Conceal, Don’t Feel, Don’t Let Them Know

Nir Chervoni

ABOUT ME

Senior Manager - Data Security at Booking.com, part of the Booking Holdings group of brands.

PREVIOUS PROFESSIONAL EXPERIENCE:

- The global CISO of Credorax (Nowadays Finaro);
- I act as board advisor for a couple of cybersecurity startups.

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

ONCE UPON A TIME

Image source: *Once Upon A Time… Man, TV series, 1978*

↘↘ THE CLASSIC MONOLITH ↙↙

Image source: *pxhere.com*

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

THE NEXT BIG COMPUTER


```
MAIN                              AS/400-HOOFDMENU
                                                    Systeem:    BIZIBITP

Kies uit het volgende:

     1. Gebruikersfuncties
     2. Office-functies
     3. Algemene systeemfuncties
     4. Bestanden, bibliotheken en folders gebruiken
     5. Programmeerfuncties
     6. Communicatiefuncties
     7. Het systeem definieren of wijzigen
     8. Problemen verwerken
     9. Een menu afbeelden
    10. Opties voor AS/400 Information Assistant
    11. Functies voor Client Access/400

    90. Zich afmelden van het systeem

Optie of opdracht:
===> _

F3=Afsluiten    F4=Aanwijzingen    F9=Terughalen    F12=Annuleren
F13=Information Assistant          F23=Beginmenu instellen
(C) COPYRIGHT IBM CORP. 1980, 1998.
```

