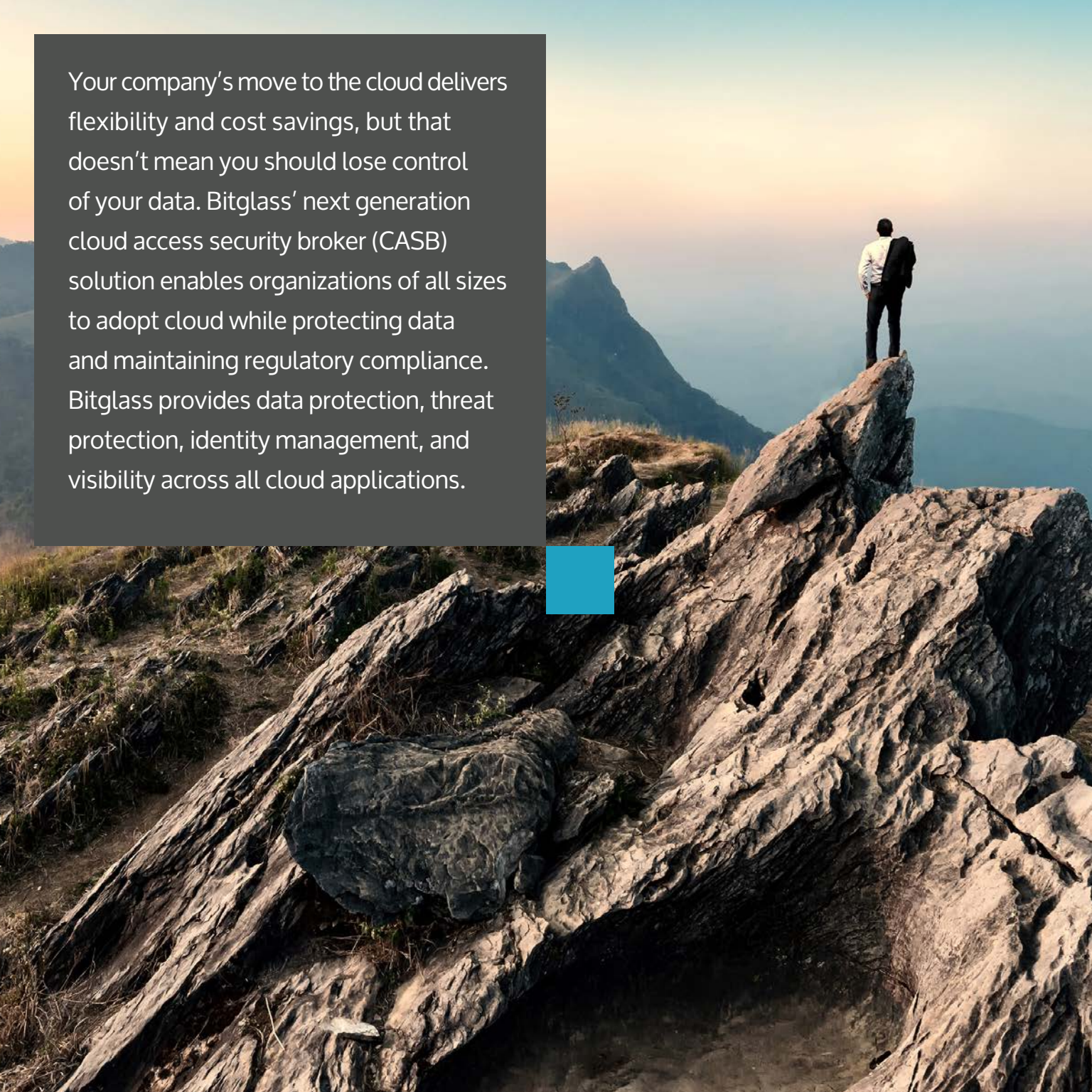
Cloud Security

Solution Brief

bitglass



Your company's move to the cloud delivers flexibility and cost savings, but that doesn't mean you should lose control of your data. Bitglass' next generation cloud access security broker (CASB) solution enables organizations of all sizes to adopt cloud while protecting data and maintaining regulatory compliance. Bitglass provides data protection, threat protection, identity management, and visibility across all cloud applications.

