A GOVERNMENT TECHNOLOGY Q&A

government technology

IT Modernization: The New Imperative

Government IT modernization took on new importance following the COVID-19 outbreak, demonstrating the value of more flexible networks and applications. In this *Government Technology* Q&A, **Marc Moffett,** Cisco systems engineering lead for state and local governments, discusses what the roadmap for modernization will look like going forward.

How is the conversation changing around the importance of government IT modernization?

Prior to March, when we were thinking about government services, everything was directed outward toward the citizen. Suddenly, millions of people were sent overnight to work from home. It drove a different conversation around business continuity and how you give government workers a quality experience despite different circumstances.

There used to be a general distrust around remote work in government. However, as we suspected from experience in the private sector, government services can be delivered effectively remotely. We have also learned many of our customers are using software-as-a-service products, which is what allowed them to send people home immediately and collaborate. Having easy-to-use applications is critical to enable a massive number of people to conduct business over virtual interactions.

What lessons can we take from ongoing modernization efforts?

Even before the pandemic, there was a steady shift of applications moving to the cloud, and a major driver was for people to have access to those applications anytime and anywhere. Now we need to rethink our network architecture to make sure we can quickly spin up a secure infrastructure so we can deliver government services in any circumstance.

What does the roadmap for modernization look like going forward?

I use the term "elastic." Organizations need to be able to move from on-premises operations to wherever the worker is based. We have talked about an end-to-end architecture for a long time but being able to abstract hardware from the services required gives you a lot more control. Three key areas are:

Applications. While governments are deploying apps predominately in the cloud today, technology like SD-WANs and software-defined access allow users to access apps remotely without necessarily having to add more bandwidth or hardware.

Security. We have to think about everything from a full-scope security standpoint. Endpoint security, virtual firewall capabilities, zero trust — all those things come together into a good solid security stack that can be delivered on premises, via the cloud or through hybrid solutions depending on the user's needs.

Infrastructure. Networking is evolving through software-defined models, automation and programmability and we need to start leveraging the infrastructure in different ways.

As the government workplace continues to evolve, what are the implications for the technology supporting it?

Some states are talking about cutting building capacity by as much as two-thirds because they have found they can deliver the same level of services without having the same real estate footprint.

Just like we think about multi-cloud and distributed applications, now we're distributing people. When you are going to let your staff work from potentially anywhere, you need to rearchitect your applications for both on premises and the cloud based on their needs. For example, SD-WANs could be employed for heavy-duty users that need a branch-like experience at home. For the mid-level user who does not need that much complexity, you can provide access through a software security stack. Lightweight users may just need collaboration-type touchpoints. In that case, you might have base-level security and something like videoconferencing that rides on top of that.