Image source: *commons.wikimedia.org*

THE NEXT BIG COMPUTER

Image source: *commons.wikimedia.org*

a little bit more

Generated by Font-Generator.com

Distributed Systems

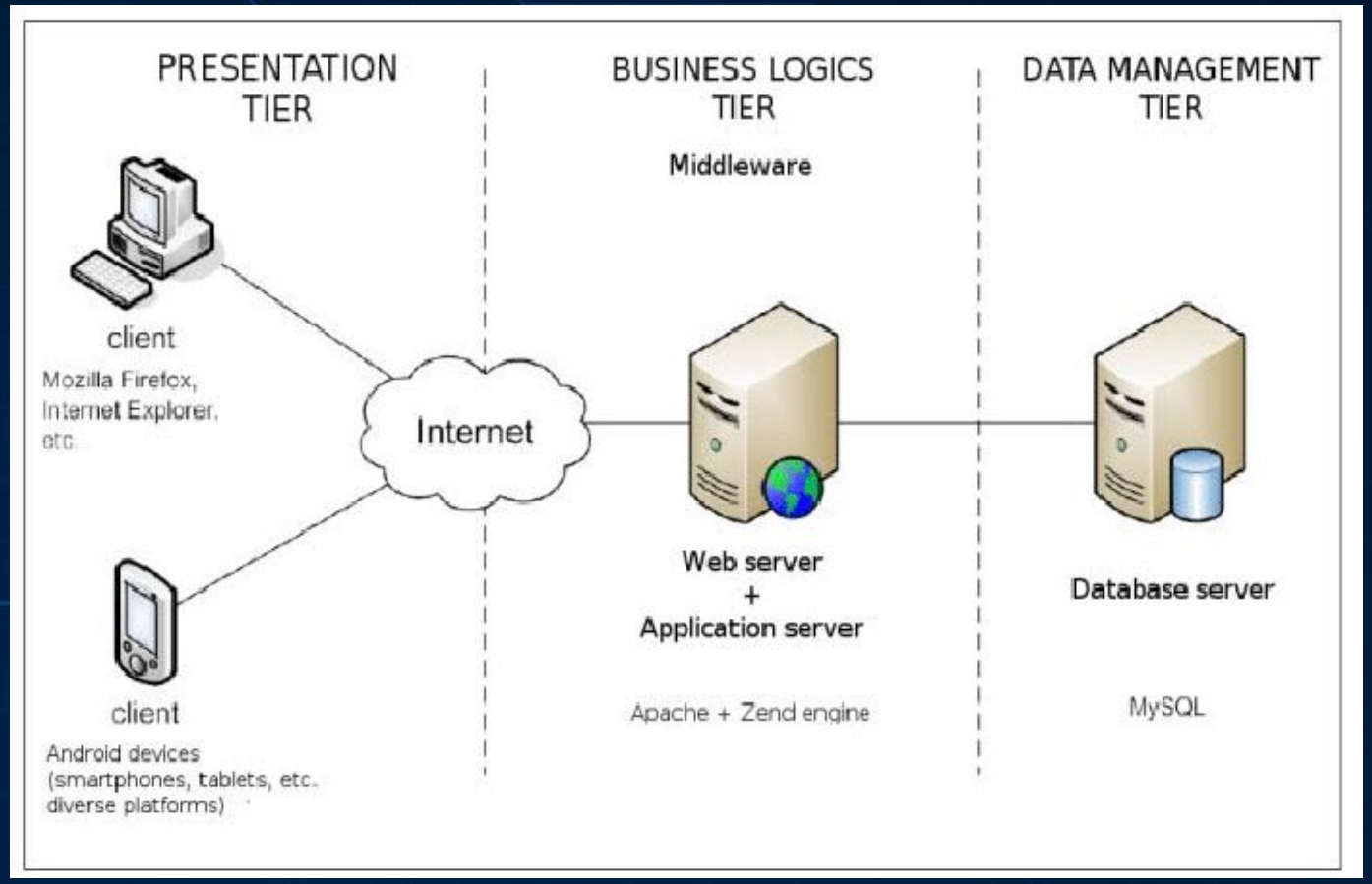


Image source: www.researchgate.net

a little bit more

Generated by Font-Generator.com