Cloud providers go to great lengths to maintain the security of their applications and infrastructure, but it is your responsibility to secure how that data is used and by whom. The top concerns for healthcare firms moving to the public cloud center around visibility, control, and compliance.

IT teams often struggle with questions like: what data is in the cloud and how are employees using it? How do we prevent users from downloading protected health information (PHI) to unmanaged devices or sharing it outside of the company? How do we stay compliant with HIPAA and other regulatory mandates that govern healthcare firms and affiliates?

Cloud Security Challenges

Managed and Unmanaged Device Access

Different devices carry different risks. Where employees are able to access corporate data on corporate and personal devices, organizations must take steps to protect that data before it's downloaded to the endpoint. Even unmanaged devices, where agents can't be installed, must be secured.

Sensitive Data within Cloud Applications

Sensitive data will inevitably find its way into cloud applications. Risky actions—external sharing of regulated data for example—can expose an organization to liability and loss.

External Threats

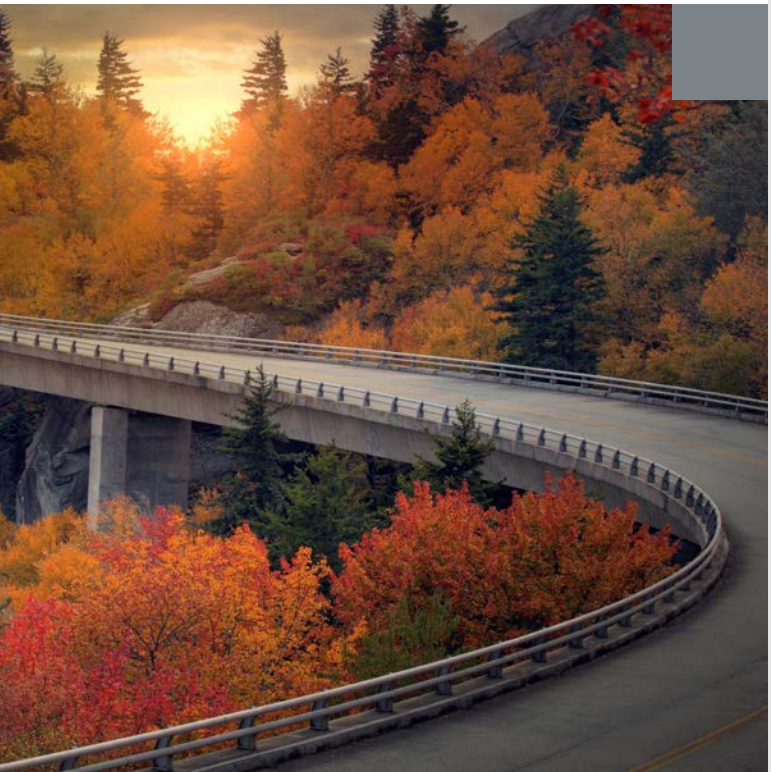
Malware and ransomware are rampant across cloud applications and on the web. Organizations need the ability to detect and remediate these threats so that endpoints aren't infected and so that data remains secure.

Suspicious Activity

Stolen credentials are the number one cause of data theft. Enforcing secure authentication, detecting suspicious activity, and limiting the impact of a breach are all critical capabilities for any organization.

Key Features:

Data Protection



Prevent Data Loss

Bitglass' DLP solution enables a customizable, fine-grained approach to data security, protecting information based on its content and the context in which it's being accessed. Use Bitglass' prebuilt data patterns, build your own, or import from on-premises DLP systems via ICAP for more granular policies.

