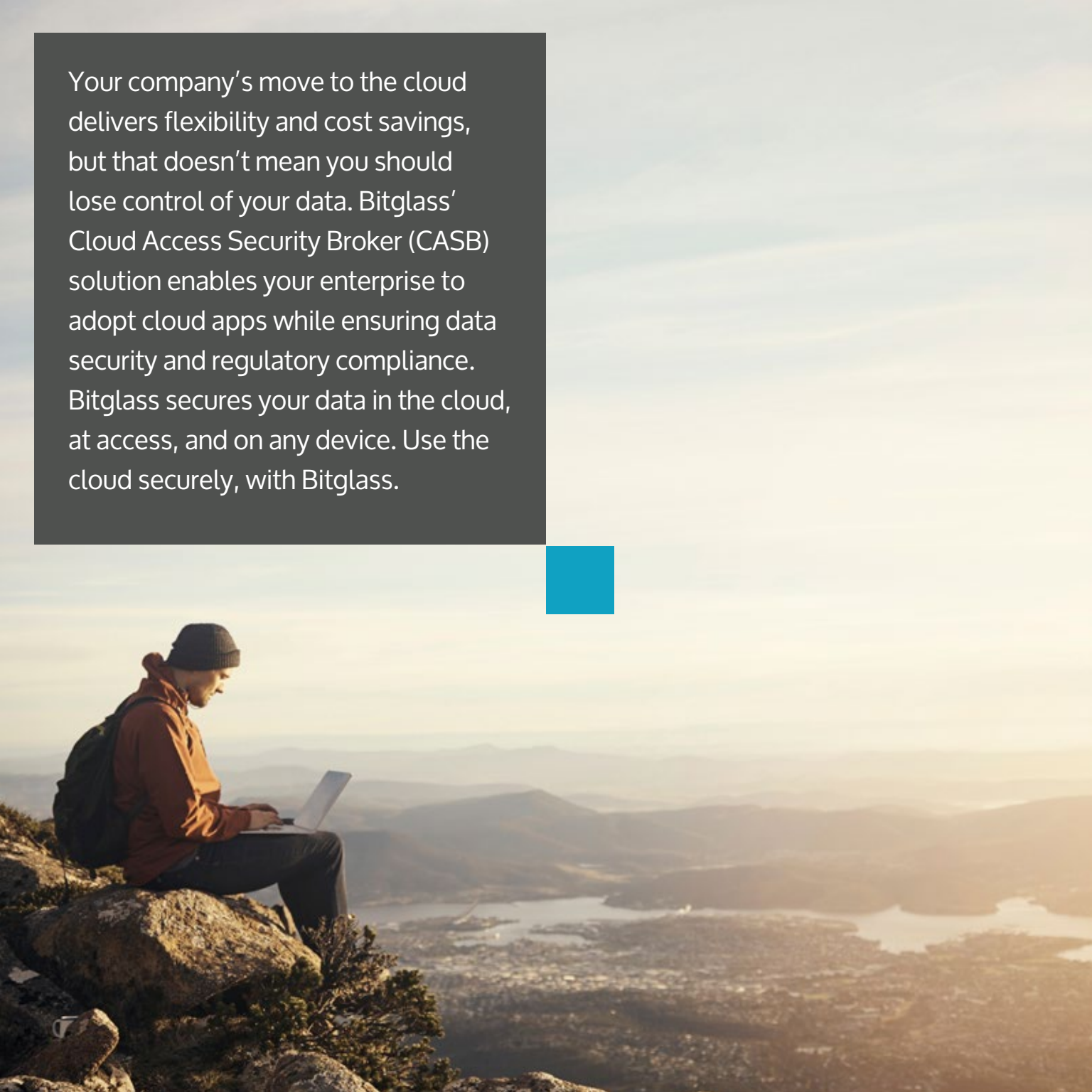
