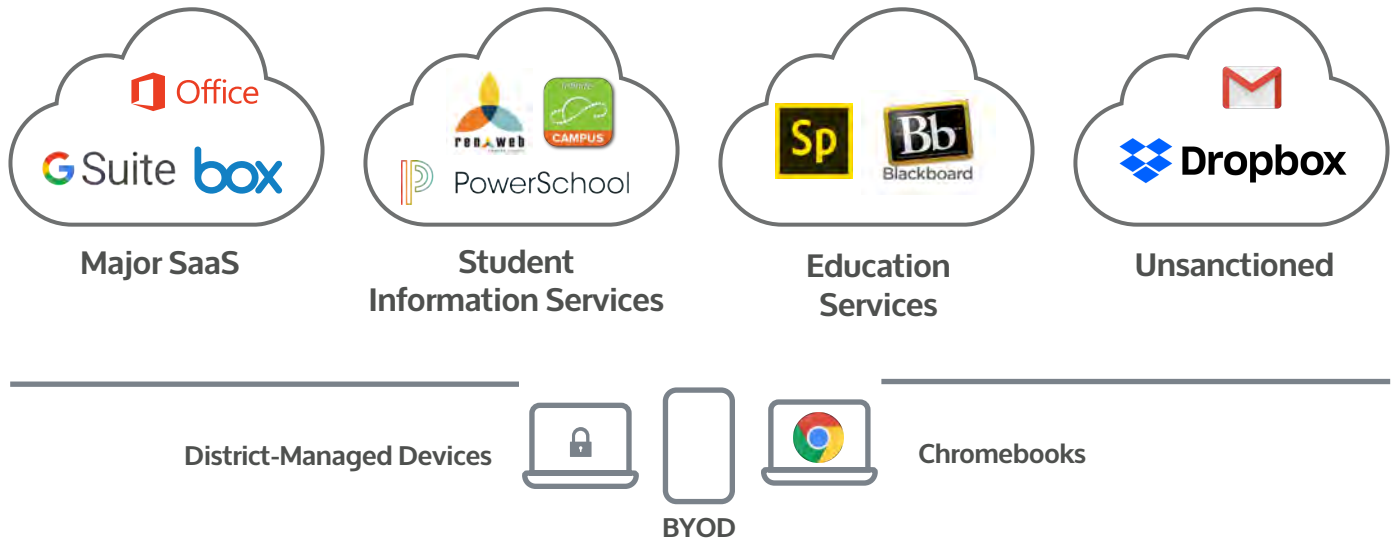




K-12 Schools Overview

Bitglass secures any app, any device, anywhere



Secure data on all one-to-one devices

Districts across the country are leveraging technology to enhance education in primary and secondary schools. One-to-one programs, where each student has access to a laptop, Chromebook, or iPad, are a critical component of any school's technology infrastructure.

Districts must consider security when deploying one-to-one programs in schools. Where endpoint-based malware protection was once an option, Chromebooks and iPads rely on the cloud for data access and require an alternative approach to threat protection. Real-time data security to limit unauthorized access to student data must also be a priority for district IT teams.

Only Bitglass provides agentless data protection, threat protection, identity management, and visibility for Chromebooks, iPads, and more.

Cloud Security and Compliance

Data Protection

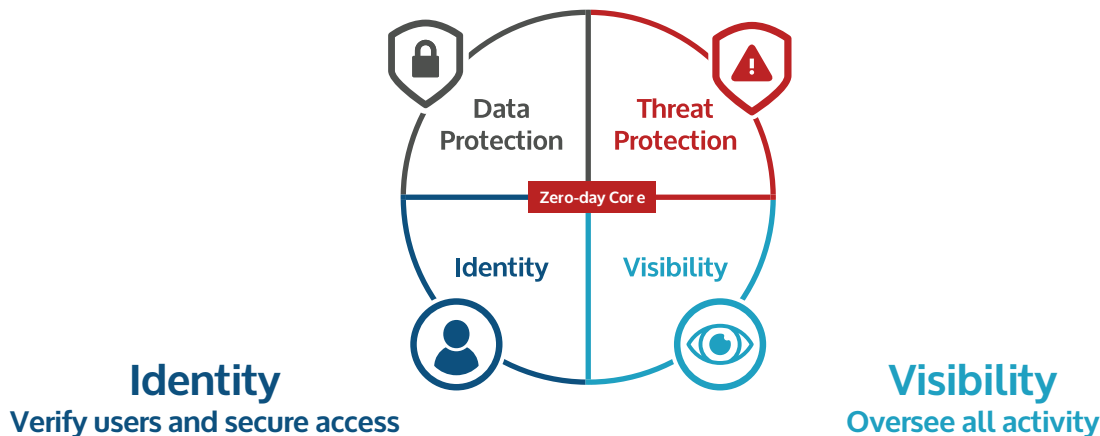
Secure data wherever it goes

- Prevent PII leakage with comprehensive, real-time DLP – watermark, redact, quarantine, and more.
- Secure mobile access without agents – selectively wipe sensitive data, enforce device policies, and stop unauthorized access.
- Meet internal security requirements by encrypting student data stored in cloud applications.

Threat Protection

Defend against any threat

- Leverage user and entity behavior analytics (UEBA) to detect suspicious behavior and halt insider threats.
- Defend against zero-day malware in any cloud app with Bitglass' Advanced Threat Protection.
- Identify zero-day threats at rest, at upload, and on download without cumbersome definition updates.



- In multi-user environments, authenticate faculty and students across all applications upon login to any device.
- Employ multi-factor and step-up authentication to confirm student and faculty identities.
- Use contextual access controls to limit access to personal data by device type, user, and more.

- Demonstrate compliance with FISMA and FERPA through one portal that offers complete visibility and insightful analytics.
- Enable audit and configure notification settings to alert IT administrators of high-risk data outflows.
- Automatically detect use of risky cloud applications through machine learning with Bitglass Shadow IT Discovery.

Our Technology

Bitglass acts as an intermediary between any device and any app, protecting data end-to-end. To achieve this, Bitglass leverages APIs and proxies to provide districts with complete control and visibility over sensitive student and faculty data.

Cost Effective Security

Deploying several point solutions for security can be difficult to manage, often require updates, and are generally costly.

With one solution for total data protection, IT staff can easily manage policies across the district, control outflows of sensitive data, and achieve visibility over high-risk activities all in one place. Updates are free and automatically rolled out to all new and existing customers.

Easy to Deploy

Bitglass is the only agentless, real-time CASB. No software installation is required on devices – freeing IT resources and enabling security on unmanaged mobile devices, Chromebooks, district-owned devices and more.

Because there are no agents to invade user privacy, impair user experience, or harm device performance, adoption is rapid and deployment is simple.

