Secure Cloud Computing Architecture

Cloud Access Points

DISA's Secure Cloud Computing Architecture (SCCA) is a suite of enterprise-level cloud security and management services. It provides a standard approach for boundary and application level security for Impact Level four and five data hosted in commercial cloud environments.

One of the capabilities, Cloud Access Points (CAPs), provide connections for mission partners applications to approved cloud providers. In addition, the solution protects DOD networks from cloud originating cyber attacks.

CAPs Provide

- ✓ Boundary Defense
- ✓ Connection to Impact Level 4/5 Approved Providers
- ✓ Uptime of 99.96% over last 24 months

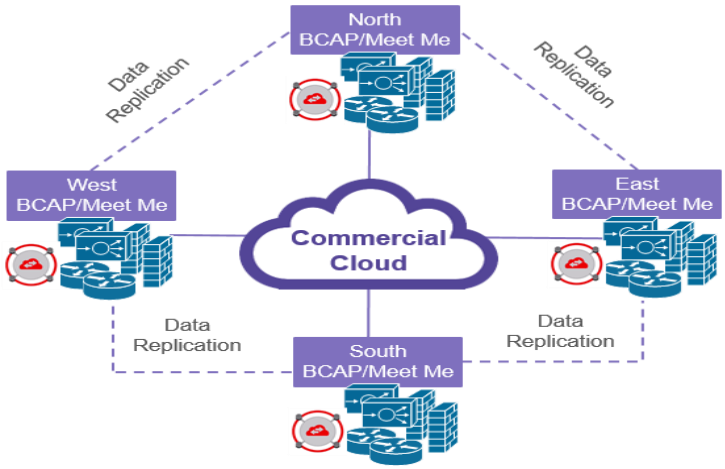
CAPs Do Not Provide

- X Break and inspect
- X Application security or management

Evolving the CAPs

As cloud service offerings continue to evolve, DISA is leading the way to meet mission partner requirements for **enterprise cloud access and security**.

In the **fall of 2019**, enterprise CAPs will be deployed directly to commercial cloud exchange points. This means increased bandwidth up to **100G per CAP**, and a reduced path to approved commercial clouds.



SCCA Services

Cloud Access Points: Provides connectivity to approved cloud providers and protects DoD networks from cloud originated attacks

Virtual Data Center Security Stack: Virtual Network Enclave Security to protect applications and data in commercial cloud offerings

Virtual Data Center Managed Services: Application Host Security and privileged user access in commercial environments

DISA Cloud Services: Host. Protect. Connect.

GETTING STARTED

For additional information on cloud services, please contact: Disa.meade.se.list.cloud@mail.mil

Sept 2019