solution brief

Securing the Department of Energy's Cloud Environment

Challenge

- DOE is a highly distributed agency—97 entities spread across 27 states—with wide-ranging levels of risk.
- Data is stored and accessed from anywhere.
- Visibility remains fragmented at the departmental level.
- Unified data protection is needed to stop bad actors from accessing cloud application data.

Solution

- Forcepoint Cloud Access Security Broker (CASB) will allow DOE to identify and categorize cloud applications to assess risk.
- Forcepoint Data Loss Prevention (DLP) cloud integration prevents cloud application data leakage without redefining policies.
- Full context behavior analytics provides risk prioritized alerts.

Benefits

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

In 2010, the federal government created the first cloud strategy, aptly titled "Cloud First." However, a number of cloud security elements were underdeveloped when the policy was introduced, resulting in slow adoption by government agencies. In recent years, agencies across the federal government have embraced cloud computing architectures and solutions to provide services to constituents and reduce the need for large-scale, traditional IT infrastructure investments.

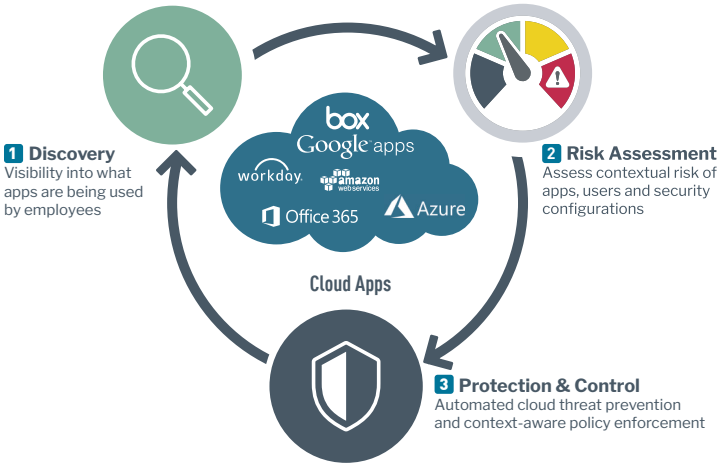
In June 2018, DOE received TMF funding to help expedite its migration to cloud. Given the wide-ranging levels of risk that exist in DOE's day-to-day operation, robust cloud security is key factor in order to ensure visibility and control of data in the cloud.

5 Considerations for DOE's cloud security strategy

- How can DOE scale its security to protect its data, wherever it is?
- How does DOE identify risky cloud applications in use?
- How does DOE securely embrace the cloud while remaining in compliance with data privacy laws?
- What are the key features to consider when implementing CASB into the environment?

Rethinking data protection for the Gov cloud

DOE's security threats are constantly evolving and there is a critical need to ensure near real-time risk insights to better protect critical data wherever it resides, including Controlled Unclassified Information (CUI) and sensitive data about the nation's power grid, nuclear weapons stockpile, energy labs and critical infrastructure. The cloud is no less at risk than an on-premise environment. For this reason, it is essential for DOE have a cloud provider that offers best-in-class security that has been customized for DOE's infrastructure.



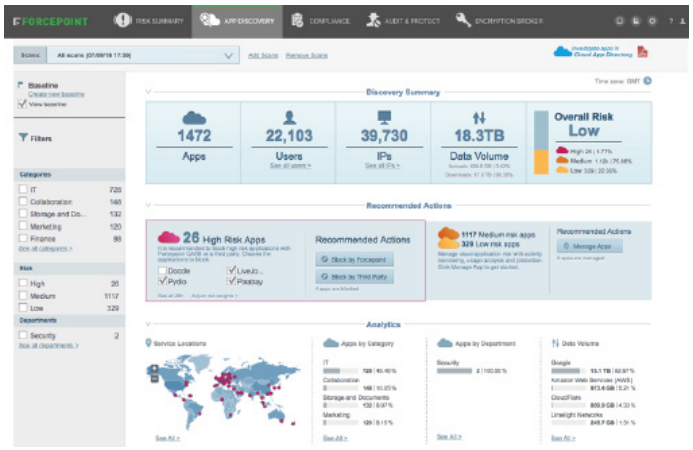
DOE needs complete security for all cloud applications

Selecting the right cloud security solution is imperative for DOE to get the best from the cloud and ensure the agency is protected from unauthorized access, data breaches, and other threats. Forcepoint is a key partner to DOE's multi-dimensional cybersecurity strategy, with solutions scaled to support the department's security program. Forcepoint CASB is a complete cloud security solution that protects cloud apps and data, prevents compromised accounts, and will allow DOE 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 will allow DOE to leverage the best that cloud computing has to offer.

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.

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 government 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.



> We have open science, which is low risk, and we've got the nuclear mission which is incredibly high risk. So, we want to make sure that we are understanding and doing that risk management apples to apples. — Max Everett, Department of Energy CIO

Contact
DOE@forcepoint.com

[SECURING DOE CLOUD ENVIRONMENT-SOLUTION BRIEF-FED-US-EN] 700017.020719