A private Cloud-based approach to being a Managed Security Services Provider

Transcript of a Patrolling the Channel podcast on how Managed Security Services Providers can take a private cloud-computing based approach to better serve their customers.

Total Duration: 17 Minutes

Jane Wright: Hello and welcome to this edition of Patrolling the Channel, a podcast to help you, the security solution provider, better serve your customers! I am Jane Wright and it's great to have you with us.

Security solution providers have a choice when offering Security Information and Event Management or SIEM services to their customers. They can install that appliance with SIEM software at the customer's site and then perform the monitoring, responding, and reporting services remotely. This is the traditional approach and it usually works pretty well.

But there is another approach that some security solution providers are taking, and like so many things today, it involves the cloud, or more specifically, a private cloud of the solution provider's own making.

These solution providers are licensing software from a Security Information and Event Management software vendor and installing the software in two places; some on their own server and some of the software on their customer's server. Then they begin to monitor and respond to the customer security events, all the while charging the customer on a pay-as-you-go basis.

What makes this a cloud-based implementation, or maybe we should call it a partly cloudy implementation, is that the customer's security data lives and stays in the solution provider's own data center. There are lots of reasons why you may be considering this approach and plenty of reasons to make you wary.

So today I have asked Dave Nelson, President of Integrity Technology Systems in Iowa to talk about this private cloud-based approach to being a Managed Security Services Provider.

He will discuss why he chose to go this route, how he sells it to his customers, and whether this is a viable approach for even small security solution providers.

Dave, thank you for joining us today!

David Nelson: Thank you Jane, it's my pleasure to be here!

Jane Wright: Dave, could you describe the Security Information and Event Management services you offer to your customers and how it's implemented in a cloud?

David Nelson: Sure! One of the overarching aspects of services that we provide to our clients is being able to be the expert when they don't have the resources to do that on staff themselves.

One of the things that we have provided to them is the opportunity to have the SIEM product in the cloud to where there is no upfront cost as far as capital hardware expenditures go, there is no upfront cost as far as human capital go for them to go out and hire and retain specialized individuals.

What we try and do is provide a Software-as-a-Service model where we can provide the infrastructure to collect all of their event logs and then analyze it with our staff in a remote environment so that they don't have the upfront cost associated with their traditional SIEM implementation.

Jane Wright: And why did you decide to start your own private cloud instead of running a more traditional SIEM operation?

David Nelson: Two factors; from a traditional SIEM implementation has a lot of upfront hardware and software cost. A lot of the traditional SIEMs have been developed for an enterprise where those enterprises are willing to have a sophisticated implementation. They also are very defined as far as the size of that implementation. And so what we decided to do was to build it in the cloud so that we could scale up as we needed to and we are not locked into a very specific sized hardware device.

Jane Wright: Do you have any concerns about maintaining uptime or dealing with downtime for your customers?

David Nelson: Oh, certainly, anytime that you are monitoring a production environment, you have the need to be able to provide certain types of SLAs, Service Level Agreements based on uptime and availability.

One of the benefits though to a cloud type of environment is the ability to have redundancy built-in. With our particular environment, our collectors and analysis engine has the ability to be developed or implemented in a highly redundant and highly available solution, such that we can limit downtime. If one particular device fails, we can go in and manage that through multiple devices, we can have that failover to another device, and so we certainly eliminate that.

When you are talking about putting this in, in a traditional SIEM environment that typically means duplicated hardware across the board and a very highly scalable and highly redundant infrastructure, whereas by going to the cloud we can leverage that single infrastructure, highly redundant infrastructure, across the board for all clients.

Jane Wright: Whose SIEM software are you using and why did you choose that one?

David Nelson: We went through a pretty direct procurement process and spent about six months looking at different solutions. We are currently using and we have settled on the AccelOps platform.

The reason that we settled on that was two-fold. One, it was developed from the ground-up, from a service provider model. Most of the other vendors that we looked at were taking a traditionally enterprise type of solution and trying to overlay service provider feature sets to that. That just didn't scale well for us. That caused a lot of issues with data redundancy or segmentation and multi-tenancy.

