ESG Lab Review

Bitglass Cloud Access Security Broker

Date: November 2017 **Author:** Tony Palmer, Senior Validation Analyst

Abstract

This ESG Lab Review examines how the Bitglass cloud access security broker (CASB) solution provides access control, data loss prevention, and threat prevention for data that has moved outside the firewall via public cloud applications and bring your own device (BYOD) policies.

The Challenges

In ESG's *2017 IT Spending Intentions Survey*, 39% of respondents identified cybersecurity as a top business initiative that would drive technology spending within their organizations during this year. Respondents also stated that providing employees with mobile devices and applications to maximize productivity (22%) and increasing interaction with customers on their mobile devices (21%) will drive technology spending (see Figure 1).[1] Further, 36% of surveyed organizations indicated that they currently deploy new applications using a cloud-first policy (i.e., using public cloud services unless a compelling case is made to use on-premises resources). 44% consider both public cloud services and on-premises technology when choosing how to deploy new applications.[2]

Figure 1. Top Ten Business Initiatives with the Greatest Impact on IT Spending Decisions in 2017

Source: Enterprise Strategy Group, 2017

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

[2] Source: ESG Brief, *Impact of Cloud-first IT on Enterprise Mobility*, October 2017.

In a world of cloud-based applications and mobile devices, IT must secure data that resides on cloud providers' servers and can be accessed across the Internet from employee-owned devices, whether desktop, laptop, or mobile—managed or unmanaged. Existing security technologies are not well suited to solving this challenge, since they were developed to secure data that resides on company-owned resources within the corporate network perimeter.

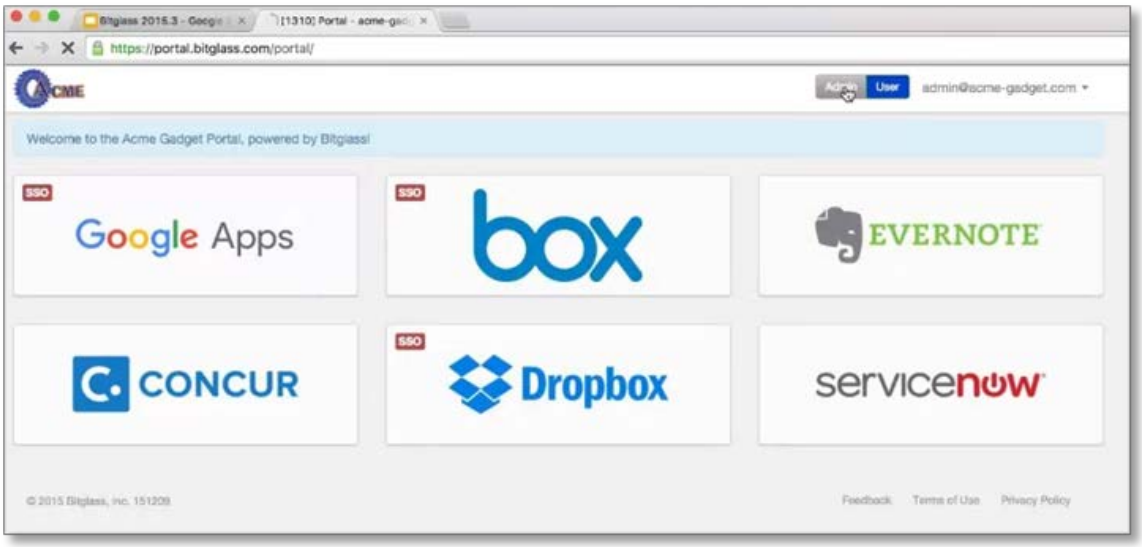
The Solution: Bitglass CASB

Bitglass is a cloud access security broker that aims to provide total data protection. The Bitglass CASB solution operates in the cloud, when users access data in any application, from any device. The Bitglass approach:

- Provides secured access from any device with contextual access control, data leakage prevention, integrated multi-factor authentication, and single sign-on (SSO).
- Uses 256-bit AES encryption to secure data in the cloud while keeping it fully sortable and searchable.
- Secures data on mobile devices and unmanaged BYOD assets without the need for agents or certificate installation.
- Detects anonymizers, malware hosts, command and control (C&C) servers, phishing attacks, and "shadow IT" activities.

