



With various forces combining to transform the IT landscape, how do you see the role of the IT department evolving?

We're in the midst of a major shift in how IT thinks about managing people, applications, data and devices. In our not so distant past, each of these items were placed behind the firewall where they were easier to integrate and control, but cloud, mobile and social computing are spreading these assets around the Internet, creating quite a challenge for IT. How will IT centrally manage and secure things that are inherently distributed and heterogeneous? And how will IT evolve to take advantage of what's new without throwing away or re-architecting what they already have? The operative word in the near-term is "hybrid," but long-term, it's all about identity and coordination.

What's the future for hybrid cloud strategies?

We have 30 years of legacy on-premise infrastructure and most of today's users, applications and data reside within the enterprise datacenter. However, as SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Service) and PaaS (Platform-as-a-Service) become ever more popular, IT's challenge is to bridge today's private infrastructure with both private and public clouds. To do so will require a hybrid approach to cloud adoption, where assets live in both places at once, but where IT extends their internal users, security policies and business processes to the cloud. This won't be easy, but that's where identity comes in.

The role of Identity in hybrid cloud computing is critical. Where "distributed" is the new norm, we believe identity will quickly emerge as the one constant capable of providing security and convenience. After all, when the device isn't yours, when the infrastructure isn't yours and when the application is outsourced, what's left to control other than who has access to what?

Leveraging identity in this manner will allow us to stitch together disparate applications run from private and public clouds so they function like a single application. In the process, we'll eliminate redundant logins and passwords, and we'll provide IT a way to centrally manage access even

though it won't own the device or the infrastructure running the outsourced applications. In this view of a hybrid world, API's take top billing, because they're the mechanism by which we'll loosely couple applications and data and within those API's, we'll leverage identity to determine the user as they traverse the Internet, moving seamlessly from one domain to another.

Does Mobile fall into one of your top 5 priorities for 2012? If so, how will you be attacking it?

Personal mobile devices are creating a myriad access, security and control issues for the enterprise. Users want access into corporate resources and are forcing IT to figure it out or make security and control compromises. As it turns out, knowing the user, not just the device, is critical to how enterprises will secure and manage this new trend as well. That's where Ping fits in. We provide enterprises with the needed identity infrastructure to know the user and secure the enterprise apps running not just within the browser, but on the iPhone or Android device as well.

In terms of our big vision, we believe the mobile phone will become the physical token (or key) to our digital world. As a powerful digital identity device, the mobile phone will help us secure and manage access while providing us the convenience of single sign-on and the control to say who sees what of our identity.

This interview was published in [SIIA's Vision from the Top](#) , a Software Division publication released at [All About the Cloud](#) 2012.