Data Masking and Exfiltration Control

Baffle Data-Centric Protection provides simplified data masking and exfiltration control to mitigate the risks of data leakage and bulk data breaches.

Baffle Data Masking and Exfiltration Control supports a variety of masked formats via its "no code" deployment model, meaning no application code changes are required. This accelerates secure data sharing, without losing control of your data.

Key Benefits

- Easily mask data with "no code" changes
- Accelerate compliance with data privacy regulations such as PCI, HIPAA, GDPR, and CCPA
- Securely share data with third parties while minimizing the risk of data leakage
- Replace production data with fake data values in non-prod environments
- Works on both encrypted and clear text data
- Enable Dynamic Data Entitlements to automatically mask data and mitigate data breach risks

Solution Overview

Organizations today are challenged with collecting, sharing, analyzing and processing data, all while keeping it secure and complying with the latest data privacy regulations.

Baffle Data Masking and Exfiltration Control allows organizations to simplify data protection by masking data without any code modifications.

The solution helps ensure data privacy and compliance by limiting access and visibility to sensitive data values while supporting a broad range of data formats and types. This capability makes complying with regulations such as PCI, HIPAA, GDPR and CCPA both faster and easier.

With Baffle, companies can build their own Data Protection Service layer to contain data at the source and enforce strong access controls. Baffle's Exfiltration Control capabilities extend data access controls by enabling Dynamic Data Entitlements -- automated masking of data by data owner and policy driven masking to mitigate bulk data exfiltrations.

Baffle Data Masking and Exfiltration Control can be deployed both on-premise or in cloud infrastructure, such as Amazon Web Services, Microsoft Azure, or Google Compute Platform.

Original Data in Clear Text or Encrypted

	category	city	country	customerid	customername	orderdate	orderid
1	Office Supplies	Houston	United States	DP-13000	Darren Powers	2013-01-03	CA-2011-103800
2	Office Supplies	Houston	United States	DP-13000	Darren Powers	2013-01-03	CA-2011-103800
3	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326
4	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326
5	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326

Masked Data with Varying Formats

	category	city	country	customerid	customername	orderdate	orderid
1	***CONFIDENTIAL***	XXXXXXXXXX	United States	584-91-6137	Darren Powers	1900-01-01	**-****-**3800
2	***CONFIDENTIAL***	XXXXXXXXXX	United States	146-52-7632	Darren Powers	1900-01-01	**-****-**3800
3	***CONFIDENTIAL***	XXXXXXXXXX	United States	516-63-9978	Darren Powers	1900-01-01	**-****-**3800
4	***CONFIDENTIAL***	XXXXXXXXXX	United States	667-73-0661	Darren Powers	1900-01-01	**-****-**3800
5	***CONFIDENTIAL***	XXXXXXXXXX	United States	384-02-6256	Phillina Ober	1900-01-01	**-****-**2326

Key Features and Capabilities

Simplified Data Masking - Baffle Data Masking enables field-level and record-level masking of data with no application code changes. This allows organizations to protect data faster and without over-hauling their architecture.

Flexible Data Formats - Support for variable formats, fixed string or numeric replacement, date and timestamp, bit or binary length fields, and random generation of characters or numbers. Broad flexibility in data formats helps ensure applications are easily supported and business processes remain in tact.

Secure Third Party Data Sharing - Easily mask and control access to specific fields to minimize the exposure of data to third party suppliers and collaborators.

Dynamic Data Entitlements (DDE) - A policy-based method to automatically apply masking based on specified parameters or data owner identification. DDE enables additional contextual controls to be applied to access to data.

Data Exfiltration Control - Data Masking can be applied based on policies and in bulk data exfiltration scenarios, can automatically mask data as it is exfiltrated. This method helps mitigate data breach risk and reduces penalties incurred under the latest data privacy regulations.

Support for Encrypted Data - Baffle Data Masking and Exfiltration Control can be applied to both clear text and encrypted data records. This capability gives customers end-to-end data-centric protection from the presentation layer to the data source.

About Baffle

Baffle is an advanced data-centric protection solution built from the ground up for distributed data and hybrid cloud environments where outdated solutions continually fail to stop breaches.

Only Baffle processes sensitive information without ever decrypting it or breaking applications. Using industry standard AES encryption and customer-owned keys, Baffle's frictionless, data-centric encryption never exposes sensitive information. Without any application changes, only Baffle protects data at rest, in memory, and while in use.

info@baffle.io
https://baffle.io
2811 Mission College Blvd., 7th Floor, Santa Clara, CA 95054