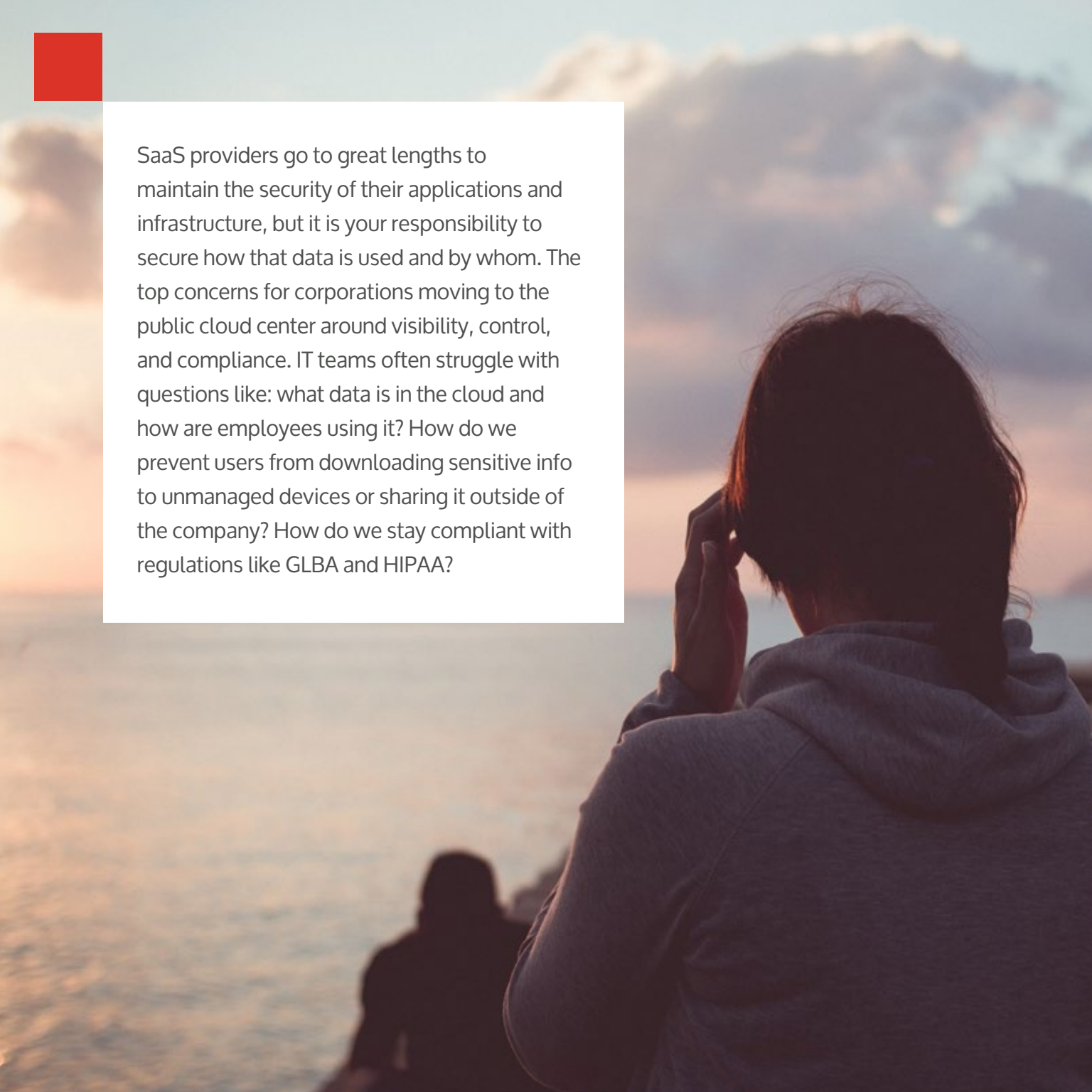
cloud security
solution brief

