

State & Local Government

Introduction

This case study of a state & local government is based on a December 2017 survey of Cisco Cloudlock customers by TechValidate, a 3rd-party research service. The profiled organization asked to have their name blinded to protect their confidentiality.



“Cloudlock helped us to recognize compromised accounts and reduce the impact of compromise.”

Challenges

The business challenges that led the profiled organization to evaluate and ultimately select Cisco Cloudlock:

- Purchased Cloudlock to solve the following challenges:
 - Protect sensitive organizational data
 - Provide visibility into connected cloud apps

Use Case

The key features and functionalities of Cisco Cloudlock that the surveyed organization uses:

- Purchased Cloudlock for the following reason:
 - Threat insight
- For connected applications, Cloudlock helped them to:
 - Identify the OAuth applications users have self-enabled
 - Understand the risk of OAuth applications connected to their environment
 - Block malicious and/or overprivileged applications

Results

The surveyed organization achieved the following results with Cisco Cloudlock:

- Achieved the following outcomes with Cloudlock:
 - Increased protection against data breaches
 - Improved compliance posture and lowered risk
 - Improved protection against account compromises
 - Achieved control over third-party cloud apps
 - Improved visibility into cloud usage
- States Cloudlock’s role in their cloud app security is very important.

Organization Profile

The organization featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Organization Size:
State & Local

Industry:
Government

About Cisco Cloudlock

Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps.

Learn More:

[Cisco](#)

[Cisco Cloudlock](#)