

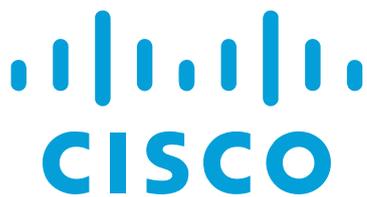
Jan 5th 2020

Customer Experience Management

CEM Data, Security, Reliability & Continuity

Nagendra C L, CTO/Chief Architect





Content Overview

CEM at a Glance

Introduction	3
Data Record	4
Insights	5

Security as a Strategy

Data Collection	6
PII Zero	7

Resiliency as a Design

Architecture	8
Global PaaS	9
Data Sovereignty	10
Controls	11

Data Security

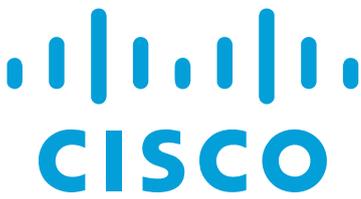
Access Control	12
Encryption	13
AI Model Control	15
Responsibility Checklist	16
Compliance	17

Security Stack

Defenses	20
Choices	21
Real Life Case Study	23

Reference

GDPR	24
Email Security	27



Introduction to Customer Experience Management(CEM)

What is CEM ?

There are always two-sides to a story.

One is the story that the brand narrates using marketing ("**the promise**"), the other side is that of the customer, on how the brands narration before purchase/experience of product or after purchase/experience have been actually perceived ("**the delivery**") by its customers.

Studying the patterns found from macro experiences and story from the customer point of view enables brands to weave a experience that sets them apart in the eyes of its customers & peers.

Why CEM ?

- Improve narration of better stories from marketing, that remain memorable for longer.
- Gain competitive differentiation in crowded industries among peers.
- Improve profitability, by being more effective with products, pricing & services.
- Proactively enable service recovery to minimize impact of exceptions.

The Customer's Journey Map:

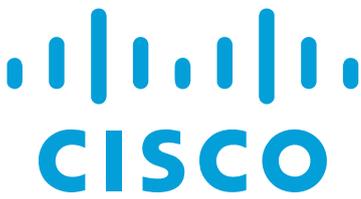
Customer experiences involves multiple points of contact a brand has with its customers, during each interaction with the products or service of the business different individual customers will experience different levels of service at every touch point over a period of time; tracking Customer Experience(CX) across all touch points enable businesses to map the journey and optimize touch points.

Consistent exemplary Customer Experience(CX) across touch-points can turn customers into advocates, resulting in a long term relationship between both parties than merely a one-time transaction, this promotes word-of-mouth and turns the customer into a powerful touch point for the brand.

Sample customer journey for a airline :



➔ Typical CEM Data Record



Look at the Typical CEM Data Record (Input)

CEM Data typically consists of anonymous/aggregate answers to a CEM Questionnaire as collectively perceived by customers of the brand. CEM Data is unlike that of data collected and stored on a CRM/Loyalty/HRM system, which use specific data, while with CEM, only aggregate data is useful for deriving macro analytics insights

Sample CEM Records (Input) :

Anonymous (Completely)	NPS® 9/10	Rating - Service ★★★★☆	Rating - Value ★★★★☆
----------------------------------	---------------------	----------------------------------	--------------------------------

Analytical Insights: Actionable Discovery of Promoters, Detractors & Passive Ratios, Service Quality Measure on Rated Areas, Influence of Value on Service.

Anonymous (Pseudonymity)	CustomerID XX-1234	NPS® 9/10	Rating - Service ★★★★☆	Rating - Value ★★★★☆
------------------------------------	------------------------------	---------------------	----------------------------------	--------------------------------

Analytical Insights: Above + Service Recovery Capability , External Ticketing(Contact Details Looked up using CRM).

Anonymous (Aggregates)	CustomerID XX-1234	NPS® 9/10	Region/City South West	Age Group 25-30
----------------------------------	------------------------------	---------------------	----------------------------------	---------------------------

Analytical Insights : Above + Regional & Demographics Grouping(Useful is Age group vs Specific Age).

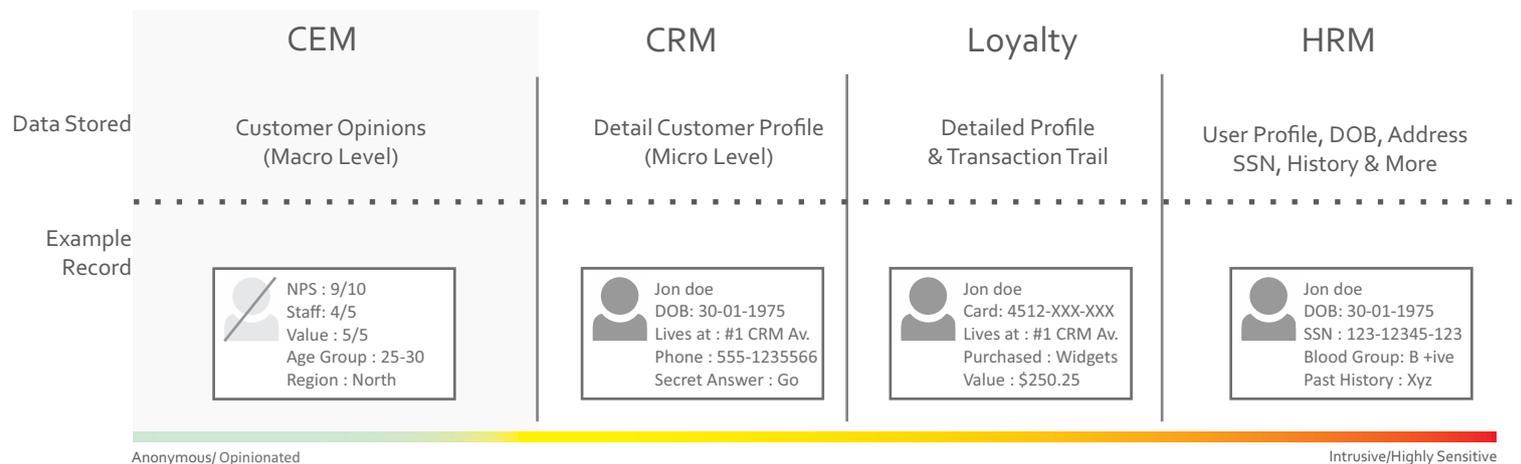
Anonymous (Transactional Aggregates)	Mobile/Email 12345-1234	NPS® 9/10	Region/City South West	Purchase Range 500-2500
--	-----------------------------------	---------------------	----------------------------------	-----------------------------------

Analytical Insights : Above + Transactional Context to Customer Experience.

Unique ID (Contact Only)	Mobile/Email 12345-1234	NPS® 9/10	Region/City South West	Purchase Range 1000-5000
------------------------------------	-----------------------------------	---------------------	----------------------------------	------------------------------------

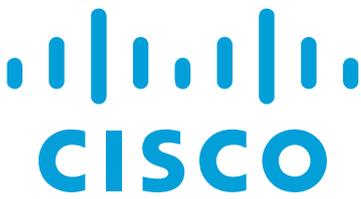
Analytical Insights : Above + Respond Back Capability, NPS Loop Soft Ticketing.

Data Not Found Nor Useful for CEM : Names, Addresses, DOB, PIN's, Passwords, SSN/KYC, Credit Card Numbers/CHDs, History.



© Net Promoter, Net Promoter Score, and NPS are trademarks of Satmetrix Systems, Inc., Bain & Company, Inc., and Fred Reichheld.

2020 Cisco and/or its affiliates. All rights reserved.



Look at the Typical CEM Analytics Insights (Output)

Actionable analytics & insights are derived from the collected customer experience data, these include : NPS, CDM, Scorecards & Insights.

Net Promoter Score® (NPS)

NPS®	65
Promoters	80
Passive	5
Detractors	15

CEM Insight : NPS® is a measure of the customer loyalty to a brand, and it has been found to correlated with revenue growth.

NPS can be as low as -100 (everybody is a detractor) or as high as +100 (everybody is a promoter). An NPS that is positive (i.e., higher than zero) is felt to be good, and an NPS of +50 is excellent.

The ability to measure customer loyalty is a effective methodology to determine the likelihood that the customer will buy again, talk up the company and resist market pressure to defect to a competitor.