With Bitglass, users can securely access any cloud or on-premises application, including productivity suites like Google Apps or Office 365, customer relationship management software like Salesforce, and file sync and share services like Box. As users connect to these corporate applications, they are transparently redirected through a proxy, which controls access, uploads, and downloads. This makes onboarding especially easy, since the users' credentials will always direct them through the proxy, no matter where or which device they connect from, and there is no need for agent or certificate installation on devices. An API connects to the application and controls data at rest in the cloud. Figure 2 displays the window where users connect to their applications, though in most use cases, users bypass this portal and simply interface directly with their applications.

Figure 2. Bitglass Portal for Application End-users

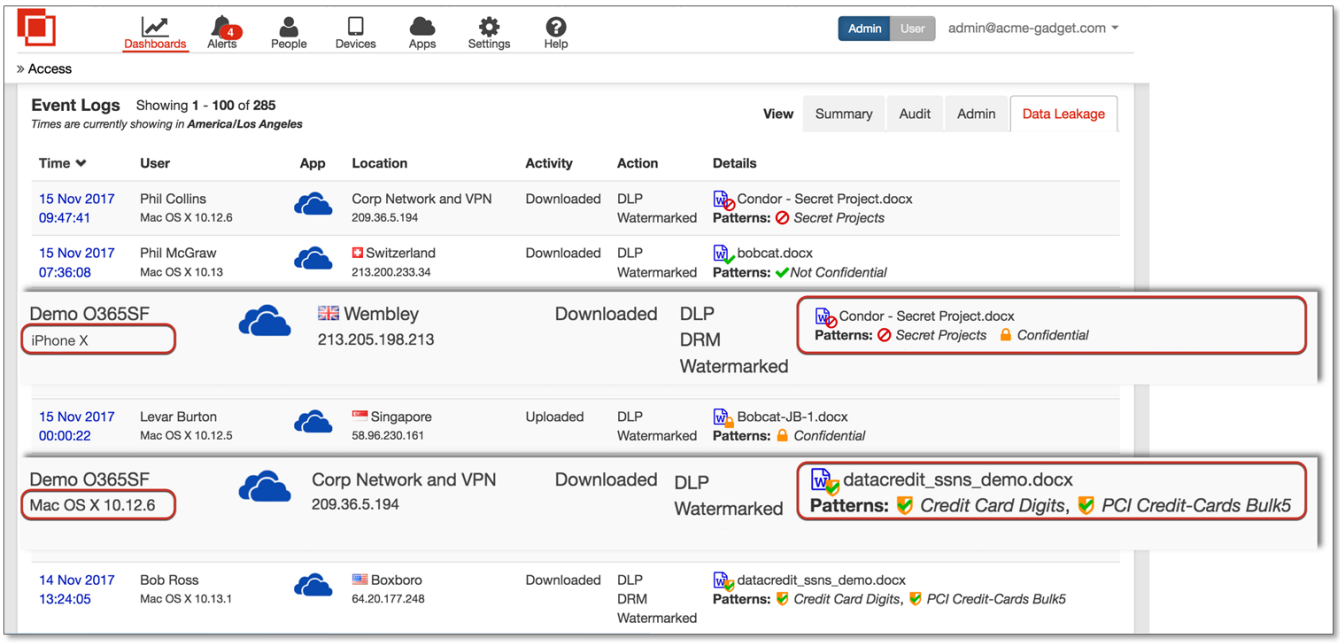


ESG Lab first looked at two aspects of the Bitglass CASB solution: securing access to data and securing data at rest. Each time data is accessed, a complete evaluation of policies occurs and appropriate controls are applied based on the permissions of the user, the attributes of the data, and the device accessing it. Organizations can use this functionality to allow access from a variety of risk contexts, while mitigating that risk with additional data-centric controls.

In the example illustrated in Figure 3, two files with similarly sensitive contents (proprietary intellectual property and credit card data) are being accessed by two different users: one using a managed, company-issued laptop and the other using a personal iPhone. The file being downloaded to the corporate laptop triggers several actions: Prior to download, the file is

watermarked and encrypted, and admins are alerted to a possible data loss event. When a similar file is accessed over Gmail by a user on her personal iPhone, the file is watermarked and admins are alerted, but the confidential information is redacted before the file is downloaded.

