link the existing security in the cloud-based systems with traditional systems. May not even have the resources to make that happen. That's the big sticking point. In other words, it's not the fact that they don't have the desire to create [00:23:00] common security layers, but in order to create a common security layer, you're going to have to basically invest in some very expensive people and some very expensive technology to really make that happen. That's where the trouble comes in, and you get the budget limitations besides the desire limitations. Where in some organizations, they have the money to spend and they go ahead and splurge on making those things happen. It may be a bit of trial and error, but they make it work.

So, it's a very small percentage of organizations out there that really have security [00:23:30] nail between traditional systems and cloud-based systems. That's going to increase over time, and certainly, as a tooling becomes better, it's going to increase over time. But the core limiting factor is not the fact they don't have the desire, it's resources, it's money, it's budgetary limitations.

Bill Murphy: It's interesting. Just before the corona hit, everybody had a series of different events, physical events that we were putting on that for CIOs and CISOs related to, believe it or not, SIM solutions. It'd [00:24:00] often come back to ... there was 10 million quarter inch drill bits that were sold in Home Depot last year, but I often say, nobody wanted a quarter inch drill bit, they wanted a quarter inch hole. It's like, nobody wants these SIMs, but they want what the outcome is. The more we dove into this, the massive ... Really, this is like an urge ... it seemed, to me, to be an urge for people to want to simplify, because in theory, if you had one of these systems, [00:24:30] if it worked, meaning if it could ingest all the unfriendly other third parties into it, in theory, that would be a step in the direction of less complexity. We're not there yet. What are your thoughts on centralized aggregated systems like that? What are you seeing?

David Linthicum: Well, we need to make architectural trade-offs as to what we can do pragmatically with the technology that's out there. I believe what you said is true right now. In other words, we don't have every perfect tool [00:25:00] to remove us from every bit of complexity within the systems. I think you architect for it ultimately. Even if you have to leverage different tooling, you minimize the amount of tooling that you're able to leverage and understand the trade off of adding additional tooling in terms of the operational costs going forward. I think that most organizations have lived through their IT careers with never meeting a tool they didn't like, and people have a tendency to jump right to the technology when they're dealing with [00:25:30] architecture. I think that's the wrong approach. I know it's something that's not popular, because people don't find architecture and planning a sexy process you're able to go through, and it's drudgery for some people, but ultimately, a bit of planning and a bit of thinking in terms of how these things are going to be done, the ability to create a logical architecture and then a physical architecture.

In the cloud complexity management stuff, what we do is ask people to create domains, cognitive domain, data domain, security domain, governance domain. I think it's nine [00:26:00] domains that we have in the stack. The idea is to look at this from a logical point of view, and look for opportunities to improve. I don't think you're going to be able to see opportunities to improve if you put limitations on your creativity, because you're leveraging tools that have a static way of doing things. You're getting the core processes, getting the core technology, you're having to go adapt to someone's vision of what security needs to be versus you creating a logical understanding of what your security patterns are, whether it's in your traditional systems, cloud systems or all of them, [00:26:30] and I typically ask you to do all of them.

Then find out the tools that get closest to solving those requirements. I think if you're able to do that, it's a much healthier exercise. You're going to get to an optimal solution. That's going to have the least amount of complexity. But it does require that you have to stop and do some planning and do some thinking and do some testing and create a lab in the organization. In some cases, create a center of excellence so people can come in and test things, things like that. Those are [00:27:00] investments that enterprises are typically lacking now. I think they should think differently.

Bill Murphy: Is there an area where outsourcing would make ... A lot of companies outsource their taxes, they outsource different elements of finance and they outsource some payroll processing, things of that nature. Are there certain areas within cloud security that you see as being just really great opportunities for businesses to leverage their party expertise?

David Linthicum: Yeah, I think SecOps [00:27:30] would be something that I would look to leverage third party expertise, because if you think about it, if you're leveraging a third party, they're really good at that security operations because they do it from multiple companies. It's almost like a practice where you go into a doctor and the doctor has had many different experiences, so they know how to cure the issue, versus someone who's sitting alone in a room who's operating these systems that hasn't seen it all. But you have to find the right outsourcer in some of these cases. [00:28:00] But SecOps and the ability to make these things scale, I like the idea of the ability to leverage managed service providers or security operational firms. They're able to probably do a better job than the people within the organization just because they have more experience in different patterns of solutions that they're experienced with over the years.

