CEO JOURNEY

Cloud Security Alliance

Best Practices for Providing Security Assurance Within Cloud Computing

Organization:	Cloud Security Alliance	**Driver:**	Jim Reavis
Type:	Non-profit	**Role:**	Co-founder, CEO

Organization profile: The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing, and provide education on the uses of cloud computing to help secure all other forms of computing. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events, and products.

> *“The need for regulatory compliance probably comes up first for organizations moving to the cloud.”*
>
> **Jim Reavis, Co-founder & Chief Executive Officer, Cloud Security Alliance**

Stiennon, Richard “Mega-Trends Drive Digital Transformation,” *Secure Cloud Transformation: The CIO’s Journey*. IT-Harvest Press, 2019, pp. 27–33.

Cloud Security Alliance (CSA) was created in 2008 to get ahead of the security issues it saw coming with the move to the cloud. Jim Reavis, the co-founder and CEO of CSA, shares in this upcoming journey what motivated the formation of this alliance in the early days of cloud adoption, and also the initiatives the alliance continues to drive to create governance and the sharing of best practices within the community and industry.

In the words of Jim Reavis:

“In 2008, I was looking for things that were going to impact the IT industry, like virtualization of operating systems. That’s when I started to see that the early adopters I respected were beginning to kick the tires of this thing called cloud.

It became apparent that we were moving to a world where someone armed with a credit card could get access to tremendous computing power to quickly mashup impactful applications.

The problem I anticipated by 2013 was that there would be a lot of cloud options available, but from a security perspective, there would not be a lot of defensible best practices and strategies for cloud adoption, and for understanding the risks in a way that could be communicated to auditors.

This line of thinking started a snowball effect, and after talking to my CISO friends, I realized we really needed to get started on creating a whole cloud security ecosystem.

In 2008, during the financial meltdown, we brought together a group of smart industry people and started creating white papers. We wanted to start from what we understood the cloud was right then, and where it could go.

I took these ideas to a group of industry experts from eBay, Intuit, Qualys, and Zscaler. They provided encouragement and access to their networks to find the resources for all the different areas. And then we went to work on it and, at the RSA Conference on April 21, 2009, we announced the Cloud Security Alliance, with a mission to promote the use of best practices for providing security assurance within cloud computing. We also published *Guidance for Critical Areas of Focus in Cloud Computing* to set the stage for what the CSA was all about.

It took a lot of people by surprise because they were thinking about the need for the same type of organization. But we put together a pretty complete version 1.0 of our

Guidance. And many of those principles are still in the many iterations we've done since then. From that point on, we were viewed as an authoritative source.

In 2013, we heard a lot of enterprises tell us that having tools like the Guidance saved millions in IT costs, and how they could make the jump to the cloud sooner, because we had some defensible, vendor-neutral, intellectual tools to help explain to the rest of the ecosystem what we were doing.

It was a community, grassroots effort—a coalition of the willing—that just happened to have more time than they normally would have in that 2008 timeframe. From there, we built on the initial success.

At the CSA, we have a philosophy of making all of our research freely available. Sometimes we don't even know how enterprises are using what we do or how they're interacting with it. We see things from a lot of different levels. For example, a large oil and gas company viewed the cloud from a lens of four main pillars: awareness, visibility, opportunism, and strategy.
You are already in the cloud. Most places find they are probably using more cloud than they know.

From credit card projects to the entertainment industry, there are small firms that do everything in the cloud. It's an important part of the supply chain, but they also may not necessarily have the same technical visibility as a larger company.

So, understanding why people are using the cloud, what they're using, what problems they're trying to solve, how they're trying to transform the business—it's all key to understanding the impact.

As for *opportunism*, it's important to know it's going to be all cloud in the future in terms of backend data centers. Understanding that, we can find the best ways to move forward on a case-by-case basis, and to use security to solve business problems.

> *“Even the U.S. Federal Government announced in 2011 that it would have a cloud-first strategy.”*

Cloud strategy

Many organizations have settled on a cloud-first strategy. Even the U.S. Federal Government announced in 2011 that it would have a cloud-first strategy.

Strategy is about how to create the organization, technical architecture, culture, communications, and platform. We need to make it much more simple to enable different parts of the business to have what I call a cloud dial-tone.

If you have the right identity federation, and the right policies in place, you can do it your own way.

