Gartner

COOL VENDOR 2019

Data Privacy Simplified

Using Data-Centric Protection to Secure Your Data

Harold Byun

VP Products

baffle

Introduction

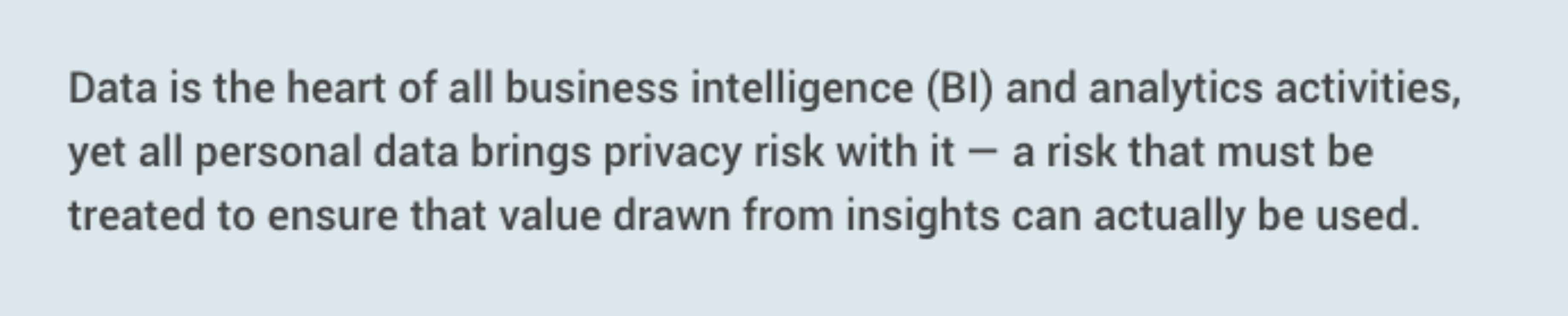
- Overview of Data Privacy Challenges and Regulations
- Data Breaches and Threat Models
- Common Data-Centric Protection Methods
- Privacy Preserving Analytics / Secure Data Sharing
- Q&A

Questions throughout – use the chat panel. Email info@baffle.io, harold@baffle.io

Privacy Preserving Analytics

What is it?

- A computational method that allows for operations, processing and analysis of data without revealing the underlying data values or violating the data privacy contract.



Data is the heart of all business intelligence (BI) and analytics activities, yet all personal data brings privacy risk with it — a risk that must be treated to ensure that value drawn from insights can actually be used.

Gartner Report on Privacy Preservation in Analytics

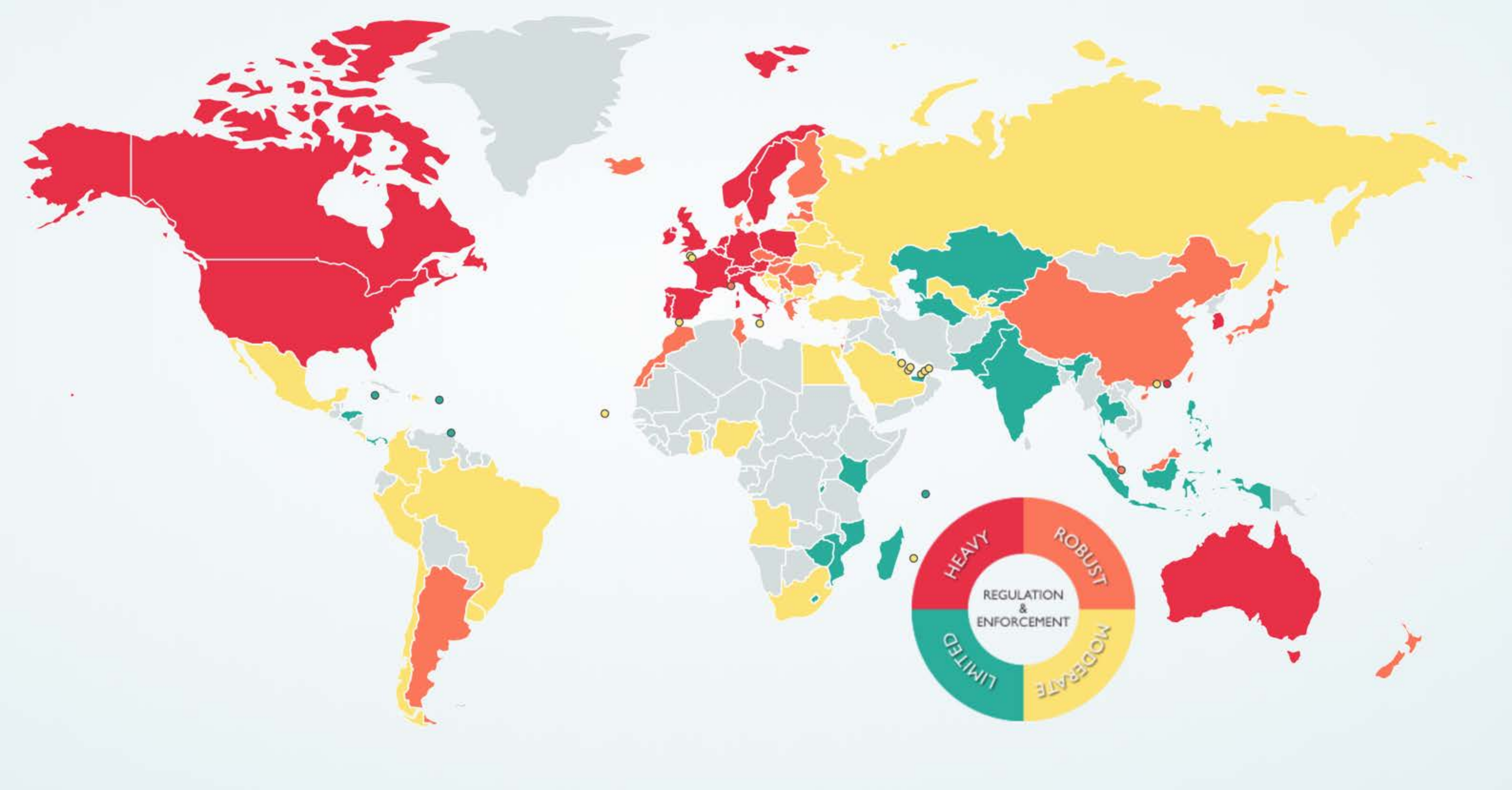
More info and resources: **https://baffle.io/privacy**

Speaker Bio

Harold Byun is VP of Products at Baffle, an end-to-end data-centric protection company. His career has focused on data containment and security technologies including data loss prevention and activity monitoring, cloud access security broker, and mobile data containment capabilities. He holds several data security related patents.

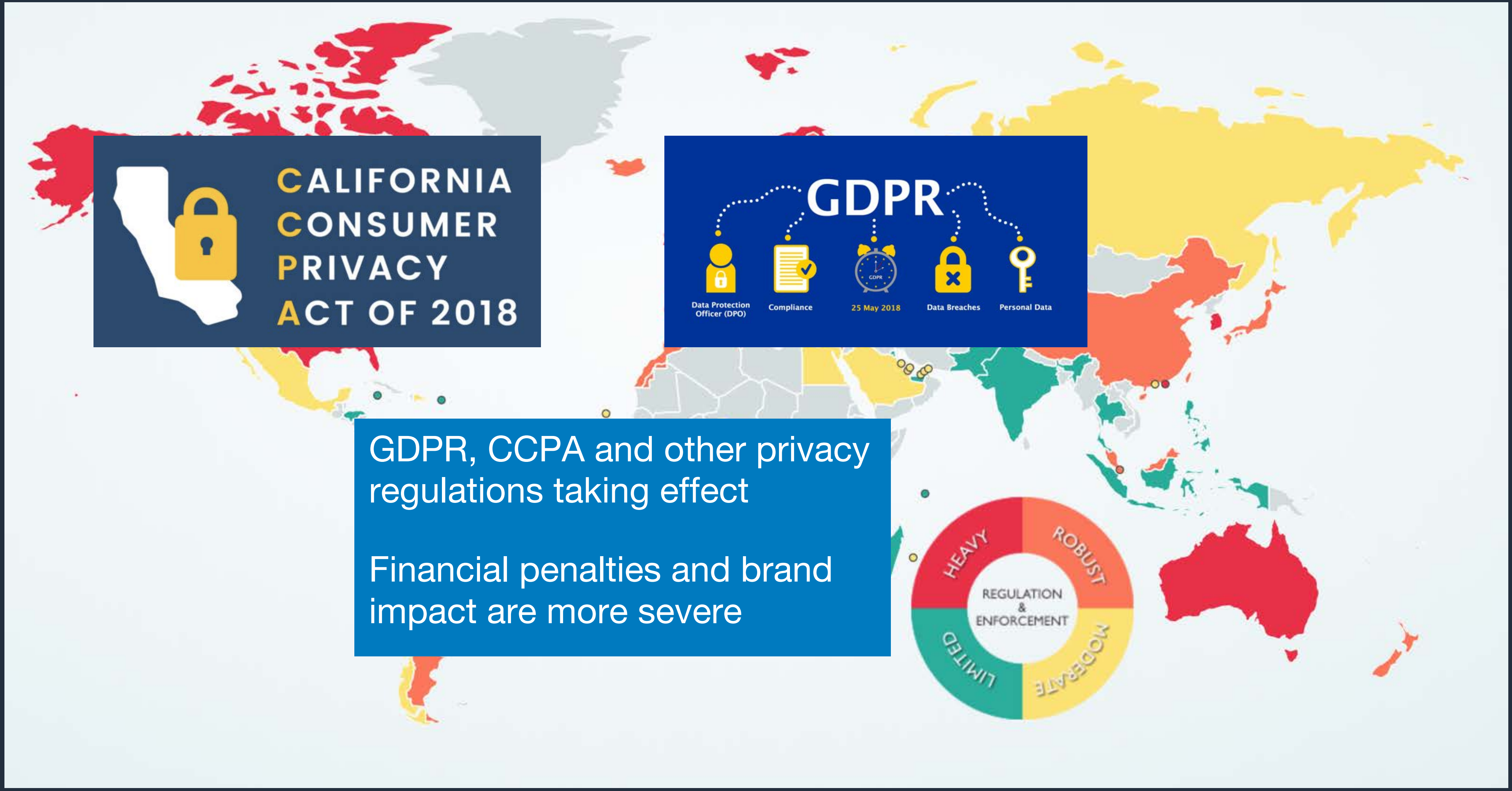
Overview on Data Privacy and Regulations

Privacy Around the World



Source: https://www.dlapiperdataprotection.com/index.html?t=about&c=AO

Privacy Around the World



GDPR, CCPA and other privacy regulations taking effect

Financial penalties and brand impact are more severe

Source: https://www.dlapiperdataprotection.com/index.html?t=about&c=AO

Consumer Rights under Privacy Regulations

Right to Know

- What information are you or your 3rd parties collecting about them? What categories of information?
- How that information is being used?
- If information will be shared and with whom

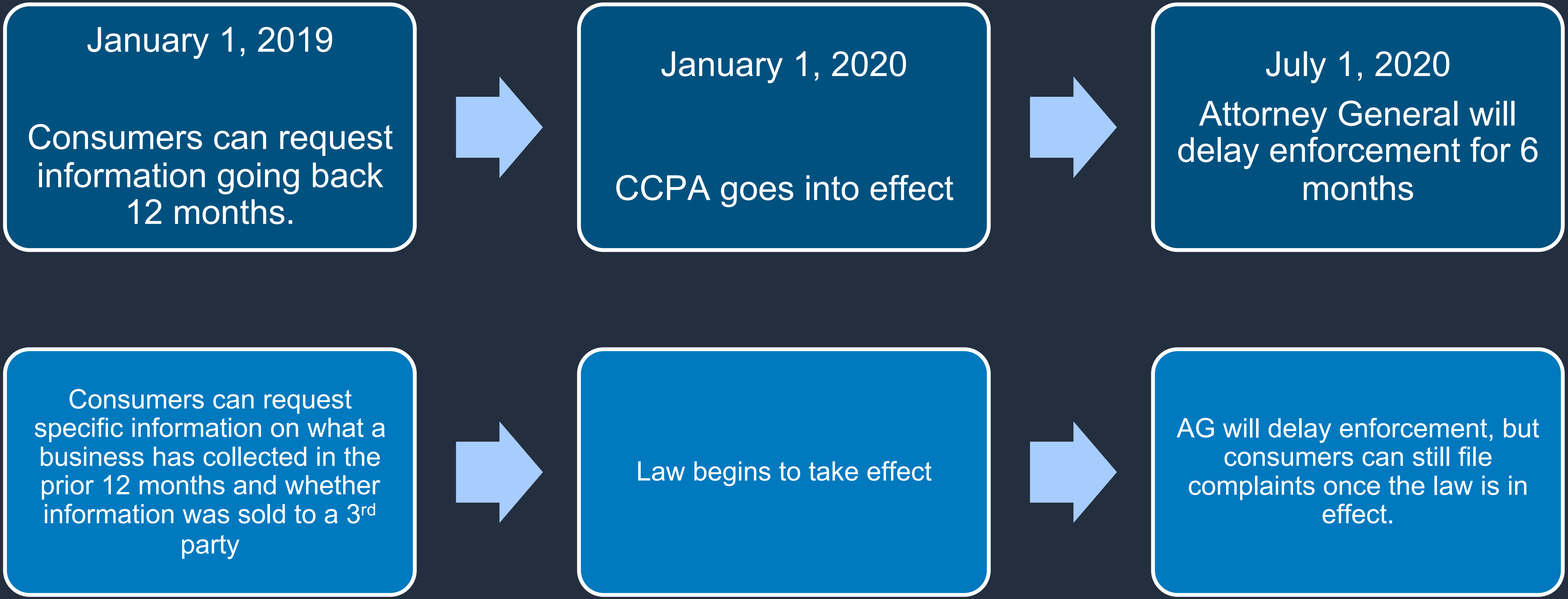
Right to Be Forgotten

- Per consumer request, companies must delete all information about the consumer
- Some exceptions apply, limited analytical use cases, some research scenarios, aggregate data, HIPAA data

Right to Control

- Consumers can opt out of the sale of their information
- Companies must present an option for consumers to opt out
- Consumers cannot be discriminated against for opting out

CCPA Timelines – Key Dates



January 1, 2019

Consumers can request information going back 12 months.

