Cisco Cloudlock

DATASHEET

Cloud Security for Government Agencies

At a Glance: The Cisco Cloudlock CASB and Cybersecurity Platform is a frictionless, cloud-native security solution that enables government agencies to securely harness the power of cloud technologies to fuel growth and innovation without sacrificing data protection. Cisco Cloudlock combats account compromises, cloud malware, and data breaches while facilitating compliance and incident forensics through an approach that deploys in minutes and has zero impact on end users. For advanced security teams that need to combat complex cyberthreats, the Cisco Cloudlock Cybersecurity Orchestrator aggregates visibility and automates threat response across existing security solutions.

Business Challenges

The notion that government agencies operate with any less efficiency is long gone. Today, federal, state, and local government all look to cloud technologies to increase employee productivity and collaboration as well as save money. However, these institutions are held to the highest standards when it comes to compliance and legal regulations. In adopting cloud-based technologies, security considerations task government institutions with three primary imperatives:

Comply with Regulations Government agencies must adhere closely to compliance mandates around a wide range of regulations, including protecting Personally Identifiable Information (PII), International Traffic in Arms Regulations (ITAR), Federal Information Security Management Act (FISMA).

Protect Sensitive Data Government institutions hold a great deal of sensitive information, including the compliance-specific information described above, but also extending to typical business-related information sets, such as employee records, financials, and intellectual property. Ensuring access to and distribution of this data is controlled is essential to the vitality of the organization, maintaining a competitive edge, and avoiding the tangible brand damage typically seen as a result of recent security breaches.

Defend Against Cyberthreats Given the many valuable information payloads residing within government agencies' cloud environments, cybercriminals target government institutions with increasing frequency and persistence. To combat cyberthreats, government agencies must be able to rapidly identify suspicious behavior and equip themselves with the tools to respond accordingly.

Solution Overview

Cisco Cloudlock is the multi-mode, cloud-native CASB and Cloud Cybersecurity Platform that helps government organizations securely leverage the cloud for apps they buy and build. Cisco Cloudlock delivers security for any cloud application and platform, including IaaS, PaaS, and IDaaS, and orchestrates security across existing investments.

Cisco Cloudlock is particularly well-suited to government agencies' environments:

- **Cloud-Native** As an API-driven solution, Cisco Cloudlock deploys full functionality in minutes, delivering immediate value without requiring resource-intensive and complex network configuration projects, and has zero negative impact on end users
- **Unparalleled Coverage** Comprehensive coverage of cloud traffic, including on-and-off network, programmatic and user-driven, by managed and unmanaged users and devices, retroactively and in real-time
- **Proven Track Record** Cisco Cloudlock has been deployed to over 750 organizations globally, including government institutions such as the City of Boston, the General Services Administration (GSA), and the United States Army
- **Security Certifications** Cisco Cloudlock has demonstrated commitment to security by achieving SOC 2 Type 2 accreditation by Ernst & Young for four consecutive years. Additionally, Cisco Cloudlock is the only CASB to achieve FedRAMP Agency-Sponsored in Process Status (ATO)

Key Benefits

- Identify and **protect sensitive information** within cloud environments and enforce automated, cross-platform response workflows
- Defend against **account compromise** with cross-platform User and Entity Behavior Analytics for SaaS, IaaS, PaaS, and IDaaS environments
- Discover and control **malicious and risky cloud apps** connected to sanctioned cloud applications and infrastructure
- Increase the value of existing security investments by aggregating data streams and enforcing automated, **cross-platform response workflows**

Key Features

- **Cloud Data Loss Prevention and Automated Remediation Workflows**
- **Apps Firewall**
- **User and Entity Behavior Analytics**
- **Cybersecurity Orchestration** for IDaaS, SWG, NGFW, Malware Detection, and SIEM Systems

Manage Compliance in the Cloud

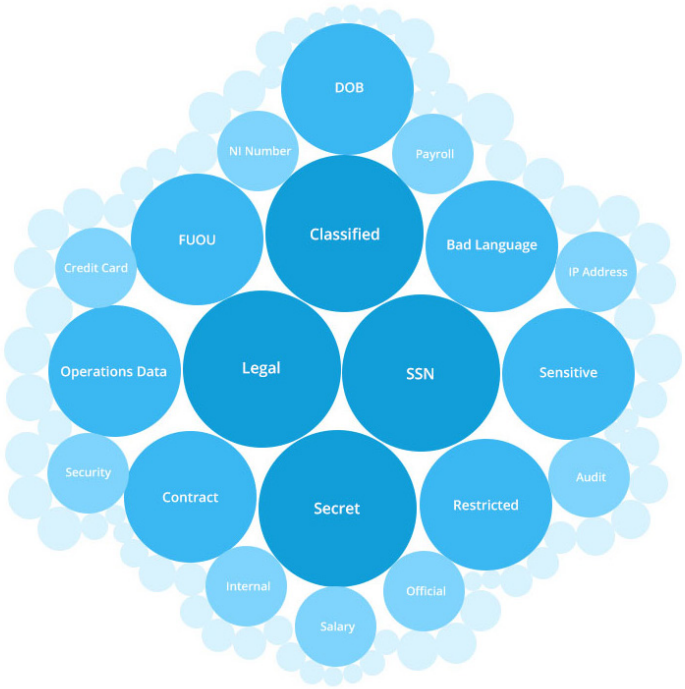
Efficiently Satisfy Regulations

- Enforce compliance through out-of-the-box policies designed for PCI-DSS, SOX, and other compliance-specific information
- Tailor policies to proprietary concerns such as intellectual property through Cisco Cloudlock's highly-configurable policy engine
- Mitigate risk rapidly through automated, policy-driven response actions, including file-level encryption, quarantine, end-user notification, administrator notification, and more

Protect Sensitive Information

Discover and Secure Sensitive Data

- Pinpoint excessively exposed sensitive information within cloud environments based on defined content or exposure criteria
- Monitor data-at-rest residing within cloud applications
- Enforce automated, contextual policy-driven response actions



The most common terms used in DLP policies in government agencies.

Source: Cisco Cloudlock "Cloud Cybersecurity Report: The Riskiest Industries"

Thwart Cyberthreats

Defend Against Malicious Actors

- Defend against account compromise with cross-platform User and Entity Behavior Analytics (UEBA) for SaaS, IaaS, PaaS, and IDaaS environmentsMonitor data-at-rest residing within cloud applications
- Leverage advanced machine learning to detect anomalies in account usage
- Detect activities outside of whitelisted countries and actions performed across distances in an impossible amount of time

Synchronize Security with the Cisco Cloudlock Cybersecurity Orchestrator

Maximize the Impact of Existing Security Investments

- Increase the value of IDaaS solutions to complement Cisco Cloudlock's User and Entity Behavior Analytics with automated response actions such as requiring multi-factor authentication, restricting application access, and reducing maximum session length
- Combat malware and ransomware in cloud environments by extending malware detection and threat emulation systems to cloud platforms
- Aggregate on-premises logs with Cisco Cloudlock app risk insight for superior Shadow IT visibility
- Manage the cloud security incident lifecycle within SIEM systems