CHEAPER, FASTER, EASIER: PUBLIC CLOUD

Bart McDonough, CEO of Agio, provides his view on Agio's soon to launch public cloud offering, along with the necessary security considerations that come along with this technology.

HFM Tech (HFMT): What factors did you pay particular attention to when developing your own soon to launch public cloud offering?

Bart R. McDonough (BM): Pricing is the number one priority for COOs and CFOs, and we're seeing more and more CTOs zero-in on the public cloud's dynamic flexibility. Keeping both of these audiences in mind was critical when designing our offering in partnership with Microsoft Azure.

More specifically, we see two major benefits to COOs and CFOs when going to the public cloud: security and disaster recovery (DR). The sophisticated security controls, governance and suite of compliance certifications Azure maintains is more robust than anything a private cloud can offer, hands down. Then there's the out-of-the-box settings like identity access management, network access controls and security centre, which Azure provides to help you create a baseline secure cloud environment. It's not a cut-and-paste job, and does take a level of expertise to take these tools and apply them to your specific environment, but that's a role for vendors like us to play. Bottom line, you don't want the security of your cloud environment to be Swiss cheese and we make it easier to shore up those holes.

When it comes to DR, funds benefit from the massive price reduction the public cloud offers when only having to pay for the CPU to invoke DR or run a test. Imagine having insurance, and rather than monthly fees, you only pay when something goes wrong. This is what the public cloud does for DR, and in doing so frees up those dollars for our clients to invest in alpha-generating technology.

Then when we take a look at CTOs, they want ease of use. Our clients want a complete solution from the Infrastructure as a Service (IaaS) to the security tools and endpoint protections. By partnering with Azure, we're able to bring clients this completion with the depth and interaction between each of Microsoft's products – Azure AD integrates with Intune, Office 365 and more. The result is an easy to deploy public cloud offering, which maintains the strongest level of security, at a low cost, with high value products to all client end points.

HFMT: Why has the public cloud become popular, and what additional security needs to be considered with the solution?

Bart R. McDonough is CEO and founder of Agio. McDonough developed his career building technology solutions for Wall Street during a time when the industry's technological complexity and data dependency experienced rapid evolution. McDonough founded Agio in 2010 and went on to acquire a cybersecurity firm in 2013, effectively bringing IT and cybersecurity under one roof to better serve the industry. Since inception, Agio has experienced tremendous success, now bolstering an international workforce of nearly 200 employees with over 300 clients across verticals.

BM: Emotionally, it's basic human nature. People fear what they don't know and what they don't understand. Things take time, and it hasn't been until recently that we've seen the market really warm to the public cloud, and instil faith in the security controls cloud providers maintain.

Logically, we've seen a healthy improvement in public cloud pricing over the past few years, and replication technology has been perfected to make putting and pulling data in and out of the cloud simpler and faster. For COOs and CFOs, this moves the needle. Our CTOs like to see the evolution from IaaS to Platform as a Service (PaaS) with the addition of Azure DB, Azure Active Directory, Intune (end-point management) and more, including management of your internal assets. The migration path to using these tools has become as simple as enabling a connector or migration of a database with no need to rewrite code or start from scratch. This is powerful for our CTOs.

Finally, on the security front, it's not about "additional" security measures so much as it is a shift in mindset from old data centre security checklists to things like storage account encryption, managing encryption keys as well as enforcing principal of least privilege use, identity access management, and things like vendor reviews instead of a perimeter review. It's just a different way of looking at security.

HFMT: What further evolutions in public cloud services do you anticipate in the future?

BM: Continued evolution of the desktop endpoint, rounding out the complete data centre from systems, networking applications, file systems, and workstations. Complete portability and accessibility at the click of a button, anywhere around the world, opens up levels of productivity, flexibility and security never experienced before – something COOs, CFOs and CTOs alike want to be able to point to and say, "I did that."

And we can help our clients get there – with the added safety, security and peace of mind that comes with working with someone who knows what they're doing, and who's done this before. If we're not making it cheaper, faster and easier for our clients, then there's no reason for them to leverage Agio. Our public cloud offering does all three. ■