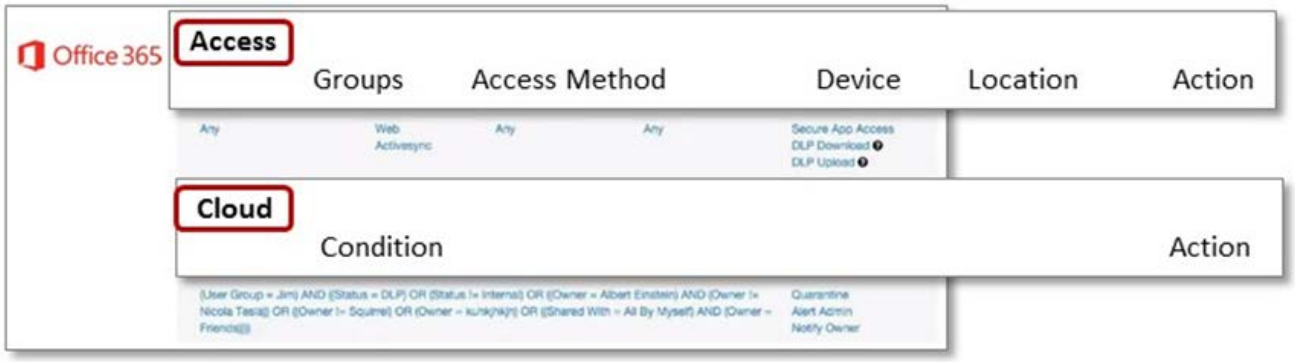
Figure 3. Securing Access to Data Based on Device – Company Issued versus Personal Device



ESG Lab next looked at one of the policies that protect data in transit (Access) and data at rest (Cloud). For each application, access and cloud policies are completely customizable and enable organizations to flexibly define access rules appropriate for their users, their data, their device types, and their access patterns, across multiple applications.

As seen in Figure 4, access to applications and the data associated with them—no matter how complex the application—can be centrally controlled with just two policies. The ***Access*** policy allows administrators to control access by group, method, device, or location and define multiple actions. The ***Cloud*** policy is focused on protection of data at rest and allows for the creation of a set of rules for each application to ensure that data is only stored on devices that are approved and authorized. The rule builder provides a simple and straightforward method for creating policies using prebuilt and custom rules. Amongst other actions, Bitglass can quarantine files when policies are violated, holding them until an administrator can take action.

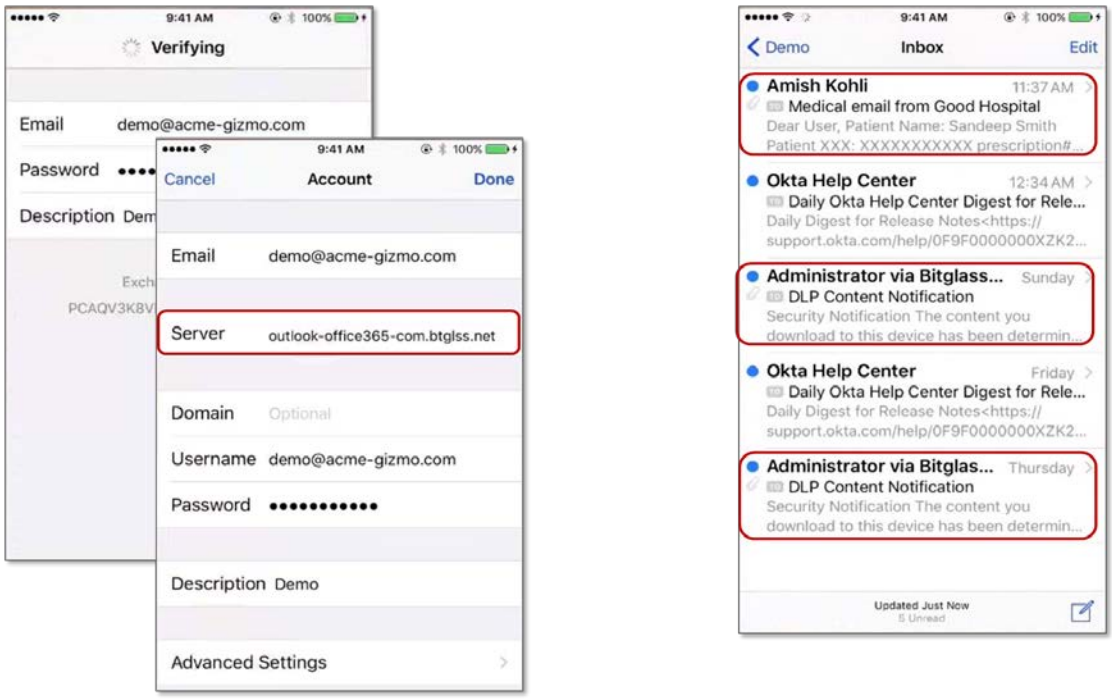
Figure 4. Attributes of "Access" and "Cloud" Policies



