bitglass for AWS

technical overview

Introduction

AWS is one of the largest public cloud platforms available. Amazon S3 alone stores trillions of objects – that's petabytes of data – much of which is made accessible to other cloud apps. Securing data in an IaaS platform like AWS brings many of the same concerns as protecting data in SaaS apps. Identifying and inventorying stored data, determining the sensitivity of the data, assessing how data can be accessed/moved/replicated/ downloaded/etc, and controlling or mitigating what was found in the prior steps.

For organizations that need to secure AWS, from the Management Console to custom apps built on the platform, Bitglass provides critical protection. By leveraging the same core Cloud Access Security Broker (CASB) capabilities that have proven effective in securing SaaS applications including integrated identity management, robust cloud encryption, and real-time inline data protection, Bitglass enables organization to meet their security and compliance needs when migrating workloads to AWS.

By sitting between cloud apps and devices, Bitglass provides a control point for complete visibility and data protection, operating across all cloud applications, including IaaS platforms like Amazon Web Services, SaaS apps like Salesforce and Office 365, and custom applications. This is all accomplished in an agentless, easy-to-deploy architecture in-use by hundreds of leading organizations across the globe.

Solution Overview

Among the most pertinent AWS security challenges are protecting data-at-rest in S3, EC2 and other services, controlling access to the AWS management console from any endpoint, and securing custom apps that are built on the platform.

In the case of the AWS Management Console, IT needs the ability to identify a risky login and limit access as appropriate. Whether it's spinning up a new VM or deleting an existing instance, unauthorized control over your AWS environment can be costly and devastating. As for data-at-rest in AWS, protecting information as it moves from S3 to data warehouses and other connected apps is essential.

BOLL IT Security Distribution
Jo Walter
Jurastr. 58
Wettingen * State / Province Switzerland
5430

Control Access to the AWS Management Console

Amazon's Management Console is a gateway to all your AWS instances, naturally cause for concern if not secured properly. While AWS natively supports grouping users and attaching permissions to those users, more granular controls can help identify and limit risky access. Without such granular controls, unauthorized or insecure access is all the more likely.

Bitglass offers contextual access controls that go far beyond Amazon's built-in capabilities, ensuring that appropriate access to AWS is provisioned based on the context by which the user is accessing the application. Policies can be defined based on access method (browser or native app), device (managed vs unmanaged), location (by country or IP address range), group, and more.

Data Leakage Prevention, Encryption and Tokenization for Data-at-Rest

For data-at-rest in AWS, encryption, tokenization, and data leakage prevention (DLP) are invaluable, particularly given the volume of data stored in S3 and connected services like RDS. In fact, Gartner estimates S3 holds 1.6 times the data of all other cloud apps combined. To leave that data unsecured and accessible from connected apps is to leave a massive security gap unaddressed.

Bitglass' integrated, high-performance DLP, part of the Citadel data protection engine, is built to be at parity or better than leading network and endpoint-based DLP systems. Paired with a comprehensive catalog of pre-built identifiers for a wide range of data types, you'll have the flexibility to build policies from scratch, pull from the Bitglass catalog, import policies from premises-based DLP solutions, or integrate via ICAP, to readily identify sensitive content in S3.

Enterprises around the globe use Bitglass' resilient cloud encryption and DLP to protect data across both SaaS applications and IaaS platforms like AWS.

Secure Custom Apps

Bitglass also secures custom apps built on the AWS platform that access your sensitive data. Whether it's a data visualization app like Tableau or any custom or third party application, Bitglass can provide real-time control and protection - whether you've deployed apps in production or for test and development.

Bitglass' contextual access controls, identity, and DLP extend to custom apps. Contextual access control ensures that appropriate accesses to custom AWS apps are provisioned based on the context by which the user is accessing the application.

Identity

Bitglass is the only CASB to offer built-in IDaaS service capabilities that extend to custom apps on AWS, allowing you to consolidate your entire cloud security strategy into a single platform. Built-in capabilities include single sign-on for protected apps that support single sign-on (SSO), Active Directory synchronization and authentication, SCIM support, SMS and email multi-factor authentication. Bitglass also integrates seamlessly with any identity management system, including Ping, Okta, OneLogin, and ADFS. Bitglass dual SAML termination ensures that the strength of SAML SSO is preserved, without the added phishing risk that comes with some proxy architectures.

Whether you use the Bitglass IDaaS or integrate with another system, Bitglass can enforce step-up authentication at any time, based on suspicious activities. For example, if a user logs in simultaneously from two different locations, Bitglass can force a re-authentication, requiring multiple factors.

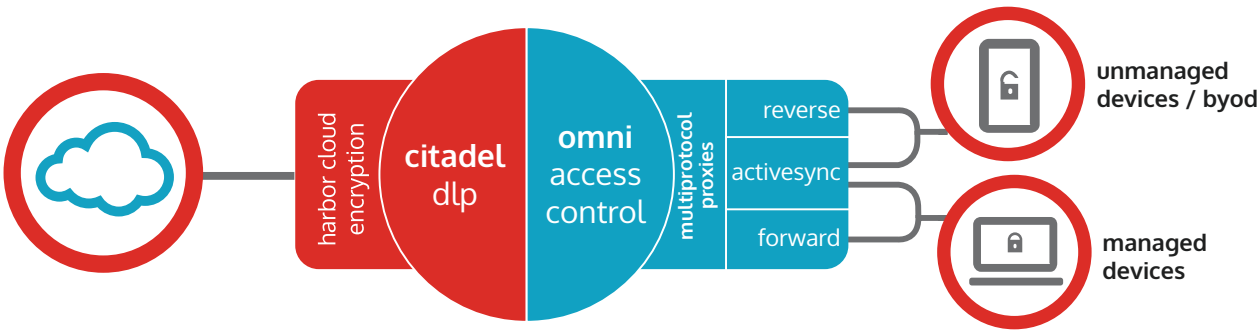
Architecture Overview

Whether a user needs to access the AWS Management Console or any custom app built on the platform that has access to sensitive data, real-time protection is critical. Only a hybrid CASB approach, leveraging both APIs and inline proxies, can ensure total data protection.

Bitglass' approach is powered by its Omni multi-protocol proxies, enabling secure data access for both managed and unmanaged devices in an easy-to-deploy agentless model. Omni's reverse proxy enables secure data access from any device, without requiring any agents or certificates, and with no changes to the user experience.

Omni's reverse proxy is uniquely resilient, powered by Bitglass' proprietary AJAX-VM technology. Designed to proxy any enterprise cloud application, AJAX-VM works in any web browser, without additional software. Unlike traditional reverse proxies, which break dynamic client-side functions, the AJAX-VM rewrites links in static server-delivered content, while also automatically wrapping browser-executed code. This allows it to intermediate and secure data in all transactions initiated by the app on the client side.

Bitglass' proxies are paired with API integration into AWS, offering visibility and control for both data-in-transit and data-at-rest.



Deployment

Bitglass' multi-protocol proxies can be deployed in minutes, without the pain that comes with traditional agent-based solutions. Setup is simple and straightforward, with nothing to install for either admins or users.

The Bitglass cloud service is hosted globally on AWS infrastructure with auto-scaling and replication. Its fully redundant architecture ensures constant uptime – Bitglass guarantees a 99.9% SLA, and greater than 99.99% historical performance. The global load-balancing of Bitglass' security application results in no perceptible latency for end users.