Customer Delight Meter (CDM)



Delight Score	76
Service Index	80
Staff Index	82
Value Index	72

CEM Insight : Customer Delight Meter (CDM) score is a multi-dimensional delight measure that can be customized by brands to fit their industry profile or to adaptively increase weights of certain metric more than others.

Many times, a single item question such as NPS is much less reliable and more volatile than a composite index, by combining multiple dimensions of ratings, a composite delight score can be built that may perform significantly better in predicting customer recommendations and retention.

Insight ScoreCard

What can we improve the most on ?

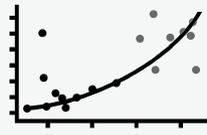


Gift Wrap	46.82%
Music	28.54%
Lighting	14.10%
Parking	10.54%

CEM Insight : Not all the insight needs to be obtained the hard way, sometimes the best way to know - what action you can take today to make the most difference to your business is to just ask your customers that straight up.

For example, asking a simple question **"what can we improve the most on ?"** can lead to a simple actionable answer - that can be acted upon; surprisingly, contrary to common wisdom of big budgets to improve satisfaction, improving upon the smallest of things can lead to a large increase in customer experience, in-turn leading growth.

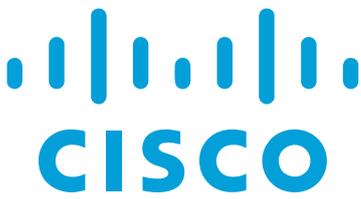
Analytics Insights (Regression Analysis)



Insight 1	Range Vs Knowhow
Insight 2	Range Vs Features
Insight 3	Service Vs Speed
Insight 4	Speed Vs Value

CEM Insight : Finding how a change in single metric impacts other metrics can lead to predictive discovery of areas that can be improved to up the overall customer experience.

Regression analysis includes many techniques for modelling and analyzing several variables, with the focus on the relationship between a dependent variable and one or more independent variables. This enables knowledgeable data scientists & statistical experts to spot hidden gems to bring unique insights on-top for action.



Secure Data Collection Strategies

Nobody likes a intrusive survey.

Collecting tons of data does not always lead to guaranteed actionable insights, but designing your questionnaire by determining what you want to know, who you want to know it from and how to collect the least information enabling a high response rate will definitely lead to actionable insights.

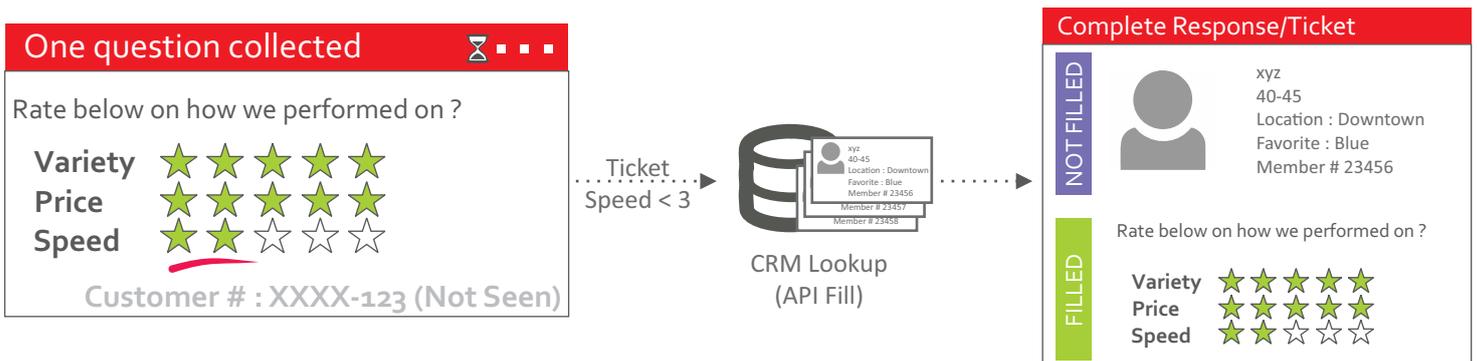
When a questionnaire is designed with set of discovery objectives of the CEM program, brands can sharp-shoot focus on the elements that need answers, while collecting minimal or as close to anonymous/non personal information as possible.

The design intention of every CEM program is to understand customers as a group at a macro level, than at a individual micro level.

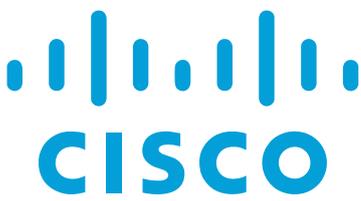
For example to derive insight, collecting a age group as a aggregate range helps to know if millennials(gen y) perceive the brand the same way as a baby boomers(gen x); same applies to other aggregates too, such as an transaction value range(not the specific \$ value), product/service category type(ex: sunglasses and not a specific model) or regional preference(region, than a specific mailing address).

All other detail data is usually not useful for any macro analysis or any CEM insights, but is only of use when the situation calls for service recovery or ticketing, even these when designed around a place-holder identifier (such as a Bill #, Transaction #, Customer #) can enable minimal data collection from the end customer, while still having the ability to lookup other systems for extended detail information on-demand/post the survey for only the select exception records/tickets.

Example using a customer #, the full profile of customer can be looked up using data from CRM over API automatically or on-demand by user using a My View that embeds a CRM lookup screen.



→ Operating a Zero Knowledge CEM Program



Operating a Zero Knowledge CEM Program

Customer Experience Management with PII Zero

CEM analytics to drive valuable insights does not have any use for PII/CHD/PHD, however there are scenarios where even potential PII contact could be avoided, such as a email address to send the survey out or a mobile number for relaying a SMS invite.

CloudCherry's survey token system enables businesses to create personalized survey invite tokens that do not encode any PII, which once generated, can be consumed by any internal system to communicate with the end-consumer without the knowledge of the CEM system itself.

Additionally for managed bulk campaigns, CloudCherry's survey dispatcher is a open-sourced project that can also be executed on-premises by businesses themselves where PII data needs to be secured within dedicated equipment or within their boundaries. This enables businesses to say poll 1 Million customers over SMS's(or emails) w/o disclosing/storing any details on the CEM platform, instead the sampled responses received/stored/analyzed for analytics would use any internal unique id such as a internal customer id(or a hashed version of it) for respondent tracking or case management.

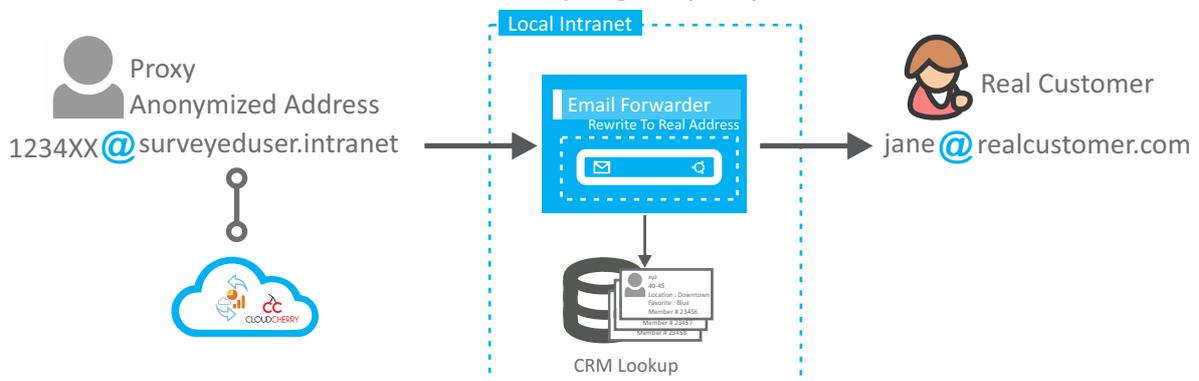
Mobile Numbers

Use any Internal Account #'s instead of Mobile # for tracking respondents

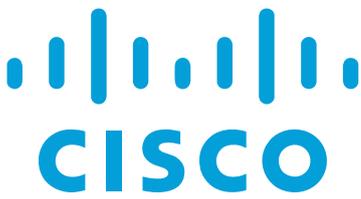
- Use survey tokens once created in your internal work-flow to invite respondents in real-time.
- Use Dispatcher on-premises to schedule survey invites, these invites do not embed any PII themselves, but just an identifier that can be used to lookup details on-demand internally.