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' Cloud Access Security Broker (CASB) solution enables your enterprise to adopt cloud apps while ensuring data security and regulatory compliance. Bitglass secures your data in the cloud, at access, and on any device. Use the cloud securely, with Bitglass.





SaaS 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 corporations 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 sensitive info to unmanaged devices or sharing it outside of the company? How do we stay compliant with regulations like GLBA and HIPAA?

bitglass enable enterprises to:

Protect corporate data on managed and unmanaged devices

Enterprises must enable employees to use cloud apps on a range of devices, both corporate and personal, while simultaneously securing sensitive data. Secure SaaS usage requires contextual control of data access from any device, even unmanaged devices where agents can't be deployed. Enterprises also need the ability to selectively wipe data from lost, stolen, or deprovisioned devices.

Secure sensitive data within SaaS applications

Sensitive data will inevitably find its way into cloud applications. Enterprises must be able to take action on risky activities, such as external sharing of regulated data, while also protecting against cloud breach risk by encrypting data-at-rest.

Detect and respond to suspicious activity

Stolen credentials are the number one cause of data theft. A security solution should detect and block anomalous user behaviors, such as a hacker (or even a rogue privileged user) logging in from new devices or locations, or attempting to download unusually large amounts of data from a cloud app. Effective cloud security requires cross-cloud visibility and real-time response to these situations and more.

Uncover hidden Shadow IT threats

It's often a mystery to CIOs what SaaS apps are being used by employees. Enterprises need to be able to discover and assess threats on their networks from shadow IT cloud app usage, malware, anonymizers, and more.

key features

Secure data in real-time

When it comes to securing data in the 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.

Dynamically remediate threats

Bitglass' Citadel DLP enables a customizable, fine-grained approach to data security, protecting data based on its content and the context in which it's being accessed. For example, you might allow employees to fully access a spreadsheet containing customer PII on their work laptops, but redact that PII when the same document is downloaded to their BYO devices. You can either import from your premises DLP system or create your own with Bitglass' extensive policy library. Prevent data leaks, don't just detect them, while fully supporting user mobility and productivity.

Gain mission critical visibility and analytics

Bitglass gives you a single-pane, cross-app view into the details of your employees' cloud usage. Uncover and automatically address potential threats via configurable actions, such as step-up multifactor authentication. Customizable alerts allow for instant visibility of emerging threats. Bitglass integrates with popular SIEMs to consolidate security awareness.

Protect data on unmanaged devices

For better or worse, cloud apps allow data to easily travel to a multitude of devices, making mobile security an inseparable part of the cloud data security puzzle. Bitglass' Omni multi-protocol proxies enable agentless data security for any app on any device and allow IT administrators to enforce corporate device security policies. Bitglass AJAX-VM technology enables proxying of even the richest applications such as Salesforce Lightning and Office Online without the need for agent software.

key features

Control your own encryption

For organizations where the integrity of data security is of the highest importance, trusting a cloud provider to protect data simply is out of the question. Bitglass' Harbor Cloud Encryption enables enterprises to encrypt data within SaaS apps and control their own encryption keys, managed via either Bitglass or an external KMS. Harbor provides full-strength FIPS-compliant 256-bit AES encryption, while maintaining normal app functionality. Establishing this dual system of control dramatically increases the safety of data in the cloud, without compromising application experience for end users.

Manage identity seamlessly

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

Detect unsanctioned cloud app threats

Bitglass' Discovery solution enables IT to discover and assess risky activity on employee networks, including shadow IT, malware, anonymizers, and more. Discovery utilizes big data analytics and several proprietary risk intelligence databases to automatically categorize and rate threats. Machine learning enables Discovery to adapt to your threat environment and improve its risk assessments over time.