But you have to find a good one. But typically, you can do it cheaper than you can if you bring it in-house. I think that we're going to start looking for these opportunities [00:28:30] to outsource some of this stuff going forward. Now, the downside of that, it's a political nightmare and people are against it, because obviously they think you're dealing with security, this is the keys to the kingdom. We probably shouldn't trust an outside organization, but the reality is we said that about cloud computing 10 years ago, and look where we are now, completely trustworthy. By the way, security is better in the cloud because more R&D dollars are flowing into cloud-based systems and are flowing into traditional systems now. Ultimately, it's just going to be a much [00:29:00] healthier way to do it.

Bill Murphy: Yeah, I think that that was probably an argument for many business departments through the years with finance and accounting and payroll and lots of different areas, accounts payable, and like. I think there's a trust factor that has to be built first. But it seems to me, if businesses, especially coming back from the potential pandemic, because they've reboot themselves, they're going to be focusing on revenue and customer acquisition and retention, and security is, [00:29:30] certainly if you're a bank, it's way high, but even then, there's going to be pressures on the offense more than the defense, so they're going to have to make some decisions about if they want Barry, who's been there for 30 years. They want to train him as a security architect or have him working with the op dev folks to put product out into the field. It's going to be interesting decisions.

David Linthicum: Yeah. I think it's going to be probably more aggressive and probably self-centered for companies going forward, because they're really primarily concerned with protecting themselves, but also, the ability [00:30:00] to get some of the costs out of the systems. We're going to find that most organizations that spent heavily on IT over the years probably had the worst experience during the pandemic because they had more systems on-premise, they had more systems in data centers and ended up digging ... couldn't get humans to get into the data center for whatever reason, lockdown or quarantine, whatever. Ultimately, the clouds kept chugging along. Anybody that had more of a progressive role and was able to move aggressively into the cloud, not only was able to save money, but [00:30:30] reduce their vulnerabilities in situations, stuff like this. Organizations that didn't spend the money in moving forward or didn't take the risk, ended up getting the ears pinned back, and I think people are going to learn from that.

Businesses have a tendency to learn from pain. So, coming out of this, the boards of directors, the investors, and I was an officer of three different public companies at different times of my career, and that's where the pressure comes. They're going to say, "How are you going to make this thing resilient? How are you going to leverage whatever technologies and resources, [00:31:00] including cloud or whatever, to make sure this doesn't happen again? How are you going to bulletproof our existing systems?" People are going to move in a much more aggressive direction. Probably not going to spend a lot of time arguing about the trust factor of moving something to a third party, it's going to be, are they cheaper? Are they better? Are they faster? Then we'll do it. Is this thing, workload more productive in the cloud? We're going ahead and make the move and do it. Different security frameworks. It's really going to be more of a [00:31:30] running gunning kind of thing. You say offense, so I think that's probably a great word.

Bill Murphy: Yeah. I agree the way you just said that. Well, you've been on publicly traded companies and seen that pressure. So, you're talking for someone who's been there. We've had these pressure points before in 2007/08, and we've seen it in 2001, the dotcom. People have a different mindset when they're in protection mode. It's just a natural human biological. [00:32:00] The irony of this is really very, very interesting in how we've been spending years protecting against the infections, the viruses, the malware, and we've been doing this on the digital framework and wanting to create systems that are very resilient, and that collapsing and security, almost security and business continuity have become almost synonymous. That pressure has been there for our digital universe, and now we have the biological, and it's funny how [00:32:30] the words are shared almost equally between them.

I'm wondering if there's a vision of having a business that has an immune system, that has an immune system response to it, of where sometimes we need to go to the hospital because we need to get manual and patch and recover, but for the most part, it's automated. There's automated response to this. I'm wondering, how close do you think we are to having something that is automated and mimics our biological response?

David Linthicum: Yeah, I think [00:33:00] for the most part, the enterprises were caught off guard by this, and they found out that they couldn't have a sale remote workforce at scale, they couldn't do manufacturing the way they could. Their core systems were exposed, even had some security issues, some performance issues that arose from this. Few companies, certainly ones that were started in the last 20 years that may be born in the cloud, much more progressive in leveraging technology, typically have a great remote workforce policy. They put in a VPN circuit. [00:33:30] That's the big thing, people were running out of those like crazy, and can scale and have this really kind of as a BCDR process that's built in, are going to do much better and did much better. The problem is that you have to get people thinking about all these different considerations.

If someone said, last year we'd be in the middle of a pandemic and dealing with all the business issues around that, I don't think I would have believed them, but I do believe in building these things in the contingencies, good news is [00:34:00] that if you go at this aggressively and progressively, that you're going to able to build a resilient business that's able to survive viruses, whether it's digital virus or the biological virus that we have today, but you have to think of all these scenarios in your mind. What if we lose our building and the people have to work remotely? Certainly, the initial terrorist attacks in New York City were kind of on that thing. In other words, they lost [00:34:30] access to the world trade center, and this is the first bombing. Ultimately, they had to go home and work. For the first time, that was hard to scale, because the internet wasn't that big of a deal back then.