January 1, 2020

CCPA goes into effect

July 1, 2020

Attorney General will delay enforcement for 6 months

Consumers can request specific information on what a business has collected in the prior 12 months and whether information was sold to a 3rd party

Law begins to take effect

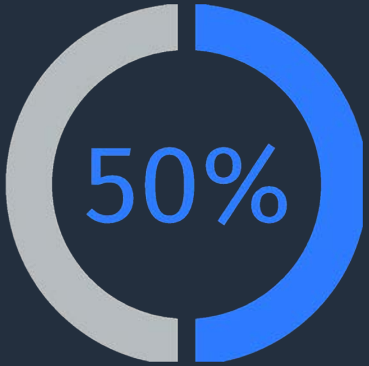
AG will delay enforcement, but consumers can still file complaints once the law is in effect.

Is Your Organization Affected?

Applies to for-profit businesses that collect and control California residents’ personal information and meet at least one of these thresholds:

$25 million or greater in annual revenue

Collect personal information of 50,000 or more California residents, households, or devices annually



Make 50 percent or greater annual revenue from selling California residents' personal information

*Non-profits and smaller companies won't have to comply.

CCPA Personal Information

- Personal information is defined under the CCPA as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” The definition is broader than the GDPR.

- Provides standard examples that include the following (partial listing):
  - Name
  - Social Security numbers
  - Drivers’ license numbers
  - Alias
  - Postal address
  - Email address
  - Passport number
  - Purchase histories
  - “Unique personal identifiers” like device identifiers and online tracking technologies
  - Online identifier Internet Protocol address
  - Biometric information
  - Geolocation data
  - Professional or employment-related information
  - Education information, defined as information that is not publicly available
  - Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

Data Breaches

- CCPA provides a right of action to individuals for data breach incidents.
- Consumers may sue an organization if it was found that the company was negligent in ensuring that proper cybersecurity safeguards were in place to protect consumer data.
- Consumers may receive between $100 and $750 without needing to prove that they were harmed in the data breach.

“Any consumer whose **nonencrypted or nonredacted personal information**, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action…” (Article 1798.150, CCPA 2018)

Penalties and Fines

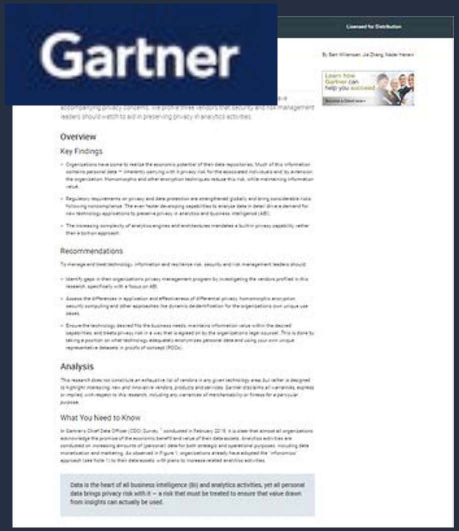
- $750 x 10000 consumers = $7.5 million

- Attorney General can fine companies $2,500 per violation and $7,500 per intentional violation. It is still not clear on what will count as a violation.

Data Privacy Resources

More info and resources: **https://baffle.io/privacy**

Gartner Report on Privacy Preserving Analytics



Gartner

Licensed for Distribution

By Bart Willemsen, Jie Zhang, Nader Henein

Learn how Gartner can help you succeed

Become a Client

accompanying privacy concerns. We profile three vendors that security and risk management leaders should watch to aid in preserving privacy in analytics activities.

Overview

Key Findings

Recommendations

Analysis

What You Need to Know

Data is the heart of all business intelligence (BI) and analytics activities, yet all personal data brings privacy risk with it — a risk that must be treated to ensure that value drawn from insights can actually be used.

CCPA Compliance Simplified

baffle

CCPA Compliance Simplified

Methods you can use to accelerate and simplify compliance with the California Consumer Privacy Act (CCPA)

Encryption Simplified White Paper

Encryption Simplified.

White Paper

Baffle Example Architecture and Configuration Overview

Sample Architecture

Configuration Overview

Email: info@baffle.io, harold@baffle.io

Data Breaches and Threat Models

Key Trends Impacting Data Security

1

Data breaches continue unabated

Data loss and leakage is the #1 cloud security concern (2019 Cloud Security Report)

2

Migration to cloud is early but continues to increase

Security controls can be misconfigured and data left exposed or overshared

3

Third party risk and data sharing

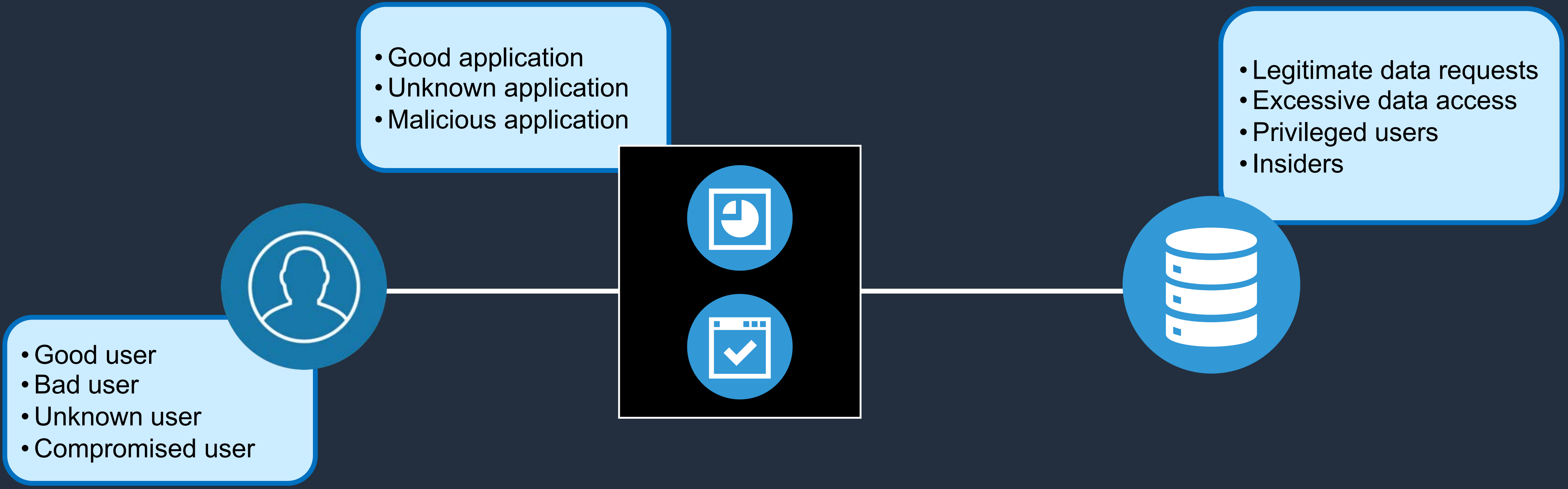
~60% of CISOs have reported data leakage via a third party in 2018. (Ponemon Institute)

Why Do Breaches Continue to Occur?

- Are hackers getting better?
- Is it because we’re not patching systems enough?
- Is it security misconfiguration?
- Security Awareness - users aren’t educated enough
- Zero day attacks and malware
- Third party risk
- Is it the business bypassing security controls?
- Is it because the ”cloud” is evil?

- It’s many or all of these things
- Security will never cover them all
- People / attackers will get to your data

The Data Access Model has Changed

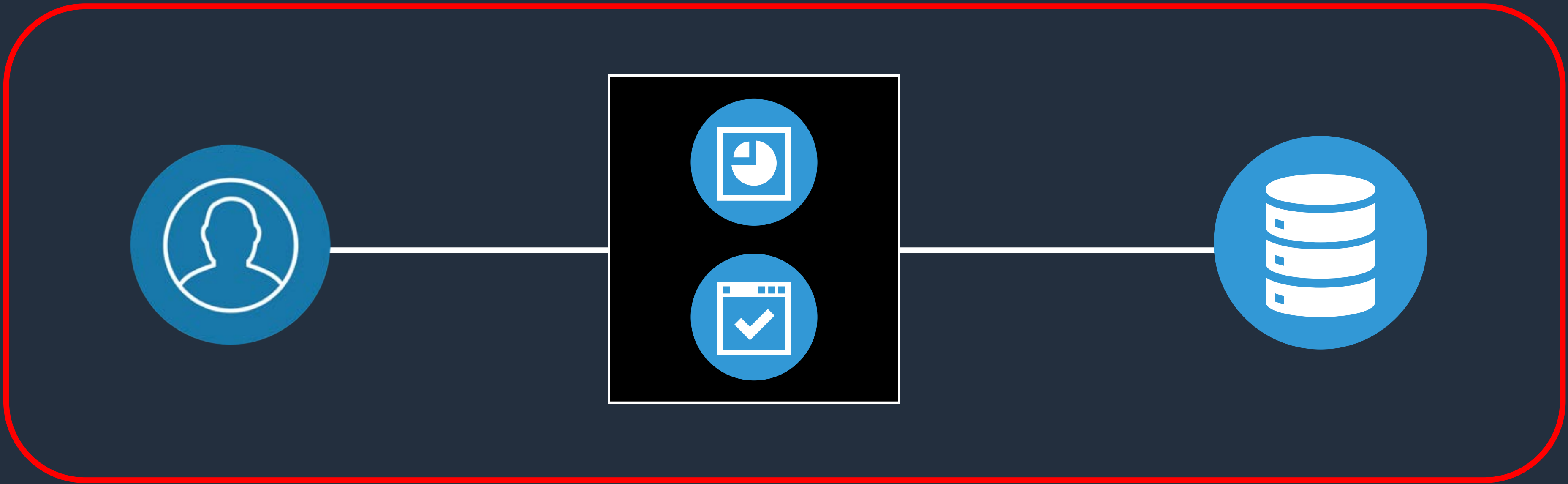


- Good application
- Unknown application
- Malicious application

- Legitimate data requests
- Excessive data access
- Privileged users
- Insiders

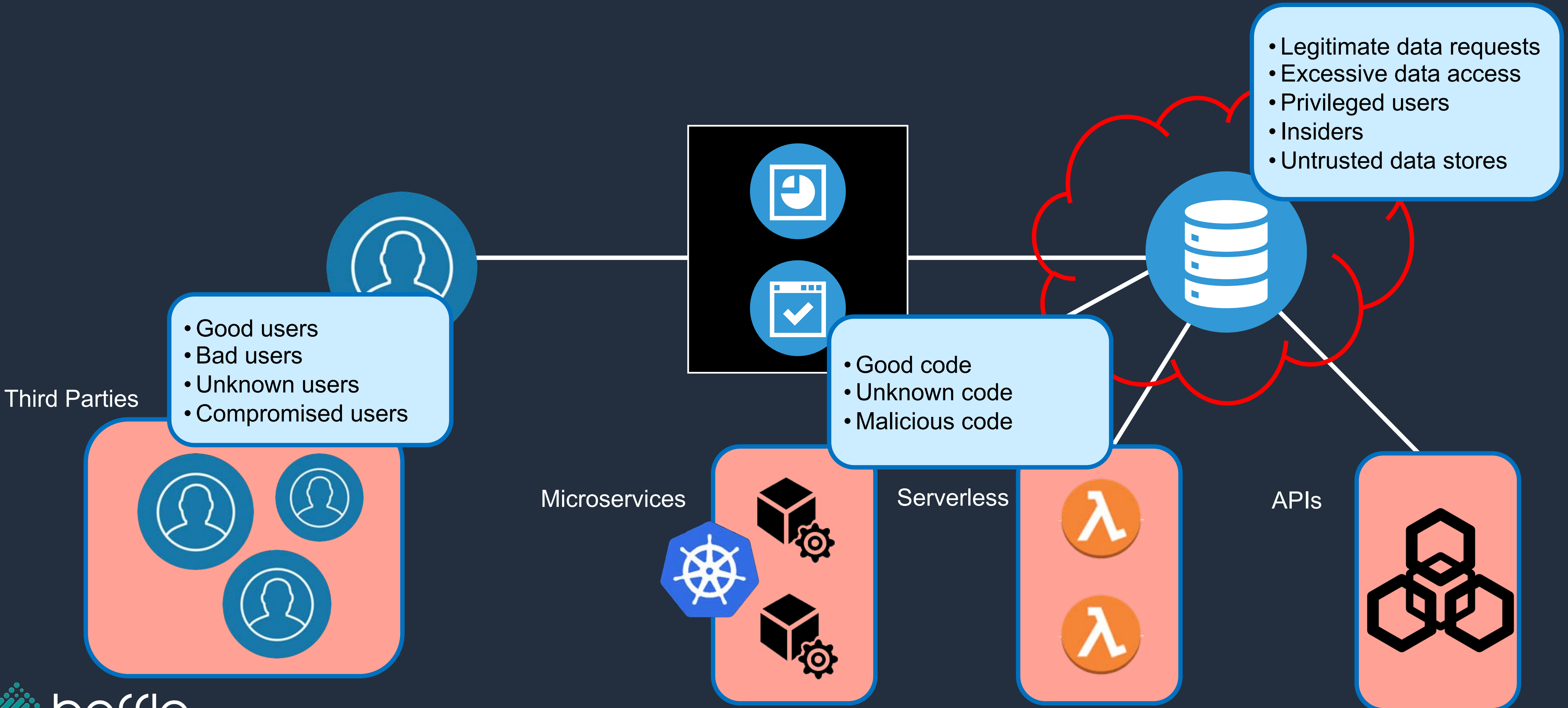
- Good user
- Bad user
- Unknown user
- Compromised user

The Data Access Model has Changed



This is an access channel that needs to be protected

The Data Access Model has Changed



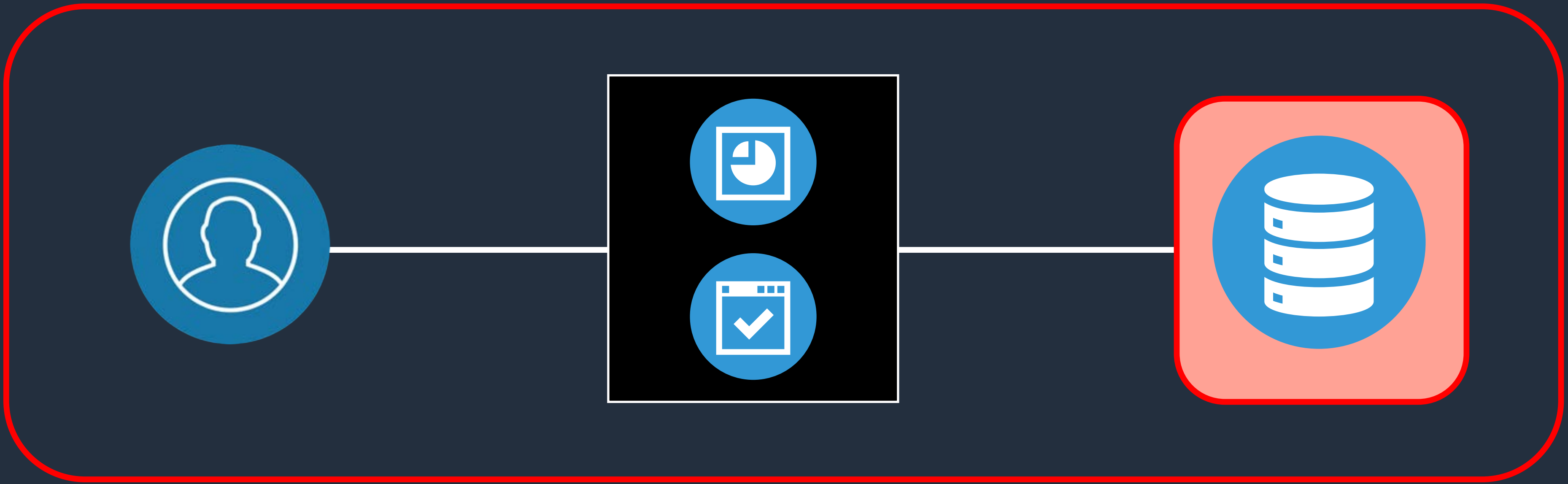
- Legitimate data requests
- Excessive data access
- Privileged users
- Insiders
- Untrusted data stores

Third Parties

- Good users
- Bad users
- Unknown users
- Compromised users

- Good code
- Unknown code
- Malicious code

Secure Information at the Data Level



Secure data access end-to-end. Protect at the data level.

