thalesgroup.com

THALES

Compliance-Ready Security for Cloud Services:

Bitglass and Thales KeySecure

Introduction

Cloud service adoption gives rise to new cybersecurity concerns in the enterprise. Organizations using the cloud are entrusting their data to someone else's data center. Regardless of any service agreement, it is the organization using the cloud service that remains responsible for protection of their data, regardless of where it is stored. While some cloud services offer encryption and key management functionality to mitigate these concerns, many find this functionality to be insufficient. As encryption keys are stored with the same provider holding the encrypted data, questions persist over data security and ownership, making demonstrating regulatory compliance difficult. Additionally, per application encryption does not extend beyond the boundary of that application to other "connected" applications. Fortunately, the Bitglass and Thales joint solution addresses these security and compliance concerns, providing the flexibility and the benefits that hosting data in the public cloud has to offer with the security and control of a premises data center.

Solution

Bitglass Cloud Encryption encrypts data with FIPS-compliant 256-bit AES keys before it is uploaded to the cloud service – all while maintaining normal app functionality. Thales's Thales KeySecure integrates with Bitglass to securely store and manage encryption keys and associated policies, separate from the environment where the data is stored, so that organizations can protect data and demonstrate regulatory compliance, all while maintaining sole visibility and control over their data.

bitglass Next-Gen CASB

Benefits

Help Meet Compliance and Regulatory Obligations

- Separate encryption keys from encrypted data to follow best practice and meet regulatory obligations
- Efficiently audit key management practices, and save staff time. Supports centralized auditing of key management practices such as FIPS 140-2, PCI-DSS, HIPAA, and GDPR.

Access Controls and Policy Enforcement

- Centrally control encryption keys for stronger oversight, more robust security and greater scalability
- Set granular access controls to tailor data access according to job roles and responsibilities
- Define and enforce policies to guard against unauthorized and rogue access to, and exposure of, high value data

Data Shredding

- Encrypt data and delete the key to ensure it is cryptographically erased in cloud environments. Cryptographically shred your data to comply mandates, such as HIPAA and PCI DSS.

Bitglass' Next-Gen Cloud Access Security Broker (CASB)

With support for software-as-a-service apps like Salesforce and Office 365 as well as custom applications and infrastructure-as-a-service platforms like AWS, Bitglass is built to protect data end to end across the entire enterprise cloud footprint. In addition to operations preserving encryption for both structured and unstructured data, Bitglass allows organizations to monitor data at rest in the cloud, take action on sensitive content with DLP, and achieve regulatory compliance. Bitglass' multi-protocol proxies provide real-time security wherever data goes. Forward, reverse, and ActiveSync proxies are used to secure corporate, personal, and mobile devices, respectively. Only Bitglass provides encryption built for the cloud, granular data protection capabilities, robust identity management, comprehensive visibility, and zero-day threat protection – all without agents.

Bitglass Features

Cloud Encryption

Bitglass provides FIPS-compliant, 256-bit AES encryption with 256-bit initialization vectors, meeting the highest standards of encryption strength. Sensitive data can be detected and encrypted automatically—whether it's at rest in the cloud or being uploaded to an app. Uniquely, this full-strength encryption for files and fields does not compromise critical functionality such as search and sort. Bitglass Cloud Encryption is secure, user friendly, requires no software installations on endpoints, and integrates with Thales so that organizations can take full control of their encryption keys.

Data Protection

Bitglass' CASB provides granular, context-aware data protection capabilities like contextual access control and data loss prevention (DLP). As such, varied levels of data access can be extended to individuals based on their job function, device type, geographical location, and more. Easily configured, automated policies can decrypt encrypted data in real time as authorized users attempt to access it from any device.

Visibility

From a single dashboard, Bitglass provides the enterprise with insightful analytics and complete visibility over its data. Activity logs detail all app, user, and file activity. This allows organizations to enable audit, demonstrate regulatory compliance, and see that their data is being accessed securely.

Thales' KeySecure

Thales KeySecure is an encryption and key management appliance (available in hardware or virtual options) that centralizes the control of an enterprise's encryption solutions, and streamlines ongoing key and policy administration for encrypted data in the cloud, on application servers, databases, and file servers. Centralized key management improves security by making key surveillance, rotation, and deletion easier while also separating duties so that no single administrator is responsible for the entire environment. Additionally, unifying and centralizing policy management, logging, and auditing makes information more readily accessible and simplifies demonstrating compliance with data governance requirements.

Features

Centralized Key Management

Thales KeySecure provides customers with control of their cloud-based data by securing Bitglass' keys, and facilitates on-going management by centralizing those keys along with the keys from a range of third-party encryption solutions. Supporting such a broad ecosystem improves security by ensuring uniform policy enforcement, and reduces the amount of time, effort, and investment administrators must make to manage security in their enterprise.

Auditing and Logging

Thales KeySecure's management functionality includes detailed logging and audit tracking of all key state changes, administrator access, and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading third-party SIEM tools.

Separation of Duties

Thales KeySecure supports segmented key ownership and management based on individuals or group owners. Separating administrative duties is an important security best practice that protects data from privileged users and facilitates regulatory compliance. Thales KeySecure's access controls restrict access to encryption keys which in turn can determine data access according to job roles and responsibilities.

Maximum Key Security

Thales KeySecure is available in a FIPS 140-2 Level 1 algorithm-safe and Level 3 tamper-proof hardware appliance. Additionally, Thales KeySecure is available as a virtual hardware appliance supported by Thales Luna HSMs (optionally available as a FIPS 140-2 Level 3 appliance) for hardware key storage.

High-Availability Configurations

Organizations can cluster multiple Thales KeySecure appliances to maintain the availability of encrypted data. For large organizations with global footprints, administrators can cluster across geographically dispersed data centers to address their worldwide reach.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com