bitglass for Office 365

technical overview

Introduction

Microsoft's Office 365 has quickly become one of the most popular enterprise cloud apps - the primary email and productivity suite for thousands of enterprises. Deploying Office 365, however, doesn't mean turning a blind eye to security and compliance. In fact, even in a trusted public cloud application like Office 365, the responsibility to protect corporate data falls squarely on IT, not on the app vendor. Your organization needs a solution that can protect data in Office 365, and across your public cloud portfolio, end-to-end. You need a Cloud Access Security Broker (CASB).

While Microsoft goes to great lengths to secure its application and infrastructure against intrusions and attacks, a large security gap exists around corporate data. Traditional security systems like secure web gateways, firewalls, and premises-based DLP solutions are powerless as data moves beyond the firewall to public cloud apps. What's more, data protection capabilities built into apps like Office are limited and single app in nature, make them poorly suited for most enterprises.

Bitglass enables IT to secure sensitive data as it moves beyond the firewall. By sitting between applications and devices, the Bitglass CASB provides a control point for complete visibility and data protection. The solution operates across all cloud applications, including SaaS apps like Salesforce, Slack and Office 365, IaaS platforms like Amazon Web Services, and custom applications, whether deployed internally or in the cloud. This is all accomplished in an agentless, easy-to-deploy architecture used by 100s of leading organizations across the globe.

Solution Overview

Only Bitglass provides comprehensive, real-time data protection from any device - for Office 365, as well as your organization's entire suite of cloud applications. Whether you want to encrypt data prior to upload, control data leakage, gain insights into suspicious user activity, or all of the above, Bitglass' market-leading data protection technologies provide the control you need.

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

Data Leakage Prevention

Bitglass' integrated, high-performance DLP 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. Most organizations choose to sync policies directly from premises-based DLP systems, avoiding severe performance penalties while ensuring consistent policy enforcement anywhere.

The Citadel DLP engine is paired with a wide range of remediation actions, built to allow you to safely extend access to sensitive data, even in risky contexts. Actions include dynamic application of encryption or rights management (DRM), redaction of sensitive content, watermarking and tracking, quarantine, share removal, and blocking.

Contextual Access Control

Contextual Access Control ensures that appropriate access to Office 365 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.

Administrators can choose to block, allow, or provide intermediate levels of access to Office by pairing access control policies with DLP policies.

Malware and APT Protection

As Office increases in popularity, its attractiveness to bad actors increases, making it a more popular delivery vehicle for malware. Bitglass' anti-malware and Advanced Threat Protection (ATP) powered by Cylance, incorporate the best of both signature/heuristic anti-malware scanning from more than 60 leading vendors to identify known malware, with ATP to stop the spread of unknown and zero day attacks, ensuring that your Office 365 deployment never becomes a proliferation point for the spread of malware across your managed or BYO devices.

User Behavior Analytics

Through the combination of API and proxy-based control over Office 365 access, Bitglass provides full visibility into every transaction conducted in Office 365. User behavior analytics, focused on suspicious activity detection, are built on that visibility and reported via alerts, dashboards, and SIEM integration.

Moreover, Bitglass provides cross-app visibility, empowering you to discover suspicious and abnormal behavior. If a user accesses Slack from LA, and then an hour later tries to access Office 365 from NYC, Bitglass can flag and prevent that login.

Identity

Bitglass is the only CASB to offer built-in IDaaS service capabilities, allowing you to consolidate your entire cloud security strategy into a single platform. Built-in capabilities include single sign-on for both protected apps, as well as any application that supports SAML for 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, ADFS, and more. 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.

Cloud Encryption

Harbor Cloud Encryption is the only offering on the market that leverages full-strength, 256-bit FIPS-compliant encryption with 256-bit initialization vectors, supporting both field-level encryption, for apps like Salesforce and file-level encryption, for any cloud application, including OneDrive and Sharepoint. The unique, patented technology preserves application functionality such as search and sort, simultaneously providing data protection and an unchanged user experience. The system integrates with a wide variety of key management systems via KMIP, in addition to the native key management option which is based on Amazon's CloudHSM.

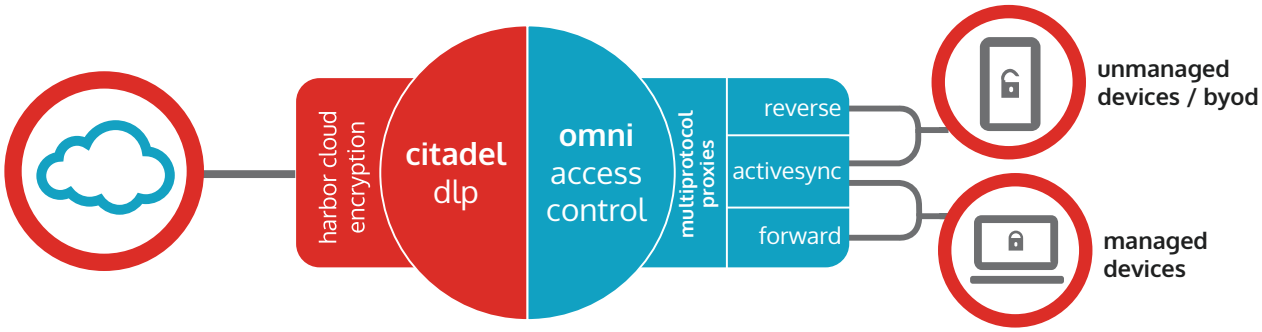
Architecture Overview

When it comes to securing data in the public cloud, real-time data protection is a necessity. Many CASB solutions rely solely upon API-based scans for data protection, leaving gaping security holes: API notification systems can take tens of minutes, if not more, to inform a CASB of sensitive data upload or download. In practice, this means that a data policy violation might occur – a user downloading customer PII to their personal laptop – and that violation might not be detected until it's too late. 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 rich SaaS applications, 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 with Office 365. API integration allows for visibility and control of data-at-rest, including discovery of sensitive data and application of Harbor Cloud Encryption to pre-existing data in Office 365.



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.