Data-Centric Protection to Address Privacy Regulations

1 **You need to implement the correct technical controls to secure the data.**

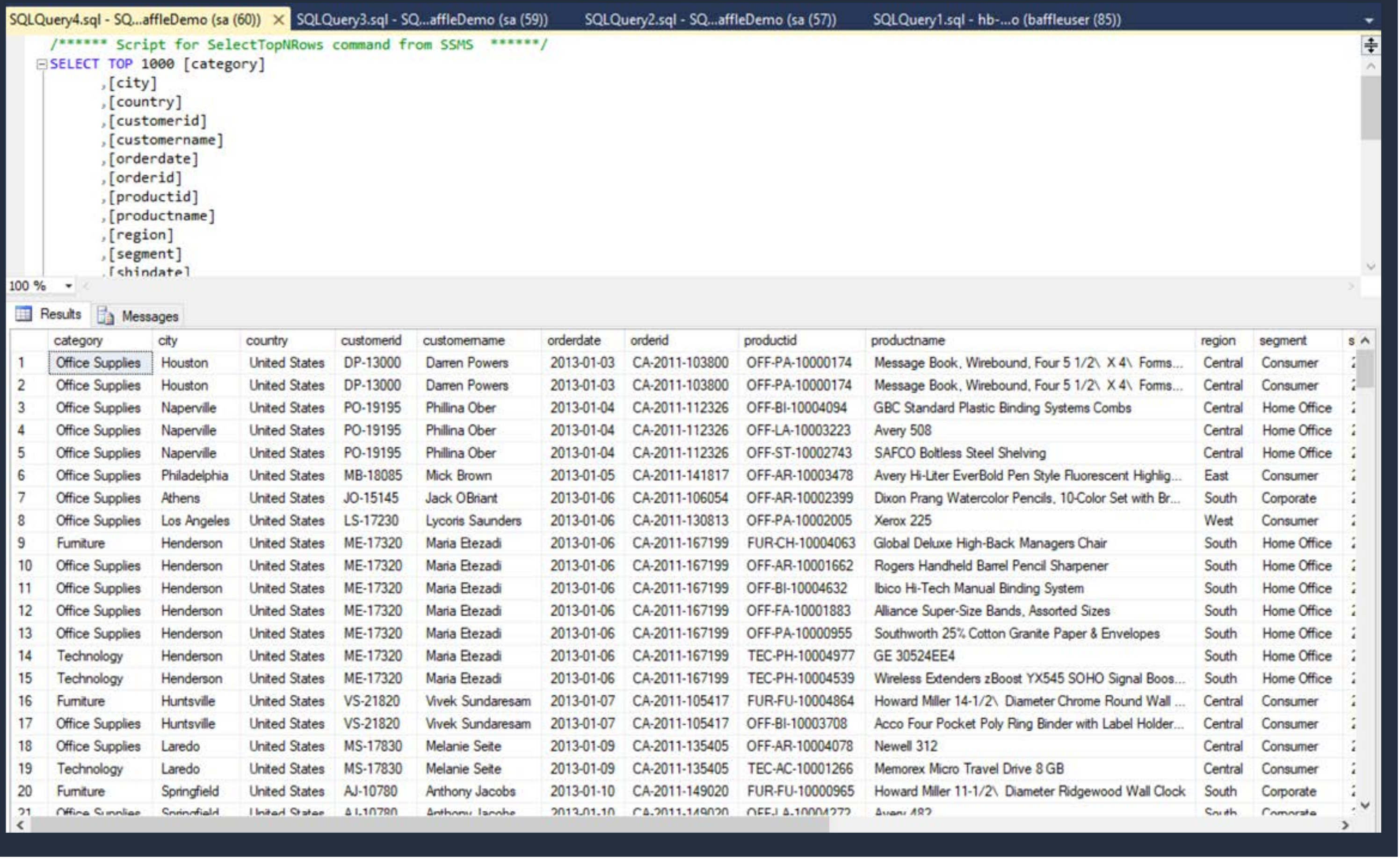
2 **All encryption does not actually protect at the data level.**

Key Benefits of Data-Centric Protection

- Protects the actual consumer data values
- Addresses encryption and redaction of data
- Easily enables the “Right to Be Forgotten”
- Requires no application code changes or architecture modifications

Non-Data-Centric Protection TDE

Transparent Data Encryption (TDE)

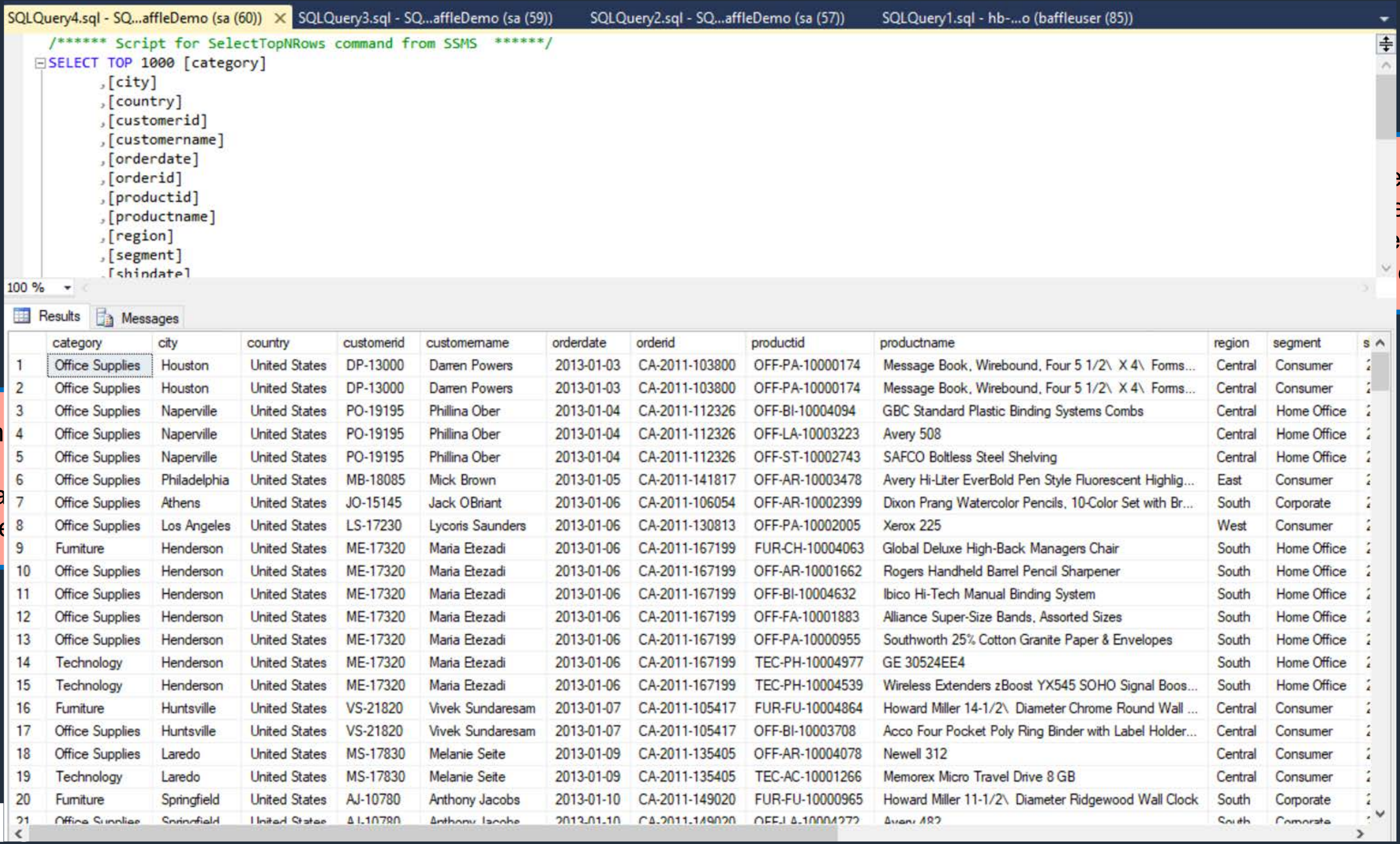

SQLQuery4.sql - SQ...affleDemo (sa (60))
SQLQuery3.sql - SQ...affleDemo (sa (59))
SQLQuery2.sql - SQ...affleDemo (sa (57))
SQLQuery1.sql - hb-...o (baffleuser (85))
100 %
Results
Messages

```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [category]
      ,[city]
      ,[country]
      ,[customerid]
      ,[customername]
      ,[orderdate]
      ,[orderid]
      ,[productid]
      ,[productname]
      ,[region]
      ,[segment]
      ,[shipdate]
```

	category	city	country	customerid	customername	orderdate	orderid	productid	productname	region	segment	s
1	Office Supplies	Houston	United States	DP-13000	Darren Powers	2013-01-03	CA-2011-103800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Forms...	Central	Consumer	
2	Office Supplies	Houston	United States	DP-13000	Darren Powers	2013-01-03	CA-2011-103800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Forms...	Central	Consumer	
3	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326	OFF-BI-10004094	GBC Standard Plastic Binding Systems Combs	Central	Home Office	
4	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326	OFF-LA-10003223	Avery 508	Central	Home Office	
5	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326	OFF-ST-10002743	SAFCO Boltless Steel Shelving	Central	Home Office	
6	Office Supplies	Philadelphia	United States	MB-18085	Mick Brown	2013-01-05	CA-2011-141817	OFF-AR-10003478	Avery Hi-Liter EverBold Pen Style Fluorescent Highlig...	East	Consumer	
7	Office Supplies	Athens	United States	JO-15145	Jack OBriant	2013-01-06	CA-2011-106054	OFF-AR-10002399	Dixon Prang Watercolor Pencils, 10-Color Set with Br...	South	Corporate	
8	Office Supplies	Los Angeles	United States	LS-17230	Lycoris Saunders	2013-01-06	CA-2011-130813	OFF-PA-10002005	Xerox 225	West	Consumer	
9	Furniture	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	FUR-CH-10004063	Global Deluxe High-Back Managers Chair	South	Home Office	
10	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-AR-10001662	Rogers Handheld Barrel Pencil Sharpener	South	Home Office	
11	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-BI-10004632	Ibico Hi-Tech Manual Binding System	South	Home Office	
12	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-FA-10001883	Alliance Super-Size Bands, Assorted Sizes	South	Home Office	
13	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-PA-10000955	Southworth 25% Cotton Granite Paper & Envelopes	South	Home Office	
14	Technology	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	TEC-PH-10004977	GE 30524EE4	South	Home Office	
15	Technology	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	TEC-PH-10004539	Wireless Extenders zBoost YX545 SOHO Signal Boos...	South	Home Office	
16	Furniture	Huntsville	United States	VS-21820	Vivek Sundaresam	2013-01-07	CA-2011-105417	FUR-FU-10004864	Howard Miller 14-1/2\ Diameter Chrome Round Wall ...	Central	Consumer	
17	Office Supplies	Huntsville	United States	VS-21820	Vivek Sundaresam	2013-01-07	CA-2011-105417	OFF-BI-10003708	Acco Four Pocket Poly Ring Binder with Label Holder...	Central	Consumer	
18	Office Supplies	Laredo	United States	MS-17830	Melanie Seite	2013-01-09	CA-2011-135405	OFF-AR-10004078	Newell 312	Central	Consumer	
19	Technology	Laredo	United States	MS-17830	Melanie Seite	2013-01-09	CA-2011-135405	TEC-AC-10001266	Memorex Micro Travel Drive 8 GB	Central	Consumer	
20	Furniture	Springfield	United States	AJ-10780	Anthony Jacobs	2013-01-10	CA-2011-149020	FUR-FU-10000965	Howard Miller 11-1/2\ Diameter Ridgewood Wall Clock	South	Corporate	
21	Office Supplies	Springfield	United States	AJ-10780	Anthony Jacobs	2013-01-10	CA-2011-149020	OFF-LA-10004272	Avery 482	South	Corporate	

- Does nothing to protect against a modern day hack or breach
- Example: Marriott was running TDE
- Anyone with access to the database sees the data in the clear
- Data in logs are in the clear
- Data in search indices are in the clear
- Data in memory are in the clear
- An attacker gaining access to the system laterally will see the data in the clear
- The encryption key is stored on the DB to decrypt all the data
- Poor key rotation support that may incur downtime

Data Breach Threat Model



SQLQuery4.sql - SQ...affleDemo (sa (60))
SQLQuery3.sql - SQ...affleDemo (sa (59))
SQLQuery2.sql - SQ...affleDemo (sa (57))
SQLQuery1.sql - hb-...o (baffleuser (85))
100 %
Results
Messages

```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [category]
      ,[city]
      ,[country]
      ,[customerid]
      ,[customername]
      ,[orderdate]
      ,[orderid]
      ,[productid]
      ,[productname]
      ,[region]
      ,[segment]
      ,[shipdate]
```

