

WAF in the Cloud – an Interview with Chris Richter of Savvis

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining me today is Chris Richter. Chris is Vice President and general manager of security products and services at Savvis, a leading network, hosting and security services provider, where he is responsible for the managed security line of business, strategy and product portfolio. Chris has assisted many enterprises in adapting their premised based infrastructure risk management programs and security controls to Savvis' outsourced virtualized and shared infrastructure services.

He brings an IT service provider's view of control requirements for virtualized and cloud based infrastructures. Chris is a member of ISACA and for more than 20 years has held various security and IT services and management and consulting positions at companies such as Digital Equipment Corporation, Compaq Global Services, 3Com, Cable & Wireless, and Sterling Software. He is a Certified Information Systems Security Professional, and a Certified Information Security Manager. And he has served as a technical advisor and board member of several Silicon Valley based IT product and services companies.

Welcome to the show Chris.

Chris Richter: Thank you Brian. Thanks for having me.

Brian Contos: Chris, before we get started, I was hoping that you could give me a little bit of background on what Savvis is and what you do there.

Chris Richter: Savvis is a network and hosting infrastructure as a service provider. We've been in business for over 10 years and most of our business is conducted through our Tier one network services infrastructure and our 29 hosting data centers located worldwide. My title is Vice President Security Products and Services and I'm responsible for established security business and product portfolio.

Brian Contos: Now Chris, I know a big part of what Savvis does is tied to cloud computing. Why is it that cloud computing is so hot now? I mean, you go to any conference - security conference, IT conference, whatever - cloud computing is talked about as much as PKI was five or six years ago; hopefully it has a better future. What's driving the business?

Chris Richter: Brian, I think the number one driver is cost. There is a rush to virtualization and cloud computing primarily because, I think, IT professionals and managers see it as a way to reduce operating expenses and IT expenses overall. That's one. Another one that

I've heard is ease of management. It's simpler to manage multiple machines if they're virtualized cloud-based. The promise of it is you can do more management via a portal as opposed to multiple consoles; a single pain as opposed to multiple pains and multiple swivel chairs. And I think there's a third driver. A lot of companies, I think, are moving away from being in the business of managing a lot of IT infrastructure. It comes down to something I heard one customer say, "Core versus context." They really want to focus on their core business and that is managing data on behalf of the revenue generating activities of the company. As opposed to managing IT infrastructure that is a step away from managing the data, which then in turn supports the revenue generating activities of the company. So, again cost reduction, ease of management, and an effort to allow them to focus more on the things that drive the top and bottom lines of their businesses.

Brian Contos: Yeah, you said something interesting there about the core competencies that made me think of the financial industry. They were probably one of the first verticals to really embrace business process outsourcing and a lot of banks would say, "We're going to focus on what we're good at. And what we're good at is banking. All these secondary and tertiary services that we can offer, all these other features and capabilities for our customer base, let's outsource those pieces to the folks that are actually the experts." And it seems to have worked very well. Getting back to the business of doing business, I think.

Chris Richter: That's right. And I had one customer tell me - you know being in the service provider business I hear these comments all the time but one customer, I think, summed it up when he said, "I'm tired of being an early adopter. There's so much new technology being thrown at us so quickly, I don't have the time, the resources to staff up and send people to training to deal with the turnover. And individual's, once they gain a certain area of expertise then they're at risk of moving on to a different job. It's much easier to focus on managing the data then it is to becoming experts in every type of technology that makes up a dedicated infrastructure." So yeah, I think that is in line with what you're hearing as well.

Brian Contos: Certainly makes the Visio diagrams easier. So, at Savvis, of course you're a partner with Imperva and I know one of the products of ours that you leverage is our WAF, or Web Application Firewall. Why are Web Application Firewalls so critical in this type of environment?

Chris Richter: That's a great question because a lot of people immediately assume that Web Application Firewalling is being driven by PCI, specifically by PCI control 6.6 and the latest data security standard. Actually our first several managed Web Application Firewall opportunities, had nothing to do with PCI. They were driven by the financial industry and it was all focused on protecting critical data, protecting critical applications that were web facing and that was being spurred by this growing occurrence of malware. Not just the kind of malware that turns your PC into a botnet, the malware that is far more insidious; designed to steal personal data, break into financial accounts and steal data. That was primarily the big drive, or I think PCI is also a big driver for Web Application Firewalls. But definitely we're seeing customers take a very strong interest in protecting their data from, in many cases, what they don't know exists out there. They're a bit concerned about the unknown and rightly so. Malware's a huge threat overall, especially to cloud computing.

