

Panel Discussion: Is Cloud Computing More or Less Secure than On-Premis IT?

Transcript of a sponsored BriefingsDirect podcast on the current state of cloud security and what's needed in the way of standards and practices. Recorded live at The Open Group's 23rd Enterprise Architecture Practitioners Conference and 3rd Security Practitioners Conference in Toronto.

Listen to the podcast. Download the podcast. Find it on [iTunes/iPod](#) and [Podcast.com](#). Download the transcript. Sponsor: [The Open Group](#).

Dana Gardner: Hi, this is [Dana Gardner](#), principal analyst at [Interarbor Solutions](#), and you're listening to BriefingsDirect.



We now welcome our listeners to a sponsored podcast discussion coming to you from The Open Group's [23rd Enterprise Architecture Practitioners Conference](#) and associated Security Practitioners Conference in Toronto. We are here in the week of July 20, 2009.

Our topic for this podcast, part of a series on events and other major topics at the conference, centers on [cloud](#) computing security. Much of the cloud security debate revolves around perceptions. ... It's about seeing the glass as half-full. Perhaps it's only a matter of proper practices and means to overcome fear, caution, and reluctance to embrace successful cloud computing.

Or is the glass half empty -- that in order to ramp up to cloud computing use and practices, a number of potentially onerous and perilous security pitfalls will prove too difficult? Is it only a matter of time before a few high-profile cases nip the cloud security wannabees in the bud?

For sure, security in general takes on a different emphasis, as services are mixed and matched from a variety of internal and external sources.

So will applying conventional security approaches and best practices be enough for low-risk, high-reward, cloud computing adoption? Is there such a compelling cost and productivity benefit that cloud computing means that if you are late, you would be in a difficult position vis-à-vis your competitors or that your cost will be high?

Most importantly, how do companies know when they are prepared to begin adopting cloud practices without undo risks?

Here to help us better understand the perils and promises of adopting cloud approaches securely, we welcome our panel. With us we have [Glenn Brunette](#), distinguished engineer and chief

security architect at [Sun Microsystems](#). He is also a founding member of the [Cloud Security Alliance \(CSA\)](#). Welcome, Glenn.

Glenn Brunette: Thank you, very much.

Gardner: We're also joined by [Doug Howard](#), chief strategy officer of [Perimeter eSecurity](#), and president of [USA.NET](#). Welcome, Doug.

Doug Howard: Thank you.

Gardner: We also welcome Chris Hoff, a technical adviser at the [Cloud Security Alliance \(CSA\)](#), and also director of Cloud and Virtualization Solutions at [Cisco Systems](#). Welcome Chris.

Christopher Hoff: Hi, there.

Gardner: And [Dr. Richard Reiner](#), CEO of [Enomaly](#). Good to have you with us, Richard.

Dr. Richard Reiner: Good to be here.

Gardner: And lastly, we welcome [Tim Grance](#), program manager for cyber and network security at the [National Institute of Standards and Technology \(NIST\)](#). Good to have you.

Tim Grance: Great to be here.

Clouds and security

Gardner: As I mentioned, the biggest hang-up people have, either in real terms or perceived terms, is security, and it's a wide-open question, because we could be talking about infrastructure, [platform as a service \(PaaS\)](#), data, or simply doing applications. All across the board people are applying the word "cloud." But I think for the intents and purposes of our discussion we want to look at what the enterprises are going to be doing. We have a crowd of architects with us.

Let me take my first question to you, Chris Hoff. When we talk about cloud and enterprise, are we talking about something that is fundamentally different in terms of securing it, versus what people are accustomed to do across their networks?

Hoff: That's a great question, actually. Again, it depends upon what you mean, and, unfortunately, we are going to probably say this a thousand times.

Gardner: Let's get the taxonomy over with.

Hoff: Yeah, what is cloud? Depending upon the application, you will have a set of practices that almost look identical to what you would use in non-cloud environments. In fact, with the CSA,

the 15 domains of areas of focus are really best practices around what you should be doing to secure your assets in your business, no matter where you happen to be doing your computing.

That being said, there are certainly nuances and permutations of certain things and activities that we do or don't do currently in applications -- of moving your information applications to the cloud that, in some cases, are operational and, in some cases, behavioral, and, in some cases, technical.



You can dive in and slice and dice up and down the stack, but it's fair to say that, in many cases, what cloud has done and what [virtualization](#) has done to the enterprise is to act as a fantastic forcing function that's allowed us to put feedback pressure on the system to say, "Look, depending on what we are doing internally in our organizations, and the care and feeding of our infrastructure applications and information, now that I am being asked to move my content applications information outside my normal comfort zone of the firewall and my policies and my ability to implement what I normally do, I really need to get a better handle on things."

This is where we're starting to see people spin up things they weren't doing before or weren't doing with as much diligence before, and operationally changing the way they behave and how they assess and classify what they do and why.

Gardner: Richard Reiner, tell me a little bit about what the pitfalls are. What makes this a little different in terms of the risks?

Hostile software

Reiner: It's an entirely different set of questions when you are talking about [software as a service \(SaaS\)](#) versus platform versus infrastructure. So, let me just answer for the [infrastructure-as-a-service \(IaaS\)](#) part of the story, which is where we play. We have a platform that does that.