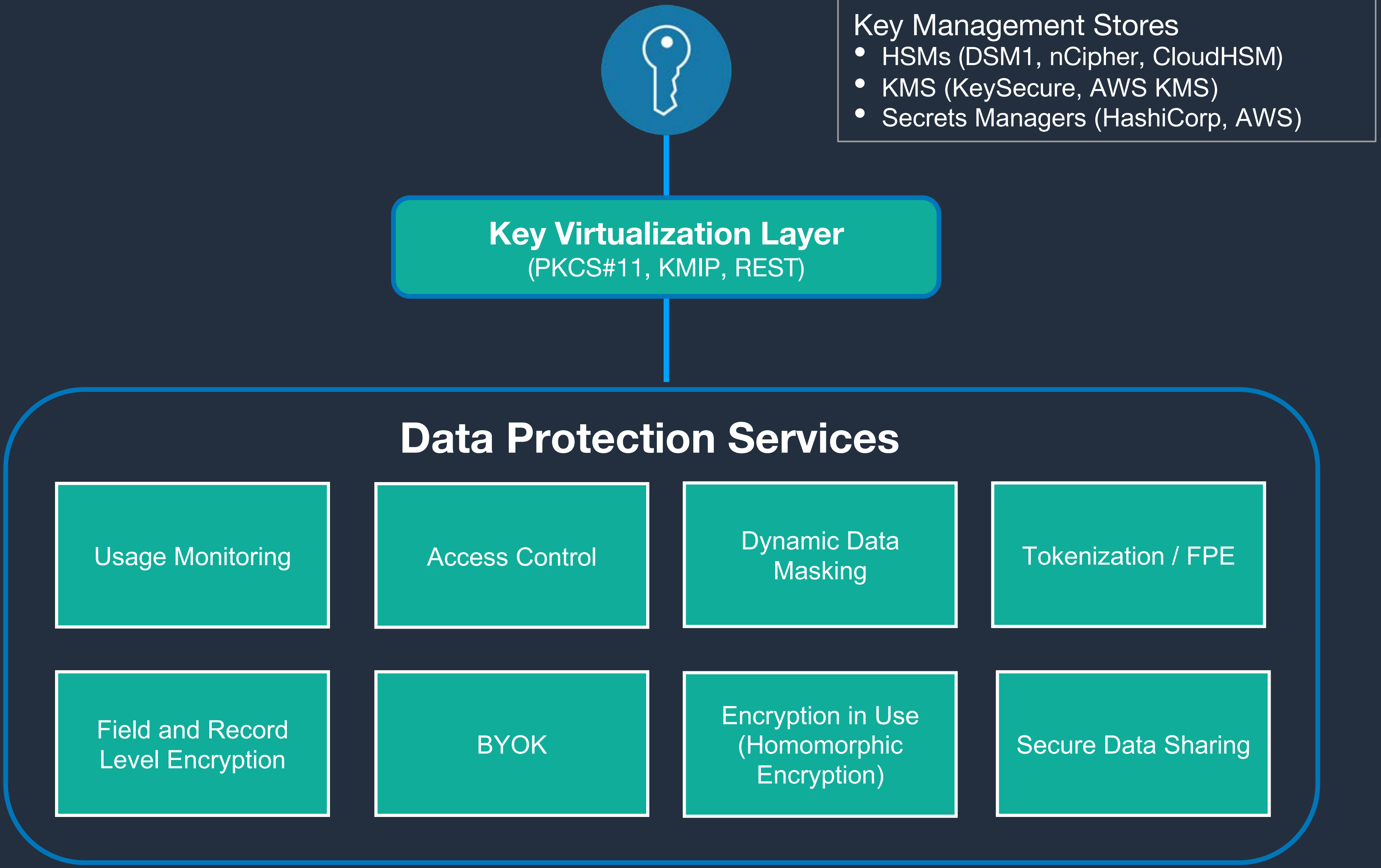
	category	city	country	customerid	customername	orderdate	orderid	productid	productname	region	segment	s
1	Office Supplies	Houston	United States	DP-13000	Darren Powers	2013-01-03	CA-2011-103800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Forms...	Central	Consumer	2
2	Office Supplies	Houston	United States	DP-13000	Darren Powers	2013-01-03	CA-2011-103800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Forms...	Central	Consumer	2
3	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326	OFF-BI-10004094	GBC Standard Plastic Binding Systems Combs	Central	Home Office	2
4	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326	OFF-LA-10003223	Avery 508	Central	Home Office	2
5	Office Supplies	Naperville	United States	PO-19195	Phillina Ober	2013-01-04	CA-2011-112326	OFF-ST-10002743	SAFCO Boltless Steel Shelving	Central	Home Office	2
6	Office Supplies	Philadelphia	United States	MB-18085	Mick Brown	2013-01-05	CA-2011-141817	OFF-AR-10003478	Avery Hi-Liter EverBold Pen Style Fluorescent Highlig...	East	Consumer	2
7	Office Supplies	Athens	United States	JO-15145	Jack OBriant	2013-01-06	CA-2011-106054	OFF-AR-10002399	Dixon Prang Watercolor Pencils, 10-Color Set with Br...	South	Corporate	2
8	Office Supplies	Los Angeles	United States	LS-17230	Lycoris Saunders	2013-01-06	CA-2011-130813	OFF-PA-10002005	Xerox 225	West	Consumer	2
9	Furniture	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	FUR-CH-10004063	Global Deluxe High-Back Managers Chair	South	Home Office	2
10	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-AR-10001662	Rogers Handheld Barrel Pencil Sharpener	South	Home Office	2
11	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-BI-10004632	Ibico Hi-Tech Manual Binding System	South	Home Office	2
12	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-FA-10001883	Alliance Super-Size Bands, Assorted Sizes	South	Home Office	2
13	Office Supplies	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	OFF-PA-10000955	Southworth 25% Cotton Granite Paper & Envelopes	South	Home Office	2
14	Technology	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	TEC-PH-10004977	GE 30524EE4	South	Home Office	2
15	Technology	Henderson	United States	ME-17320	Maria Etezadi	2013-01-06	CA-2011-167199	TEC-PH-10004539	Wireless Extenders zBoost YX545 SOHO Signal Boos...	South	Home Office	2
16	Furniture	Huntsville	United States	VS-21820	Vivek Sundaresam	2013-01-07	CA-2011-105417	FUR-FU-10004864	Howard Miller 14-1/2\ Diameter Chrome Round Wall ...	Central	Consumer	2
17	Office Supplies	Huntsville	United States	VS-21820	Vivek Sundaresam	2013-01-07	CA-2011-105417	OFF-BI-10003708	Acco Four Pocket Poly Ring Binder with Label Holder...	Central	Consumer	2
18	Office Supplies	Laredo	United States	MS-17830	Melanie Seite	2013-01-09	CA-2011-135405	OFF-AR-10004078	Newell 312	Central	Consumer	2
19	Technology	Laredo	United States	MS-17830	Melanie Seite	2013-01-09	CA-2011-135405	TEC-AC-10001266	Memorex Micro Travel Drive 8 GB	Central	Consumer	2
20	Furniture	Springfield	United States	AJ-10780	Anthony Jacobs	2013-01-10	CA-2011-149020	FUR-FU-10000965	Howard Miller 11-1/2\ Diameter Ridgewood Wall Clock	South	Corporate	2
21	Office Supplies	Springfield	United States	AJ-10780	Anthony Jacobs	2013-01-10	CA-2011-149020	OFF-LA-10004272	Avery 482	South	Corporate	[illegible]

er moving
ets your data in
even if you use
cryption at-rest

Com
third
extra
in the

Data-Centric Methods to Protect Data

Data Protection Services



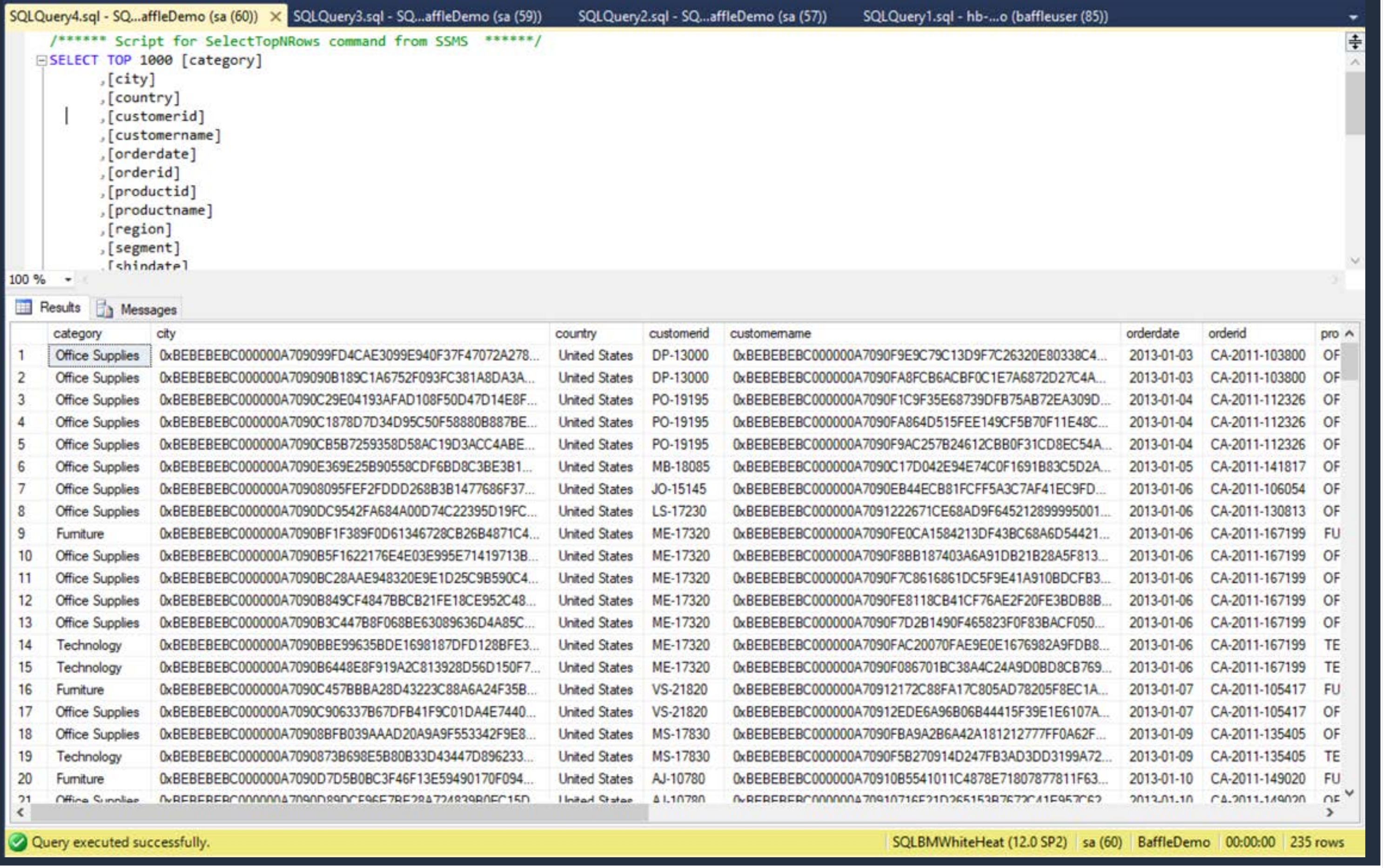
Key Management Stores

- HSMs (DSM1, nCipher, CloudHSM)
- KMS (KeySecure, AWS KMS)
- Secrets Managers (HashiCorp, AWS)

Key Virtualization Layer
(PKCS#11, KMIP, REST)
Data Protection Services
Usage Monitoring
Access Control
Dynamic Data Masking
Tokenization / FPE
Field and Record Level Encryption
BYOK
Encryption in Use (Homomorphic Encryption)
Secure Data Sharing

Data-Centric Encryption Method

Data-Centric Encryption



SQLQuery4.sql - SQ...affleDemo (sa (60))
SQLQuery3.sql - SQ...affleDemo (sa (59))
SQLQuery2.sql - SQ...affleDemo (sa (57))
SQLQuery1.sql - hb-...o (baffleuser (85))
100 %
Results
Messages

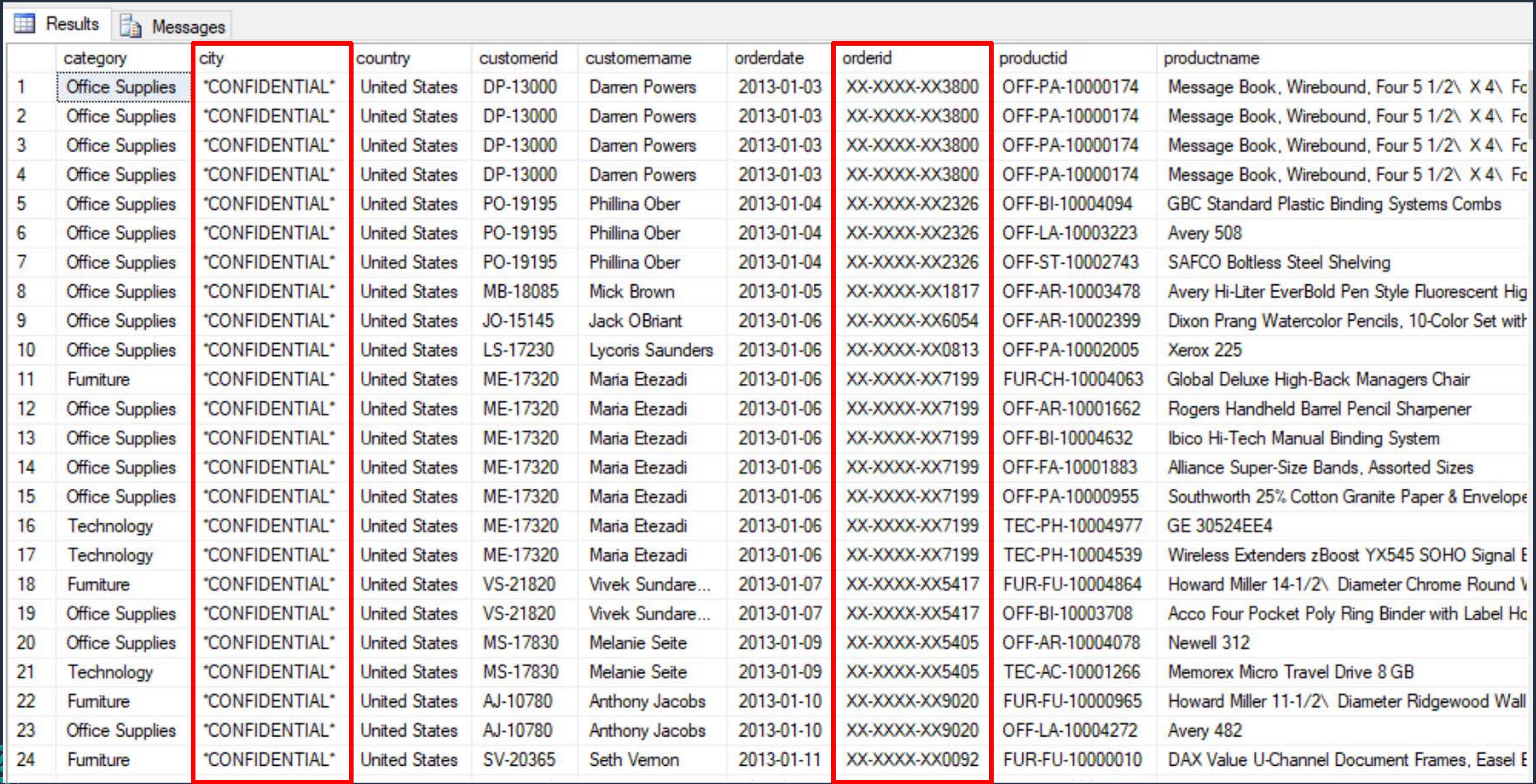
```sql
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [category]
      ,[city]
      ,[country]
      ,[customerid]
      ,[customername]
      ,[orderdate]
      ,[orderid]
      ,[productid]
      ,[productname]
      ,[region]
      ,[segment]
      ,[shipdate]
```