Email Addresses

Use an Internal anonymized forwarding email proxy address that mask real-addresses behind the account numbers/identifier, accessible/accepting relay only from internal network/addresses.



This also provides advantage of not needing to sync email addresses as and when they are updated in internal systems, this can run on any small server running an open-source MTA such as [exim](#) and can be transparently automated via internal db lookup.



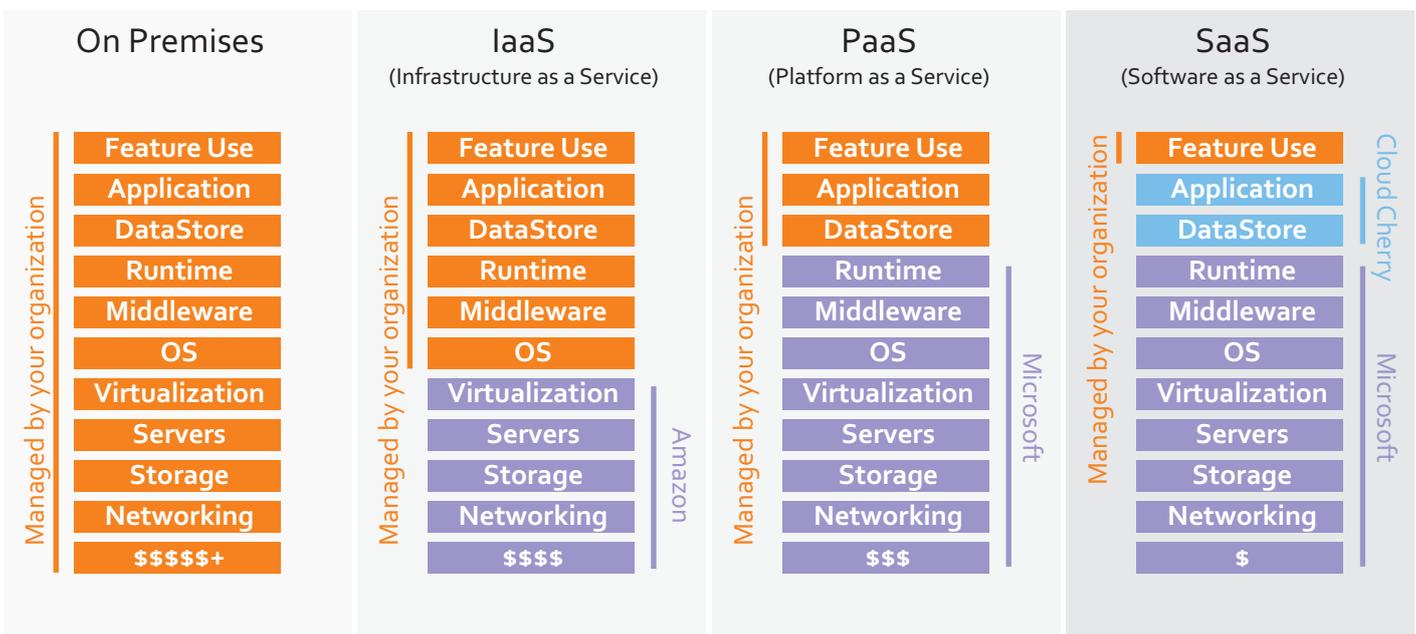
Enterprise CEM Platform Architecture

Cloud Cherry's Customer Experience Management Platform is architected and designed leveraging the best practices of secure cloud computing, the platform is architected to be open (Open Standards/Open Data/Open API), to perform (see benchmarks), to be secure (PCI-DSS Level 1) and long lasting (based upon enterprise grade Microsoft's Azure Platform).

The platform is offered as a Software as a Service (SaaS) solution to businesses, while being deployed on the cloud as a Platform as a Service (PaaS) on-top of Microsoft Azure. SaaS frees businesses from chores of running a complex IT system just to support data collection, and lets their technical teams to better utilize time to develop systems and install interactive and dynamic visualization tools that allow decision makers to analyze, view and benefit from the data, than to be occupied collecting it.

The platform's open philosophy of implementing Open Standards and Open API allows businesses full control to own their data in-contrast to online applications owning the data that customer's generate; unlike proprietary solutions that only facilitates easy collection of data, but no way for data to exit the system, your data is best trusted with open platforms that don't mine it themselves or use it for advertising.

**CloudCherry CEM SaaS =
CX Data Science Analytics + Open Standards + Enterprise Reliability from Microsoft**



➔ Global CEM API Network

Aquire

Analyze

Insight

Customer Experience Management Global API

Resiliency Matrix
api.getcloudcherry.com

CEM Global Users
Collection & Analytics

CEM API Monitoring
Real-Time Routing

Resiliency Matrix

	Server Failure	OS Failure	DC Failure	Region Failure	Country Failure
Single Server	x	x	x	x	x
IaaS	✓	x	x	x	x
PaaS	✓	✓	✓	x	x
Global PaaS+	✓	✓	✓	✓	✓

+ Each Global Region is Independent of Other Data Store Zones are Spread Within Country



1 DNS Lookup (which IP do we talk to?)



4 East US - This Way!

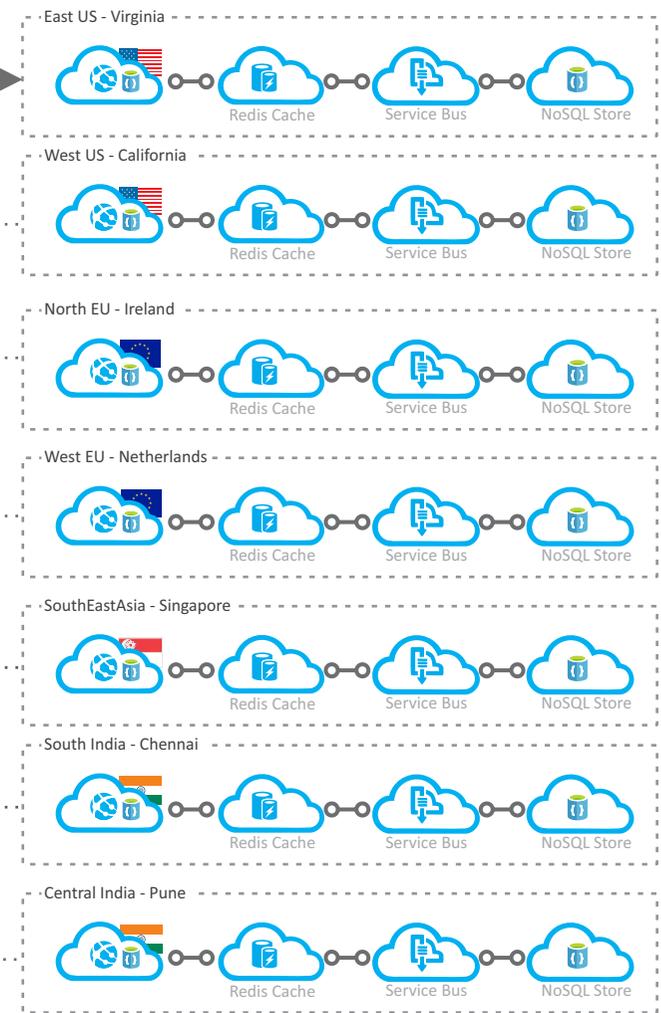
3 Talk to East US it's Online and Super Fast to your location(20ms)

Azure Traffic Manager
api.getcloudcherry.com

2 Lookup Best Route Right Now

Global Monitored Routes

East US	Online	20ms
West US	Online	100ms
North EU	Online	120ms
West EU	Online	140ms
Singapore	Online	150ms
South India	Degraded	600ms
Central India	Online	160ms



Globally Available On





Choice of 5 Continents for Data Residency & Sovereignty

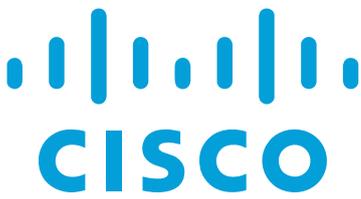
CloudCherry CEM Platform provides more than 5+ global locations as option for CEM programs to operate out of, these enable security conscious businesses to maintain control over the location where regulated data and documents physically reside.

Privacy and data residency requirements vary by country and customers of CEM services need to consider the rules that cover each of the jurisdictions they operate in as well as the rules that govern the treatment of data at the locations where the CEM service provider provisions their services (e.g., their data centers), with CloudCherry customers can select their choice of location to meet the regulatory requirements.