Fundamentally, when you look at infrastructure-on-demand services, they are delivered by means of virtualization and, for most enterprises, probably a very large majority of enterprises, it's the first time that they have even considered, much less actually deployed, infrastructure of a nature that is simultaneously shared and virtual.

Shared means something hostile could be there alongside your workload as the customer, and virtual means that fundamentally it's a software-induced illusion. If something hostile in there can subvert one of the software layers, take control of it, or make it behave differently than what is expected, the customer's workload could find itself executing on a virtual server, running code on a virtual processor that is nothing short of hostile to it.

A virtual processor could be programmed, for example, to wait until secrets are decrypted from disk and then make off with the plain text. That's a fundamental new risk and it's going to require new controls.

Gardner: Glenn Brunette, perhaps another way of posing this question is not whether the cloud is secured or not, but whether [client-server](#) architectures are secured or not? And, is the risk with cloud less than the risk with client-server? Is that fair?

Brunette: That's an interesting way to put it, for sure. To echo my fellow panelist's previous statements, a lot of it depends on how you look at cloud and what your definition is, whether you're dealing in a SaaS model, where you have a very specific well-defined interaction method, versus something, maybe IaaS, where you have a lot more freedom, and with it a lot more risk.



Is it more or less secured than client-server? I don't think so. I don't think it is either more or less secured. Ultimately, it comes down to the applications you want to run and the severity or criticality of these applications, whether you want to expose them in a shared virtualized infrastructure.

With respect to how these applications are managed, a lot of the traditional client-server applications tended to be siloed, and those siloed applications had problems for scalability and availability, which posed problems for providing continuity of service. So, I don't think they are necessarily better or worse than one another. Their issues are just little bit different.

Gardner: Doug Howard, maybe this is back to the future. There was a time when those things were centralized and they only went out through the interface to a green terminal. That had some advantages. Are we looking at similar advantages now with cloud computing, where you can control a single code base or you can manage only the amount of information you want to go across the wire, without risk of data being left on clients and all that difficulty of managing different application variations and platforms at the edge?

Things are different today

Howard: Clearly, if you look at where client-server was many years ago, as compared to where it is today, it's significantly different. The networks are different, the infrastructure is different, and the technology is different. So, the success rate of where we are today, compared to where we were 10 and 15 years ago trying the same exact thing, is going to be different.



At the end of the day, it's really about the client experience and, as you guys sitting in the audience are probably thinking right now, everything that we talk about starts with, "Well, it depends" and various other alternations to that. From your perspective, the first thing that you need to know is, "Am I going to be able to deliver a service the same way I

deliver it today at minimum? Is the user experience going to be, at minimum, the same that I am delivering today?"

Because if I can't deliver, and it's a degradation of where my starting point is, then that will be a negative experience for the customers. Then, the next question is, obviously, is it secured as a business continuity? Are all those things and where that actual application resides completely transparent to the end user?

I'll give you a key example. One of the service suites that we offer is messaging. It's amazing how many times you walk into a large enterprise client, and they go, "Well, I'd like to see a demo of what the user experience of getting messaging services from a hosted or from a shared infrastructure is, compared to what it would look like in-house."

Well, open your [Outlook](#) client, because if it's different than what it would be in-house and out of house, we're starting at the wrong point. We shouldn't be having this conversation. The starting point you need to really think about, as you go through this, is does it look like it did 10 years ago or 15 years ago? It doesn't really matter. The client experience today is going to be significantly different from what we tried 10 or 15 years ago.

Gardner: Tim Grance, it sounds like we have a balancing act, risks and rewards, penalty, security. It's not going to be all on one side, but you want to make the right choice and you want to get the rewards of the economic benefits, the control, the centralization, and, of course, you don't want to have to deal with a major security blow-up that gets a lot of bad publicity. How are you approaching this from that risk-rewards equation?

Grance: Anytime you do things at scale, it's like standards. If you do it really well, it's great, because you have a systemic answer. If you don't, you get ugly really fast. God and the devil both dwell in the details, depending on how well you do these things. But, it's hard elevating it as just another cold-hearted business decision you have to make.

If you aggregate enough demand in your enterprise or across your area of work, and you can yield enough dollars to put up for someone to bid on, people will address a lot of these security concerns -- I don't have a transparent security model -- I don't know exactly how you are protecting my data -- I don't know where you are putting your data.

If you give them a big enough target, you aggregate enough demand to make it attractive. You can drive the answers to all of these questions, but you do have to ask for the full set of business use cases to be addressed.

New business model

Gardner: Chris Hoff, back to you. We're really not only talking about a shift in the technology, in the delivery, and then evaluating the risks and rewards as result. We are also talking about a

fundamentally different business model of how to acquire services, instead of a license model with a lot of upfront capital expenditures.

You might be able to examine certain aspects of what you do. Instead of having an overabundance of resources for a small peak period or occasional explosion of demand, you can meter this out and pay on a per-use basis, or perhaps even get subsidized by something like advertising or some other business model.

So, the rewards, when we compare and contrast the monetization and the costs, could be very lopsided. This is going to, I think, appeal to a lot of people, particularly in a recession. For those people who want to dive into this right away and take advantage of those big dollar savings, what do they first and foremost need to think about for protecting themselves and be secure in doing so?