	category	city	country	customerid	customername	orderdate	orderid	pro
1	Office Supplies	0xBEBEBEBC000000A709099FD4CAE3099E940F37F47072A278...	United States	DP-13000	0xBEBEBEBC000000A7090F9E9C79C13D9F7C26320E80338C4...	2013-01-03	CA-2011-103800	OF
2	Office Supplies	0xBEBEBEBC000000A709090B189C1A6752F093FC381A8DA3A...	United States	DP-13000	0xBEBEBEBC000000A7090FA8FCB6ACBF0C1E7A6872D27C4A...	2013-01-03	CA-2011-103800	OF
3	Office Supplies	0xBEBEBEBC000000A7090C29E04193AFAD108F50D47D14E8F...	United States	PO-19195	0xBEBEBEBC000000A7090F1C9F35E68739DFB75AB72EA309D...	2013-01-04	CA-2011-112326	OF
4	Office Supplies	0xBEBEBEBC000000A7090C1878D7D34D95C50F58880B887BE...	United States	PO-19195	0xBEBEBEBC000000A7090FA864D515FEE149CF5B70F11E48C...	2013-01-04	CA-2011-112326	OF
5	Office Supplies	0xBEBEBEBC000000A7090CB5B7259358D58AC19D3ACC4ABE...	United States	PO-19195	0xBEBEBEBC000000A7090F9AC257B24612CBB0F31CD8EC54A...	2013-01-04	CA-2011-112326	OF
6	Office Supplies	0xBEBEBEBC000000A7090E369E25B90558CDF6BD8C3BE3B1...	United States	MB-18085	0xBEBEBEBC000000A7090C17D042E94E74C0F1691B83C5D2A...	2013-01-05	CA-2011-141817	OF
7	Office Supplies	0xBEBEBEBC000000A70908095FEF2FDDD268B3B1477686F37...	United States	JO-15145	0xBEBEBEBC000000A7090EB44ECB81FCFF5A3C7AF41EC9FD...	2013-01-06	CA-2011-106054	OF
8	Office Supplies	0xBEBEBEBC000000A7090DC9542FA684A00D74C22395D19FC...	United States	LS-17230	0xBEBEBEBC000000A7091222671CE68AD9F64521289995001...	2013-01-06	CA-2011-130813	OF
9	Furniture	0xBEBEBEBC000000A7090BF1F389F0D61346728CB26B4871C4...	United States	ME-17320	0xBEBEBEBC000000A7090FE0CA1584213DF43BC68A6D54421...	2013-01-06	CA-2011-167199	FU
10	Office Supplies	0xBEBEBEBC000000A7090B5F1622176E4E03E995E71419713B...	United States	ME-17320	0xBEBEBEBC000000A7090F8BB187403A6A91DB21B28A5F813...	2013-01-06	CA-2011-167199	OF
11	Office Supplies	0xBEBEBEBC000000A7090BC28AAE948320E9E1D25C9B590C4...	United States	ME-17320	0xBEBEBEBC000000A7090F7C8616861DC5F9E41A910BDCFB3...	2013-01-06	CA-2011-167199	OF
12	Office Supplies	0xBEBEBEBC000000A7090B849CF4847BBCB21FE18CE952C48...	United States	ME-17320	0xBEBEBEBC000000A7090FE8118CB41CF76AE2F20FE3BDB8B...	2013-01-06	CA-2011-167199	OF
13	Office Supplies	0xBEBEBEBC000000A7090B3C447B8F068BE63089636D4A85C...	United States	ME-17320	0xBEBEBEBC000000A7090F7D2B1490F465823F0F83BACF050...	2013-01-06	CA-2011-167199	OF
14	Technology	0xBEBEBEBC000000A7090BBE99635BDE1698187DFD128BFE3...	United States	ME-17320	0xBEBEBEBC000000A7090FAC20070FAE9E0E1676982A9FDB8...	2013-01-06	CA-2011-167199	TE
15	Technology	0xBEBEBEBC000000A7090B6448E8F919A2C813928D56D150F7...	United States	ME-17320	0xBEBEBEBC000000A7090F086701BC38A4C24A9D0BD8CB769...	2013-01-06	CA-2011-167199	TE
16	Furniture	0xBEBEBEBC000000A7090C457BBBA28D43223C88A6A24F35B...	United States	VS-21820	0xBEBEBEBC000000A70912172C88FA17C805AD78205F8EC1A...	2013-01-07	CA-2011-105417	FU
17	Office Supplies	0xBEBEBEBC000000A7090C906337B67DFB41F9C01DA4E7440...	United States	VS-21820	0xBEBEBEBC000000A70912EDE6A96B06B44415F39E1E6107A...	2013-01-07	CA-2011-105417	OF
18	Office Supplies	0xBEBEBEBC000000A70908BFB039AAAD20A9A9F553342F9E8...	United States	MS-17830	0xBEBEBEBC000000A7090FBA9A2B6A42A181212777FF0A62F...	2013-01-09	CA-2011-135405	OF
19	Technology	0xBEBEBEBC000000A7090873B698E5B80B33D43447D896233...	United States	MS-17830	0xBEBEBEBC000000A7090F5B270914D247FB3AD3DD3199A72...	2013-01-09	CA-2011-135405	TE
20	Furniture	0xBEBEBEBC000000A7090D7D5B0BC3F46F13E59490170F094...	United States	AJ-10780	0xBEBEBEBC000000A70910B5541011C4878E71807877811F63...	2013-01-10	CA-2011-149020	FU
21	Office Supplies	0xBEBEBEBC000000A7090D89DCF96F7BF28A724839B0FC15D...	United States	AJ-10780	0xBEBEBEBC000000A70910716F21D265153B7672C41F957C62...	2013-01-10	CA-2011-149020	OF

Query executed successfully. | SQLBMWhiteHeat (12.0 SP2) | sa (60) | BaffleDemo | 00:00:00 | 235 rows

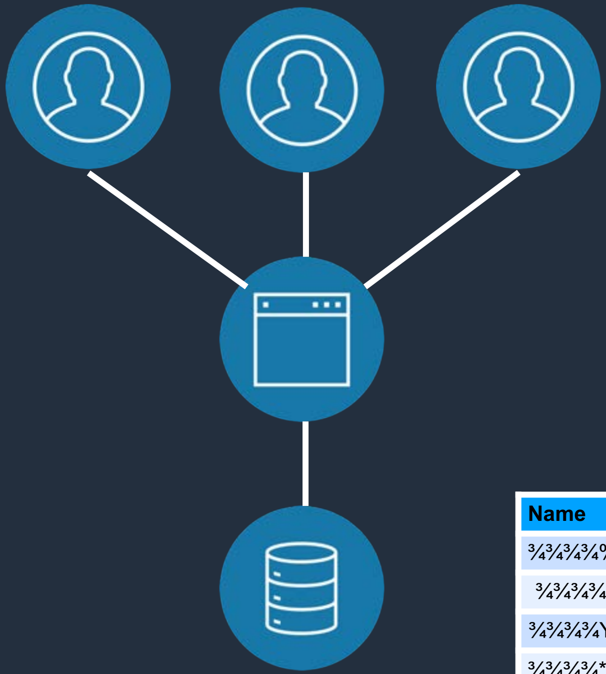
- Privileged users and insiders with access to the system sees the data encrypted
- Attackers accessing the system laterally through the network see encrypted data
- Data in logs are encrypted
- Data is memory are encrypted
- Data in search indices are encrypted
- Supports key rotation and multiple key versions
- Encryption keys are not stored on the database
- Supports data shredding for compliance with privacy regulations

Data-Centric Masking and Redaction



	category	city	country	customerid	customername	orderdate	orderid	productid	productname
1	Office Supplies	*CONFIDENTIAL*	United States	DP-13000	Darren Powers	2013-01-03	XX-XXXX-XX3800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Fo
2	Office Supplies	*CONFIDENTIAL*	United States	DP-13000	Darren Powers	2013-01-03	XX-XXXX-XX3800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Fo
3	Office Supplies	*CONFIDENTIAL*	United States	DP-13000	Darren Powers	2013-01-03	XX-XXXX-XX3800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Fo
4	Office Supplies	*CONFIDENTIAL*	United States	DP-13000	Darren Powers	2013-01-03	XX-XXXX-XX3800	OFF-PA-10000174	Message Book, Wirebound, Four 5 1/2\ X 4\ Fo
5	Office Supplies	*CONFIDENTIAL*	United States	PO-19195	Phillina Ober	2013-01-04	XX-XXXX-XX2326	OFF-BI-10004094	GBC Standard Plastic Binding Systems Combs
6	Office Supplies	*CONFIDENTIAL*	United States	PO-19195	Phillina Ober	2013-01-04	XX-XXXX-XX2326	OFF-LA-10003223	Avery 508
7	Office Supplies	*CONFIDENTIAL*	United States	PO-19195	Phillina Ober	2013-01-04	XX-XXXX-XX2326	OFF-ST-10002743	SAFCO Boltless Steel Shelving
8	Office Supplies	*CONFIDENTIAL*	United States	MB-18085	Mick Brown	2013-01-05	XX-XXXX-XX1817	OFF-AR-10003478	Avery Hi-Liter EverBold Pen Style Fluorescent Hig
9	Office Supplies	*CONFIDENTIAL*	United States	JO-15145	Jack OBriant	2013-01-06	XX-XXXX-XX6054	OFF-AR-10002399	Dixon Prang Watercolor Pencils, 10-Color Set with
10	Office Supplies	*CONFIDENTIAL*	United States	LS-17230	Lycoris Saunders	2013-01-06	XX-XXXX-XX0813	OFF-PA-10002005	Xerox 225
11	Furniture	*CONFIDENTIAL*	United States	ME-17320	Maria Etezadi	2013-01-06	XX-XXXX-XX7199	FUR-CH-10004063	Global Deluxe High-Back Managers Chair
12	Office Supplies	*CONFIDENTIAL*	United States	ME-17320	Maria Etezadi	2013-01-06	XX-XXXX-XX7199	OFF-AR-10001662	Rogers Handheld Barrel Pencil Sharpener
13	Office Supplies	*CONFIDENTIAL*	United States	ME-17320	Maria Etezadi	2013-01-06	XX-XXXX-XX7199	OFF-BI-10004632	Ibico Hi-Tech Manual Binding System
14	Office Supplies	*CONFIDENTIAL*	United States	ME-17320	Maria Etezadi	2013-01-06	XX-XXXX-XX7199	OFF-FA-10001883	Alliance Super-Size Bands, Assorted Sizes
15	Office Supplies	*CONFIDENTIAL*	United States	ME-17320	Maria Etezadi	2013-01-06	XX-XXXX-XX7199	OFF-PA-10000955	Southworth 25% Cotton Granite Paper & Envelope
16	Technology	*CONFIDENTIAL*	United States	ME-17320	Maria Etezadi	2013-01-06	XX-XXXX-XX7199	TEC-PH-10004977	GE 30524EE4
17	Technology	*CONFIDENTIAL*	United States	ME-17320	Maria Etezadi	2013-01-06	XX-XXXX-XX7199	TEC-PH-10004539	Wireless Extenders zBoost YX545 SOHO Signal B
18	Furniture	*CONFIDENTIAL*	United States	VS-21820	Vivek Sundare...	2013-01-07	XX-XXXX-XX5417	FUR-FU-10004864	Howard Miller 14-1/2\ Diameter Chrome Round W
19	Office Supplies	*CONFIDENTIAL*	United States	VS-21820	Vivek Sundare...	2013-01-07	XX-XXXX-XX5417	OFF-BI-10003708	Acco Four Pocket Poly Ring Binder with Label Ho
20	Office Supplies	*CONFIDENTIAL*	United States	MS-17830	Melanie Seite	2013-01-09	XX-XXXX-XX5405	OFF-AR-10004078	Newell 312
21	Technology	*CONFIDENTIAL*	United States	MS-17830	Melanie Seite	2013-01-09	XX-XXXX-XX5405	TEC-AC-10001266	Memorex Micro Travel Drive 8 GB
22	Furniture	*CONFIDENTIAL*	United States	AJ-10780	Anthony Jacobs	2013-01-10	XX-XXXX-XX9020	FUR-FU-10000965	Howard Miller 11-1/2\ Diameter Ridgewood Wall
23	Office Supplies	*CONFIDENTIAL*	United States	AJ-10780	Anthony Jacobs	2013-01-10	XX-XXXX-XX9020	OFF-LA-10004272	Avery 482
24	Furniture	*CONFIDENTIAL*	United States	SV-20365	Seth Vernon	2013-01-11	XX-XXXX-XX0092	FUR-FU-10000010	DAX Value U-Channel Document Frames, Easel B

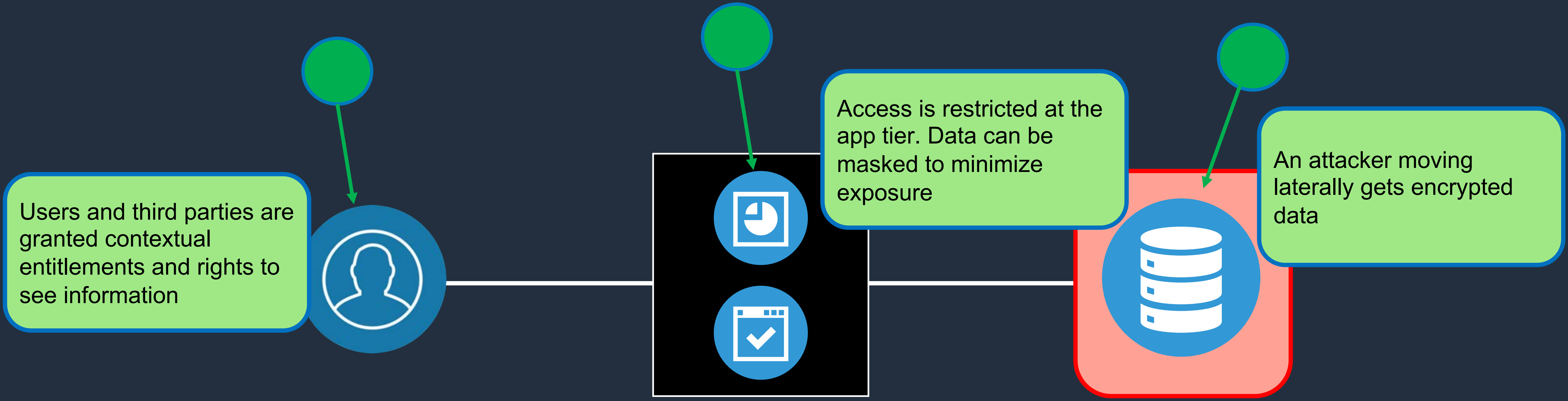
Enabling Dynamic Entitlements and Right of Revocation



Name	Date	Transaction	Credit Card
¾¾¾¾%^&#@	2/1/13	¾¾¾¾rjkkjkjkj23	¾¾¾¾r□ÕS:VÞýÉ
¾¾¾¾MN<*&	2/13/13	¾¾¾¾,.<>/;{}\dd	¾¾¾¾r°+x□,êS6
¾¾¾¾YUt45^#	2/14/13	¾¾¾¾&*^%$#@	¾¾¾¾r°+x□x□@#$r
¾¾¾¾*&^ty72	2/18/13	¾¾¾¾UIU^&$#9	¾¾¾¾r°+x□(527x□
¾¾¾¾jkj789d	1/10/13	¾¾¾¾*7%4lk;8	¾¾¾¾r°+*702jmkib

- Support billions of key mappings at the record level
- Enables data shredding and “right to be forgotten” per data owner
- Selective data masking for different data owners

Data Breach Threat Model with Data-Centric Protection



Users and third parties are granted contextual entitlements and rights to see information

Access is restricted at the app tier. Data can be masked to minimize exposure

An attacker moving laterally gets encrypted data

Secure data access end-to-end. Protect at the data level.

