Secure Cloud Computing Architecture

A Scalable, Cost-Effective Approach for Cloud Access, Security, and Management Services

Overview

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.

Features

- **Boundary Defense**
- **Web Application Firewall**
- **Next Generation Firewall**
- **HBSS**
- **ACAS**
- **Operating System Patching**
- **Security Incident and Event Management**
- **Key Security and Management**
- **Behavior Analytics**

Connect: Access DoD approved level 4/5 cloud services

Secure: Extend application and data-level security services to commercial cloud environments

Manage: Obtain custom analytics and intelligence data for host based security and role based access controls

Services

Cloud Access Point: Provides connectivity to approved cloud providers and protects DoD networks form 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

Trusted Cloud Credential Manager: Cloud Credential Manager to enforce Role Based Access Control and least privileged access

SCCA Program Office: disa.meade.sd.mbx.scca@mail.mil

Current as of June 2018