Distributed Systems

SIEBEL®

Image source: *commons.wikimedia.org, mynewsdesk.com*

BOOKING HOLDINGS
CENTERS OF EXCELLENCE
BPORK

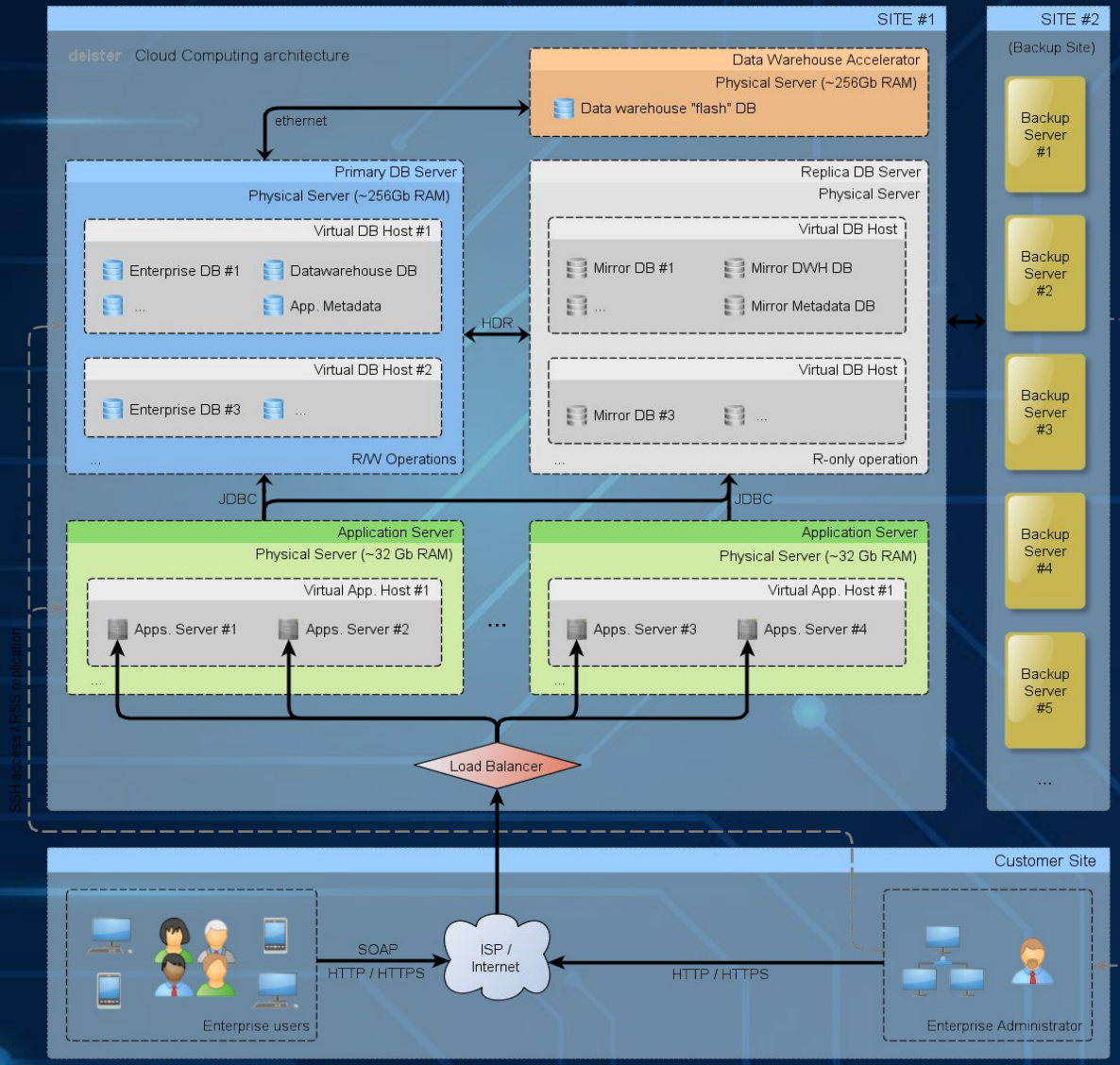
PC

😱😱😱

Image source: commons.wikimedia.org

BOOKING HOLDINGS
CENTERS OF EXCELLENCE
BPOK

New Architectures



