Unsanctioned or Shadow IT

Overview

Given the increased importance of heightened security controls for shared services and cloud under the Presidents Cybersecurity Executive Order and associated Cybersecurity Framework, the need for clarity in the cloud has never been more urgent.

As DoD employees seek ways to streamline archaic or burdensome processes within the mission, they adopt an increasing number of cloud services to enhance productivity and shorten tasks. Unbeknownst to the employee, this behavior often causes greater risk to the mission as these cloud services offer ubiquitous connection and are not pre-vetted by the mission before being accessed. This is known as Shadow IT. To date, legacy methods utilized by the CAP, TIC or SOC have proven unsuccessful in hindering this type of access due to the porous and dynamic nature of the cloud. Since there is little to no visibility into shadow cloud services from the onset, the impact of this behavior results in deficient policy enforcement and renders spill response detection non-existent.

Skyhigh Networks FedRAMP Compliant cloud security platform provides continuous deep-level inspection and control of the global cloud footprint. With over 30 million users across 700+ global enterprises, Skyhigh allows the mission to identify and analyze cloud service usage as well as evaluate the risk profile of the cloud service provider, working in conjunction with CAP egress technologies to safely enable secure usage of the cloud. The size of the user base directly supports the accuracy and scale of Skyhigh's cloud registry by combining user behavior analytics with a powerful machine-learning back end, enabling Skyhigh to continuously adapt and understand the porous nature of the cloud, enforce policy and provide governance, compliance and risk data for each cloud service across Infrastructure (IaaS), Platform (PaaS) and Software (SaaS).

The recent Cloud Adoption & Risk Report by Skyhigh showed that 15.4% of the documents uploaded to the cloud contained confidential data including financial records, business plans, source code, trading algorithms, personally identifiable information (PII) and personal health information (PHI). If this data is leaked outside the company, it can not only adversely impact a command's defensive security posture, but also put the agency at risk of a compliance breach, resulting in huge penalties and loss of reputation.

As DoD approves and adopts cloud/web services, IT teams are facing a cloud services governance challenge. According to a CSA survey, IT professionals receive, on average, 10.6 requests each month for new cloud services, and that it takes an IT security team 17.7 days to evaluate the security of a cloud service provider. So, in addition to protecting their data from leakage via shadow cloud/web services, companies are looking for a solution to address their cloud governance challenges.

The following figures illustrate the inefficacy of traditional enforcement technologies and the breadth of the challenge:

Figure 1: Illustrates the gap in enforcement when relying solely upon tradition egress technologies in the CAP

