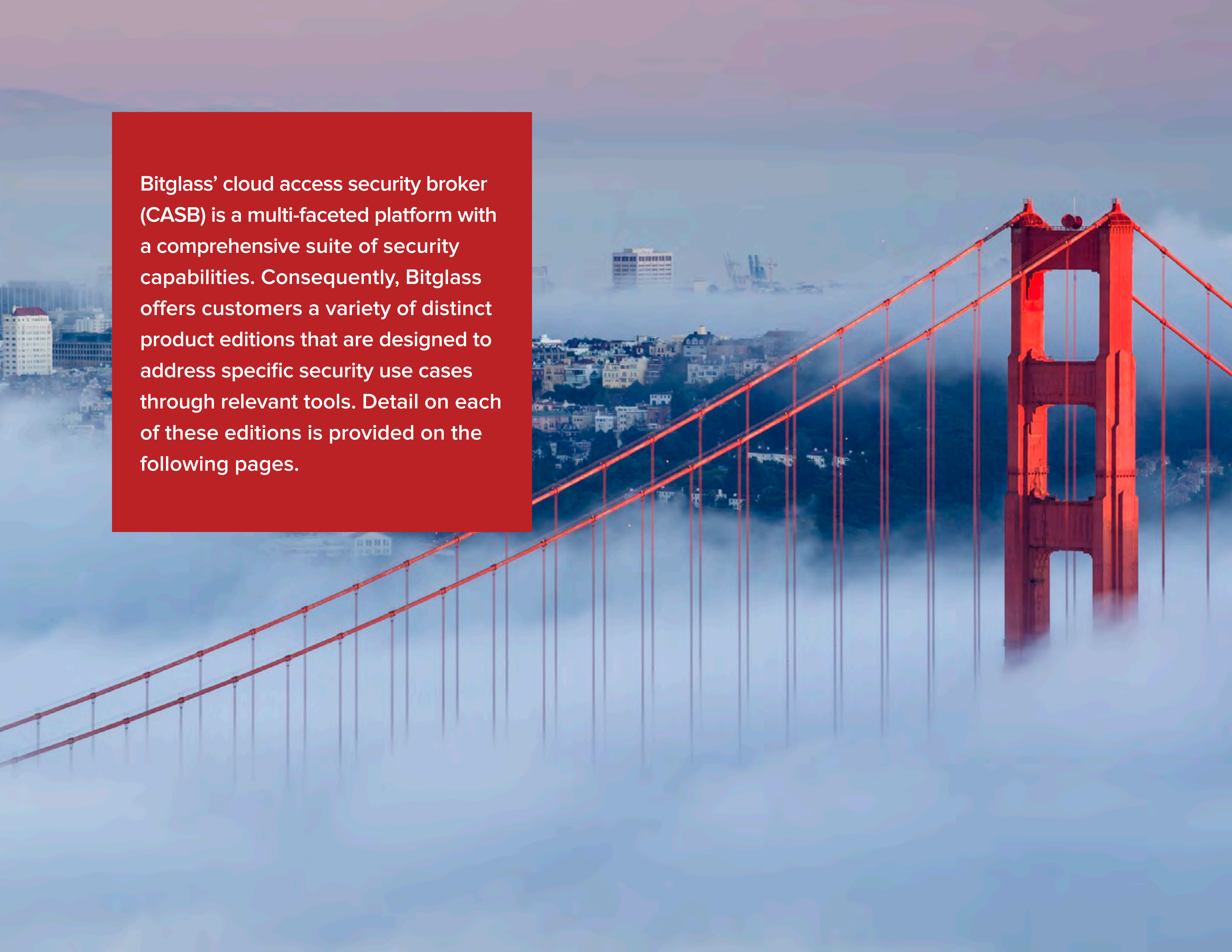
bitglass

Product Edition Guide

Bitglass' cloud access security broker (CASB) is a multi-faceted platform with a comprehensive suite of security capabilities. Consequently, Bitglass offers customers a variety of distinct product editions that are designed to address specific security use cases through relevant tools. Detail on each of these editions is provided on the following pages.



API

Description

- API Edition provides out-of-band visibility and control for data at rest within cloud applications. It is useful for detecting and securing sensitive data in the cloud when real-time protections at access are not required.

Architecture

- Integration with application programming interfaces (APIs).

Data Protection

- Data loss prevention (DLP) detects sensitive data at rest and enforces policies including quarantine, create copy, remove share, and alert.

Threat Protection

- Add-On: Detect and remediate known and zero-day malware at rest within cloud apps through behavior-based threat detection powered by Cylance.

Visibility

- Cross-app visibility and analytics provide a comprehensive view of user and file activity, offer reports, and enable audit.

Licensing

- Pricing is per application. This can be done in a three-app or a five-app bundle.
- Contracts come with twelve, twenty-four, or thirty-six month terms.

Mobile

Description

- Mobile Edition secures data flowing to mobile devices and agentlessly provides basic mobile device management (MDM) functionality. This edition is ideal in organizations that have remote and mobile employees using personal and mobile devices.
- Mobile Edition's protections are applicable to mail, calendar, and contacts only—native, ActiveSync mail clients are required.