But the ability to either think in how you're going to configure your business so it's prepared to deal with that so you're not changing anything, it's just basically is, and therefore defensive against whatever's going to happen, or your ability to, in essence, be defensive and be able to change the business around the [00:35:00] way in which you want to consume the technology. I think that those are hard questions. I think that they're going to be asked now, but, it's a shame that a lot of the organizations that are really, truly going to be damaged to the point of being taken out of the market didn't ask these questions last year.

Bill Murphy: Well, I just had a couple ... actually, one major question that hopefully you could help out with. I know you have this cloud complexity methodology through Deloitte, and you had talked about developing an ops playbook. I think that, [00:35:30] that's interesting, because an ops playbook, and then you talked about common directory structure, common encryption, and common abstraction. What did you mean by common abstraction?

David Linthicum: Yeah, what we're doing is in essence, removing the human beings from dealing directly with the complex systems. We're creating, probably a better term would be a single pane of glass, where we're able to see security parameters, security processes. We're able to find policies, we're able to define and configure different [00:36:00] encryption systems, things like, that through a common mechanism. Whether it's implemented natively in AWS or Microsoft or Google, it doesn't matter to me. I don't have to understand those native API. I'm able to leverage some sort of a dashboard that's able to take care of those on my behalf. So, I'm dealing with security the same way with AWS, Google, Microsoft, and even my on-premise systems. The ability to do that gives you a much better view in terms of what security [00:36:30] is doing holistically, in and between the various systems.

Typically, applications and datasets and things like that, typically span these things. They span different clouds and certainly, they span the on-premise systems. If you don't have that view, I think you're missing part of the picture, and if you're missing part of the picture, you're going to end up getting into trouble. I think that we need to think about how we're going to build these abstraction layers and tools to build these abstraction layers. Right now we have security managers, which are basically just abstraction layers. We have cloud management [00:37:00] platforms, cloud service brokers. We have things that are emerging tools and technology, certainly the AI ops stuff that's emerging right now, and which ones should we use? If we use more than one, are able to integrate the views into a single pane of glass or single tool-based systems? Well, we're probably not there yet, but we do have some tools that we're able to do some abstraction, and moving to those layers, I think, are going to be hugely beneficial going forward.

Bill Murphy: [00:37:30] Does that mean that we're going to have to really get good with APIs being able to pull our data out of specific tools and be able to see this and get really good at ingesting APIs into some type of a single tooling system?

David Linthicum: Well, if you get a tool that is doing its job, then shouldn't have to deal with the APIs. It's dealing with the API for you. It's providing the abstraction layer between the different APIs and the common way than you're looking at encryption and identity [00:38:00] access management, and all these things that are important in security stuff.

Bill Murphy: Okay. Fascinating. Well, this is great. What a great conversation, David. Before we go, I wanted to ... So, where can people find you? We covered a lot of ground here today, but I'm to put on the show notes ways for people to reach out and learn more about your expertise in ways that they can start listening to you related to cloud security.

David Linthicum: Yeah. I've got lots of stuff out on deloitte. [00:38:30] com, including the On Cloud Podcast, which we do about once a week. I'm very proud of that, and it's growing in audience all the time. Also, got many cloud computing courses on Lynda.com, and including The Cloud Complexity Management Course, which is three hours, but worth it. Also, find me on InfoWorld, I'm the cloud blogger there.

Bill Murphy: You are also teaching at LSU, you said?

David Linthicum: Yeah, I'm doing some of the online courses at LSU, having a great time doing that.

Bill Murphy: That's fantastic. Fantastic. [00:39:00] Was there anything that you wanted me to ask you that I haven't and you're dying to get out there, or have we covered everything?

David Linthicum: I think we covered everything, at least what we should be covering in one episode, but we can do it again soon.

Bill Murphy: Absolutely. David, I appreciate you sharing your wisdom and your guidance for everybody here, and stay healthy here.

David Linthicum: You got it. You too, man.

Bill Murphy: Thank you. There you have it. This wraps another episode of Bill Murphy's RedZone Podcast. To get all the relevant [00:39:30] show notes, please go to our blog at ww.redzonetech.net/podcast. Additionally, make sure you go to iTunes and leave your comments in iTunes about the show. This helps our show rankings enormously and helps support the show. Until next time, I appreciate you very much for listening. Thank you.