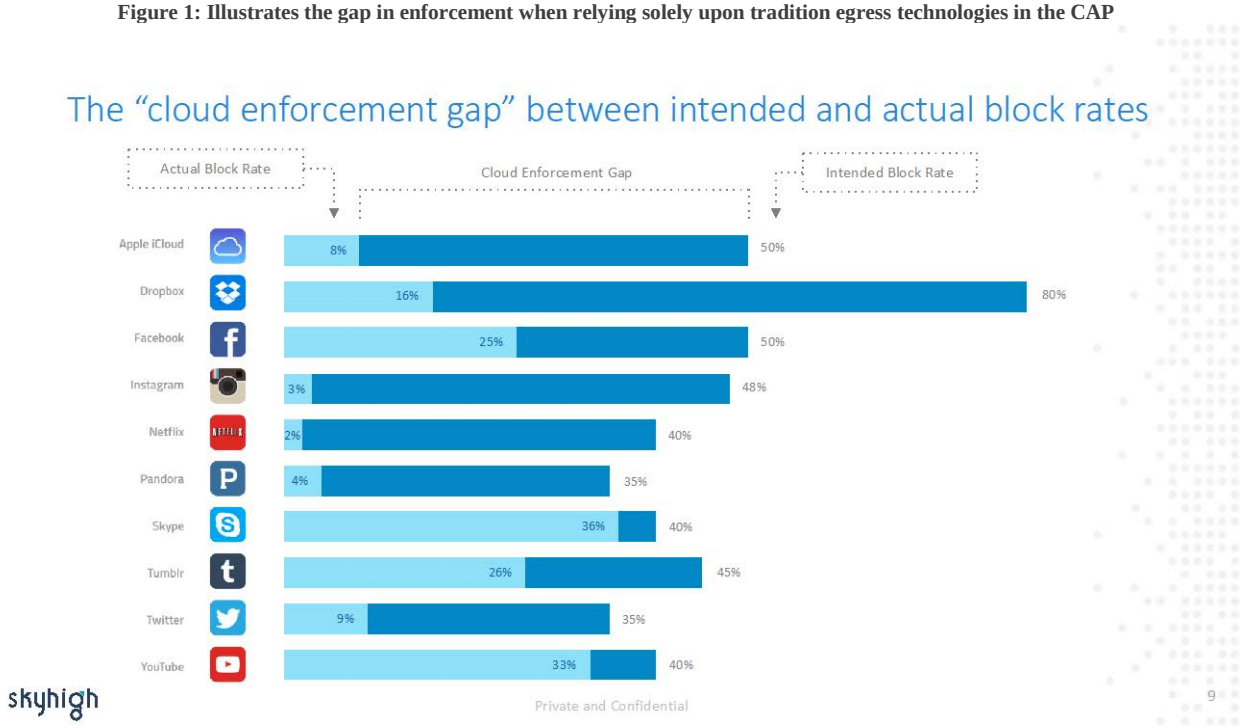

Figure 2: Illustrates an actual example of "Shadow Cloud" within an increasingly popular DoD service: SLACK

skyhigh

Objective

Skyhigh for Shadow IT provides enterprises with the visibility into all cloud/web services used by employees along with the associated risk ratings. Skyhigh has multiple deployment options, including forward proxy, log collection from enterprise egress devices, and inspection of traffic via ICAP and API. DoD missions can remedy risky services, enforce DLP policies, streamline processing of cloud service approval requests and detect activity indicative of insider threats, botnets and data breaches. Skyhigh's cloud registry of over 26,000 services contains detailed signatures of the security information that helps IT quickly onboard cloud services and enforce policies on shadow cloud usage.

Skyhigh for Shadow IT capabilities can be organized into 4 categories: Visibility, Threat Protection, Compliance, and Data Security:

1. Visibility

Cloud Registry

Delivers a comprehensive registry of cloud services, including thousands of services uncategorized by firewalls and proxies.

CloudTrust Ratings

Assigns a risk rating for each service based on 65+ attributes. Modify attribute weights and add custom attributes to generate personalized ratings.

Cloud Usage Analytics

Visually summarizes key usage statistics including the number of cloud services in use, traffic patterns, access count, and usage over time.

Cloud Service Governance

Provides a proven workflow for processing large volumes of cloud service approval requests and a consolidated database to track and manage all approved services.

Cloud Service Comparison

Enables side-by-side comparison of cloud services across 50 risk attributes, data transfer volume, user count, and service category to streamline the evaluation process.

CloudRisk Dashboard

Provides an enterprise Cloud Risk Score aggregated from service, user, data, business, and legal risk, and includes risk benchmarks and trends over time.

Cloud Enforcement Gap Analysis

Presents allowed and denied statistics and highlights gaps in cloud policy enforcement along with recommendations to close gaps.

Coaching and Enforcement

Displays just-in-time coaching messages guiding users from unapproved services to sanctioned

alternatives and enforces granular policies such as read-only access.

Customizable Views and Reporting
Delivers pre-built reports and enables users to create custom views and reports, schedule periodic email reports, and share with other Skyhigh users.

Activity Drilldown
Provides clickable drilldown to navigate from service-level upload statistics to granular user-level and event level statistics and a complete activity feed for additional context

2. Threat Protection

Cloud SOC
Delivers a security intelligence dashboard and incident-response workflow for potential insider/privileged user threats, compromised accounts, and flight risks.

Cloud Activity Monitoring
Provides a comprehensive audit trail of all user and admin activities to support post-incident investigations and forensics.

User Behavior Analytics
Automatically builds a self-learning model based on multiple heuristics and identifies anomalies indicative of insider threat data exfiltration.

Data Exfiltration Analytics
Leverages machine learning to identify traffic patterns indicative of malware or botnets exfiltrating data from on-premises systems via shadow IT cloud services.

Darknet Intelligence
Identifies stolen credentials leaked from breached cloud services to reveal users and services at risk.

3. Compliance

Sensitive Data Analytics
Provides a detailed and continuous view of sensitive data uploaded to cloud services including the type of content, the user who uploaded it, and the activity type.

Cloud Data Loss Prevention
Enforces DLP policies based on data identifiers, keywords, and regular expressions and supports alerting, blocking, and tombstoning actions.

Purpose-Built Native DLP Engine
Provides a native DLP engine designed specifically for DLP, resulting in greater accuracy and fewer false positives/negatives than third-party engines built for search.

Enterprise-Class Remediation
Provides remediation options that include blocking or tombstoning and enables tiered response based on the severity of the violation.

Policy Violation Management

Offers a unified interface to both review and remediate all DLP and access control policy violations.

4. Data Security

Contextual Access Control

Enables on-premises and mobile access control policies based on user, device, activity, and geography with coarse blocking and granular view, edit, and download permissions.

Digital Rights Management

Defines a circle of trust for any document and enforces rights management policies through integration with DRM solutions.