Next, ESG Lab looked at the onboarding process for an unmanaged device. In this case, a remote user accesses email through Office 365 from her or his iPhone. As seen in the left graphic of Figure 5, all the user has to do is select Exchange

and enter their login credentials. Data is automatically redirected through the Bitglass proxy and email and attachment downloads are restricted according to policy. The right graphic in Figure 5 shows a number of emails that have triggered actions. The message at the top contains confidential patient data that has been redacted by Bitglass, and the two messages below have triggered DLP notifications, telling the user that the downloaded data contains sensitive information and the organization's IT department may block the download of this content in the future. Finally, ESG Lab looked at remote wipe functionality. When users are permitted to work with unmanaged BYO devices or public cloud applications, the ability to remotely delete data or completely wipe devices is essential.

Figure 5. User Access to Email – Login Process and Redacted Data Notifications



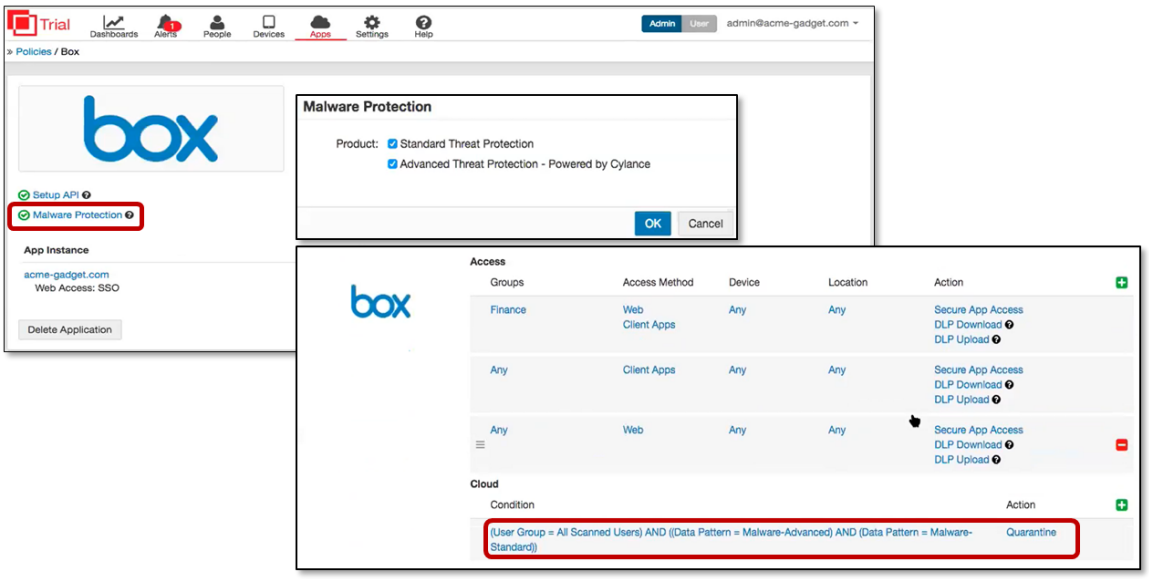
Remote wipe was fast and simple to execute. ESG Lab selected the iPhone from the user's page in the Bitglass admin portal and clicked on the Wipe link next to the device name. The option to selectively wipe corporate data was selected in the pop-up window, and the next time the phone synced with the corporate email service (within a few seconds), all corporate email on the phone was removed and replaced by a message telling the user that the account was blocked on that device. Organizations can also wipe the entire device and perform a factory reset, all with no agent on the device and no mobile device management software required.

ESG Lab then examined how IT administrators can secure custom applications, discover cloud applications in use within an organization, and protect users from malware attacks. IT administrators can add custom applications—e.g., applications that are developed in-house or SaaS applications not specified in the Bitglass application catalog—to the interface displayed in Figure 2. Using the *Any App Configuration* link in the Admin View, the IT administrator can specify the application name and URL so that it appears in the user interface. In addition to defining the "access" and "cloud" policies for custom applications, the administrator can also enable data encryption and key access if desired.

