Becoming Cloud-Ready

State and local governments are turning to the cloud to accelerate the deployment of digital government services and ultimately improve the citizen experience, but just adopting the cloud itself doesn't ensure success. In this Government Technology Q&A, **Abel Ramirez,** Senior Solutions Architect with Cisco, discusses how a cloud-ready network positions agencies for the future, all while delivering operational simplicity, application visibility and end-to-end security.

What are the biggest roadblocks state and local government agencies encounter with cloud implementation?

Agencies often layer various software-as-a-service (SaaS) solutions and cloud platforms on top of their traditional data centers to fit specific needs, which can become unwieldy for central IT and security to support. The skillsets and tools that worked in on-premises data centers often don't span to cover SaaS and cloud platforms, as well as different application delivery methods such as containers. Increasingly, agencies need an application performance management tool to ensure end-to-end visibility. Similarly, consistent controls and visibility are needed to maintain a strong security posture. Gaps in either area increase risk and costs.

Another common roadblock is the need for additional governance and coordination among agencies and central IT teams. This often starts with an application rationalization exercise to compare agency needs and plans, as well as what applications and data lend themselves to the cloud. As cloud adoption increases, this lifecycle management and portfolio approach and the continued adaptation of security controls will be important aspects of ongoing governance.

What does today's cloud environment look like, and what are the benefits of hybrid and multicloud environments?

Today, most agencies are using several types of SaaS applications like email, conferencing, customer support and file sharing. We are also seeing agencies adopt one or more infrastructure-as-a-service (IaaS) platforms for new applications, and some have migrated existing cloud-friendly workloads. Leading governments are accelerating the transition of their traditional data centers to private cloud. Once state and local governments have positioned their IT architecture and operations to securely and reliably leverage multiple clouds, they will be able to deploy new digital government applications and services faster.

What is needed to migrate from traditional network designs to take full advantage of cloud?

Traditional state and local government networks rely heavily on a centralized approach for WAN and branch security. This architecture model backhauls all traffic to one or more central data center or headquarter locations for security enforcement and provides a common exit point for internet services, SaaS and IaaS. As organizations start or accelerate cloud adoption, this model becomes inefficient and costly.

To meet evolving cloud expectations, we are seeing a shift to a new network architecture called cloud-ready network (CRN). CRN uses a software-defined WAN (SD-WAN) fabric to establish points of presence in various clouds to every branch — enabling optimized traffic flows, user experience monitoring and common security policy enforcement. CRN provides the best application experience possible in today's multicloud world and consistent unified threat protection from branch to cloud edge.

What are the key characteristics of a mature CRN?

A CRN enables architectures that provide simplicity, adaptability, automation, embedded security and application awareness across private data centers and public cloud platforms. These characteristics are key to accelerating cloud adoption and mitigating risk.

For instance, by leveraging SD-WAN, agencies can build a scalable, carrier-independent WAN that reduces transport costs and network operating expenses. By bringing SD-WAN points of presence into leading IaaS platforms and high-speed co-location facilities, CRNs extend management and visibility beyond the traditional network perimeter all the way to the cloud. SD-WAN fabrics continuously measure application performance and adjust dynamically to work around failures and bottlenecks. The embedded security capabilities protect data passing to and from branch systems, private data centers and public cloud platforms. In addition, the security stack guards against attacks that originate from compromised internet connections and applications.

What does effective security look like in a CRN?

To protect data, infrastructure and networks in today's connected world, agencies must adopt a zero-trust approach. The zero-trust approach is centered around one guiding principle: Security must extend throughout the network, not just at the perimeter. CRN fits into a broader zero-trust model. The essential tenets of a zero-trust model are:

- Eliminate network trust. Assume all traffic, regardless of location, is a threat until it is verified (authorized, inspected and secured).
- Segment network access. Adopt a least-privileged strategy and strictly enforce controls.
- Gain visibility with analytics. Continuously inspect and log all traffic internally and externally, using real-time protection capabilities.
- Act in real time. When anomalous activity is detected, act immediately to limit the threat impact and manage risk.

We recommend agencies take a holistic approach and extend zero trust to their workforce (all users), workloads (all applications and data) and workplace (including IoT and other devices not specifically associated with a user). Using a CRN helps optimize user experience, speed and security, which are all required to enable a zero-trust approach.

CISCO

For more information, visit: www.cisco.com/go/cloudready

© 2020 e.Republic. All rights reserved.