Foundation First

Why network planning is essential to cloud success

There is no denying the future of Federal IT is dependent on the successful implementation of cloud solutions.

With cloud technologies, agencies unlock several opportunities previously unattainable, including access to commercial innovation, better use and understanding of their data, and the agile achievement of agency missions.

Recent policies have established the pace and sophistication of Federal cloud-based network adoption. First, the Office of Management and Budget's (OMB) Cloud Smart Policy, released in June 2019. Cloud Smart[1] finalized the Federal government's shift toward a new approach that "offers practical implementation guidance for Government missions to fully actualize the promise and potential of cloud-based technologies." Cloud Smart emphasizes three pillars – security, procurement, and workforce – and sets a total of 22 action items.

Second, the Cybersecurity and Infrastructure Security Agency's (CISA) draft guidance documents for version 3.0 of its Trusted Internet Connections (TIC)[2], released in December 2019. TIC broadly aims to improve network and perimeter security across Federal networks. The latest proposed iteration is intended to provide a better approach by giving agencies flexibility to use modern security technologies.

While the power and backing of Federal cloud migration is undeniable, agencies are lacking the proper foundation to support the quickly evolving modernization efforts necessary for mission success. Now, one less discussed component begins to play a vital role in the future of Federal IT – the network.

What barriers can be eliminated as a result of foundational network planning and how will the cloud-ready network architecture deliver on organizational and mission goals?

[1] https://www.meritalk.com/articles/omb-finalizes-cloud-smart-policy/
[2] https://www.meritalk.com/articles/cisa-releases-draft-tic-guidance-documents/

Blueprint for cloud success

Until recently, agencies have relied on a strictly on-premise approach. Facilities housed applications, data, and security components on site and under agency ownership – serving as the central gateway to the public network.

The introduction of the cloud challenged the legacy on-premise approach and necessitated a total restructuring in the definition of the application "location." Now, agencies are experiencing understandable growing pains in terms of how they approach security and wide area network (WAN) design. Maintaining control and visibility of applications and data that now reside in the remote and uncertain public cloud has become a concern.

Additionally, establishing a scalable and secure connection from on-premise environments to cloud service providers is critical to a successful migration. Applications are also growing increasingly distributed across virtual machines (VM), containers, and bare-metal hardware present in data centers and cloud environments. Agencies require a network that can handle the growing diversity of applications needed to meet mission needs.

These challenges have resulted in agencies struggling to keep pace.

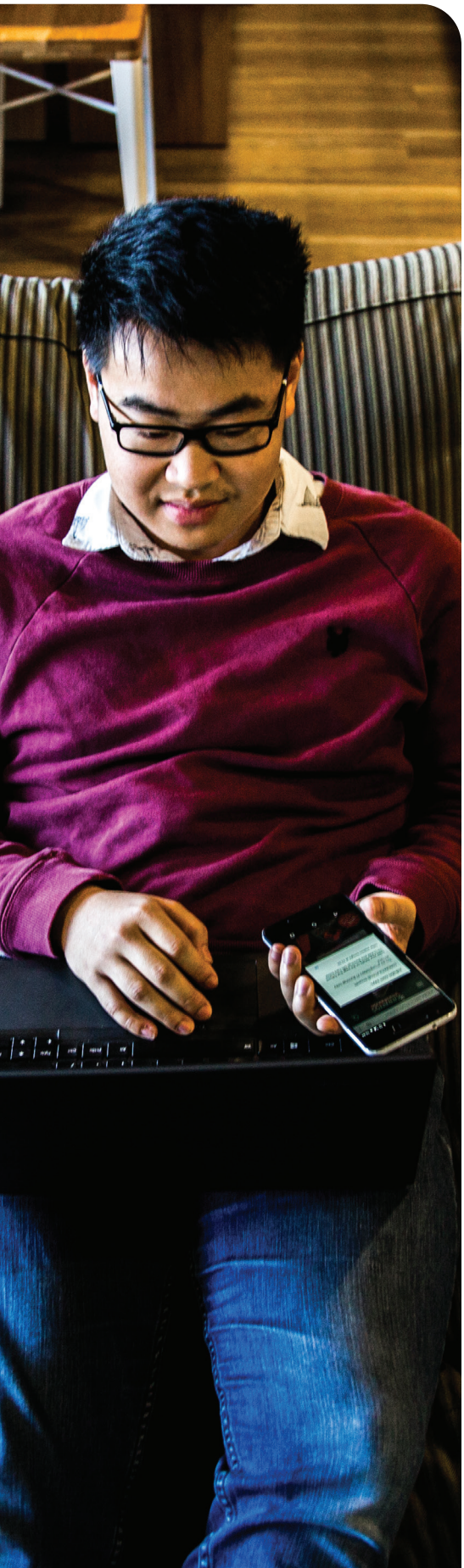
Get cloud ready with cloud-ready networks

As agencies migrate applications to the cloud, a solid, deterministic, and secure network becomes the lifeblood of the end-user experience. The cloud-ready network approach enables architectural shifts that supports Federal cloud adoption.

With the cloud-ready network approach, the cloud edge demarcation point is redefined. By leveraging co-location centers (co-lo), agencies can establish a security control point for any and all traffic leaving the agency. The cloud edge could be established inside an agency's walls; however, co-lo's offer exclusive services essential to modernization, including scalable connections, secure hosting facilities, foundational security, and partnerships with cloud providers.

By extending the cloud edge to co-lo centers, agencies now operate adjacent to cloud providers on local connections. This translates into more deterministic latency and a new defined security perimeter for tighter security control and visibility. These offerings make co-lo centers and the cloud ready network approach an obvious choice for establishing the cloud edge and building in-depth security controls.

As agencies make decisions on what cloud capabilities are essential to their mission, the cloud-ready network framework provides validated architecture principles that can be leveraged to build secure, agile, and scalable connections to multiple cloud providers.



Count on cloud-ready networks, count on Cisco

As you work toward your agency's modernization goals, Cisco is prepared to help you innovate with confidence on a solid, deterministic, and secure network essential to end-user experience and mission success. Cisco is uniquely positioned as a cloud enabler to ensure your agency's missions are optimized in a multi-cloud, Cloud Smart, Zero Trust world.

Cisco plays everywhere. With our extensive network expertise and ecosystem of solution partners we deliver innovation-forward that powers mission-critical IT modernization. We're secure, integrated, and we own most of the network out there, so we see things others don't see. When you innovate with confidence, you propel Federal forward.

To learn more, please visit: https://www.cisco.com/go/cloudready

CXX-XXXXXX-00 XX/XX