Hoff: Previously, I talked about the forcing function of cloud as an intersection of the economy, where cost savings is a huge motivator from the perspective of economics. Extrapolating that a little bit further, the answer is really interesting, when you add the dimension of the consumerization of IT. What I mean by that is consumer-like experiences, leaking themselves into the enterprise, and, in some cases, vice-versa.

One of the interesting notions of how cloud computing alters the business case and use models really comes down to a lot of pressure combined with the economics today. Somebody, a CIO or a CEO, goes home and is able to fire up their Web browser, connect to a service we all know and love, get their email, enjoy a robust Internet experience that is pretty much seamless, and just works.

Then, they show up on Monday morning and they get the traditional, "That particular component is down. That doesn't work. This is intrusive. I've got 47,000 security controls that I don't understand. You keep asking for more money."

Trying to reconcile those two models is very interesting, because when it comes down to what you should look out for, in many cases, there is one other element that leaks into that and that's the generational question.

I've now taken your very simple question and made it multi-dimensional. But, if you're a consumer and are 17 years old, your idea of security, privacy, confidentiality, access, and availability are very, very different than mine or somebody else's in the corporate environment.

The model starts with understanding, first of all, who the consumer is, and how that applies to the scenario we're talking about, what type of information we're trafficking in, and how that ultimately affects and translates down to managing risk. Ultimately, the difficulty with all of that is that multi-dimensional mouthful, which I just came up with, is exactly what we have to face in

the enterprise every day with every business decision when we talk about the cloud or moving a service or an application content to the cloud.

Once we get pass the definitional issues, the things you have to look at are to the point that was made previously. If my user experience isn't the same or isn't offset tremendously by cost, that's a problem. If my privacy and my compliance are not at par with what I have today, that's a problem.

We don't have a very good way today of assessing those gaps. That's the first thing I would look at -- understanding where you are, versus where you want to go in relation to the pressures we are facing to move our content and apps to the cloud.

Where's the sweet spot?

Gardner: For the next point, let's go to Glenn. Thinking about the whole of cloud benefits for those people who do want to get in, take advantage of some level of the productivity, but without a lot of risk, what's available? Would you say that application development is a place to start? Is it to look at data that might not be critical data and move it off of your servers? Where is this sweet spot, rather than waiting for the whole methodological approach to be sussed out in the cloud alliances and for the work groups to do their thing. Where can you go right away? What's the low-hanging fruit on this?

Brunette: There are actually a lot of different areas, depending on what your own business is and what you are interested in doing. Certainly, you see a lot of people doing initial development, also quality assurance and testing of applications using dummy data out in the cloud, assuming the applications themselves don't contain sensitive data in some way, such as a trading algorithm or something like that.

You also see cases where you have historical data, where it's no longer of interest, but you may want to use it for analytic purposes. There has been work done by some of the trading exchanges to make that data public, so people can perform an analysis on past historical trends in the market and could perhaps develop new trading algorithms and new things on their own.

In addition to that, you may find that there are cases where you are doing high-performance computing kinds of workloads that are non-sensitive. You could be, for example, doing video transcoding, movie-rendering, things like that. Again, you see people with open-source movies, and open-source songs and things like that. You could certainly put that out there.

Really, it's a wide-open field, and I've been focusing on compute. With storage, you see people encrypting [BLOBs](#) and putting just their storage out there or making it available for content distribution, because of the widely available high bandwidth channels to the cloud storage provider.

Unfortunately, there is no one answer, but the good news is there are quite a number of answers. There are a lot of opportunities, depending on what you are doing.

Gardner: Let's flip that question. Richard Reiner, what are some areas you should back off from? What is not ready for prime time when it comes to secure, safe cloud computing?

Reiner: To try to give a good answer to that question, you've got to dig down one level to think about how our decisions about what can be deployed are made in the enterprise. What's the right way of doing that? There are any number of dimensions that come into play. There are concerns about availability, access, and interactive performance.

There are security concerns. Relative to the security concerns in the ideal enterprise mode of operation, there is some good systematic risk analysis to model the threats that might impinge upon this particular application and the data it processes, and then to assess the suitability of different environments for potential deployment of that stuff.

Questions on public clouds

There are a lot more question marks around today's generation of public-cloud services, generally speaking, than there are around the internal computing platforms that enterprises can use. So it's easier to answer those questions. It's not to say the answers are necessarily better or different, but the questions are easier to answer with respect to the internal systems, just because there are more decades of operating experience, there is more established audit practice, and there is a pretty good sense of what's going to be acceptable in one regulatory framework or another.

Trying to pull that together into an answer to the question, I guess what you could say is that the more of those unknowns arrive in conjunction with a particular application or a particular dataset that someone is considering deploying in the cloud, the harder it's going to be to actually do that.

Gardner: Tim Grance, same question. What would you really keep away from, in terms of network security and cyber security, when it comes to interest in the cloud?

Grance: Public facing content, collaboration with the public -- those are good things. Anything closer to the mission critical side, whether you want to outsource it or not, that's something you want to be a lot more careful with.

