SOLUTION BRIEF

Cloud Security for Government Environments

Agencies must protect sensitive information wherever it resides

CHALLENGE

- Data is now stored and accessed from anywhere. Visibility remains fragmented.
- Agencies need unified data protection on-premises and in the cloud.
- Agencies must stop bad actors from accessing cloud application data.

SOLUTION

- Forcepoint CASB allows agencies to identify and categorize cloud applications to assess risk.
- Forcepoint DLP cloud integration prevents cloud application data leakage without redefining policies.
- Full context Behavior Analytics provides risk prioritized alerts

BENEFITS

- Discover cloud application use, analyze risk, and enforce controls for SaaS and custom applications.
- Comprehensive visibility and control over sanctioned/unsanctioned cloud apps.
- Minimize threats in near real-time and maintain equal protection everywhere.

In 2010, the Federal Government created the first cloud strategy, aptly titled "Cloud First." Reaffirming the commitment to the cloud, President Trump's Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" calls for agency heads to show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.

Under this directive, agencies are continuing to prioritize cloud computing initiatives as part of their IT modernization plans. To be successful, they must consider their unique missions and determine a cohesive cloud strategy that provides security, savings, and faster delivery of each agency's unique mission requirements.

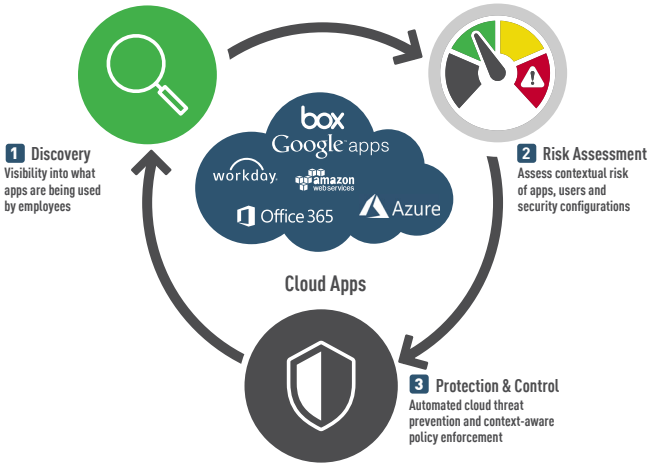
When considering security solutions for the cloud, agencies must first determine:

- How can you scale your security to protect your data, wherever it is?
- How do you identify risky cloud applications in use?
- How do you securely embrace the cloud while remaining in compliance?
- What features to consider when implementing CASB?

RETHINKING DATA PROTECTION FOR THE GOV CLOUD

For agencies making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and the cloud is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure. Selecting the right cloud security solution for your agency is imperative if you want to get the best from the cloud and ensure you are protected from unauthorized access, data breaches and other threats. Forcepoint CASB is a complete cloud security solution that protects cloud apps and data, prevents compromised accounts and allows you to set security policies on a per-device basis. The result is a cloud infrastructure that is fully protected from known and emerging threats and which allows your organization to leverage the best that cloud computing has to offer.

Forcepoint CASB offers enhanced security for data in cloud apps, so users can access their favorite apps without restriction.



AGENCIES REQUIRE COMPLETE SECURITY FOR ALL CLOUD APPLICATIONS

The benefits of cloud-based delivery models have incentivized agencies to adopt cloud apps and services. Forcepoint eliminates security blind spots as data leaves agency networks, providing visibility and control of end-user behaviors and data in the cloud and in SaaS solutions. Forcepoint CASB supports any application—even custom apps—offering app discovery, governance, compliance, analytics, and protection in a single solution. Delivering quick time-to-value via API and Proxy Modes, Forcepoint CASB expedites implementations and enables audit and app protection in a matter of hours or days. In addition, Forcepoint CASB integrates with Web and Email Security, Next-Generation Firewall, DLP and more to provide discovery and control for all data and to unify data protection from on-premises to your agency's cloud environment.

> Forcepoint CASB provides visibility and control over both sanctioned and unsanctioned cloud apps.

THE FORCEPOINT CASB VALUE

- Discover and risk-prioritize all unsanctioned cloud use (Shadow IT) to quickly and easily determine if applications meet governance rules and avoid compliance issues
- Unleash the power of BYOD with improved employee productivity and cost savings while ensuring security of employees and corporate resources in the cloud
- Identify anomalous and risky user behavior in the cloud to stop malicious users, as well as clamp down on user activities that don't meet best practices
- Reduce the risk of exposing sensitive cloud data to unauthorized users in violation of governance and regulatory rules
- Identify potentially inappropriate privilege escalation and implement geo-location-based access and activity monitoring for legitimate users and malicious actors

SCHEDULE A CLOUD THREAT ASSESSMENT TODAY

It is crucial you understand the requirements for securing information stored within your agency's cloud applications. Forcepoint offers a complimentary Cloud Threat Assessment, to detail your cloud-application risk exposure.

- **Cloud usage patterns.** How potentially harmful activities happen in cloud applications across your organization.
- **Geographical usage.** Which countries your data is traveling to and from (you may be surprised).
- **Privileged users.** Do you have more administrators than you need?
- **Dormant users.** Are you overspending on unused licenses?
- **Riskiest users.** Who are your riskiest users and why?

SCHEDULE A CASB THREAT ASSESSMENT

CONTACT
www.forcepoint.com/contact