Bitglass also enables IT administrators to protect users against malware. As shown in Figure 6, administrators can click on the ***Malware Protection*** link and choose the ***Standard*** or ***Advanced*** levels of threat protection for known SaaS applications such as Box, Salesforce, and Office 365. Standard Threat Protection is based on hash- and signature-based matching and is included at no additional cost. Bitglass licenses the Advanced Threat Protection feature through Cylance, which bases its threat protection on artificial intelligence and machine learning for new and unknown threats. The IT administrator can then

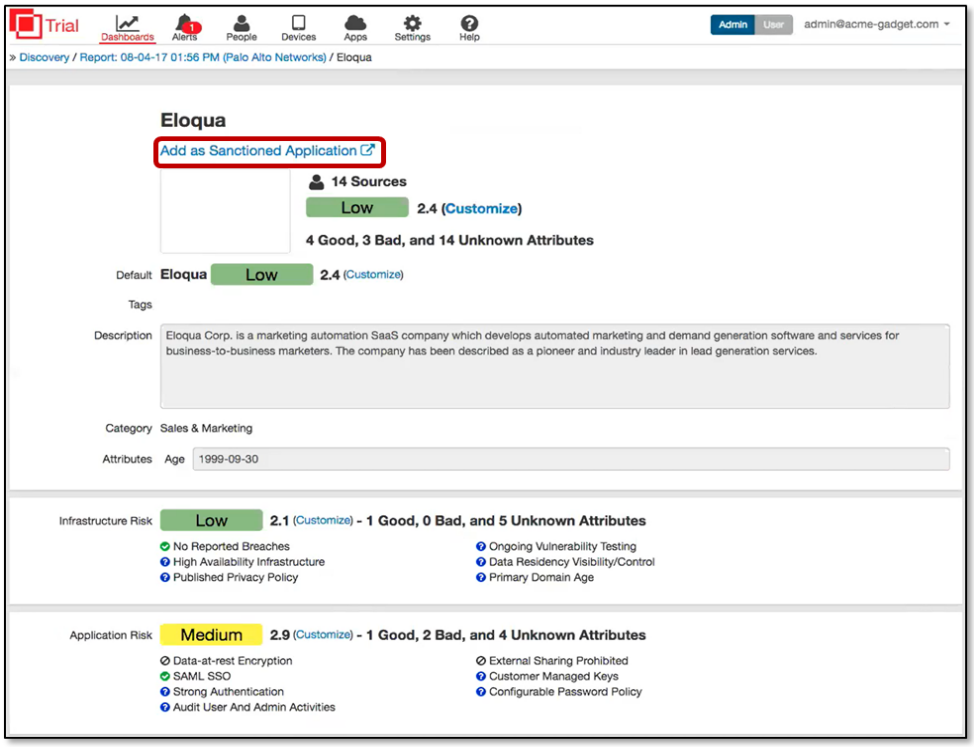
define the actions taken on application data when malware is detected via the "access" and "cloud" policies, such as quarantining data.

Figure 6. Enabling Malware Protection for Known SaaS Applications



SaaS applications that are used within an organization but not approved for corporate-wide use (or "shadow IT") can also be protected. If the administrator deems the application to pose low risk from an infrastructure, application, or compliance risk perspective, the application be added to a Sanctioned Application group such that the CASB enables user access, thus allowing an organization to protect any application. Figure 7 shows the metrics the administrator uses to gauge an application's overall risk profile and the option to *Add as Sanctioned Application*.