Brian Contos: Yeah, it makes sense. I assume if you can take out one system in a cloud computing environment, that's potentially hundreds or thousands, if not more, organizations. So it's a target rich environment for an attacker probably looking to cause the maximum amount of casualties with the least amount of effort.

Chris Richter: Indeed. And you know, Brian, we're seeing increased movement more than I have over the past 10 years in just general application security and application security best practices. We're seeing more and more of our largest customers begin adopting and deploying application security, best practices, guidelines, processes and procedures. And Web Application Firewalling is a part of... they consider it to be a part of a best practices procedure. That includes... it's everything from secure coding, to vulnerability scanning, to proper architecting of their infrastructure and putting the right security controls in place, one of which involves deploying Web Application Firewalls. And I'm just skimming the surface but application security is something that we've really seen a strong increase in.

Brian Contos: Yeah, I'm glad you mentioned that, the whole notion of security development life cycle, black boxing, white boxing, vulnerability assessment software, vulnerability assessment services, WAF. I think several years ago when budgets were smaller around security, or specifically application security, everybody saw everybody else as competitive. Even though today you look at it and it's clear that they're actually synergistic and complementary solutions to address a common problem which is application security. And certainly WAF plays a part in that but, yes, you're absolutely right, there's many other flavors as well that also help.

One of the things that we hear from a number of our listeners when they send emails to blog@imperva.com saying, "Hey, we'd like to hear this on the podcast," or, "Discuss this subject," is time and time again are stories from the trenches. What are some of the real-life war stories? Are there some stories that you can share with us around WAF and say cloud computing, SaaS virtualization, that type of arena where you've actually leveraged WAF and it's been part of the solution?

Chris Richter: Yeah again, a lot of customers who are considering making the move into cloud computing are customers looking at our cloud computing offerings, often ask the question, "Well, how do we deploy a Web Application Firewall in the cloud?" Not every service provider can deploy a WAF in a cloud computing environment. The approach that we take, and I'm not trying to advertise here, but the approach that we take is to use Imperva Web Application Firewall system in our cloud computing environment we can basically mix what is a dedicated piece of infrastructure, the WAF, with a virtualized computing environment. And we build our cloud computing environment to accommodate dedicated devices where necessary; it's not a one or the other scenario.

And that comes as a relief to a lot of customers who must have dedicated Web Application Firewalling in an environment that they want to make completely virtualized. So that's one scenario that we're seeing customers take interest in.

Brian Contos: Interesting. What are some of the good lessons learned for those that are thinking about leveraging cloud computing solutions?

Chris Richter: That's a good question because a lot of customers are thinking that the lessons must change; cloud computing is completely different so this is a whole new modality, a whole new paradigm. What do we have to consider? Is everything different? The fact is that the same types of security controls that would apply to a physical environment should also be deployed and applied to a virtualized environment. The only real difference is making sure that you can attest to their existence; the existence of these controls. If you're considering a service provider, you want to make sure that service provider is transparent with regard to their security policies, how they go about providing security controls. You're going to want to make sure that that service provider shares with you their architecture,

where your data is located, whether or not they'll allow you to conduct a vulnerability scan externally, for example. What are the policies around that?

We consider it standard best practice of security is to conduct periodic external vulnerability scans. If your service provider won't let you do that then you may want to reevaluate. So, most of the lessons learned, I think, are just insuring that you can get the same kind of information and assurances from a cloud-based scenario, whether you're outsourcing to a service provider or doing it yourself, you want to make sure that you still can attest to the same types of security controls that you would otherwise have in a physical environment.

Brian Contos: Well put. I'm not sure if this is an accurate analogy, and certainly correct me if I'm wrong, but it almost seems like we're getting back to the architectures that existed at the birth of the Internet. And I'm talking way back in DARPA net, and ARPANET where you had Node 1, some kind of big cloud and then Node 2. You know, here I send email and there I get email. Here I get to look at a document, here I upload a document. Where it wasn't just the routing and everything that was taken care of at some cloudy mix in the middle, but pretty much everything was done there. And as things started to grow and expand, they got a little bit more distributed and complex. It's almost like we're moving back to that original paradigm.

Chris Richter: Yeah, I think so. And I put a blog together and some of the responses I'm getting to that blog indicate that there was a prediction that there may be a resistance on the part of the some IT professionals to hold onto the old ways. But what's old is actually new again as we move into cloud computing. Are you familiar with, I'm sure you are Brian, the paper written by Nicholas Carr, "Does IT Matter?" Back when he was writing for "Harvard Business Review."