Protect Mobile

Where mobile devices are widely used, organizations must consider mobile security when choosing a solution to protect cloud data. Bitglass' agentless proxies enable data security for any app on any mobile device without sacrificing user privacy. Enforce device-level security policies, selectively wipe mobile data, and more.

Access Control

Contextual access control governs where and how employees can access corporate data. Granular policies can be defined based on access method, device, location, and more. Organizations can block, allow, or provide intermediate levels of access based on a user's access context.

Encrypt Cloud Data

For organizations where the integrity of data is of the highest importance, Bitglass Cloud Encryption enables encryption of data-at-rest. Bitglass provides full-strength FIPS-compliant 256-bit AES encryption, while maintaining normal app functionality—a dual system of control that dramatically increases the safety of data in the cloud.

Key Features:

Threat Protection

Dynamically Remediate Threats with ATP

Only Bitglass' Advanced Threat Protection, powered by Cylance machine learning, is able to identify both known and unknown malware in real-time. By analyzing hundreds of file characteristics, the system can detect and stop zero-day threats at upload and on download.

User and Entity Behavior Analytics

With user and entity behavior analytics (UEBA), Bitglass can generate baselines for user behavior in order to detect and respond to unusual activity in real time. In the event of compromised credentials and account hijacking, UEBA is a must for distinguishing legitimate data access from malicious data access.

Key Features:

Identity

Manage Identity Seamlessly

Ensuring proper control over identity is essential in protecting data in the cloud. Bitglass has a native IAM system, complete with adaptive step-up multi-factor authentication. Bitglass also integrates with Active Directory and all major IDaaS solutions. Bitglass dual-SAML termination ensures that the strength of SAML SSO is preserved, without the added phishing risk that comes with some proxy architectures.

Step-Up Multi-Factor Authentication

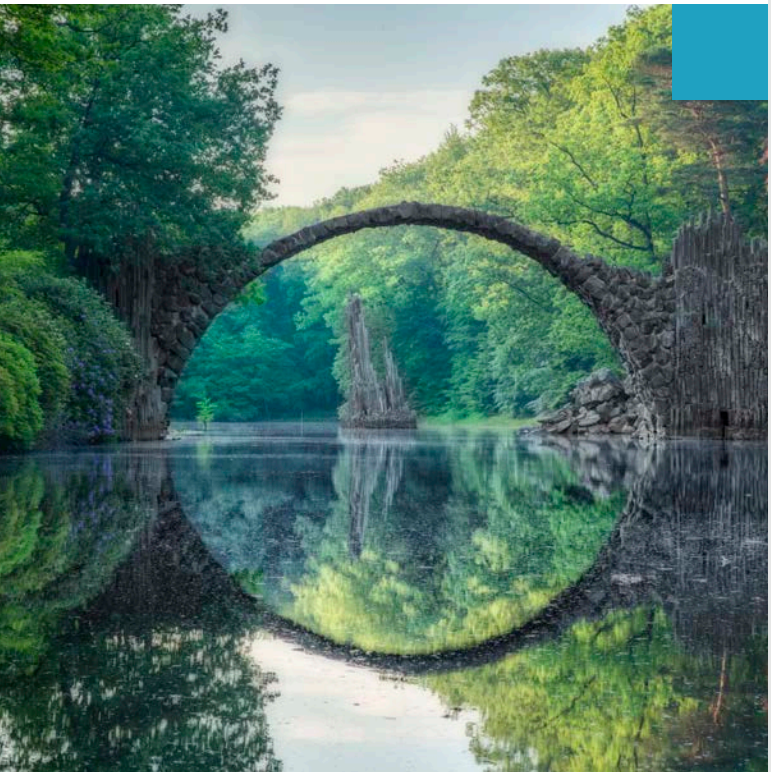
Bitglass offers multi-factor authentication (MFA) to verify users' identities. Authentication methods include passwords, SMS tokens, hardware tokens, and more. In the event of a suspicious login, MFA can be used in a step-up fashion, requiring users to provide additional authentication to access corporate data.