The second was that most of those providers, because they were enterprise level, they were designed around a specific piece of hardware or a specific size of software to be placed on the customer's hardware.

With AccelOps, they have a virtual appliance. So we can quickly and easily get that appliance out to a customer. It can run in a VMware environment or on a basic Linux environment and we are not tied into hardware. We are just simply using a license key to increase or decrease the licensing as we need to for each of our clients.

Jane Wright: Which other vendors did you consider and why didn't they fit your needs?

David Nelson: We looked, and we actually had utilized Splunk for a while. We looked at TriGeo, Q1 Labs, NitroSecurity, ArcSight. Most of them, like I said, were built around the tenet of placing this in a single enterprise. So the feature sets are very good, but sometimes the service provider needs were a little bit different and we didn't feel like they were baked in quite as well.

Really the biggest issue though was around hardware. Most of these vendors require you to buy some sort of hardware device to place out in a data center to collect all of the logs, and it has to be sized appropriately. And if you start out small and then try and increase the capacity later on, sometimes you are pitching that old hardware and starting from scratch.

Some of the vendors do give you a kind of an upgrade path, but not all of them do. So we really liked the functionality and the feature set of having that virtual appliance that we can put in and we can scale it up and scale it back as we need.

Jane Wright: A lot of security solution providers may prefer to continue offering SIEM services in the traditional manner. They may be concerned about operating a private cloud or being responsible for the clear separation of boundaries between all their customers' data. Are there other reasons to be wary and how do you respond to all of this?

David Nelson: Sure! One of the issues that I think a lot of service providers are going to run into is, where do you draw the line between simply monitoring and then responding to an incident? So those lines have to be very clearly drawn with clients. You have to have specific contracts in place that spell out when are you going to monitor a device, how will you provide that information about a specific security threat or a security breach back to the client, and then whose responsibility is it to actually investigate and remediate that.

In our case, we typically have a monitoring contract and a services contract where we are doing consulting on the backside. So it falls to us on both sides. However, if you choose not to do that, there really certainly can be some big issues on who is going to address that vulnerability or who is going to address that breach once it has been discovered.

Jane Wright: So you are essentially operating a private cloud from which you deliver your SIEM services. Isn't it kind of expensive and how can smaller solution providers do this?

David Nelson: Certainly, it can be expensive, but one of the things that we found is that the return on investment is typically pretty quick. When you are looking at the startup cost, certainly you are going to have some infrastructure cost, you are going to have a specific cost for the licensing of whatever tool it is that you end up utilizing, and you are going to have the cost of your human capital; the people that run the system, the people that manage the alerts and the events and communicate with your customers don't come cheap.

But one of the things that we find is, for us at least, we were already doing a significant portion of that and so it was just adding on to the services that we were already providing and the return on that investment was pretty quick for us.

The benefit of being able to add yet another service offering to our clients, something that differentiated us between the other security providers in the area certainly made it as a great value proposition for us. So it was worth the expenditure.

Jane Wright: You mentioned that the AccelOps Security Information Event Management Software is installed as a virtual appliance on the customer's own server, or the cluster is installed as a virtual appliance on the customer's own server. What if your customer doesn't have VMware or virtual environment, or also you mentioned Linux, but what if they don't have Linux?

David Nelson: Sure! Well, the benefit of this particular implementation is that it runs on EFXi, which is a free version of VMware. So as long as the customer has a server of some type, and it doesn't matter if it's a specific brand, it just has to meet the requirements, they can install it.

Certainly, if they don't want to, we have the option, and we do provide customers with a server that's completely managed by us and we just load it up there. We don't particularly like that option because then we are back in the hardware business. We are providing a device that's a piece of hardware that we have to support and maintain. We have to worry about warranty and outages and those types of things.

But in this day and age, almost every single customer that we come across, no matter how large or small, has the capacity to run some sort of virtualized environment, and most of them would much prefer to have their own server hardware in there, so that it matches all of the rest of their infrastructure, it can be monitored and maintained versus having us in there doing that on their behalf.