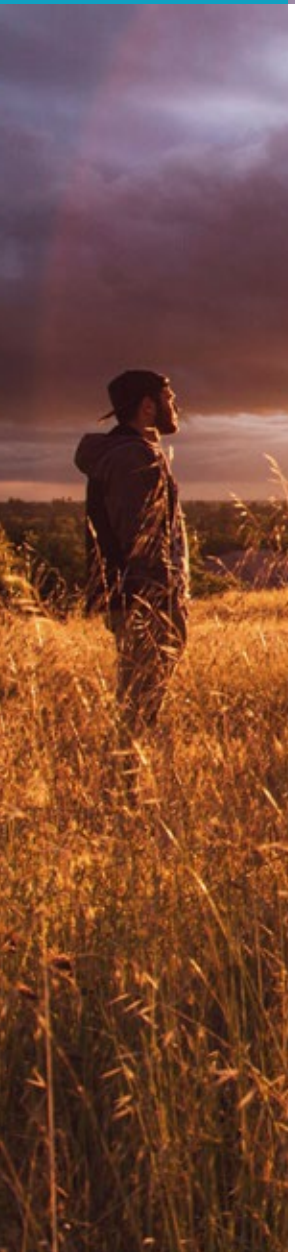
Build one security policy for your entire cloud app suite

As enterprises move toward a more flexible and agile cloud-first future, their security needs to keep up with the times. Bitglass' CASB solution enables you to be prepared for that eventuality. Avoid a patchwork of point solutions, and deploy one set of security policies across your entire cloud app suite. Make your security future-proof.

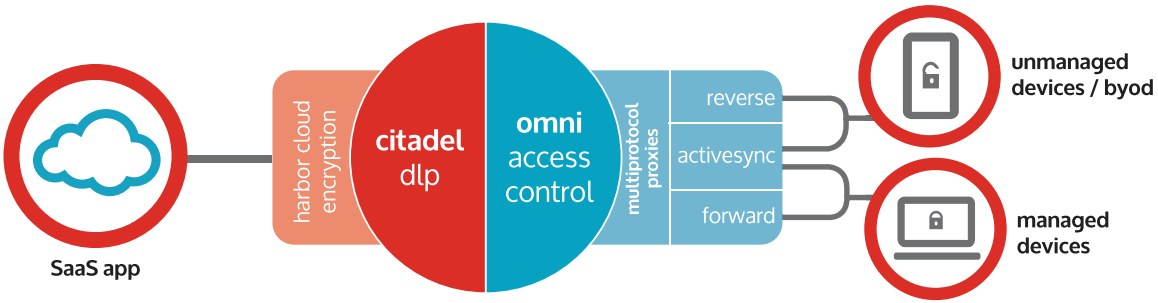
Rapid deployment

Bitglass' multi-protocol proxy can be deployed in minutes, without the pain that comes with traditional agent-based CASB or MDM solutions. 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 technology



At the core of Bitglass' CASB solution are three unparalleled technologies:



Citadel Data Protection

Citadel is a native, high performance DLP engine, that functions bidirectionally. It allows you sync policies with your existing DLP system, or choose from a library of prebuilt ones to detect and remediate sensitive data like PHI and PII. Citadel provides dynamic remediation options, from redaction and encryption to blocking.