Would I put the Department of Defense's mission-critical apps? No, I wouldn't do that, because it's just not worth that effort and risk to even try to answer those questions. No one should take the truly core mission-critical things and put them out at this point in time. I'd even be nervous on the internal cloud, just because the dangers and the risks are large. What's the payoff is really the risk appetite question you have to answer.

Gardner: Doug Howard, data. Some data good, some data bad in the cloud. You guys are involved with trying to protect and manage a lot of mission-critical data. Do you have a certain metric that you would apply to deciding which datasets can go outside of your organization?

Howard: We're probably a little ahead of the marketplace in some areas, relative to mission-critical data in the cloud.

Just to give you a little bit of a review. we provide services to about 2,000 banks and credit unions. We do most of their core access into infrastructure. On a global basis, about 10,000 customers rely on us for messaging infrastructure and so forth. I would argue that for every one of those companies -- banks, large enterprise, so forth -- messaging, Internet, Web access is mission-critical to their enterprises. If that was to drop off for hours or for days, their infrastructure and their companies would come to a halt.

If you look at what can be put in the cloud, I wouldn't necessarily say mission-critical can't be placed in the cloud. I would probably alter that a little bit. You need to put what you are comfortable with in the cloud, and you need to be comfortable with whatever the infrastructure provider can step up with.

Generally speaking, the infrastructure providers that are providing services in the cloud are today pretty candid about what they can and can't do relative to reporting, governance, risk, and compliance. Those types of things are the questions that are going to define what can go into the cloud. The performance tends to be less of a concern, because everything is relative.

Everything is relative

Can you provide a global infrastructure? Can you provide high availability with a budget that you have today, compared to the cloud provider? A lot of times the answer to those questions is "no." So, everything is relative to what you can do yourself, as well.

Going back to that user experience. If you can get a higher user experience and you're comfortable with all the [governance, risk, and compliance \(GRC\)](#) and security elements, then ultimately you're better off putting those types of things in the cloud than trying to build it yourself on something that you know will not be able to deliver the user experience that you're trying to attain.

Gardner: A question from our audience comes in about federation. You're probably going to have both internal and external environments and aspects of business process and resources. How do you manage them in some concerted effort that works? This is probably not too different than how you manage integration and collaboration among different services internally. It's taking those services from a variety of different sources.

Let's go to Chris Hoff. This is really a governance question. Where is security, in terms of its maturity, when it comes to mixing and matching services, internal and external?

Hoff: Glenn and I were actually discussing some of this prior to the panel. The interesting thing that cropped up was about the effectiveness of compensating controls today. My friend, [Gunnar Peterson](#), has this great chart, where he shows that it's a kind of matrix. He shows the innovation or development of programmatic capability over time and the advancement of programming languages way back to C and Java, etc.

On the second column he shows the security industry's response to each of these brand new developments. The funny thing is, they're amazingly consistent, because you have the words [SSL](#) and firewall, SSL and firewall, SSL and firewall.

So, it may very well be a governance question today, but as the other sessions during the conference have pointed out quite glaringly, what we have settled for, what we have allowed ourselves to settle for, and the way in which we “collaborate” today means you have a firewall rule that says, "source, partner, destination, all my internal resources, protocols, whatever, action allow, and log."

The level of collaboration really comes down today to the advancement of technology, which hasn't happened as far as we needed it to. More importantly, as we extend into the cloud -- and this is what I was talking about in terms of this forcing function -- we need to be a lot better about what we mean by collaboration, who participates, and how we identify them. It goes back to basic practices that we haven't done a very good job of dealing with over time.

It's one thing if your constituency is known to you and, if you happen to collocate your resources internally, it's quite another, when you make them available externally and have to start looking at how you identify, and then federate even a basic externally hosted, but internally consumed, set of applications and resources.

Challenging the model

We have an awful lot of work to do, as it relates, on one hand, to challenging the model -- is this the right way to go? -- but secondarily, bringing forth all the things that we should have done for quite a number of years to make that a reality.

Glenn and I were discussing the fact that we have an awful lot of solutions, as was alluded to before -- I think Doug brought it up -- that from a timing perspective just weren't mature, ready, or catalytic enough to be adopted. But, now is an opportunity to look at those as being a valid set of alternatives.

Gardner: Glenn, you've had this discussion with Chris. Is it safe to integrate, to interoperate, and should governance be something that resides entirely within an enterprise that's consuming

cloud services? Does governance need to be extended from the cloud to the consuming organization, or some interaction or hybrid between them?

Brunette: When you start looking at the cloud usage patterns and the different models, you're going to see that governance does not end at your organization's border. You're going to need to understand the policies, the processes, and the governance model of the cloud providers.

Unfortunately, we really have a fair degree of work to do in this area. There's a lot of work that needs to be done around transparency, compliance, and governance. But, those are problems that can be solved, at least for those organizations willing to take that step. Those will be the ones that will be more attractive in the marketplace, especially to the enterprise market, as they look to take advantage of cloud computing.

It's going to be important that we have a degree of transparency and compliance out in the cloud in a way that can be easily consumed and integrated back into an organization. At the same time, I would also caution, though, to Chris' point.