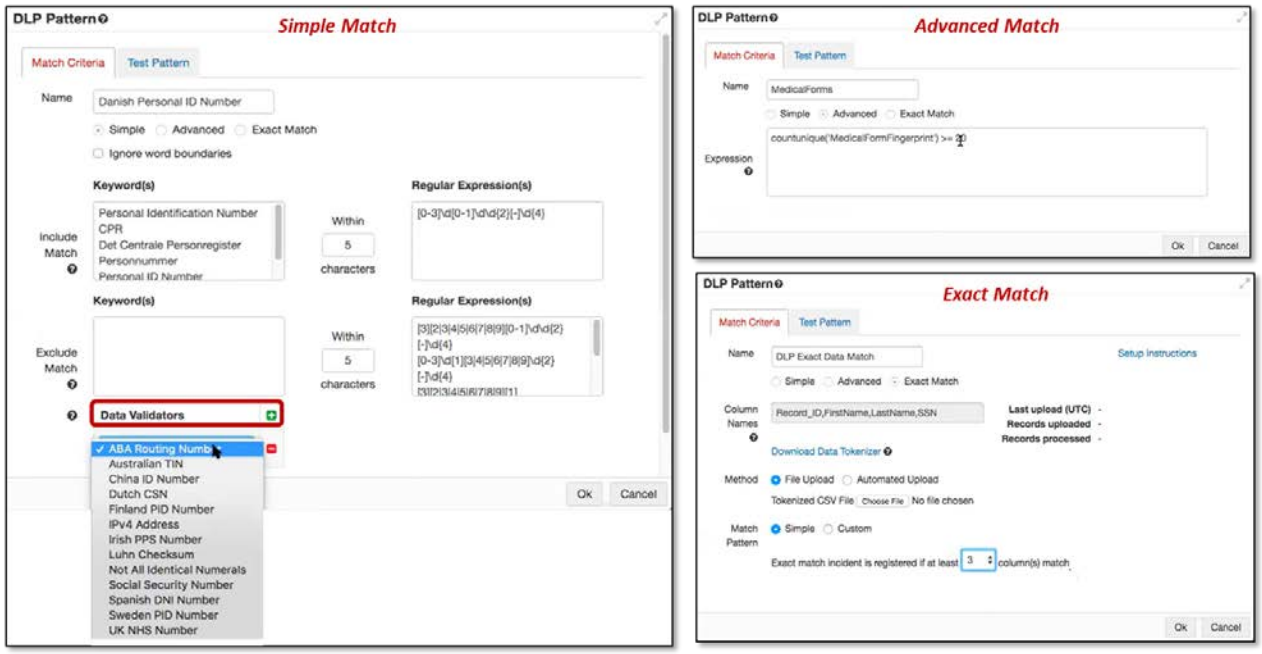
Figure 7. Classifying a "Shadow IT" Application as a Sanctioned Application



Organizations can also control access to unsanctioned applications and direct end-users to use alternative applications already managed by the Bitglass CASB, or simply block access to those applications.

Finally, ESG Lab examined how the Bitglass CASB handles data loss prevention (DLP) via simple, advanced, and exact matches of data patterns. Figure 8 shows how the IT administrator defines these matches.

Figure 8. DLP – Simple, Advanced, and Exact Matching



The simple match consists of comparing data to character string patterns (Regular Expressions). Bitglass' CASB solution allows an IT administrator to ensure that the expressions conform to known patterns via *Data Validators*, such as a bank routing number. The *Advanced Match* will use criteria such as count of document fingerprints in predefined forms (such as medical forms), a step above just matching certain character patterns. Finally, *Exact Match* will employ database files uploaded by the IT administrator. Bitglass offers a "data tokenizer" that anonymizes the uploaded data. The CASB will use the "tokenized" data to scan for exact matches. All three match types allow an organization to define how granular the CASB scans uploaded and downloaded data to prevent unnecessary data loss.

The Bigger Truth

The vast majority of organizations today are either already using applications on public cloud services or have plans to deploy cloud apps. Combined with the increasing use of mobile devices and BYOD for access to potentially sensitive data, this presents a unique challenge to CISOs and IT departments. An effective solution must provide access control, data loss prevention, and threat detection across all devices and all applications. CASB functionality was designed to address all of these issues.

Bitglass is a cloud access security broker whose technologies are designed to operate within and outside of the network perimeter with the ambitious goal of delivering total data protection for the enterprise—for any app, in the data center, in the cloud, on mobile devices, and anywhere on the Internet.

ESG Lab confirmed that Bitglass is doing just that for managed and unmanaged devices, with no agents or certificates required. In our testing, Bitglass provided protection for data at rest in multiple public cloud-based applications, including data loss prevention and suspicious activity alerting. ESG Lab was able to scan and identify data at rest, set up DLP patterns, and set up policies for multiple predefined, custom, and "shadow IT" applications quickly and easily. ESG Lab also looked at mobile access security—onboarding, securing access to and storage of data that users sync to their devices, and remotely wiping a device in seconds.

In ESG Lab's opinion, Bitglass provides a comprehensive CASB solution for an impressively large list of predefined applications and the added flexibility of support for any other custom or unknown application. Bitglass also protects mobile data as well as traditional mobile device management applications without using on-device software or agents. If your organization is currently using or planning to use public cloud applications with or without BYOD and mobile access, ESG Lab recommends taking a very close look at Bitglass.