bitglass

Bitglass for Securing Popular Apps

Employees need access to a myriad of cloud apps beyond just Office 365. So how are enterprises securing these countless apps? Read on to learn how the Bitglass SASE platform addresses some popular use cases in different app categories.

Messaging

Enterprise messaging applications are now in use across countless organizations for rapid communication and file sharing. As users often upload sensitive documents, they are a prime candidate for leakage.

Use Cases

- Secure sensitive files at upload, at download, and at rest.
- Identify and protect key data patterns within users' messages themselves.
- Prevent access to unmanaged messaging apps where visibility is lacking.

Functionality

- Crawl previously shared files for regulated information and prevent downloads.
- Scan user messages and file uploads for sensitive data and prevent sends as needed.
- Coach users to authorized messaging apps and block shadow IT.

Example Apps

- Slack
- Glip
- Microsoft Teams
- Flock
- Google Chat
- Telegram
- WhatsApp
- LINE
- Facebook Workplace

Project Management

Apps in this category enable teams to plan, track, and manage various projects, from PR initiatives to sales strategies. Project management apps frequently contain strategy details and other proprietary information.

Use Cases

- Deny unauthorized parties access to sensitive strategic information.
- Prevent the spread of malware by blocking uploads of threats from personal devices.
- Prevent the incidence of data leakage by prohibiting risky access.

Functionality

- Require single sign-on and MFA before granting access to confidential data.
- Leverage agentless ATP that blocks zero-day malware uploads even for BYOD.
- Achieve zero trust with access control that considers user context and accessed content.

Example Apps

- Smartsheet
- Asana
- Workfront
- Pipefy
- Wrike
- Zoho Sprints
- monday.com
- Airtable

Bitglass for Securing Popular Apps

bitglass

ERP

Enterprise resource planning applications enable organizations to manage business processes. Used across industries, they integrate organizations' departments and coordinate activities throughout their supply chains.

Use Cases

- Deny risky access to reports about workflow, inventory, production, and quality control.
- Prevent threat actors and careless users from uploading malware into the platform.
- Identify and protect regulated information to achieve compliance.

Functionality

- Block unauthorized access to key files (e.g. quality reports only accessible for QA).
- Identify and remediate malware at upload or download for any user on any device.
- Scan at-rest or in-transit files for regulated data in order to quarantine or block.

Example Apps

- SAP ERP
- Sage ERP
- Oracle ERP
- Exact MAX ERP
- Microsoft Dynamics
- Epicor ERP
- NetSuite ERP
- Syspro

Product & Software Development

These apps are powerful work management tools that address use cases like test case management and agile software development. Naturally, they end up housing extensive proprietary and product information.

Use Cases

- Safeguard mission-critical information like intellectual property.
- Maintain visibility over the data users are accessing and downloading.
- Deny access to users on unsafe devices or in unsafe regions.

Functionality

- Encrypt the files and fields that house IP and your most sensitive data.
- Comprehensive activity logs detail all file, user, and app activity in a single dashboard.
- Prevent access for users on BYO devices and users outside of HQ's home country.

Example Apps

- Jira
- GitLab
- Confluence
- SourceForge
- Trello
- ProjectLocker
- Bitbucket
- CloudForge
- GitHub
- Windchill

Bitglass for Securing Popular Apps

bitglass

CRM & Ticketing

Customer relationship management apps allow companies to manage and analyze their interactions with past, present, and future customers. They are filled with confidential and regulated data.

Use Cases

- Shield sensitive customer data like SSNs or credit card details from insider threats.
- Maintain regulatory compliance while handling PII and PIFI like bank account numbers.
- Prevent unauthorized access to the CRM platform.

Functionality

- File and field encryption obfuscate sensitive data while preserving search and sort.
- Use DLP to identify and protect regulated data with prebuilt patterns or Exact Match.
- Verify user identity with authentication options like SSO and MFA.

Example Apps

- ServiceNow
- Zendesk
- Zoho
- Salesforce
- Freshworks
- Nimble
- Insightly
- Bitrix24
- Agile CRM

File Sharing

File-sharing applications allow users to share and store files, sync them across multiple devices, and collaborate on them with others. Due to the volume of data within them, they are regularly targeted by malicious actors.

Use Cases

- Govern shares of files in order to prevent threatening viewing and downloading.
- Prevent sync clients from being used to exfiltrate company documents.
- Defend against malware stemming from infected file uploads.

Functionality

- Sharing controls identify and revoke risky shares with external or unauthorized parties.
- Enable sync clients on managed devices but block them on BYOD and mobile.
- Use agentless ATP to block malware at rest and at upload or download for any device.