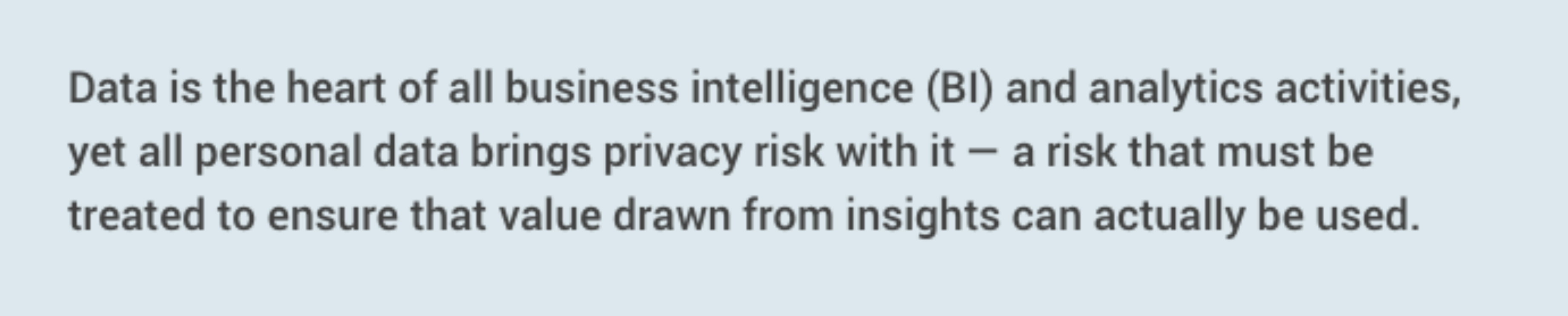
Demo #1 – Data-Centric Controls

Privacy Preserving Analytics and Secure Data Sharing

Privacy Preserving Analytics

What is it?

- A computational method that allows for operations, processing and analysis of data without revealing the underlying data values or violating the data privacy contract.



Data is the heart of all business intelligence (BI) and analytics activities, yet all personal data brings privacy risk with it — a risk that must be treated to ensure that value drawn from insights can actually be used.

Gartner Report on Privacy Preservation in Analytics

More info and resources: **https://baffle.io/privacy**

Secure Data Sharing

What is it?

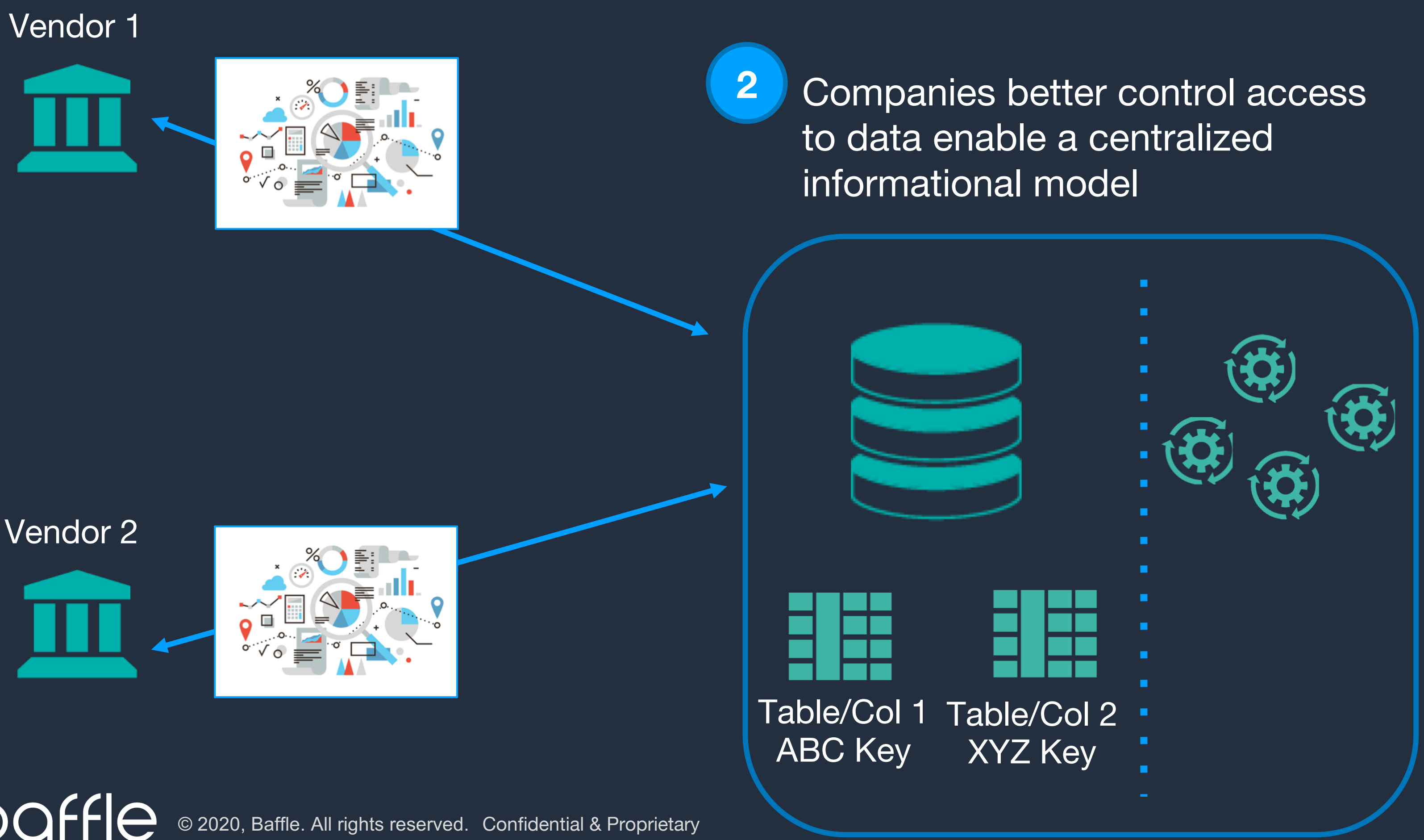
- A method that allows data to be used for intelligence or aggregate analysis across multiple parties, without revealing the underlying data values or violating the data privacy contract.

USE CASE

Data as a Service - 3rd Party Data Access Control

1 3rd party organizations can be granted granular access to a subset of a data store

2 Companies better control access to data enable a centralized informational model



Key Benefits

- Organizations can control and minimize data sharing via a centralized data model
- Rather than spend time vetting 3rd parties via questionnaires and then giving the your data, allow them to securely integrate into your centralized data management structure
- Achieve the benefits of sourcing specific operations, without compromising your security posture

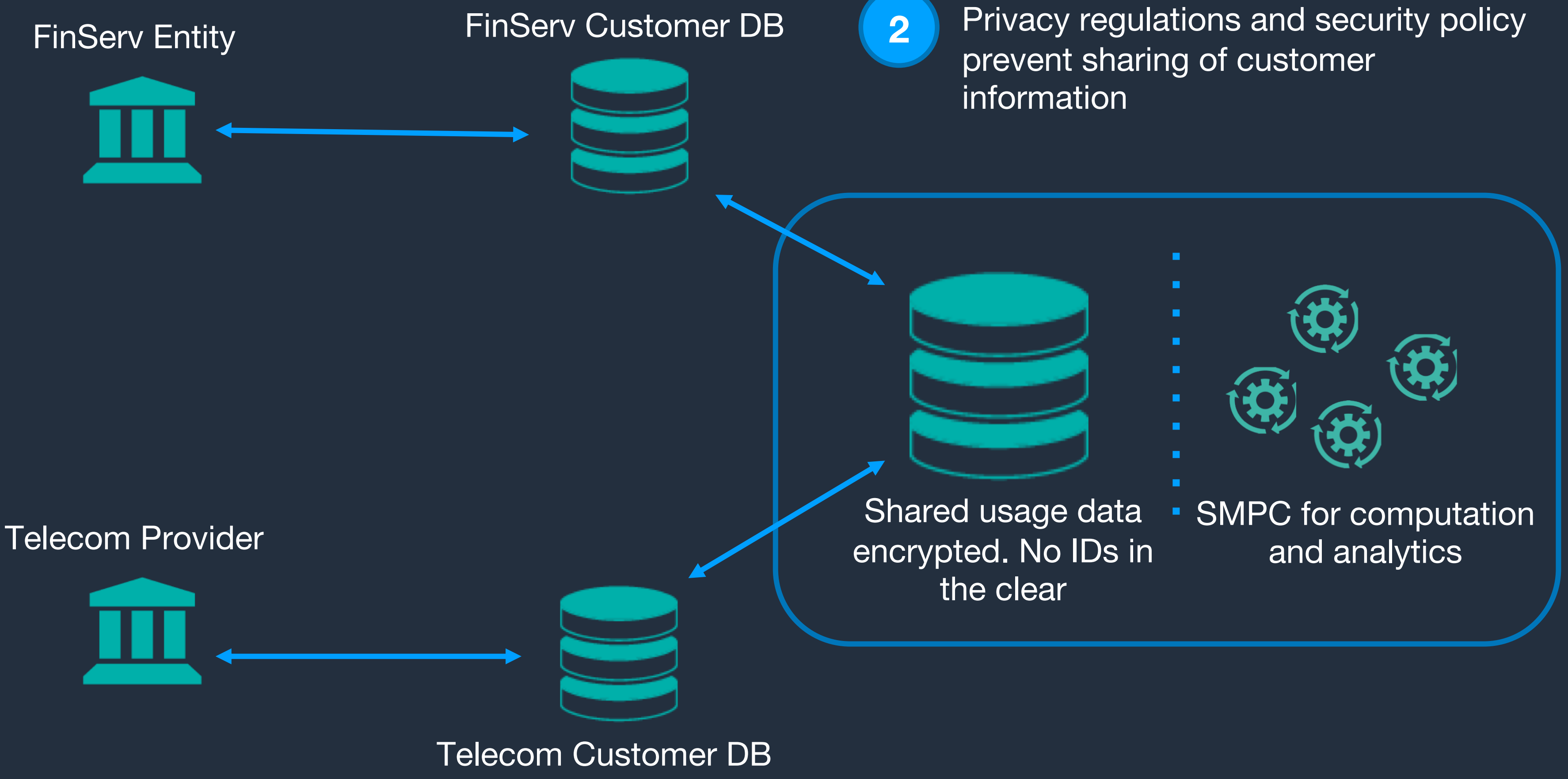
USE CASE

Cross-Party Data Sharing

1 Two entities believe that sharing of usage and access data will enhance fraud detection

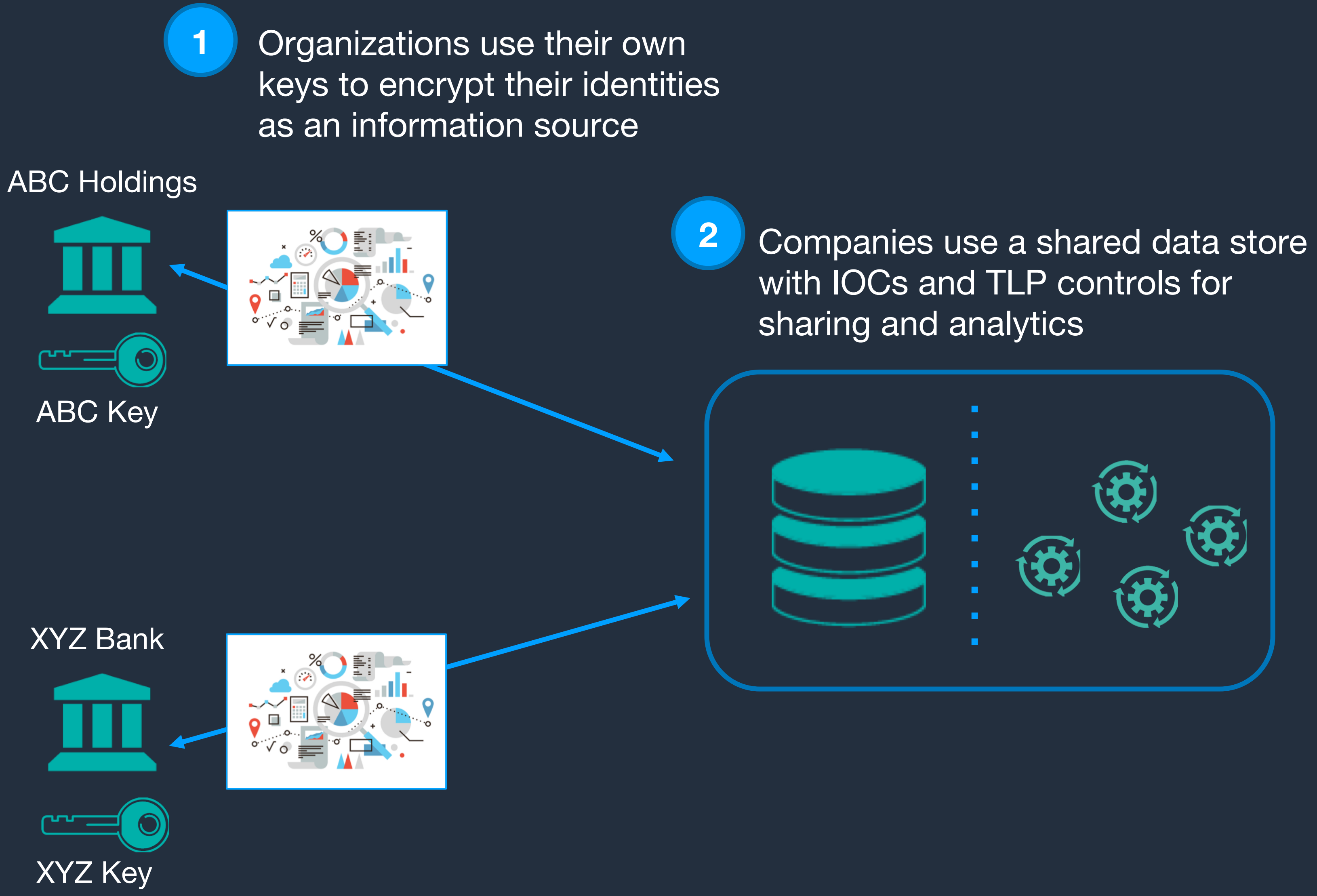
2 Privacy regulations and security policy prevent sharing of customer information