Earlie, he talked about the onslaught of audit requests. I think we need to come up with some standards in this space, so that organizations can measure against some common ground, so that cloud providers aren't effectively going under a denial of service just on the sheer weight of audit requests from their consumers. There is a balance here that needs to be struck.

Gardner: Going to the audience once again. Another question about third-party risk assessment. Is this a field day for third-party consulting organizations that will walk in and spread the pixie dust?

I'll throw this out to anyone on the panel. How much of this is going to fall into the hands of third-party consultants to decide what you should or shouldn't use vis-à-vis the cloud.

Potential for disintermediation

Grance: I'll start on that one. It's funny, cloud has a vast potential to cause a disintermediation, just like in power and other kinds of industries. I think it may run eventually through some of these consulting companies, because you won't be able to get as rich off of consulting for that.

In the meantime, I think you're going to face that situation. As you can see with the SAS 70 audience, where people can simply just roll their own. Here's my magic set of controls. It may not be all of them. It may just be a few of them. I think people will shop around for those answers, but I think the marketplace will punish them.

Reiner: Another comment here, and this takes the form of a war story, so I apologize for that. About a year-and-a-half ago, a friend of mine, who was, at the time, the CIO of a Fortune 100 company, asked me to take a look at an agreement that he was actually already party to. He had

inherited it from his predecessor, and it was between his organization and a Fortune 100 outsource or integrator type of entity. He asked me to look at the security aspects of it.

It was interesting. On one hand, there were security aspects, which are not universally the case in these things. But when you came down to it, what it said under security was that, "the integrator undertakes to have firewalls" -- not to plug them in, not to operate them, not to maintain them, not to see them inserted in a network, not to see them doing anything whatsoever.

The remarkable thing about all this is not just that the gap had occurred, but that both organizations felt good about it. Both organizations felt that they had successfully washed their hands of the risk. Until as a community we all get better at not letting those things happen, maybe it's useful to have third parties who can help find them.

Gardner: Anyone else on the third-party risk assessment opportunity?

Howard: I'll take a slightly different angle on it. Going back to one of the things Glenn said, if you look at a lot of the cloud providers, we tend, in many cases, to fight some standards, because, in reality, we want to have competitive differentiators in the marketplace. Sometimes, standards and interoperability are key ones, sometimes standards create a lack of our ability to differentiate ourselves in the marketplace.

However, on the security side, I think that's one of the key areas that you definitely can get the cloud providers behind, because, if we have 10,000 clients, the last thing we want is to have enough people sitting around taking the individual request of all the audits that are coming in from those customers.

For example, if they just wanted to send us a questionnaire of 150 questions, to do that 10,000 times is a significant effort. So, to put standards behind those types of efforts is an absolute requirement in the industry to make it scalable, not just beyond the infrastructure, performance, availability, and all those things, but actually from a cost perspective of people supporting and delivering these services in the marketplace.

Hoff: Just to take an angle on your angle. What's interesting is that many times, from the security perspective, security teams have not done a good job of looking forward to what is coming as a disruption, and some are caught flatfooted and react oftentimes in an emotional manner that does not contribute well to their status in the organization.

A good illustration of this is when someone says no or attempts to block the movement to a cloud by suggesting, "Well, the cloud provider does not have X, Y, and Z in place." Sometimes, management turns around and says, "Well, do we have X, Y, and Z in place? And, they say no.

Answering to a higher standard

It's kind of like the Hebrew National hot dog version of security for the cloud, which is being held to a higher standard. This is kind of funny, because, in many cases, they will write, you know what, I'm outsourcing this. I may not be able to effect the same types of governance and control, but at the same time, we should be fair and circumspect, when we look at the overall security posture and we look at the controls that we have.

Firewalls aren't bad things. They've served us well. Our application of them may be ill tuned, but the reality is that "good enough" security, for the most part, is what we like to suck up and admit is good enough. It always has been. That's the trend with outsourcing in general before the cloud showed up as a popular culture term.

If they deliver to me a service level that is legally binding in some form or another, whether they plug in the firewalls or not, the reality is that from a cost center view, and we're looking to trim money, good enough is good enough. We're going to be facing much, much more of that as time goes on.

Gardner: That gets to the point of authority and responsibility. Security, as we pointed out, is often a function of perception. Will the cloud perhaps improve this by creating one throat to choke? If the cloud provider is responsible for performance, security, liability, low cost, and for all of the other requirements that you might throw into your service-level agreement, isn't that, in a sense, a little bit better than having a distributed, amorphous, unknown set of security requirements within the organization?

Glenn, is there a silver lining to the cloud in terms of the one throat to choke?

Brunette: I would say it depends. Well, it does, but I would say that for certain classes of cloud computing models, a SaaS model, it really could be the case, where those providers have an opportunity to hire best of breed, be able to build that into their applications, and design that into their processes and their policies, so that what you get is actually representative of a strong security model.

At the same time, you need to recognize that there is a shared responsibility here, especially as you get further down the stack. Once you get to the IaaS provider, if the provider is not providing you with the machine images that you're loading, you really can't blame them, if you've deployed a poor one. So, depending on what level of the stack you're going toward, there may be some benefits.

One of the other things I'd point out is that, it's not just about the cloud providers and the cloud consumers, but there are also other opportunities for other vendors to get into the fray here.