Session Management

Bitglass offers session management to defend against account hijacking. If a user is inactive for an extended period of time, Bitglass can force a timeout or require reauthentication to prevent malicious parties from accessing any cloud app session.

Key Features:

Visibility



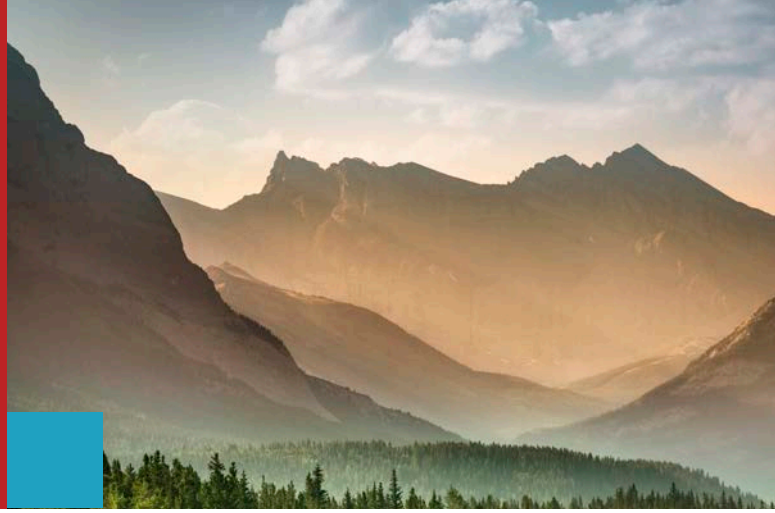
Gain Mission-Critical Visibility and Analytics

Bitglass gives you a single-pane, cross-app view into the details of employees' cloud usage. Uncover and automatically address potential threats via configurable actions, such as step-up multi-factor authentication.

Unsanctioned Shadow IT Applications

Bitglass utilizes big data analytics and risk intelligence to discover Shadow IT applications, automatically categorize those apps, and rate apps based on risk. Leverage Bitglass unmanaged app controls to block these apps or encourage use of alternative sanctioned applications.

Bitglass Architecture



Data-at-rest Protection

Bitglass leverages APIs for additional visibility and control over data stored in cloud apps. Within any app that provides access via an API, Bitglass crawls files to identify sensitive data and threats. This informs the placement of controls around data so that organizations can govern sharing and access more effectively.

Data-in-transit Protection

Bitglass uses a combination of reverse, forward, and ActiveSync proxies to protect data-in-transit. Reverse and ActiveSync proxies are an agentless means of securing access to any cloud app from any device or network. Forward proxies can secure traffic from managed devices, detect shadow IT, block risky unsanctioned applications, and redirect users to safe, sanctioned apps.

Intelligent Zero-day Protection

Only Bitglass features AI-based Zero-day detection and app protection. A combination of intelligent Shadow IT discovery capabilities and unmanaged app controls enable Bitglass to prevent data loss from any application, including previously unknown apps. The Zero-day engine automatically detects new upload paths in known and unknown apps to immediately restrict the upload of sensitive regulated data.

One Security Policy for your Entire Cloud App Suite

As organizations adopt a cloud-first approach to IT, they must also avoid a patchwork of point solutions that can't provide cross-app controls. Bitglass' CASB solution is built from the ground up for visibility, control, and compliance in the cloud. Secure data across managed and unmanaged Shadow IT apps all with one solution.

Rapid Deployment

Bitglass' agentless proxies can be deployed in minutes—setup is simple and straightforward, with nothing to install for either admins or users. Bitglass is hosted globally on elastic AWS infrastructure, making it highly scalable.

Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver data and threat protection for any app, any device, anywhere. **For more information, visit www.bitglass.com**

bitglass