3 The shared data store is treated as an untrusted entity, but still allows for encrypted queries and operations.


FinServ Entity
FinServ Customer DB
Shared usage data encrypted. No IDs in the clear
SMPC for computation and analytics
Telecom Provider
Telecom Customer DB

USE CASE

Anonymized Threat Intel Sharing


1
Organizations use their own keys to encrypt their identities as an information source
ABC Holdings
ABC Key
2
Companies use a shared data store with IOCs and TLP controls for sharing and analytics
XYZ Bank
XYZ Key

Key Benefits

- Participating organizations encrypt threat intel before sending to a shared repository
- Threat intel application can analyze encrypted data from all organizations and generate valuable insights to benefit all participants

Demo #2 – Privacy Preserving Analytics

Baffle Privacy Preserving Analytics

Secure Computation on Encrypted Data

Baffle SMPC Implementation

Name	Date	Transaction	Credit Card
Sanjit Chand	2/1/13	$78.28	4556813980198887
Guy Armstrong	2/13/13	$48.50	5442422511459373
Michael Grace	2/14/13	$11.75	6011722895036963
Sue Ann Reed	2/18/13	$59.87	5197497496125980
Steven Roelle	1/10/13	$29.56	4532521184024986

Customer Owned Key

Key Management (KMIP or PKCS #11) – Utilize existing protocols such as KMIP or HSM interfaces such as PKCS #11 to source keys from existing key stores

Baffle SMPC Implementation

Name	Date	Transaction	Credit Card
Sanjit Chand	2/1/13	$78.28	4556813980198887
Guy Armstrong	2/13/13	$48.50	5442422511459373
Michael Grace	2/14/13	$11.75	6011722895036963
Sue Ann Reed	2/18/13	$59.87	5197497496125980
Steven Roelle	1/10/13	$29.56	4532521184024986

AES Encryption

Name	Date	Transaction	Credit Card
¾¾¾¾%^&#@	2/1/13	¾¾¾¾rjkkjkjkj23	¾¾¾¾r□ÕS:VÞýÉ
¾¾¾¾MN<*&	2/13/13	¾¾¾¾,.<>/;{}\dd	¾¾¾¾r°+x□,êS6
¾¾¾¾YUt45^#	2/14/13	¾¾¾¾&*^%$#@	¾¾¾¾r°+x□x□@#$r
¾¾¾¾*&^ty72	2/18/13	¾¾¾¾UIU^&$#9	¾¾¾¾r°+x□(527x□
¾¾¾¾jkj789d	1/10/13	¾¾¾¾*7%4lk;8	¾¾¾¾r°+*702jmkib

Customer Owned Key

Key Management (KMIP or PKCS #11) – Utilize existing protocols such as KMIP or HSM interfaces such as PKCS #11 to source keys from existing key stores

AES Encryption – Implements AES algorithms for field level encryption. Leverages hardware acceleration

Baffle SMPC Implementation

Name	Date	Transaction	Credit Card
Sanjit Chand	2/1/13	$78.28	4556813980198887
Guy Armstrong	2/13/13	$48.50	5442422511459373
Michael Grace	2/14/13	$11.75	6011722895036963
Sue Ann Reed	2/18/13	$59.87	5197497496125980
Steven Roelle	1/10/13	$29.56	4532521184024986

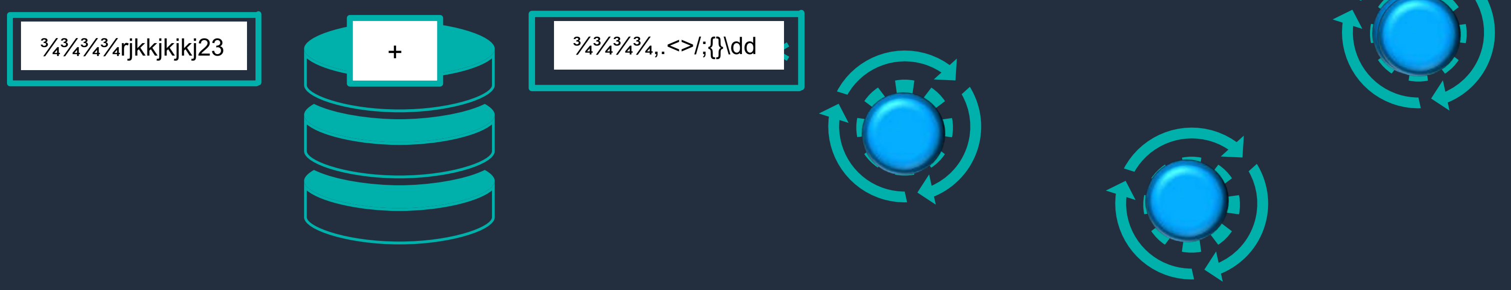
AES Encryption

Name	Date	Transaction	Credit Card
¾¾¾¾%^&#@	2/1/13	¾¾¾¾rjkkjkjkj23	¾¾¾¾r□ÕS:VÞýÉ
¾¾¾¾MN<*&	2/13/13	¾¾¾¾,.<>/;{}\dd	¾¾¾¾r°+x□,êS6
¾¾¾¾YUt45^#	2/14/13	¾¾¾¾&*^%$#@	¾¾¾¾r°+x□x□@#$r
¾¾¾¾*&^ty72	2/18/13	¾¾¾¾UIU^&$#9	¾¾¾¾r°+x□(527x□
¾¾¾¾jkj789d	1/10/13	¾¾¾¾*7%4lk;8	¾¾¾¾r°+*702jmkib

Customer Owned Key

Key Management (KMIP or PKCS #11) – Utilize existing protocols such as KMIP or HSM interfaces such as PKCS #11 to source keys from existing key stores

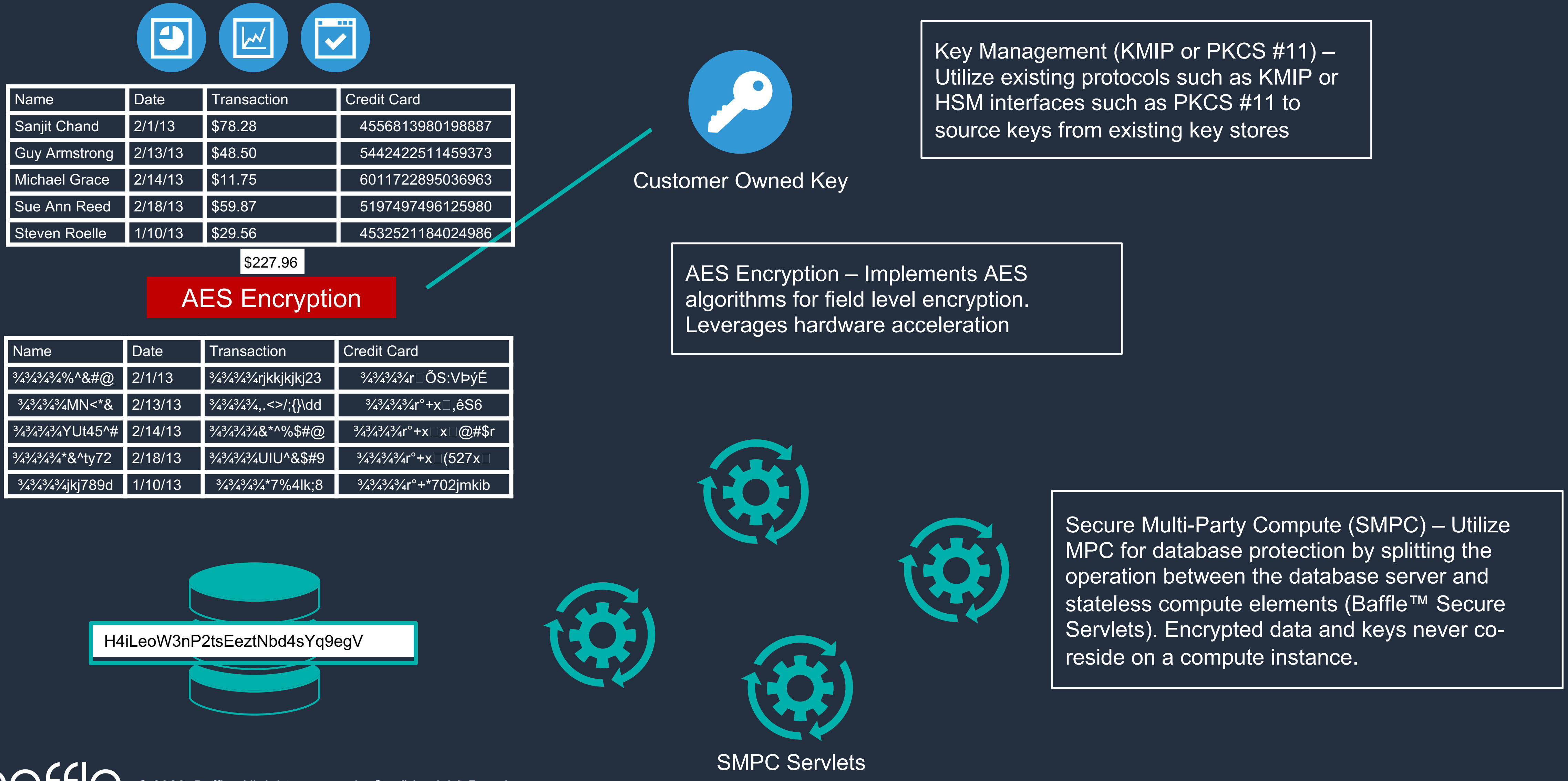
AES Encryption – Implements AES algorithms for field level encryption. Leverages hardware acceleration



Secure Multi-Party Compute (SMPC) – Utilize MPC for database protection by splitting the operation between the database server and stateless compute elements (Baffle™ Secure Servlets). Encrypted data and keys never co-reside on a compute instance.

SMPC Servlets

Baffle SMPC Implementation



Name	Date	Transaction	Credit Card
Sanjit Chand	2/1/13	$78.28	4556813980198887
Guy Armstrong	2/13/13	$48.50	5442422511459373
Michael Grace	2/14/13	$11.75	6011722895036963
Sue Ann Reed	2/18/13	$59.87	5197497496125980
Steven Roelle	1/10/13	$29.56	4532521184024986

$227.96

AES Encryption

Name	Date	Transaction	Credit Card
¾¾¾¾%^&#@	2/1/13	¾¾¾¾rjkkjkjkj23	¾¾¾¾r□ÕS:VÞýÉ
¾¾¾¾MN<*&	2/13/13	¾¾¾¾,.<>/;{}\dd	¾¾¾¾r°+x□,êS6
¾¾¾¾YUt45^#	2/14/13	¾¾¾¾&*^%$#@	¾¾¾¾r°+x□x□@#$r
¾¾¾¾*&^ty72	2/18/13	¾¾¾¾UIU^&$#9	¾¾¾¾r°+x□(527x□
¾¾¾¾jkj789d	1/10/13	¾¾¾¾*7%4lk;8	¾¾¾¾r°+*702jmkib

H4iLeoW3nP2tsEeztNbd4sYq9egV

Customer Owned Key

Key Management (KMIP or PKCS #11) – Utilize existing protocols such as KMIP or HSM interfaces such as PKCS #11 to source keys from existing key stores

AES Encryption – Implements AES algorithms for field level encryption. Leverages hardware acceleration

Secure Multi-Party Compute (SMPC) – Utilize MPC for database protection by splitting the operation between the database server and stateless compute elements (Baffle™ Secure Servlets). Encrypted data and keys never co-reside on a compute instance.