One of the things that I've been a strong proponent of is, for example, OS vendors producing better, more secured, hardened versions of their operating systems that can be deployed and that are measurable against some standard, whether a benchmark from the [Center for Internet Security](#), or [FDCC](#) in the commercial or in the federal space.

Everyone benefits

The other thing that comes to mind is that you may also have the opportunity of third parties to develop security-hardened stacks. So, you'd be able to have an [AMP stack](#), a [Drupal stack](#), an [Oracle](#) stack, or whatever you might want to deploy, which has been really vetted by the vendor for supportability, security, performance, and all of these things. Then, everyone benefits, because you don't all have to go out there and develop your own.

Gardner: I am going to riff a little bit on a well-known tagline and say that the architecture is the cloud. What I mean by that is that it's hard for enterprises to change their architecture, but it might not be that difficult for a cloud provider. Somebody who has, for example, a very low-margin commoditized business, needs to look for, as you say, best-of-breed approaches, not necessarily best-of-breed products.

We heard earlier today about a change in how an application might be delivered, that the whole stack, an optimized stack, might be integrated and optimized between the code that's generated in the application and the stack itself, no more or no less that's required. It's tightly integrated, highly parallelized, highly efficient, comes down across the wire, you use it when it's done, it goes back up, and it comes down the next time with all of the security patches installed. This is an architectural shift, not just a sourcing change.

Does the cloud offer us the opportunity to move our architectures, in a modernization sense, far and away more than we might be able to do in our own organizations? Let me take that to Richard Reiner first.

Reiner: Well, if the question is does that opportunity exist, certainly it exists. It's going to come down to the business models of individual cloud providers as to whether they are willing on one hand and able on the other.

Gardner: Will I, as an end user, care what the architecture is?

Reiner: Well, you'll care in terms of its functional results. You may not care what's behind the scenes, but you'll care whether you are receiving configuration updates as a service as part of what you've contracted for. Certainly, you'll care.

Gardner: How about Doug Howard?

Howard: Unfortunately, I think a lot of it plays out over time. I mean, at the end of the day, if you engineer, if you develop and you deliver a service, regardless of what the underlying infrastructure is -- going back to the user experience -- if the user experience is positive, they're going to stay with the service.

On the flip side, if somebody tries to go the cheap way and ultimately delivers a service that has not got that high availability, has got problems, is not secure, and they have breaches, and they have outages, eventually that company is going to go out of business. Therefore, it's your task right now to figure out who are the real players, and does it matter if it's an Oracle database, [SQL](#) database, or [MySQL](#) database underneath, as long as it's meeting the performance requirements that you have.

Unfortunately, right now, because everything is relatively new, you will have to ask all the questions and be comfortable that those answers are going to deliver the quality of service that you want. Over time, on the flip side, it will play out and the real players will be the real players at the end of the day.

Gardner: Chris Hoff, is it possible that the cloud providers will run circles around the enterprise and that they will come up with a better architecture? It will be more secure. It will be more reliable. It will be robust. It will have business continuity. It will be cheap. It will be effective. You guys are pessimists today. I don't get it?

It depends on what you pay

Hoff: It will make me a ham sandwich too. It depends on what you pay for it, and I think that's a very interesting demarcation point. There is a service provider today who doesn't charge me anything for getting things like mail and uploading my documents, and they have a favorite tag line, "Hey, it's always in beta." So the changes that you might get could be that the service is no longer available. Even with enterprise versions of them, what you expect could also change.

So the answer is yes, given one of the hallmark benefits of cloud, which is agility and flexibility and the "push once -- make available to everyone" is certainly fantastic. However, in the construct of SaaS, can that provider do a better job than you can, Mr. Enterprise, in running that particular application?

This comes down to an issue of scale. More specifically, what I mean by that is, if you take a typical large enterprise with thousands of applications, which they have to defend, safeguard, and govern, and you compare them to a provider that manages what, in essence, equates to one application, comparing apples to elephants is a pretty unreasonable thing, but it's done daily.

What's funny about that is that, if you take a one-to-one comparison with that enterprise that is just running that one application with the supporting infrastructure, my argument would be that you may be able to get just as good as, perhaps even better, performance than the SaaS provider.

It's when you get to the point of where you define scale, it's on the consumer side or number of apps you provide where that question gets interesting.

I bristle at the fact that, for example, SaaS vendors can do a better job at securing your apps than you can. So you run a mail system inside, and you outsource to them, and they will do better job. Strangely enough -- and it may be a case I will grant of you of adoption and use -- but the three biggest breaches we have currently had in terms of privacy, as it relates to well-known cloud applications, have all been SaaS. These are the guys who are supposed to be doing a better job than we do.

It's applying a realistic and pragmatic set of filters to that questions. One to one, that becomes a more difficult question to answer. I've got a thousands apps, where I am distracted and I've got to pour more and more money and more and more people into it. Then, you start dealing with a reasonable question.

But, what happens then when I end up having 50 or 60 cloud providers, each running a specific instance of these applications. Now, I've squeezed the balloon. Instead of managing my infrastructure, I'm managing a bunch of other guys who I hope are doing a good job managing theirs. We are transferring responsibility, but not accountability, and they are two very different things.