The cloud security landscape

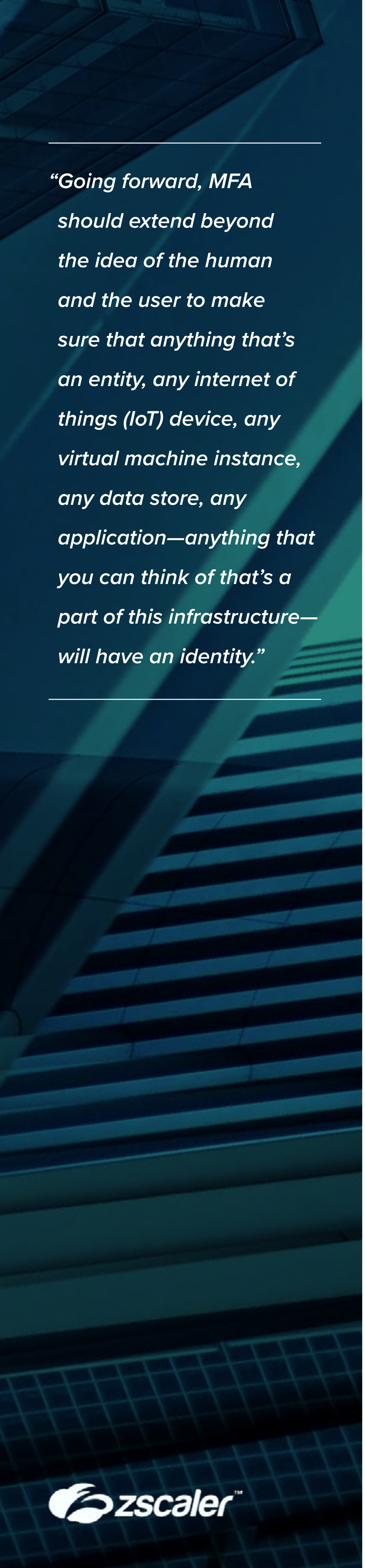
The need for regulatory compliance probably comes up first for organizations moving to the cloud. The data sovereignty and data protection aspects of it are of particular concern because you don’t necessarily have control of your own data. If you have a global utility that’s overlaid on multiple nation-states with their own regulatory regimes, that makes data sovereignty a paramount issue.

From a technical security perspective, the raw security concerns I see have become more nuanced. We hear from a lot of enterprises that top-tier providers do get it now. They have matured quickly and because of the scope of their platforms, they have visibility into attacks globally.

Cloud service providers have a security responsibility and enterprises need to be able to vet them properly. They need to understand that the cloud isn’t just the top five infrastructure providers, but it’s thousands of other entities that provide services on top of the infrastructure.

CSA engagement

More than any other sector, the financial services sector is participating heavily in the Cloud Security Alliance. This sector tends to be more sophisticated when it comes to IT. They engage with us more directly and want to share best practices and share their pain points with their peers.



> *“Going forward, MFA should extend beyond the idea of the human and the user to make sure that anything that’s an entity, any internet of things (IoT) device, any virtual machine instance, any data store, any application—anything that you can think of that’s a part of this infrastructure—will have an identity.”*

We receive many requests to engage with governments on behalf of our members—engage with regulators and provide the sort of vendor-neutral voice to help them understand what we see. We have to explain what the cloud is, where the risks are, and what they need to be thinking about.

It’s exciting times as organizations are trying to become more agile, to be “software-defined” in many aspects of their business.

Identity and federation

With identity and federation, there has been enormous progress. There isn’t as much pain involved in being able to take any new application and have the right way to plug that in with SAML (Security Assertion Markup Language) and other federation schemes.

We haven’t moved as quickly as I had hoped in having pervasive, multi-factor authentication (MFA) everywhere, but it’s certainly in a lot of places, and it’s certainly well understood. Going forward, MFA should extend beyond the idea of the human and the user to make sure that anything that’s an entity, any internet of things (IoT) device, any virtual machine instance, any data store, any application—anything that you can think of that’s a part of this infrastructure—will have an identity. It will have certificates. It will have the ability for us to understand it as a discrete and trusted component so that we can pull things out of it, and we can build a continuous audit trail or whatever else we need based on identity.

Impact on workforce

A big issue we hear about is the retooling of the workforce. Unless you go with some different definition, no one has 20 years’ experience in cloud, and so Global 2000 companies are hiring people fresh out of college and training them. You can’t run your IT organization on newly minted college graduates, but you need a strong infusion of fresh talent.

At the major cloud provider conferences like AWS re:Invent and some of the others, attendees get excited and charged up about what’s possible. It is creating a hunger—but, it’s a lot harder to flip a switch on people than it is on systems. It’s a slog to get people to change. The work is not all in retraining. We need more bite-sized education on how to do this, across the board, for every role in IT.

Better security through automation

Automation has created a different approach to security. The ability to instantiate and decommission compute, virtual machines, or containers can shrink your attack surfaces. Systems don't degrade with time and vulnerabilities have a much shorter half-life. The traditional ways of very carefully curating servers, like a thoroughbred, are over. Slow regression testing for understanding changes gets replaced by rapid instantiation and decommissioning of systems.

The ability to use automation tools to deploy pristine images decreases the opportunity for vulnerable systems to be attacked. It is so much better than we've ever had before.

What not to do on your cloud journey

It's a new world. Don't take all of your old approaches with you. The other aspect of all this is that it's really cloud-native. You can't assume that there's any physical choke point that's bringing everything back to a corporate enterprise perimeter and analyzing things. You have to understand what a true virtual, cloud-native architecture looks like. When you understand that, you can understand how to move to the cloud securely.

Ready to transform your company?

Create business value with Zscaler today.

CONTACT US REQUEST DEMO

https://www.zscaler.com/company/contact

https://www.zscaler.com/custom-product-demo

About Zscaler Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.