Example Apps

- Box
- Dropbox
- OneDrive
- Citrix ShareFile
- Google Drive
- Hightail
- Amazon Drive
- Tresorit

Bitglass for Securing Popular Apps

bitglass

HR

HR apps automate numerous HR job duties and enable employees to manage their own profiles directly, granting access to their payroll, tax, and health information. They contain extensive amounts of PII.

Use Cases

- Safeguard personally identifiable information from prying eyes.
- Securely allow BYOD access to managed apps for self-service.
- Defend against the spread of malware on countless personal devices.

Functionality

- Use Exact Match to find and protect specific data with actions like encrypt on download.
- Allow uploads from personal devices but limit downloads of sensitive personnel files.
- Use agentless ATP to block malware at rest and at upload or download on any device.

Example Apps

- Workday
- UltiPro
- WorkBright
- Namely
- Zenefits
- Halogen TalentSpace
- Justworks
- ClearCompany
- Optimum HRIS
- Benefits Connect
- Everyday HR
- Axiom HRS

Payroll

Payroll applications streamline needed employee activities such as managing sick leave, absences, and overtime, and provide self-service for items like viewing paystubs and changing 401(k) contributions.

Use Cases

- Ensure proper authentication as users attempt to access the application.
- Safeguard private employee information (like W-2 forms) at rest.
- Deny access to critical data like employee PII for users with risky contexts.

Functionality

- Leverage single sign-on (SSO) and reenforce identity verification with MFA.
- Protect employee data with full strength cloud encryption that preserves search and sort.
- Use contextual access control to govern access by variables like user device or location.

Example Apps

- Paychex
- Square Payroll
- SurePayroll
- QuickBooks
- ADP
- Gusto
- Patriot Software
- Expensify
- Concur
- Bill.com

Bitglass for Securing Popular Apps

bitglass

FP&A

Financial planning and analysis apps provide automated functionality and generate reports as needed on the fly. They contain sensitive financial data like invoices and bank account information.

Use Cases

- Prevent the leakage of PII like SSNs and other financial information at rest.
- Secure access to key documents like accounts payable files.
- Ensure regulatory compliance with frameworks like PCI DSS, SOX, and others.

Functionality

- Encrypt file and field level data with full-strength encryption that enables search and sort.
- Prevent access to certain files for unauthorized or risky users and log all activity.
- Automatically detect regulated data and apply DLP policies like DRM and quarantine.

Example Apps

- QuickBooks
- GoDaddy
- Xero
- Wave Accounting
- Zoho Books
- FreeAgent
- ZipBooks
- Adaptive Insights
- Hiveage

EHS Apps

Environment, health, and safety applications enable organizations to implement practical steps to achieve environmental workplace safety. Naturally, the organizational and employee data therein needs to be secured.

Use Cases

- Prevent the leakage of incident and risk reports as well as audit details.
- Block application access for unauthorized or risky endpoints.
- Defend against the spread of malware within the EHS platform.

Functionality

- Use DLP to find and quarantine sensitive or HIPAA-regulated data.
- Access control blocks BYOD and mobile but grants access for managed computers.
- Agentless ATP blocks malware at rest as well as threats in transit for any app or device.

Example Apps

- Intelex
- Cority
- Vera EHS
- BasicSafe
- EHS Insight
- LifeSaver
- SiteDocs
- Pro-Sapien

Bitglass for Securing Popular Apps

bitglass

EMR Apps

Electronic medical records are filled with PII and PHI like patient treatment details and medical history. As these EMR apps are a top target for malicious actors, healthcare organizations must prioritize their security.

Use Cases

- Identifying and defending protected health information (PHI).
- Preventing data leakage on unmanaged devices like personal phones.
- Ensuring that users are properly authorized to view healthcare data and files.

Functionality

- Use prebuilt identifiers to protect PHI and PII with DLP actions like DRM and redact.
- Block sensitive file downloads for BYOD while allowing them on managed devices.
- Deploy SSO and MFA to verify users' identities before granting them access.

Example Apps

- AdvancedMD
- athenahealth
- DrChrono EHR
- PrognoCIS
- Kareo Clinical EHR
- AllegianceMD
- Compulink Healthcare Solutions
- NextGen Healthcare
- PointClickCare

Your organization will need to secure countless applications in order to protect your sensitive and regulated data. These apps cross a variety of categories and all require granular security. At Bitglass, we are committed to securing any interaction between any device, app, web destination, on-premises resource, or infrastructure. Want to see how we can help your enterprise?

Request a free trial.

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company 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.

(408) 337-0190 • info@bitglass.com • www.bitglass.com