Gardner: Glenn, to this point of modernization and the pace of innovation, many enterprises have five- or seven-year cycles. A cloud provider might have a three-, six-, or nine-month cycle. It wouldn't take too long for that cloud provider to be way ahead in terms of adopting the latest and greatest security and optimize the infrastructure.

Do you see that the cloud providers, if given a chance, if given a business model and it's sustainable, could technically, and in terms of business requirements, very quickly get out in front and, therefore, become an offer that people can't refuse?

Advantages of older technology

Brunette: I think that's possible, although probably for different reason. The hardest thing is that they may want the latest and greatest, but more often that is in terms of what they are exposing to their customers and also in the tools and techniques they will use to manage their infrastructure. In terms of the actual technology, sometimes using older technology may be more advantageous to them from the cost perspective.

You asked earlier whether this is an opportunity for architects and for changes in architecture, and I would say a resounding yes. There are things we can do today, in terms of horizontal scale, caching of systems, and caching of applications, that would allow us to use, rather than the latest quad-core processors, maybe dual-cores, but more of them, or using older disk-drives, but with Flash-based technologies to help accelerate the reads.

In almost every case, the cloud providers can hide all of that complexity, but it gives them a lot more flexibility in terms of which technology is right for their underlying application. But, I do believe that over time they will have a very strong value proposition. It will be more on the services that they expose and provide than the underlying technology.

Gardner: Any other takes on that? Yes, Richard?

Reiner: Just kind of a comment. Sometimes we risk taking something for granted that we shouldn't, which is that every customer, even every business customer of cloud services, will want a cloud that is managed to maximize security and availability.

To the extent that a cloud is managed that way, you take on some of the characteristics of large enterprise IT, which is to say slow and bureaucratic, and all the things that people complain about. While some customers will want their cloud services that way, others will want one that maximizes price performance, even if that comes at the expense of other dimensions. So, we just need to be careful on that one.

Grance: This goes back to the business case argument. You have to know what your risk appetite is and what risks you are willing to take. If you can give an aggregate demand and enough dollars behind that, you can get your requirements met.

Of course, we could come up with this novel thing 10 years later called IT. So, there will always be this ebb and flow back and forth. A technical point is that, regardless of which one you choose, which model, which method, you are going to ask all of these hard questions about the provisioning service and how well this is done, and with virtualization, you are still trusting a million lines of code.

Regardless of which model, there is no way to say there is no risk in any of the issues. It's another coldhearted business decision that has to be made.

Brunette: Just one comment in terms of optimization. It's an excellent point, because I think what we will see today is that if you want a compute or storage service, you tend to get the same flavor. Now, you get different providers, but it's similar in nature. Over time, we're going to see a much higher degree of specialization.

You may see more [HPC](#)-oriented clouds, which utilize different types of interconnects, different types of file systems that deliver on those requirements, whereas something, perhaps in the financial services or healthcare, may orient themselves more toward those regulatory environments.

Robust marketplace

Gardner: Okay, and to that point of a robust and highly energized marketplace, where the best and brightest and most secure will rise to the top and it will be clear and transparent to everyone what those are, how do we provide for transparency and utility and portability, especially early on?

It seems to me that we have a limited number of cloud providers, for at least enterprise caliber activities now a days, and, with a small number, comes perhaps market power, beyond what we would expect in terms of a pure market environment.

Any thoughts about what we need, perhaps external or perhaps with the clout of the enterprises. If we're going to be buying the stuff, we want X, Y, and Z. What needs to happen in terms of providing for neutrality, which is an important aspect of security? Let's start at one end and work away down. What do you think, Doug?

Howard: Neutrality, from a portability prospective specifically. Most of us who have provided SaaS services in the cloud provide some reasonably easy way for customers to gain access to their content and withdraw that from our infrastructure.

That's one of the questions that most customers, when they come to us today, have key on their mind. "How can I get my data out of your infrastructure, if I want to? If you end up being the provider and if you end up going out of business, whatever it may be, how can I get my data out of your infrastructure?"

Those APIs, those, capabilities, those exports pretty much exists today, relative to getting the compliance information, the [GRC](#) information out of their infrastructure and into their infrastructure. Those are the key areas that we have been focused on.

There's probably an evolution, as well, that you will see the industry go through as they figure out, "I can make you comfortable with getting your data. I can make you comfortable getting your applications out of my infrastructure, if you are worried about me and move it to somebody else."

The next evolution is making sure that my business processes and my compliance work with the outside as well. For example, we do external scanning by a third party. We do internal scanning ourselves. We have a third-party FFIC review that comes in. That happens with us. Then, we have a third-party review that comes in.

Those are made available to our clients as part of the process. They then go into their policy and into their GRC process, so that they can fulfill their compliance requirements as well.

Gardner: Chris Hoff, do we need a "good clouds keeping seal of approval?" Who would provide it? Wouldn't a network services company be a good possibility?

Open standards

Hoff: To answer your original question about what we need to make that a reality. The words "open standards" float to the top of my head. We've been talking a lot about the enterprise here, and so we'll make that assumption -- large, well-established enterprises with good, decent practices, and with established burdens and infrastructure already.