Depending on the specific countries in which businesses operate, companies may need to keep certain types of information within a defined geographic jurisdiction. Additionally global API locations also provides shortest latency to improve speed of access to your customers.

Sovereign Zones	Locations	Azure Regulatory Compliance
United States	California + Virginia California + Virginia Oregon (Encrypted)	
European Union	Netherlands + Ireland Netherlands + Ireland Frankfurt (Encrypted)	
Indian Subcontinent	Chennai + Pune Chennai + Pune Mumbai (Encrypted)	
Singapore(+SE-Asia)	Singapore Singapore Singapore (Encrypted)	MTCS Level 3
United Kingdom	London + Cardiff Ireland (Encrypted)	G-Cloud v6
Canada	Toronto + Quebec Oregon(Encrypted)	

➔ Data Transmission, Security, Ownership & Control



Data Transmission, Security, Ownership & Control

Transmission Security :



All API endpoints use HTTPS Secure Protocol with Extended Validation(EV), the EV SSL Certification is 2048 bit key, with public key signed by GeoTrust using SHA-256. Sensitive API Calls are SSL enforced(where it refuses to connect unencrypted), while rest of the calls connect in both encrypted and normal mode providing control and choice to the business users.

Storage Security :



Typical CEM's systems does not store any credit card numbers or sensitive information, however CloudCherry's CEM Platform data is still stored on PCI-DSS Level 1 compliant storage as the platform is deployed upon Microsoft Azure and Azure has been validated for PCI-DSS Level 1 compliance.

Data is asynchronously backed up on a continued basis, snapshots for responses collected exists with a history of 30 days, all copies of backup of data at rest is encrypted using AES-256 standard.

Data Ownership & Control :



Customer data belongs to you, CloudCherry's staff does not have access to customer accounts, unless customers share their login/password for assistance in setup or support.

Customer have full ability via OpenAPI to import/export data as and when they need, all data collected can also be deleted using the web dashboard, once deleted, the data is automatically purged even from encrypted backups within 30 days.

Security By Conscious Choice :



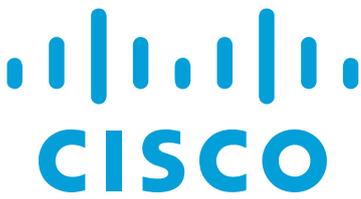
Security and privacy have been planned in the CloudCherry CEM platform using the Security Development Lifecycle (SDL) from initial architecture to deployment of continued new features.

Infrastructure, Network, PaaS Security Safeguards:



All Security safeguards and reliability assurances for Azure PaaS of Microsoft Azure Apply to CloudCherry Platform, Refer to Azure Security, Privacy, and Compliance Whitepaper to learn more. (<http://go.microsoft.com/fwlink/?linkid=392408&clid=0x409>)

➔ Security Brewed Your Way



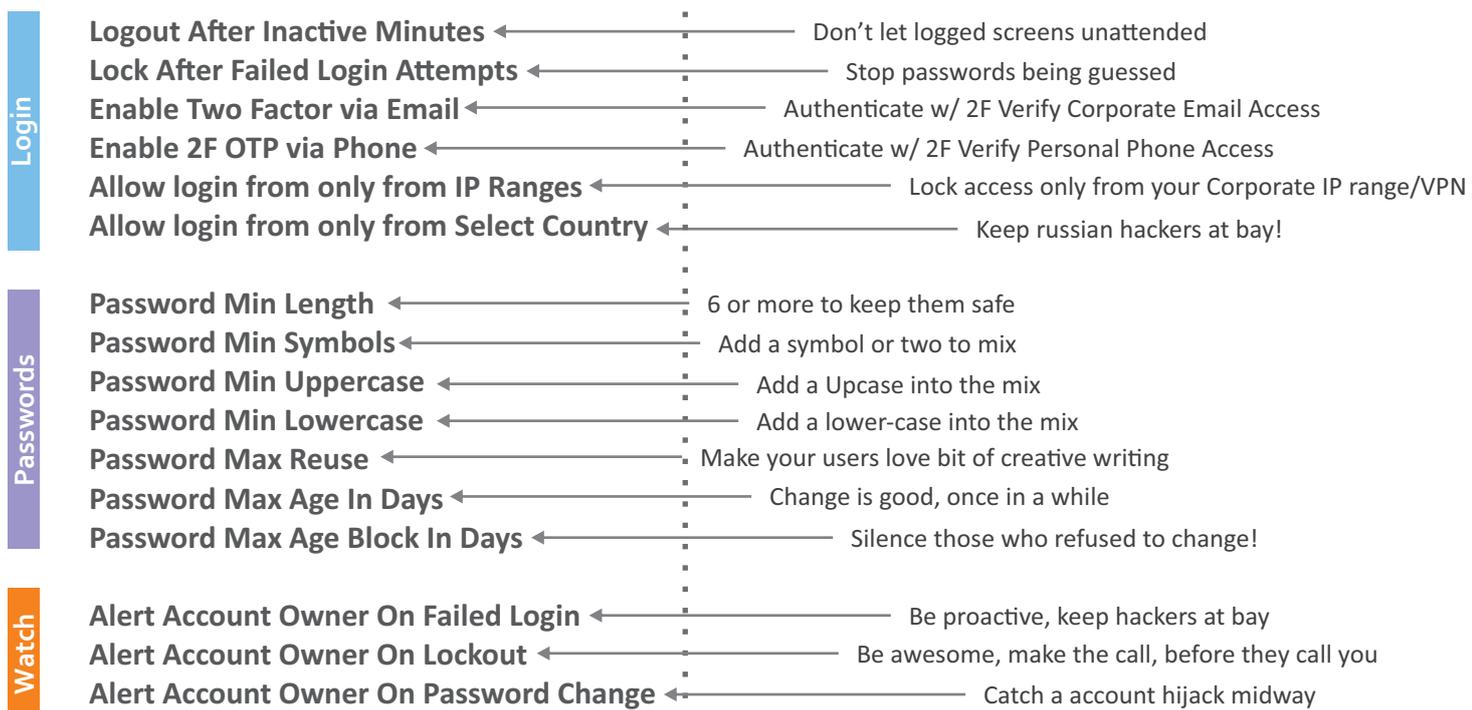
Security Brewed Your Way!

Security or Usability ? You get to pick and choose the right mix.

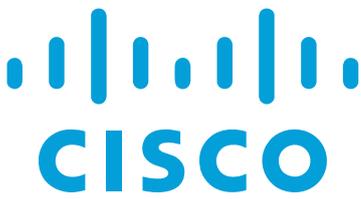
Securing human user access systems can in-practice become bit of a paradox, often the more secure (thus harder for them) you make things the less usable and more insecure it becomes, in many instances when security got too effective, sensible, well-meaning, dedicated people developed hacks and workarounds that defeated the security, for instance, having in place a extremely detailed password requirement, say by making every password real hard with 3 symbols, 3 numbers, 2 Uppcase and then finally have it expire every 30 days to prevent users from reusing any previous passwords, usually leads to passwords pasted on the fronts of monitors - not something that was intended.

Security for user access is best designed with context to the thing being secured, tuned to your situation, for example, if you are just collecting customers opinion in a structured way than what could have anyway ended up on facebook or twitter, then the need to go for very tight security while important may not be that much of value; or you may be storing bits of sensitive information, in all cases **CEM analytics to drive valuable insights does not have any use for PII/CHD/PHD**, for most CEM scenarios, a middle ground approach of keeping the systems accessible to users while preventing any unauthorized use would serve the best policy.

Make the right choice for yourself by setting up your own security policy at your account level that works best for you and your organization.



➔ Encryption Control : Bring Your Own Master Key



Update: 12/2020 - Soft HSM is no longer available on multi-tenant/shared deployments, Hard HSM (via Azure KeyVault) BYOK is available as an add-on for purchase with dedicated single tenant deployment. Newer Hard HSM Add-on may be offered for multi-tenant customers by late 2021.