Jane Wright: Why don't you just resell the AccelOps software and then add your own services? That's an option for you, I think, and wouldn't that be an easier way to make a living?

David Nelson: Certainly, one of the things that we did look at was just reselling the services that AccelOps offers and then utilizing a services contract on

the backside to maintain and monitor the alerts that occur in that environment.

One of the things that we looked at though was being able to create a unified marketing and messaging. So with this particular platform, we have the ability to white box the solution so that when a customer logs into the portal, they don't see the AccelOps license, they don't see the AccelOps logo, they don't see the AccelOps software, they see it completely branded as Integrity. And that really helps us strengthen our brand. It helps us have some legitimacy to the services and offerings that we are providing.

One of the other things is customization. Whenever you move something to the cloud, you end up having to be, to some degree, in a cookie cutter environment. If you fit into the environment, that's great, but you can't make changes.

There are certain options or configurations or features that may be available in the full-blown version of the product, but because you are in a cloud environment, you can't customize that.

We really wanted to be able to completely customize the solution for our inner workings, something that would meet our needs, and then also that we could provide a full-blown feature set to our clients. And so that's why we chose to do it in-house versus just resell the AccelOps service and then monitor our clients through that service.

Jane Wright: There are other solution providers who are doing something similar, licensing SIEM software on behalf of their customers, adding services, and then running it all in their own private clouds. Can you tell us how you differentiate your offering, the Integrity Technology Systems offering, from these other solution providers?

David Nelson: Sure! The offering itself is very similar. I think from our standpoint we look at it and say the experience of the people running it certain makes a difference. Our staff, our team of highly trained experts, is what really differentiates us from any of our competitors. We believe that the training, and the customer service, the level of commitment to our customers, really makes a difference to them.

One of the things that we feel differentiates ourselves from just about everybody else in the marketplace is our commitment to a partnership with our clients. We don't want this just to be a financial arrangement; we don't want this to be something that is just simply a way for us to make money. We look at it as if we can help our clients succeed, if we can help them reduce their risk and become more profitable, that in turn helps us become more profitable, it makes us a better value to our customers. And so that's what we really believe differentiates us from our competition.

Jane Wright: I wanted to ask you how you position all this to your customers. What are the main messages you communicate to potential customers as they are considering hiring your company to watch over their security in this way?

David Nelson: One of the big things that we really go after is compliance. A lot of companies would like to be able to do some sort of security event and incident management or event log management or event log correlation type of work, but they try and look at it from the simple cost perspective and they say, I can't afford to do that.

One of the things that we really look at is, can you afford not to do that? From two perspectives:
First, from a compliance perspective. Is there somebody out there telling you, you need to do this? If you are HIPAA compliant or you need to be SOX compliant or PCI compliant, this certainly is a component of that compliance need that is a requirement that those organizations are going to have in front of them on a daily basis, and so they have to be able to provide that mechanism.

The second is from a risk perspective, for business leaders. Are there any gaps? Is there anything in your organization that you don't know about, things that you are not monitoring, are there any blind spots? And I know for me, for a business owner, if I have blind spots in my organization, I need to find ways to get visibility into those.

So we really pitch event management and security and event monitoring from that perspective, being able to say, we can show you the holes, we can add some light into those dark areas of your organization and help either, A, point out some things that maybe aren't going so well, or B, give you reassurances that everything is being taken care of.

But either one, either the risk or the compliance needs to be addressed, and one of the things that we can do is also provide the independence. Whether you are looking at this from a risk prospective or a compliance perspective, it's no good having the fox watch the henhouse. You don't want the same system administrators who are responsible for administering, designing, overseeing the systems, also being the ones who are monitoring and managing the security. You really need to have some independence, and that's one of the big selling points is that we can maintain an independence that nobody on the internal network can.

Jane Wright: Dave Nelson, President of Integrity Technology Systems, thank you for joining us today!

David Nelson: Thanks you, Jane! It has been my pleasure. I really appreciate it!

Jane Wright: And thanks to all of our listeners. Until next time, I am Jane Wright.

Total Duration: 17 Minutes