That paper was published back in 2003. And I don't mean to promote Mr. Carr's paper or his books, but it is worth mentioning again because, back in 2003, he did sort of predict cloud computing. And back then, I think he took quite a bit of criticism for it, in saying that infrastructure was going to move into more of a service model, into more of a cloud model. I think we're starting to see strong evidence of that, as companies focus on what their core capabilities are, versus managing infrastructure, which, in most cases, is not a core competency.

Brian Contos: That's really the essence of this conversation. It's just being able to focus on what your business is trying to do, what's impacting your top line and your bottom line. And the more you think about it, a lot of things--like turning on the water, flipping on a light switch, perhaps even the idea of taking the garbage pails out and setting them in front of your house--these are all things that we take for granted. But there's a complex, very complex in many cases, [laughs] infrastructure that goes on behind the scenes. But we, of course, have a very myopic perspective of things. But it allows us to not have to concern ourselves with them and focus on our daily lives without having to have a deep understanding of the electric grid or the water system or waste disposal, right?

Chris Richter: Indeed. One of my favorite quotes is from a customer, who said that he made the decision to outsource to a cloud model. These folks had a glass-house, raised-floor infrastructure, the classic IT, glass-house environment. They took the leap. To them, it was a leap of faith, to move their infrastructure, not just to a service provider but also to a service provider who was managing a cloud. And they were moving into that cloud. And he called the staff together and sat down with his team and said, "Folks, I've got news for you. You're not going to hear the hum of the fans and the cooling units. You're not going to drive up and see the backup generators anymore. We're moving into a new facility."

You're not going to be able to walk downstairs and look through the windows and see all those racks. Everything is moving to a service model in the cloud."

The quote that I like is he said, "Folks, we're moving from being infrastructure custodians to data custodians. Our job is changing, and we're focusing on the data and how it's treated and how it's handled and what we do with it and how we value it, because the data is our most valued asset. It's not the infrastructure. The infrastructure should be left for someone else to take care of."

I thought that was very eye-opening. And I believe this company is on the right path. And it ties back into what Carr was predicting. I wanted to share that quote with you.

Brian Contos: That's a great story. It just goes back to: what's your sensitive asset? Is it the server? Is it the hard drive in the server? Or is it the data that sits on the hard drive in the server? It's generally the data. And I like that; we've become data custodians. Very well put. We have just a couple minutes left, but I did want to ask you one final question. You're sort of at the front lines of this whole world of cloud computing and virtualization. Where do you see it going? What are, perhaps, some of your predictions for where it will be in five years?

Chris Richter: Well, I see the trend continuing, Brian. Much like this customer took what was, for him, a leap of faith, I think more companies will begin moving that direction. It will become less of a pioneering kind of move, as opposed to more mainstream. I think there are a couple of things that need to happen before it becomes mainstream, and one is a greater confidence in the security of the data that is cloud-based. And I think that's going to come as more standards emerge. We haven't seen any what I would call ratified security standards for cloud computing. But it's my understanding that NIST is going to be rolling out something as part of its 800 publication series later this year. There's also the Cloud Computing Alliance, which has published a fantastic document. But more and more things are going to help drive what is considered to be a standard for cloud-computing security.

There also has to be more standards and best practices around authentication and federation. So I see that industry picking up some steam and driving some innovation there, because if you don't access your infrastructure through your own private network or your local area network--you're having to do it over the Internet in many cases--authentication and federation are going to be key elements of that.

But, on the whole, I see the direction going toward, obviously, moving infrastructure as a job function to an outsourced model, where companies turn to service providers to manage that infrastructure. So I think, in five years, will we see a 100-percent migration? No. And I'm not a professional analyst in the industry who looks this far out, but I would say that it would be a much greater percentage than we might expect today, taking that step.

Brian Contos: Absolutely. And Chris, if people want to read your blog, where can they find that?

Chris Richter: They can find it, Brian, at blog.savvis.net. I'll post up there, and looking forward to folks reading and responding and carrying on the discussion. I think this is an important area that needs to be vetted by the IT community in general and discussed further.

Brian Contos: Thanks for spending some time with us today and getting some information about this very important topic out to our listening audience.

WAF in the Cloud with Chris Richter

Chris Richter: My pleasure, Brian. And thanks again.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200