Encryption Control: Bring Your Own Master Key

The ultimate form of data ownership is to bring your own encryption key

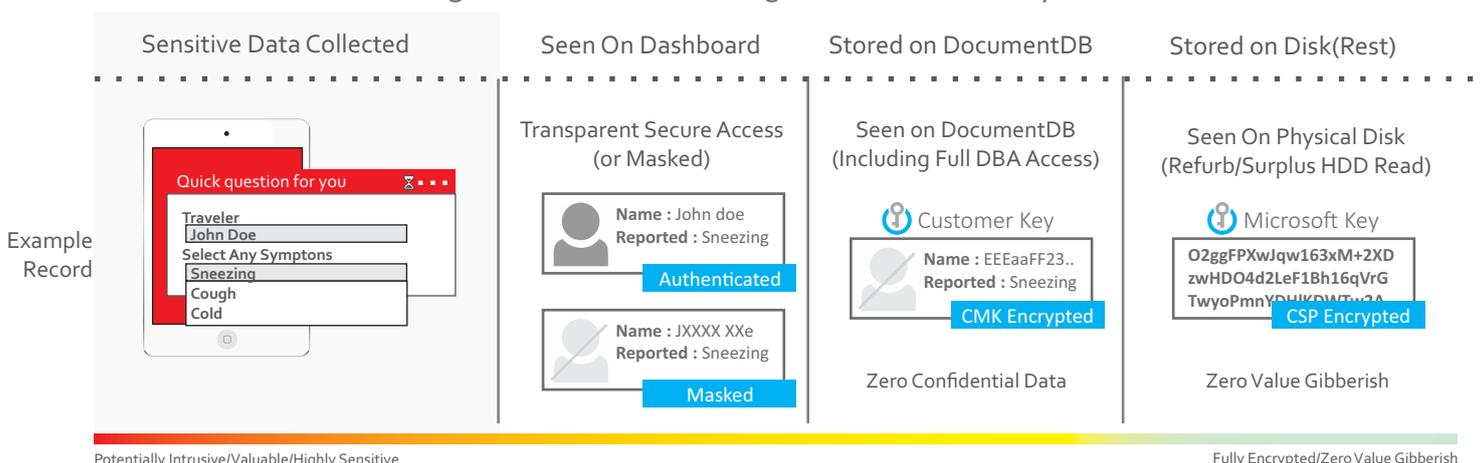
Most cases when a survey is designed correctly, there is no need to collect, store, or transmit PII/CHD/PHI data within a CEM program, however there are certain times, where an organization may need to operate in an emergency situation with the customer interacting front-line staff wanting to override good design choices in-order to quickly collect few data points than as a planned activity, much more for micro data inputs, than for larger CEM insights.

For instance, an airline may need to execute an emergency survey on tablet at arrival gate to check for symptoms after a long distance flight that may be at risk of H1N1, here, the local arrival staff who may have access to a tablet, may want to collect a quick survey with details of all arrived passengers and any possible reports of symptoms to report or comply with destination health/travel regulations.

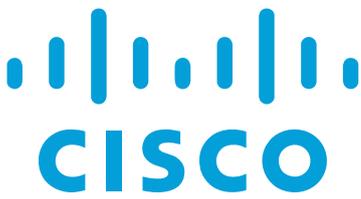
Ideally this questionnaire should use an identifier that is pseudonymous, like that of a PNR along with a checklist of symptoms, however assuming the emergency conditions and this ad-hoc survey being administered by the arrival gate staff than driven by the CX program, it may collect potential PII such as a name of traveler instead of ideally the anonymous PNR. These bits of sensitive data become challenging to track how it comes into your CEM program or where it is processed or where it's stored or where it ends up, customer master encryption key ownership puts you in a proactive position to incorporate ultimate access controls for your data.

Key ownership simplify CEM data security:

- Exceed compliance and best practice requirements by proactively protecting sensitive data, rather than waiting to react.
- Address new data security requirements by having choice to encrypt anything on-demand.
- Seamless, non-disruptive on-demand/scheduled key rotation via OpenAPI.
- Combine with data masking for effective data storage and access security.



➔ Encryption Control : Bring Your Own Master Key



Update: 12/2020 - Soft HSM is no longer available on multi-tenant/shared deployment, Hard HSM (via Azure KeyVault) BYOK is available as an add-on for purchase with dedicated single tenant deployment. Newer Hard HSM Add-on may be offered for multi-tenant customers by late 2021.

Encryption Control: Bring Your Own Master Key

You can create a Customer Master Key using Open API, by default Open API will generate a unique very strong random key, while you can also choose to create one using your own external key to remain responsible for the key material while allowing CloudCherry API to use a copy of it.

Key material is different from key, where the master encryption key is derived using key material to provide flexibility of using any strength key material or even a pass phrase, for example a pass phrase itself may be good key material if complex enough.

Some example key materials you could provide:

- **(simple secret word)** : *"supersecret"*
- **(pass phrase)** : *"up above the clear blue skies..100 thousand stars shine bright!"*
- **(openssl rand key)** : `> openssl rand -base64 512`
"MvbcBXR53wYwuw53MO8LbmKHIB8qE7zRFzYk1asJb6ldefvNGQxnI37akY13OSN..."



Your key material is combined with our secure key to derive your master key that is used to encrypted/decrypt data, this unique key is never persisted to disk anywhere, even encrypted or on backups.

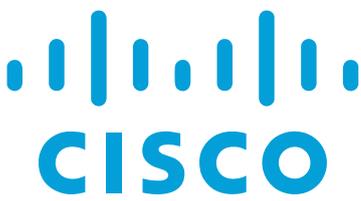
What all is secured/encrypted ?

- (automatic) : All typed free text entry inputs collected (excluding programmatic fill).
- (marked as sensitive questions) : Any text field (including programmatic fill).

Once a valid customer key exists, data is automatically encrypted using the latest version of key at the time response gets collected, these are stored encrypted using AES 256 Cipher w/ a random IV each time, so no two plain text answers will result in a same encrypted hash, however this also will make encrypted fields not searchable by the database, as these strings are no longer plain text nor replicable.

Second time onwards, creating a fresh key generates a new version of master key, making that to become primary to be used to encrypt any new data, older key versions remains available for decrypting data. **Retiring(reversible)** a key will put the key out of circulation and all data that was encrypted using this version of key cannot be decrypted. **Deleting(non reversible)** a key, after a 30 day wait from retirement will lead to permanent loss of decryption ability on the data that was originally encrypted using this key. This is not recommended unless your intent is to effectively destroy data irrevocable that was encrypted using this key.

➔ Bring Your Own AI Models



AI/ML Model Control: Bring Your Own Artificial Intelligence

Establish "Meaningful Control" over AI/Autonomous systems

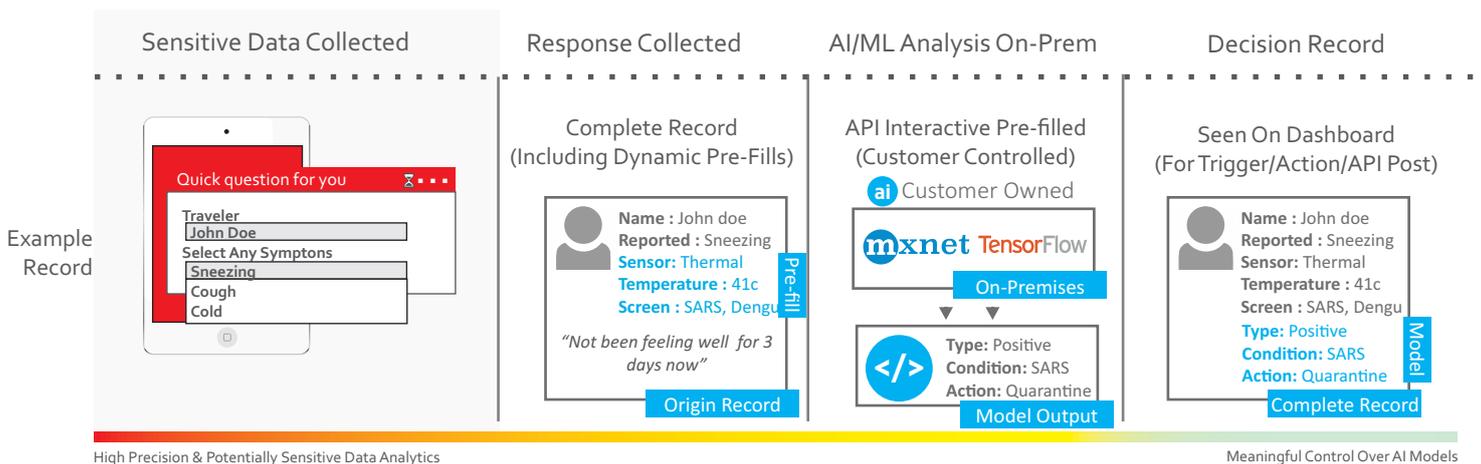
The world has not entered the age of the killer robot, at least not yet, however with increasing use of AI/ML models in data analysis with autonomous systems enabling decision everyday, AI models have become more unpredictable and harder to supervise; and they make it harder to assign responsibility for what happens during a decision.