Architecture

- An agentless, ActiveSync proxy secures any device and enforces real-time security.

Data Protection

- Contextual access control governs data access through variables such as managed vs unmanaged device, user group, geographical location, access method, application, and more.
- Data loss prevention (DLP) detects sensitive data in transit and enforces policies including allow, block, enforce digital rights management (DRM), and redact.
- Agentless MDM functionality such as PIN code enforcement, screen timeouts, selective wipe for removing corporate data from devices, device encryption, and full wipe for removing all data from devices.

Threat Protection

- User and entity behavior analytics (UEBA) scrutinize user behavior to detect suspicious activity.
- Add-On: Detect and remediate known and zero-day malware in transit from mobile devices through behavior-based threat detection powered by Cylance.

Visibility

- Visibility and analytics provide a comprehensive view of user and file activity, offer reports, and enable audit.

Licensing

- Pricing is per user per year—it is not per device, as a single user may have multiple devices that she or he uses to access data.
- Contracts come with twelve, twenty-four, or thirty-six month terms.

Standard

Description

- Standard is used for securing sanctioned, or managed, applications and gets inline via single sign-on. Standard protects data as it is stored and accessed in any app, whether it is a major SaaS app, a less popular or long-tail SaaS app, a custom application, or something else.
- Standard Edition contains all of API Edition's capabilities as well as more advanced, real-time security at access via proxy for any device. It provides comprehensive data protection, threat protection, visibility, and identity and access management—wherever data goes.
- File-level encryption is included.
- When securing Office 365 or G Suite, Standard includes everything in Mobile Edition, including basic MDM functionality in an agentless format.

Architecture

- Out-of-band visibility and control via integration with APIs.
- In-line agentless proxies secure any device and enforce real-time security.
- Forward proxies secure managed devices and enforce real-time security.

Data Protection:

- Contextual access control governs data access through variables such as device type, job function, geographical location, and custom factors.
- Data loss prevention (DLP) secures sensitive data in transit through policies like allow, block, enforce digital rights management (DRM), encrypt, and redact, and secures data at rest via quarantine, create copy, encrypt, remove share, and alert.
- File-level encryption adds an extra layer of security for sensitive information in the cloud.

Threat Protection

- User and entity behavior analytics (UEBA) scrutinize user behavior to detect suspicious activity.
- Add-On: Detect and remediate known and zero-day malware at rest within cloud apps or in transit through behavior-based threat detection powered by Cylance.

Identity

- Native single sign-on (SSO) functionality authenticates users across the enterprise cloud footprint.
- Session management imposes controls on a user's cloud app sessions in order to prevent account hijacking.
- Step-up multi-factor authentication automatically seeks additional verification under risky or suspicious circumstances—via a hardware token, an SMS token, or a third-party tool like Google Authenticator.

Visibility

- Cross-app visibility and analytics provide a comprehensive view of user and file activity, offer reports, and enable audit.

Licensing

- Pricing is per user per year—it is not per device, as a single user may have multiple devices that she or he uses to access data.
- Standard Edition can be purchased for a three-app bundle, a five-app bundle, or an unlimited number of apps.
- Contracts come with twelve, twenty-four, or thirty-six month terms.

Enterprise

Description

- Enterprise is used for securing sanctioned, or managed, applications and gets inline via single sign-on. Enterprise Edition protects data as it is stored and accessed in any type of app, whether it is a major SaaS app, a less popular long-tail SaaS app, a custom application, or something else. It secures any device, whether managed or unmanaged.
- Enterprise Edition is perfect for highly security conscious organizations. It contains field-level encryption and everything within Standard Edition and API Edition.
- When Office 365 or G Suite is secured, Mobile Edition's agentless MDM capabilities are included with Enterprise.

Architecture

- Out-of-band visibility and control via integration with APIs.
- In-line agentless proxies secure any device and enforce real-time security.
- Forward proxies secure managed devices and enforce real-time security.

Data Protection:

- Contextual access control governs data access through variables such as device type, job function, geographical location, and custom factors.
- Data loss prevention (DLP) secures sensitive data in transit through policies like allow, block, enforce digital rights management (DRM), encrypt, and redact, and secures data at rest via quarantine, create copy, encrypt, remove share, and alert.
- Full-strength file-level encryption adds an extra layer of security for sensitive information.
- Full-strength field-level encryption that enables search and sort secures data at rest within cloud apps like Salesforce and ServiceNow, as well as any custom application.
- Regional data sequestration encrypts sensitive cloud data and decrypts it only for users in authorized locations like the country of the data's origin—perfect for complying with data sovereignty requirements.

Threat Protection

- User and entity behavior analytics (UEBA) scrutinize user behavior to detect suspicious activity.
- Add-On: Detect and remediate known and zero-day malware at rest within cloud apps or in transit through behavior-based threat detection powered by Cylance.

Identity

- Native single sign-on (SSO) functionality authenticates users across the enterprise cloud footprint.
- Session management imposes controls on a user's cloud app sessions in order to prevent account hijacking.
- Step-up multi-factor authentication automatically seeks additional verification under risky or suspicious circumstances – via a hardware token, an SMS token, or a third-party tool like Google Authenticator.