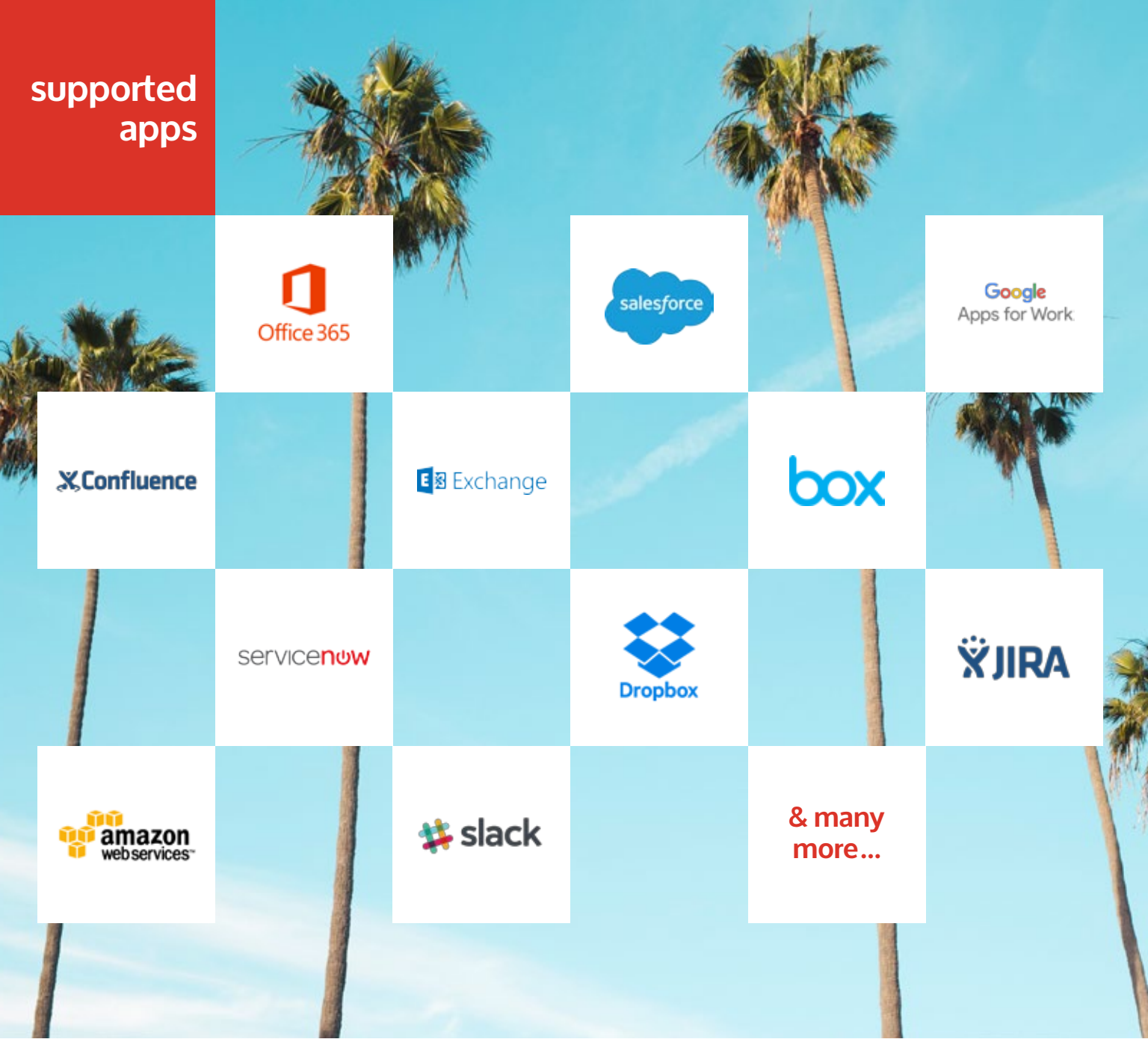
Omni Multiprotocol Proxies and Access Control

Omni enables dynamic access control and consistent data protection across a multitude of devices without additional software. Omni's Activesync proxy protects data traveling to both managed and unmanaged mobile devices. Omni's reverse proxy enables secure data access from any web browser, without requiring any agents or certificates. Powered by Bitglass' proprietary AJAX-VM technology, it offers robust performance and resilience.

Harbor Cloud Encryption

Harbor is full-strength FIPS-compliant 256-bit AES encryption for data stored in cloud apps. Harbor allows apps like Salesforce or Box to retain full functionality, while protecting data from hackers and malicious vendor insiders. SaaS apps maintain their normal user experience – the encryption is invisible to end users.

supported apps



For more information, visit www.bitglass.com

bitglass