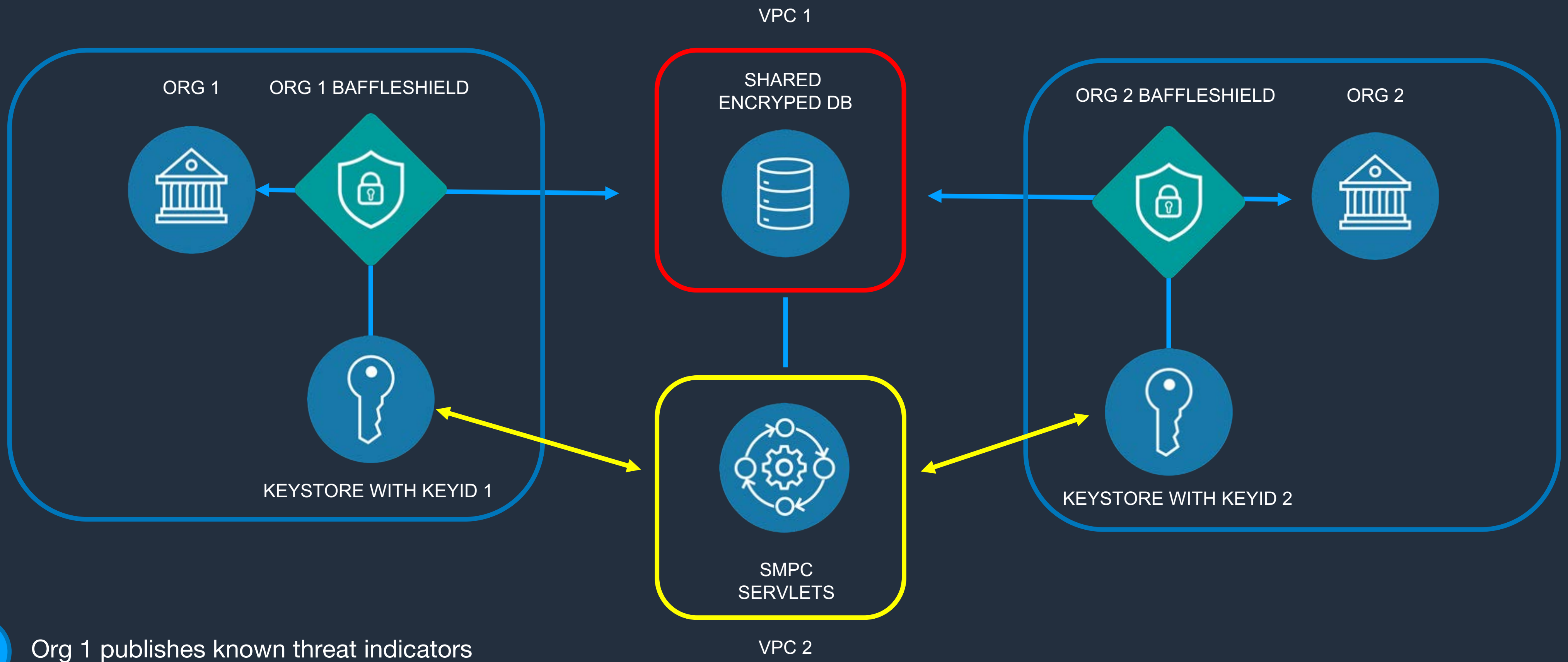
SMPC Servlets

Secure Data Sharing

Share Data without “Sharing” It

USE CASE

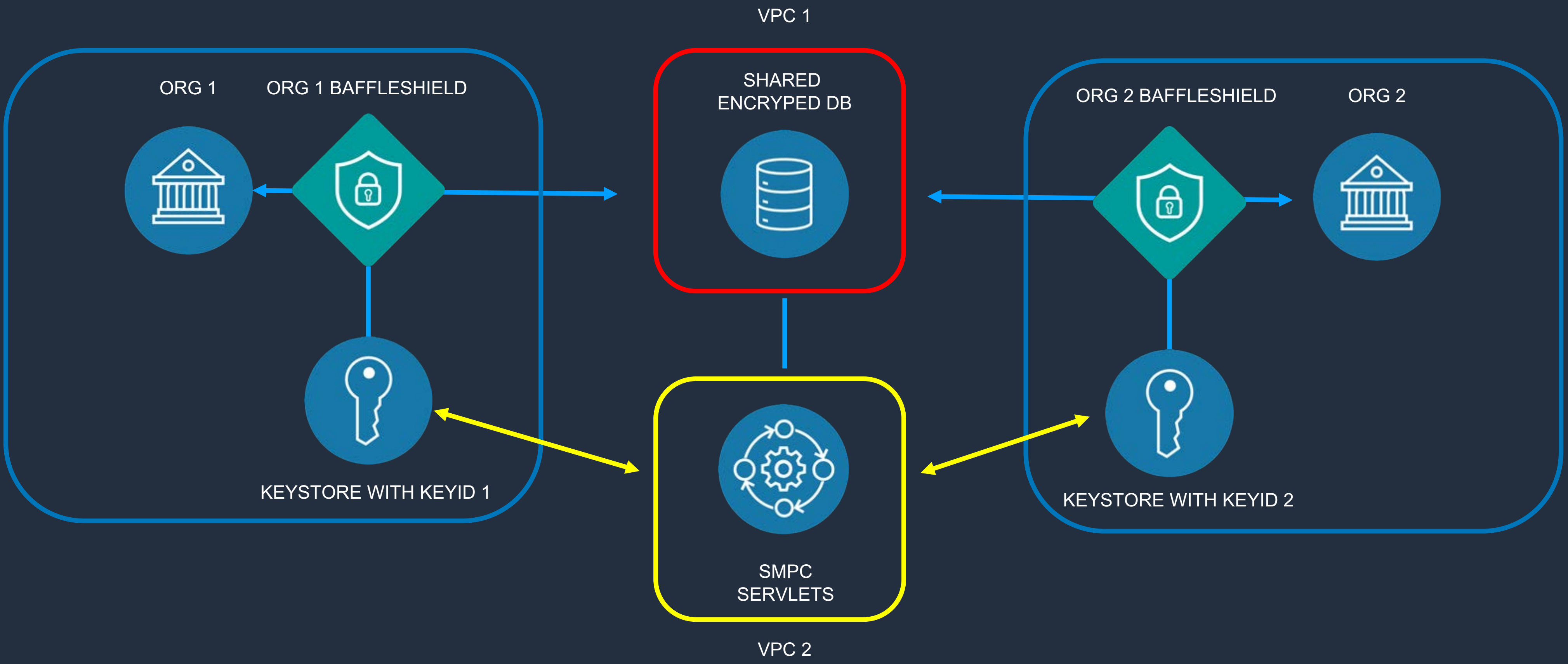
Anonymized Threat Intel Sharing



1 Org 1 publishes known threat indicators to a shared database encrypting the indicators with their own encryption key.

USE CASE

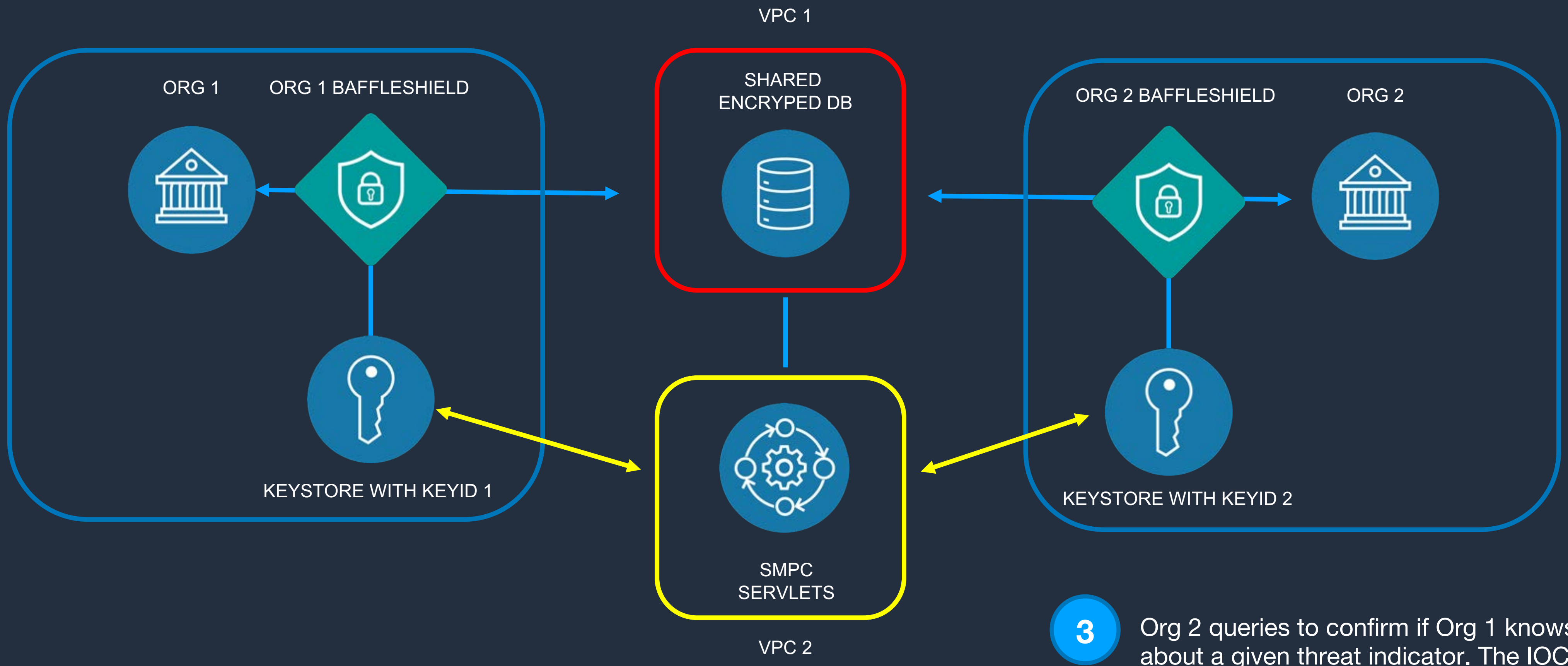
Anonymized Threat Intel Sharing



2 There are no encryption keys present in the shared database and no access to keys.

USE CASE

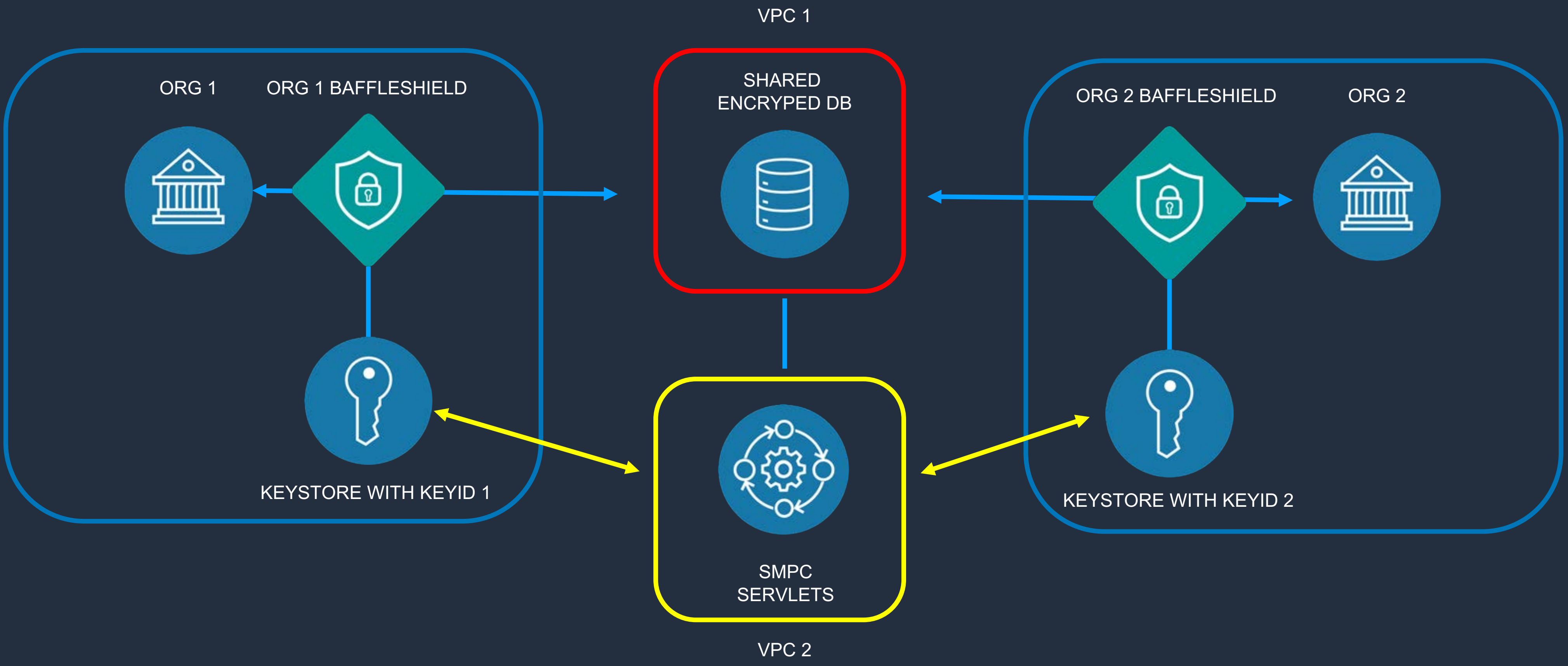
Anonymized Threat Intel Sharing



3 Org 2 queries to confirm if Org 1 knows about a given threat indicator. The IOC value is encrypted using Org 2's encryption key.

USE CASE

Anonymized Threat Intel Sharing



4 SMPC performs a comparison operation on using different keys without ever accessing the encrypted data values. The results are returned without decrypting the data.

Demo #3 – Secure Data Sharing

Summary

- Existing at-rest encryption and container encryption methods (e.g. TDE) do not adequately protect your data from modern day attacks.

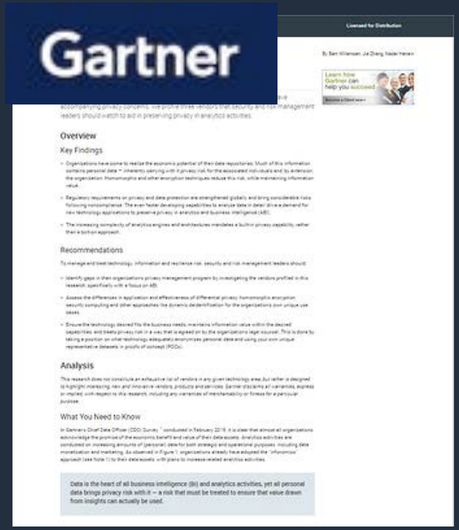
- In a world with distributed access points to distributed data, and within the context of zero trust, data-centric protection methods can mitigate risk and help comply with data privacy regulations.

- Privacy preserving analytics and secure data sharing methods can help your business monetize data and share information securely without violating confidentiality.

Data Privacy Resources

More info and resources: **https://baffle.io/privacy**

Gartner Report on Privacy Preserving Analytics



Gartner

Licensed for Distribution

By Bart Willemsen, Jie Zhang, Nader Henein

Learn how Gartner can help you succeed

Overview

Key Findings

Recommendations

Analysis

What You Need to Know

Data is the heart of all business intelligence (BI) and analytics activities, yet all personal data brings privacy risk with it — a risk that must be treated to ensure that value drawn from insights can actually be used.

CCPA Compliance Simplified

baffle

CCPA Compliance Simplified

Methods you can use to accelerate and simplify compliance with the California Consumer Privacy Act (CCPA)

Encryption Simplified White Paper

Encryption Simplified.

Email: info@baffle.io, harold@baffle.io

Events and Resources

Feb 24 – 28
San Francisco, CA

RSAC®
2020

Book a meeting: info@baffle.io

Free Drinks and Cocktails Mixer on 2/26

IT Security Leadership Exchange
Point Verdra Beach, FL
4/27 – 4/29

IT Security Leadership Exchange

Get an invitation: info@baffle.io

Q & A

Thank You!

harold@baffle.io