Visibility

- Cross-app visibility and analytics provide a comprehensive view of user and file activity, offer reports, and enable audit.

Licensing

- Pricing is per user per year—it is not per device, as a single user may have multiple devices that she or he uses to access data.
- Enterprise Edition can be purchased for a single application, a five-app bundle, or an unlimited number of apps.
- Contracts come with twelve, twenty-four, or thirty-six month terms.

IaaS

Description

- IaaS Edition defends platforms like AWS, Azure, and GCP. With Bitglass, govern access to management consoles and detect and secure sensitive data at rest within tools like S3 and Blob.
- IaaS edition is available for private clouds.

Architecture

- Out-of-band visibility and control via integration with APIs.

Data Protection:

- Data loss prevention (DLP) secures sensitive data in transit from IaaS platforms to any device, and secures data at rest within services such as S3 via quarantine, create copy, encrypt, remove share, and alert.
- Full-strength file-level encryption adds an extra layer of security for sensitive information.

Threat Protection

- Add-On: Detect and remediate known and zero-day malware at rest within the cloud or in transit through behavior-based threat detection powered by Cylance.

Visibility

- Cross-cloud visibility and analytics provide a comprehensive view of user and file activity, offer reports, and enable audit.
- Add-On: Cloud security posture management (CSPM) allows you to detect costly IaaS misconfigurations as defined by various benchmarks such as CIS, HIPAA, and PCI DSS. Custom benchmarks are also available.

Licensing

- Pricing is per gigabyte of data scanned within IaaS platforms secured.
- Contracts come with twelve, twenty-four, or thirty-six month terms.
- For the CSPM add-on, pricing is per tenant.

Discovery

Description

- Bitglass' Zero-day Shadow IT Discovery is used to identify the unmanaged apps that employees are using—without IT's approval—to store and process corporate data.
- Applications are automatically evaluated across various security factors and compliance frameworks, and are then given trust scores. In this way, IT departments can know which apps to block and which apps to safely enable.

Architecture

- Out-of-band visibility requiring that firewall or proxy logs are fed to the CASB.
- Forward proxy installations on managed devices used to access shadow IT.

Visibility

- Shadow IT discovery that leverages Bitglass' library of 500,000 cloud apps and employs machine learning to evaluate new apps automatically.

Licensing

- Pricing is per user per year—it is not per device, as a single user may have multiple devices that she or he uses to access data.
- Contracts come with twelve, twenty-four, or thirty-six month terms.

Unmanaged App Security

Description

- Unmanaged App Security allows organizations to take control of the unmanaged applications that are uncovered through Bitglass' Zero-day Shadow IT Discovery.
- Shadow IT can be allowed or blocked entirely. Users can also be coached to sanctioned alternatives to unmanaged applications. Additionally, Bitglass can render any application read only through machine learning and natural language processing. In this way, employees can access the tools they need, but be prevented from leaking data.

Architecture

- Forward proxies (via agent or PAC file) secure unmanaged app access on managed devices.

Data Protection:

- Contextual access control governs access through variables such as device type, job function, geographical location, and custom factors.

Threat Protection

- User and entity behavior analytics (UEBA) scrutinize user behavior to detect suspicious activity.
- Add-On: Detect and remediate known and zero-day malware at rest within the cloud or in transit through behavior-based threat detection powered by Cylance.

Identity

- Session management imposes controls on a user's cloud app sessions in order to prevent account hijacking.

Visibility

- Cross-app visibility and analytics provide a comprehensive view of user activity, offer reports, and enable audit.

Licensing

- Pricing is per user per year—it is not per device, as a single user may have multiple devices that she or he uses to access data.
- Contracts come with twelve, twenty-four, or thirty-six month terms.
- This edition supports an unlimited number of applications.

Cloud Security Posture Management

Description

- For organizations using AWS, Azure, or GCP, Bitglass CSPM detects misconfigurations that can expose corporate data. Misconfigurations can be detected with respect to CIS, HIPAA, PCI DSS, or custom benchmarks.
- Bitglass offers manual remediation steps and provides automated correction of uncovered issues.

Architecture

- API integrations enable Bitglass to scan IaaS instances for misconfigurations.

Licensing

- Pricing is per tenant.
- Contracts come with twelve, twenty-four, or thirty-six month terms.

Malware Protection (Cylance) (Add-On)

Description

- Bitglass Malware Protection detects and remediates known and zero-day malware through behavior-based threat detection powered by Cylance. Files are scanned for infections at upload, at download, and at rest in the cloud.
- Malware Protection is available with all editions except for Discovery and CSPM.

Architecture

- API integrations enable the detection of threats at rest in the cloud.
- In-line agentless proxies and forward proxies detect threats in transit regardless of device type.

Licensing

- Pricing is per user per year—it is not per device, as a single user may have multiple devices that she or he uses to access data.
- Contracts come with twelve, twenty-four, or thirty-six month terms.

bitglass | Product Edition Guide

Phone: (408) 337-0190
Email: info@bitglass.com
www.bitglass.com

About Bitglass

Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.