Bitglass Data Loss Prevention

Technical Brief

Cloud and remote work drive corporate data beyond the firewall, a risk that many organizations have mitigated by deploying secure access service edge (SASE) platforms for control and visibility. Data loss prevention (DLP) capabilities are core to any complete data protection solution. Bitglass' award-winning DLP solution protects data in real time, in any app, device, web destination, on-premises resource, or infrastructure. Organizations can easily define policies to identify and protect sensitive content. Bitglass offers the only granular DLP solution that prevents leakage on any interaction.

Key Features

- Protect data with automated actions based on file content and user access context.
- Quickly set up new policies using Bitglass' extensive library of pre-built data patterns, create your own, or import existing policies via ICAP.
- Allow, watermark, encrypt, DRM, or block access in any app.
- Apply DLP measures across the web and the network.
- Log all DLP policy violations and actions taken by Bitglass in one detailed dashboard.
- Leverage Bitglass' public-cloud-based, Polyscale Architecture, which ensures maximum uptime, performance, and scalability.
- Use Field Programmable SASE Logic (FPSL) to address uncommon, fringe use cases.

Why Bitglass DLP?

In the era of the cloud, organizations need a DLP solution that works across applications, web destinations, infrastructure, and endpoints. Where an employee's unmanaged mobile phone, an enterprise file sync and share (EFSS) app, or a personal cloud storage service are unsecured, sensitive data can be left exposed.

Bitglass' Total Cloud Security Platform integrates multi-mode cloud access security broker, SmartEdge Secure Web Gateway, and zero trust network access (ZTNA) technology to provide real-time, inline and out-of-band DLP for all data, making it the only DLP solution that secures any interaction.

Bitglass' integrated DLP also ensures compliance with regulations such as HIPAA, GDPR, HITEC, PCI DSS, FISMA, FERPA, SOX, GLBA, CCPA, and more.

Detection Mechanisms and Supported Actions

Bitglass DLP provides a comprehensive set of capabilities that can be leveraged by enterprises to protect data in any form and type. Some of the unique capabilities of the data protection engine include Exact Match, advanced regex, file fingerprinting, and text extraction from images with OCR. With a variety of detection mechanisms, organizations can easily identify the files, fields, and data patterns that they want to secure.

Remediation actions allow you to extend access to data in a risk-appropriate fashion for select applications. This includes dynamic watermarking/tracking, encryption, DRM, quarantine, share removal, redaction, and blocking of sensitive content.

- Exact match and document fingerprinting support for cloud policy rules.
- Granular remediation actions across applications.
- DLP based on extension, name, file properties, and more.
- Push files to other integrated services for deeper inspection.
- Upload DLP protects files without timeouts.

Spotlight: Exact Match

Relying solely on simple pattern-based DLP policies can generate large volumes of false-positives. The detection engine does its job by identifying data patterns that match a policy, but only a subset of matches represent true risk.

- With Bitglass, you can identify specific attribute values in your applications by surgically matching against attributes in a data set. Examples include policies that apply to:
  - Specific credit card numbers that are used for sensitive transactions; rather than all credit cards
  - The identification numbers (e.g. Social Security numbers) of a subset of users; rather than all identification numbers
  - An attribute pair belonging to an individual (e.g. a specific user's address and Social Security number)

The Exact Match approach is storage and compute intensive and, consequently, requires a highly scalable platform that accommodates its processing demands. Because of its Polyscale Architecture, Bitglass addresses Exact Match requirements without impacting performance while raising visibility into incidents in real time.

Configuration and implementation can easily be completed in minutes.

Configuration

Bitglass DLP works on any device, protecting email content, files, and all other corporate data. A single dashboard is used to configure universal policies that are enforced consistently wherever data goes, securing all cloud applications, web destinations, and on-premises resources.

Pre-defined DLP templates allow easy identification of common content types such as PII, PHI, and credit card data. Bitglass offers hundreds of pre-defined DLP templates, covering the needs of customers in all major industry verticals and geographic regions, that can be used for building comprehensive data protection policies.

Bitglass' custom policy builder incorporates a range of identifiers including keywords, regular expressions, proximity, and frequency of occurrence. The solution also ingests policies from most leading DLP solutions, making for a seamless transition where premises-based DLP is already deployed.

Field Programmable SASE Logic

There are custom use cases for which security teams will need to employ even more granular capabilities. For example:

- Preventing files containing sensitive or regulated information from being uploaded and shared in non-traditional or custom applications.
- Stopping sensitive data patterns from being sent in messages in specific Slack channels, but otherwise allowing unfettered use of the application.
- Automatically identifying when a user clicks the share button for a sensitive file in Office 365 in order to prevent unauthorized sharing in real time rather than after the fact.
- Keeping users from editing a Google Docs document based on predefined policy in order to preserve data integrity and prevent leakage.
- Detecting when a user attempts to sign into a non-corporate SaaS or IaaS instance and preventing the login.

Highly specific use cases like the above are what Field Programmable SASE Logic (FPSL) is designed to address. With FPSL, admins are given the freedom to code to their exact needs directly in the Bitglass dashboard, giving unprecedented granularity and control to their DLP policies. This is accomplished by scrutinizing attributes like domain, URI, query string, cookie, and method (PUT, POST, GET, and others), as well as scanning for sensitive data through predefined patterns (Exact Match, advanced regex, et cetera). The unlimited flexibility that this customization provides allows organizations to address any use case in a highly surgical fashion. Additionally, Bitglass provides built-in data patterns that include FPSL to address key use cases out of the box.