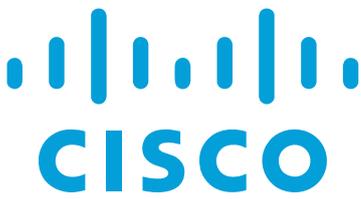
Increasingly many regulators require entities operating in critical areas to have "Meaningful control" over AI, this in turn, requires an understanding of the context in which the AI is being used as well as capacity for timely and reasoned intervention, whether the like of self-driving cars or those that help in deciding the fate of common citizens, should be "explainable". Humans should be able to understand how a machine took a decision when things go wrong - essentially the buck must stop with humans.

CloudCherry's bring your own AI Model option provides for 100% control/ownership (than just access rights via SaaS) over AI Models, enabling customers to meet strictest of compliance requirements for operating in sensitive segments or geographies. Organizations can deploy and bring their own AI models that may be operating on-premises in full oversight directly from their trainers and managers to provide high precision "human-in-the loop" coverage.

Customer owned/operated AI/ML Models enables to:

- Exceed compliance and best practice requirements by proactively establishing meaningful control over AI/Autonomous systems, rather than waiting to react.
- Deploy/Configure any implementation of any algo/solution - on-premises or on your own cloud.
- Understand how your machine learning model took a decision when things go wrong.
- Retain, secure, control fully your own IP, configuration tuning and training for AI models.





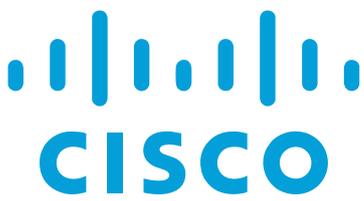
Security Responsibility Checklist

Coverage By :



Application	Application Security	Yes	
	Strong Auth Mechanism(oAuth2)	Yes	
	Strong Hashed Passwords	Yes	
	OWASP Top 10 / Weekly VA Scan	Yes	
	Strong SSL Encryption(2048/SHA2)	Yes	
	SQL Injection Safety(NoSQL)	Yes	
	Performance Monitoring(App Insights)	Yes	
	Exception Management(App Insights)	Yes	
Windows Azure Managed Security Features	Activity Logging(DocumentDB)	Yes	
	Data Centre Physical Security		Yes
	DC Personal Access Control		Yes
	Encryption of Data at Rest/In-Transit		Yes
	DC Fail-Over Management		Yes
	Secure Key Management		Yes
	Network Layer Security		Yes
	Network Fail-Over Management		Yes
	DDoS Protection		Yes
	Storage Layer Security		Yes
	PCI Compliance		Yes
	Encrypted Backups		Yes
	Storage Fail-Over Management		Yes
	Server Security		Yes
	Physical Access Security		Yes
	Server Fail-Over Management		Yes
	OS Security		Yes
	OS Updates & Patching		Yes
	Virus/Malware Protection		Yes
	Runtime Protection		Yes
Proactive Monitoring		Yes	
Access Audit Logging		Yes	
100+ PaaS Managed Feature Coverage		Yes+	

→ CEM PaaS Platform Compliance



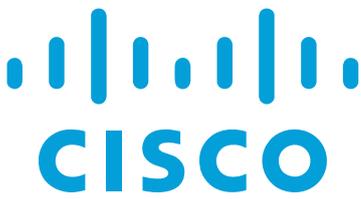
Azure PaaS Platform Compliance

Industry-verified conformity with global standards

To help our customers comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, CloudCherry's SaaS CEM Platform hosted on Microsoft Azure offers the most comprehensive set of certifications and attestations of any cloud service provider.



➔ [Frequently Asked Questions](#)



Frequently Asked Questions(FAQ)

What is PaaS ? How is it Different from IaaS ?

PaaS is Platform as a Service, a model where underlying Hardware/OS/Network Infrastructure is abstracted and managed completely by the cloud provider, including security, health, monitoring and load-balancing are fully managed services in this context by Microsoft for Azure.

CloudCherry is all Azure with PaaS - so What happens if azure were to go dark ?

CloudCherry has setup a recovery storage location at AWS(Amazon Web Services) that is set to store delayed incremental backups for all but responses collected during last 4 hours(less than 0.04% missing data for a account operating for a year), in the event of azure disappearance, you will be able to access your data within 24hrs from this offsite location, eventually using Azure Stack - CloudCherry Platform can be deployed & operated out of a different data centre.

Do you offer a on-premisis version of the platform ?

Unlike CRM/HRM/Loyalty systems, CEM systems do not store any high value confidential data, but hold only anonymous or near-anonymous opinionated data collected from sample respondents; the power of the CEM system itself is not the data it holds, but in spotting patterns in the ordinary data - collectively analytics, than the individual data records itself; Considering this CloudCherry intends to only provide a elegant, agile, easy-to-deploy, auto-adminstered solution as a SaaS - that just works to drive CEM programs for brands and businesses world-wide.

What if there is a change of focus or control ?

You would know in advance, you will have a choice to move your data away(one of the benefit of a open platform), as you sign up today, our terms guarantee that your data belongs to you & yours only, we do not use it to sell it to any other entity or use it for any commercial purpose.

Can I see your architecture ? or Can I see your code ?

Yes you can, download full architecture whitepaper from [here](#). You can also drop by to any of our development offices to chat with our talented developers who do all the work, they will be happy to chat with customers and even preview exciting features that they are working on.

I'm still not convinced! Nobody ever got fired for buying IBM/Microsoft, so why should we buy from you ?

IBM & Microsoft do not offer CEM Platforms, until the time they do, CloudCherry is your best bet, underlying the CloudCherry CEM Platform is actually Microsoft & IBM(Watson), so your are in good hands.

CEM Defense In-Depth Security Stack

CEM Domain & Data

1

"CEM analytics to drive valuable insights does not have any use for PII/CHD/PHD"

Security planned is best in being over-prepared, when it comes to securing sensitive data from leaks, prevention is better than cure, when confidential data is more cosmetic use than of any real value, it's best to not use it.

User Access

2

"You get to set up your own security policy at your account level that works best for you and your organization"

Two factor, three factor, corporate white listed IPs, white listed countries, and more are possible.



Data Transmission

3

"All API endpoints use HTTPS Secure Protocol with Extended Validation(EV), the EV SSL Certification is 2048 bit key, with public key signed by GeoTrust using SHA-256"

SSL Endpoints at all times carry a A/A+ Rating and are fully managed by Microsoft for Azure PaaS.



Data Segregation

4

"Each CEM response is stored as separate JSON Document", each JSON document has a partitionkey that is set to the account owner, all queries for data require a partitionkey, partitionkey is automatically determined by Security Principal of the calling request. All requests are authorized via OAuth 2.0.



Data Storage

5

"Customer master encryption key ownership puts you in a proactive position to incorporate ultimate access controls for your data using first and only publicly accessible cipher approved by the National Security Agency (NSA) for top secret information"

Even the azure's administrator on server cannot access sensitive data marked and encrypted using your customer master key.



Controls

6

"Even our dev staff do not have access to your data", we do not have a network infra team/admins, nor the data can be queried directly from any database. The only way to access data in PaaS scenario, is to write core platform application code and re-deploy this core platform code that can in-turn access or authorize and break permission boundaries.

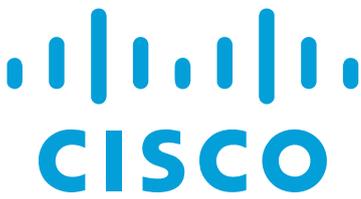


Enterprise Trust

7

*CloudCherry CEM :
= CX Data Science Analytics + Open Standards
+ Enterprise Reliability from Microsoft*





Frequently Asked Questions(FAQ) - Controls

In Context of PaaS : Who all can access customer data w/o customer's login/password ?

None; none of our staff have access to data, we do not have a network infra team/admins, nor the data can be queried directly from any database. The data is stored on a NoSQL datastore(Azure Document DB/MongoDb) - behind a private VNET firewalled, not accessible on the public internet - even if the keys were leaked on to internet, but only to the API endpoint's network security group.