For [small and medium businesses \(SMBs\)](#), most of them could care less. It's all about agility. "I don't want to buy anything, I'm just putting this stuff in the cloud today." They don't see any difference. It's fantastic.

If we focus on the enterprise side, you brought up earlier that a lot of these folks are already on multi-year road maps that talk about progression of how their infrastructure is going to move and migrate. It's like turning an oil tanker left. It takes five miles in many cases.

In the long-term, open standards with contributions from larger enterprises and providers are going to be incredibly important, because there is a natural progression in large enterprises that's occurring, regardless of what label you slap on it.

That is a direct result of the consolidation and virtualization we have been seeing happening over the last five years anyway. They're looking to reduce carbon footprint, save on power, and all that stuff and that's happening. That's led currently by a few vendors, who are working, as their market dominance, to export what they do, both to allow federation with the business part and what's been turned out into a cloud process.

We flip that even further. The reality is, portability and interoperability are going to be really nailed to firstly define workload, express the security requirements attached to that workload, and then be able to have providers attest in the long-term in a marketplace.

I think we called the Intercloud, a way where you go through service brokers or do direct interchange with this type of standards and protocols to say, "Look I need this stuff. Can you supply these resources that meet these requirements?" "No? Well, then I go somewhere else."

Some of that is autonomic, some of it's automated, and some of it will be manual. But, that's all predicated, in my opinion, upon building standards that lets us exchange that information between parties.

Gardner: Richard Reiner, Everyone agrees that portable neutrality and openness is a good thing, but how do we get there?

What we need now

Reiner: That's a good question. I don't think anyone would disagree that learning how to apply audit standards to the cloud environment is something that takes time and will happen over time. We probably are not in a situation where we need yet another audit standard. What we need is a community of audit practices to evolve and to mature to the point where there is a good consensus of opinion about what constitutes an appropriate control in a cloud environment.

The other question that arises there is how easy or hard it is for an auditor to get to that opinion, and what can we do, as technologists, that might make it easier. This is one area where we're putting a lot of our attention, and we have a cloud infrastructure platform that service providers around the world are starting up and running revenue-generating services on. This is a question that we are seeking the answer for.

Gardner: Glenn, portability, how do we get there?

Brunette: As Chris said, it comes down to open standards. It's important that you are able to get your data out of a cloud provider. It's just as important that you need to have a standard representation of that data, something that can be read by your own applications, if you want to bring it back in house, and something that you can use with another provider, if you decide go that route.

The other concern that comes up, if you get to that point where you the need to extract your data, what if we are talking about [petabytes](#) or [exabytes](#) of data? Where do you go with that? How do you get it from provider to provider? Are you going to get it there over some sort of network link or do you have other vehicles for that? Those are things that you would need to negotiate with your provider?

Gardner: Pick up trucks.

Brunette: Right, exactly.

Gardner: Last word to you, Tim.

Grance: I'm going to out on a limb and say that NIST is in favor of open, voluntary consensus, but data representation and APIs are early places where people can start. I do want to say important things about open standards. I want to be cautious about how much we specify too early, because there is a real ability to over specify early and do things really badly.

So it's finding that magic spot, but I think it begins with data representation and APIs. Some of these areas will start with best practices and then evolve into these things, but again the marketplace will ultimately speak to this. We convey our requirements in clear and pristine

fashion, but put the procurement forces behind that, and you will begin to get the standards that you need.

Gardner: We have been discussing whether or not it's safe to go to cloud computing, and we have come up with number of different positions and a variety of perspectives. I hope it's been edifying for you. I have certainly enjoyed it and I hope you can join me in again thanking our panel.

We have been joined by Glenn Brunette; distinguished engineer and chief security architect at Sun Microsystems, as well as the founding member of the Cloud Security Alliance. Thank you, Glenn.

Brunette: Thank you.

Gardner: Doug Howard, chief strategy officer, Perimeter eSecurity, and president of USA.NET. Thank you, Doug.

Howard: Thank you.

Gardner: Chris Hoff, technical advisor for the Cloud Security Alliance and director of Cloud and Virtualization Solutions for Cisco Systems. Thank you, Chris.

Hoff: Thanks, very much.

Gardner: Dr. Richard Reiner, CEO of Enomaly. Appreciate your input.

Reiner: Thank you.

Gardner: And Tim Grance, program manager for Cyber and Network Security at the National Institute of Standards and Technology. Thank you.

This is Dana Gardner, principal analyst at Interarbor Solutions. You have been listening to a sponsored BriefingsDirect podcast, coming to you from The Open Group's, 23rd Enterprise Architecture Practitioners Conference in conjunction with the Security Practitioners Conference in Toronto in the week of July 20th, 2009. Thanks for listening, and come back next time.

Listen to the podcast. Download the podcast. Find it on [iTunes/iPod](#) and [Podcast.com](#). Download the transcript. Sponsor: [The Open Group](#).

Transcript of a BriefingsDirect podcast on the current state of cloud security and what's needed in the way of standards and practices. Recorded live at The Open Group's 23rd Enterprise Architecture Practitioners Conference in Toronto. Copyright Interarbor Solutions, LLC, 2005-2009. All rights reserved.