Only way to access data in PaaS scenario, is to write core platform application code and re-deploy this core platform code that can in-turn access or authorize and break permission boundaries.

Controls exist for code, as only code live can access data :

- All code written goes through Source Control Management(SCM) leaving a clear audit trail.
- Access to this private code repository(Git) is only using private keys(SSH) to select background checked full-time staff developers.
- No live code is deployed w/o going through staging & review.

So, w/o code changes, who can still in theory can access and how ?

The management including CEO/CTA/VP-Engineering/VP-Branding, these positions have access to administer the Role account from which Azure PaaS Platform rules of access itself can be changed, in theory, they can remove the firewall, reset the access keys and then proceed to query the database directly, this will however still leave a clear audit trail log on azure management console.

So what is the recommendation ?

Do not trust CEM platforms(not just CC, but any CEM) to store Personally Identifiable Information(PII) as CEM systems are designed & optimized for CX/CEM Analytics than a traditional CRM data stores.

Is CEM system useful w/o any PII information ?

Absolutely, a typical CEM record involves collecting experiential data of a existing customer w/ any choice of pseudo-id leading back to customer for contact, this identifier is often a internal customer id, which only will make sense to the organization collecting it verses the operator of the platform.

Which security focussed institutions already use CloudCherry CEM and how ?

Banks of course are on top of security, India's top 3 out of 5 private banks use CloudCherry, between them, they have a listed market cap of over \$82 Billion as of 2016 Q2. CEM for banking is implemented over multiple channels to measure customer experience across online(netbanking/website) and offline(Branch/ATM/Kiosk) modes.

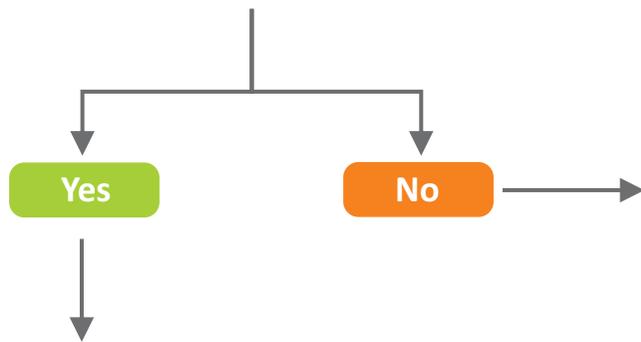
Start

Did you know CloudCherry Operates CEM Platform as a very modern Global PaaS ?



Checkout our CEM Data Security Whitepaper (p7,8,9,10,14)

Do you know CC does not really maintain/secure the actual Infra, but Microsoft does for Azure, and DR is real-time with PaaS ?



Resiliency Matrix

Single Server
IaaS
PaaS
Global PaaS⁺

	Server Failure	OS Failure	DC Failure	Region Failure	Country Failure
Single Server	x	x	x	x	x
IaaS	✓	x	x	x	x
PaaS	✓	✓	✓	x	x
Global PaaS ⁺	✓	✓	✓	✓	✓

⁺Each Global Region is Independent of Other Data Store Zones are Spread Within Country

Perfect!, Also you get 100% uptime SLA when you select Global Residency.

All services online are independent of CloudCherry's physical existence, for instance in a hypothetical thought experiment, if all offices of CC were to disappear! fresh feature updates will come to halt, but you would still have 3 months more of perfect online record & full platform access with all that was functional up until that time.

CloudCherry also enables :

- OpenAPI to access your data anytime(your data belongs to you)
- Real-time Push To Offsite Storage(Azure Queue/On-Premises Archival)

In Real Life Breach Incidents

What Occured

How It Occured

CloudCherry's Security By Design

Equifax
(Sep 2017)

Cybercriminals accessed approximately 145.5 million U.S. Equifax consumers' personal data, including their full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers.

Equifax said the breach was facilitated using a flaw in Apache Struts (CVE-2017-5638).[34] A patch for the vulnerability was released March 7, yet the company failed to apply the security updates before the attack occurred 2 months later

Scenario **SAFE**

CloudCherry is 100% PaaS with Microsoft, which also happens to be the creator of .NET/Windows responsible not just for creation/release of the patches, but applying the patches in-time as-well, this in practice occurs even earlier than the broad availability of a patch due to Azure PaaS being fully managed by Microsoft.

Verizon/Nice
(July 2017)

Security lapse at Nice Systems(Also a CX Systems Vendor) exposed data from millions of Verizon customers, leaking names, addresses and personal identification numbers, and PINs.

Employee at Nice Systems left dump of data on a public S3 bucket.

Scenario **SAFE**

Our Staff do not have access to customer data in the backend by design, but only the code(logic) does, unless/until customers share their existing credentials or create sub-users for assistance from our staff.

DR is Real-time and encrypted backups are fully automated(No human involved).

NSA Leaks
(2013)

Top secret documents leaked by ex-NSA systems administrator Edward Snowden.

Systems administrator moved bulk cache of gigabits of data to be leaked.

Scenario **SAFE**

Being 100% PaaS, CloudCherry systems are administered by a staff administrator on payroll of Microsoft for Azure.

Using BYOK, even Microsoft Admin will not be able to access sensitive data texts that has been encrypted using your own key.

Malaysia Teleco
(2017)

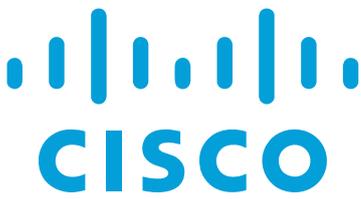
Personal data of millions of Malaysians(all telcos) was up for sale for an unspecified amount in bitcoin, virtually everyone in the country was affected by the data breach at the Malaysians telecoms providers such as DiGi.Com and Celcom Axiata.

PII stored on connected systems that did not gain any features/use of it.

Scenario **SAFE**

CEM does not require PII for delivery of valuable insights and our recommendation is not to collect/store PII where not needed.

What doesn't exist, can't be lost or stolen and to err on the side of caution is always better when it comes to security.



GDPR Compliant Surveys

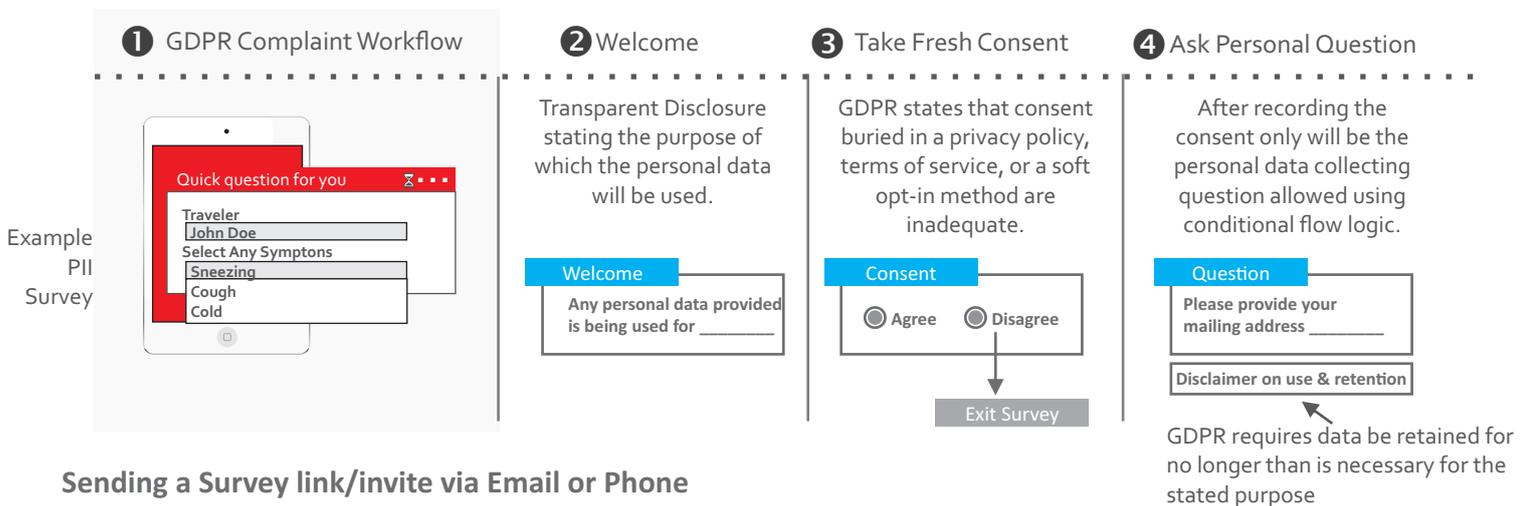
GDPR focuses on personal data privacy, example of personal data is [PII](#) such as full name, address, SSN, phone or other personally identifiable information, while example of non-PII data is any pseudonymous identifier internal to customer's organization such as member-id, customer no, order #, role name, etc.

PII has little value with-in CEM, and we do not recommend or ask our customers to collect PII, primarily CEM systems are not intended to be store of PII unlike that of a CRM and these topics are discussed extensively in p3,5,6,11,12,13,14,16,17 and p18.

You are already compliant if you :

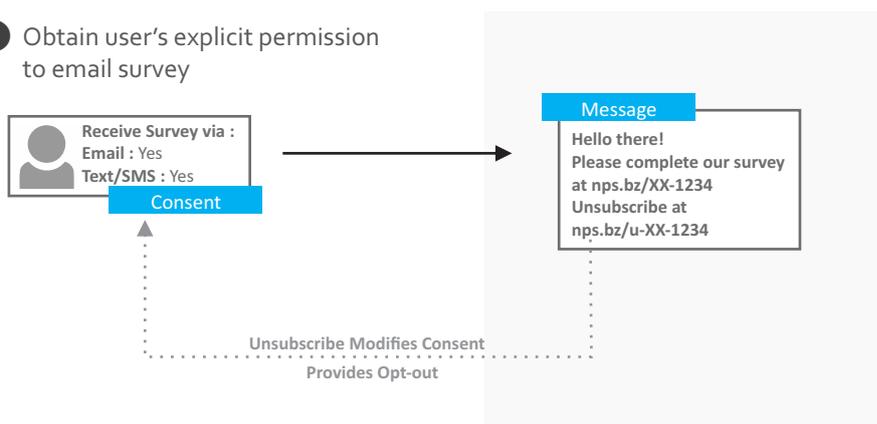
- Do not collect any PII or operate a internal VoE program.
- (and) Never send survey links/invite emails with-out opt-in consent.

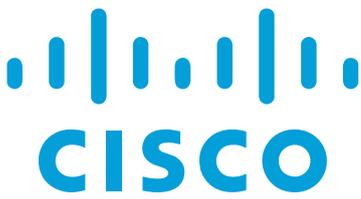
Designing GDPR Compliant Surveys when collecting PII



Sending a Survey link/invite via Email or Phone

- 1 Obtain user's explicit permission to email survey





GDPR Compliance How-To/Tasks:

1. Answer a GDPR personal data subject request : *“customer John Doe needs to know if you have collected any personal data”*

Login to dashboard > responses > Filter for “John Doe” as name(if you have collected that with a question in the survey)

2. Data subject needs a copy of personal data

After discovering as above, extract personal data contained in responses for a subject in an open machine readable format such as excel/csv.

3. Data subjects needs data to be deleted (right to be forgotten)

After discovering as above, click delete responses to delete it forever immediately.

4. Automatically limit retention of data to ‘x’ days

Organizational wide :

Automatic organizational wide retention limit can be set via Settings > Data Retention Limit Month (Min = 1 Month, Max = 48 Months)

Per Questionnaire :

Per Location/Questionnaire limit can be set via Questionnaire Settings> Data Retention Limit Days (Min = 7 days, Max = 1095 Days)

More precise limits can be enforced for any data collected and filterable via :

Login to dashboard > responses > Filter for all response collected before x days, click delete to remove it forever, any automated archive for DR will elapse within 30 days automatically beyond which it can not even be restored during a disaster recovery.

5. Automatically anonymize data by removing collected PII

Select Questions collecting PII : Settings > Data Field Anonymization Ids

Set Number of Day After To Take Effect : Settings > Data Field Anonymization Days (7 to 1096 Days)

Optionally to replace collected text with a placeholder : Settings > Data Field Anonymization Place Holder

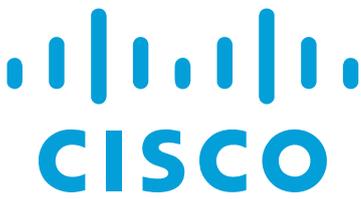
Skip being tracked in your activity log(retained upto 6 months) : Set Data Field Anonymization DoNotLog

6. Are surveyed users tracked using their precise IP or cookies with personal information ?

No!

7. Any Other GDPR request ?

We’re here to help, ask us anything, just email support@getcloudcherry.com for assistance.



GDPR Compliance FAQ

What is GDPR, what it requires and why does it apply to non-europeans ?

[GDPR overview whitepaper](#) provides high-level overview of GDPR structured as a series of questions and answers.

Does CloudCherry provide tools to help customers with GDPR obligations ?

Yes

Who decides what to collect?

Customer; End customer setting up questionnaire and sending out the link to collect information.

Who physically stores/secures/administers our collected data?

Microsoft under the Azure's PaaS shared responsibilities model is responsible for choosing the encryption standards, transmission, picking the physical servers, restricting access, segregating roles, patching and notifying in a event of any data storage breach.

Is our data stored "secured" to be GDPR compliant?

Yes w/ Azure.

How Azure helps organization in being GDPR compliant ?

Refer "[How Microsoft Azure Can Help Organizations Become Compliant with the EU General Data Protection Regulation \(GDPR\)](#)"

Email Delivery Security

Secure Survey Invite Email Delivery Methods

- 1 Your own SMTP via Relay
- 2 Your own Domain w/ DNS Entry
- 3 Fresh Domain/SubDomain
- 4 Spoofed Display Name

	Your Brand Name	Your Own Domain	Your Own Server	Your Own IP	Deliverability	Response Rate	Trust Score	Chance of Marking as Spam	Marked as Phishing	Setup Effort	Example SaaS Service*
1	Yes	Yes	Yes	Yes	Max	Max	Max	None	None	1 Min	SalesForce, SurveyMonkey
2	Yes	Yes	No	No	High	High	High	Low	None	5 Min	Zendesk, MailChimp
3	Yes	Yes	No	No	Moderate-High	Moderate-High	Moderate-High	Moderate	Low	1 Hr	(Startup option to avoid #4)
4	Yes	No	No	No	Low	Moderate	Low	High	High	1 Min	Some Legacy Survey Vendors

[* As seen by sample email/delivered found by sampled internet users]

RECOMMENDED ✓

Your own SMTP Relay

From : ACME Bank <survey@acmebank.com> ✓
 Subject : Please share your experience
 mailed-by: acmebank.com ✓
 signed-by: acmebank.com ✓

Key Benefit

- Authentic all the way
- Already trusted & whitelisted domain before landing.
- High on user trust score.
- High on authentic branding.
- Easy to plug & go.
- Full control/log & audit trail of what email is relayed/not via your own SMTP/Staff.

BEST PRACTICE ALTERNATIVE ✓

Your own Domain w/ DNS Entry

From : ACME Bank <survey@acmebank.com> ✓
 Subject : Please share your experience
 mailed-by: acmebank.com ✓
 signed-by: acmebank.com ✓

Key Benefit

- DNS Entry authorized to be authentic origin.
- Receiving server already trusts & white lists domain.
- Industry best practice for email deliverability, proven as offered by specialist email services such as MailChimp, Zendesk.

WORKAROUND ✓

Fresh/Sub Domain

From : ACME Bank <survey@acmebankcx.com>
 Subject : Please share your experience
 mailed-by: acmebankcx.com ✓
 signed-by: acmebankcx.com ✓

Key Benefit

- Alternative when no DNS control exists or is accessible.
- Retains branding.
- Reputation/deliverability not impacted by any other users of same domain.
- Alternative to #4, Spoofing displayed name.

PILOT/DEMO ONLY

Spoofed Displayed Name

From : ACME Bank <acemesurvey@cx.getcloudcherry.com> ✗
 Subject : Please share your experience
 mailed-by: cx.getcloudcherry.com ✗
 signed-by: getcloudcherry.com ✗

Key Benefit

- Quick and dirty, great for pilots or one-time use.
- Risks brand reputation Damage on being flagged spam or worse phishing by any other customer using the same shared domain/ip.
- Likely to be flagged by most ML/AI spam filters over time.