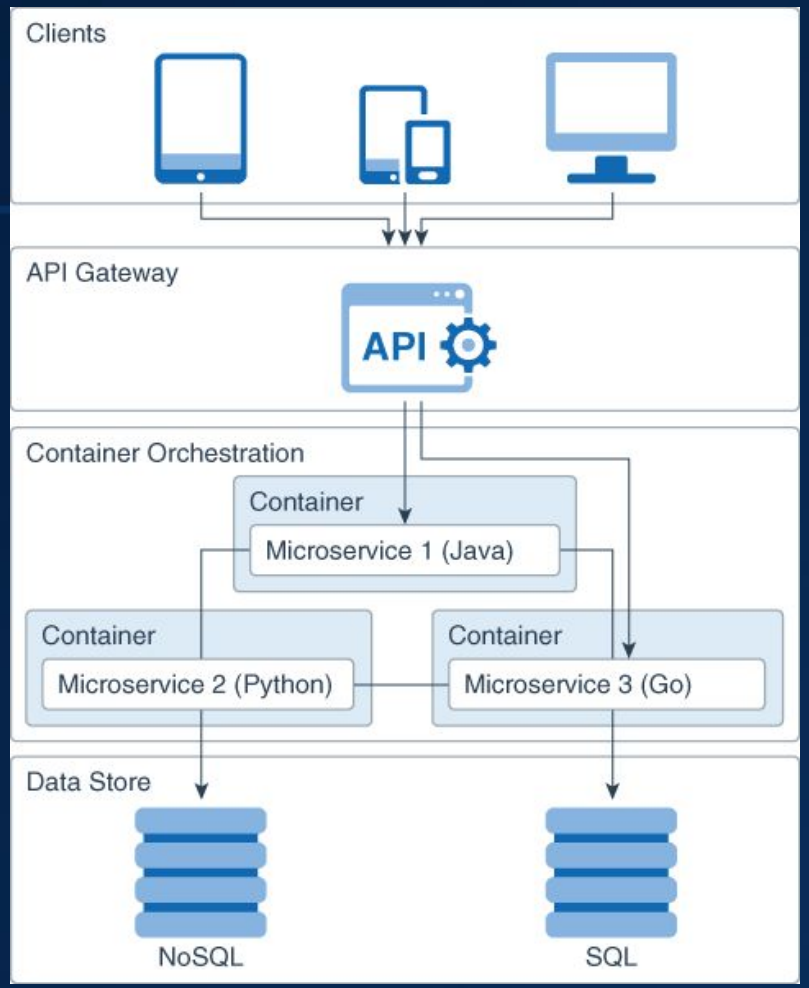


Image source: *docs.oracle.com*

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Scale-Out Capabilities

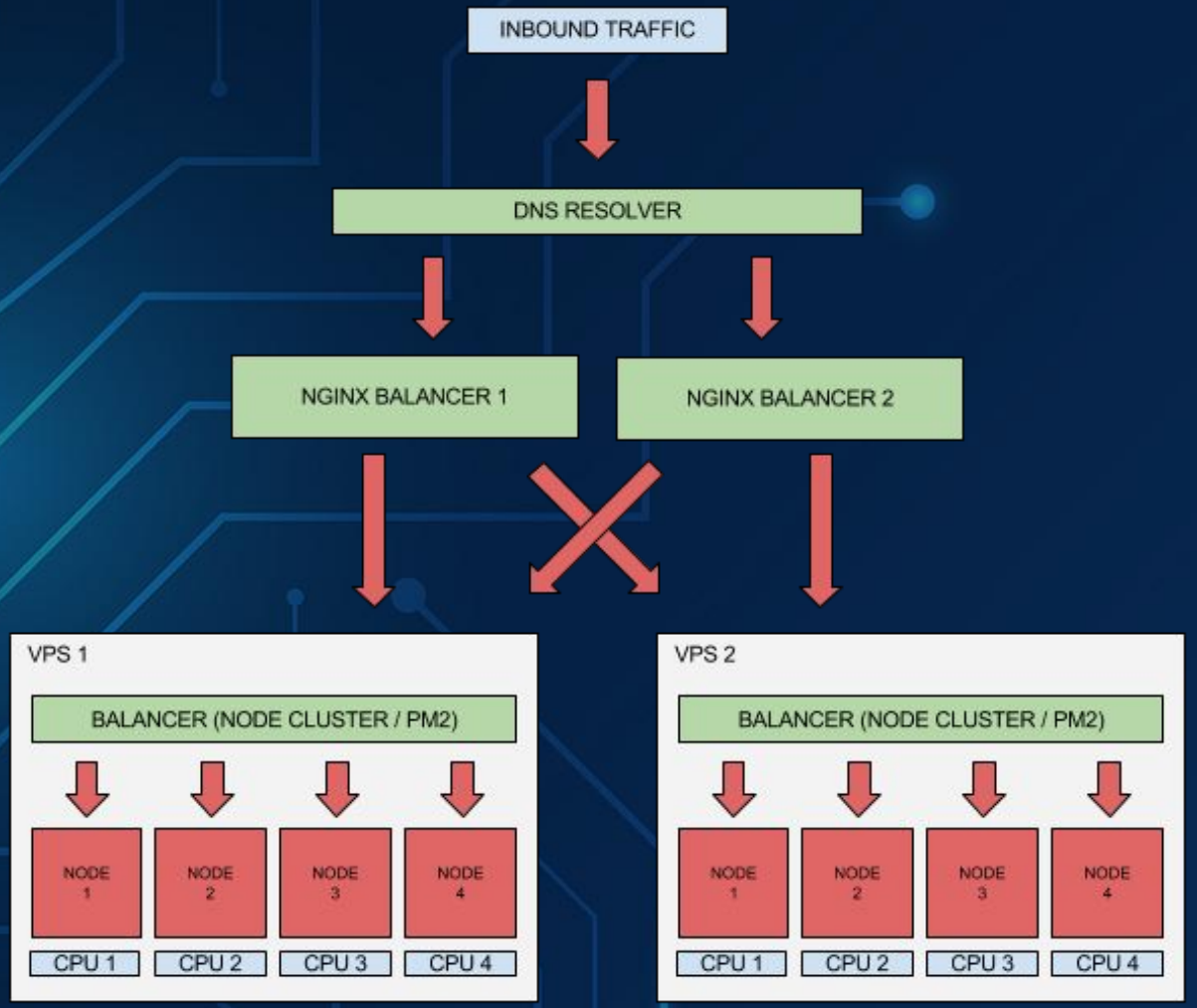


Image source: medium.com

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Cloud

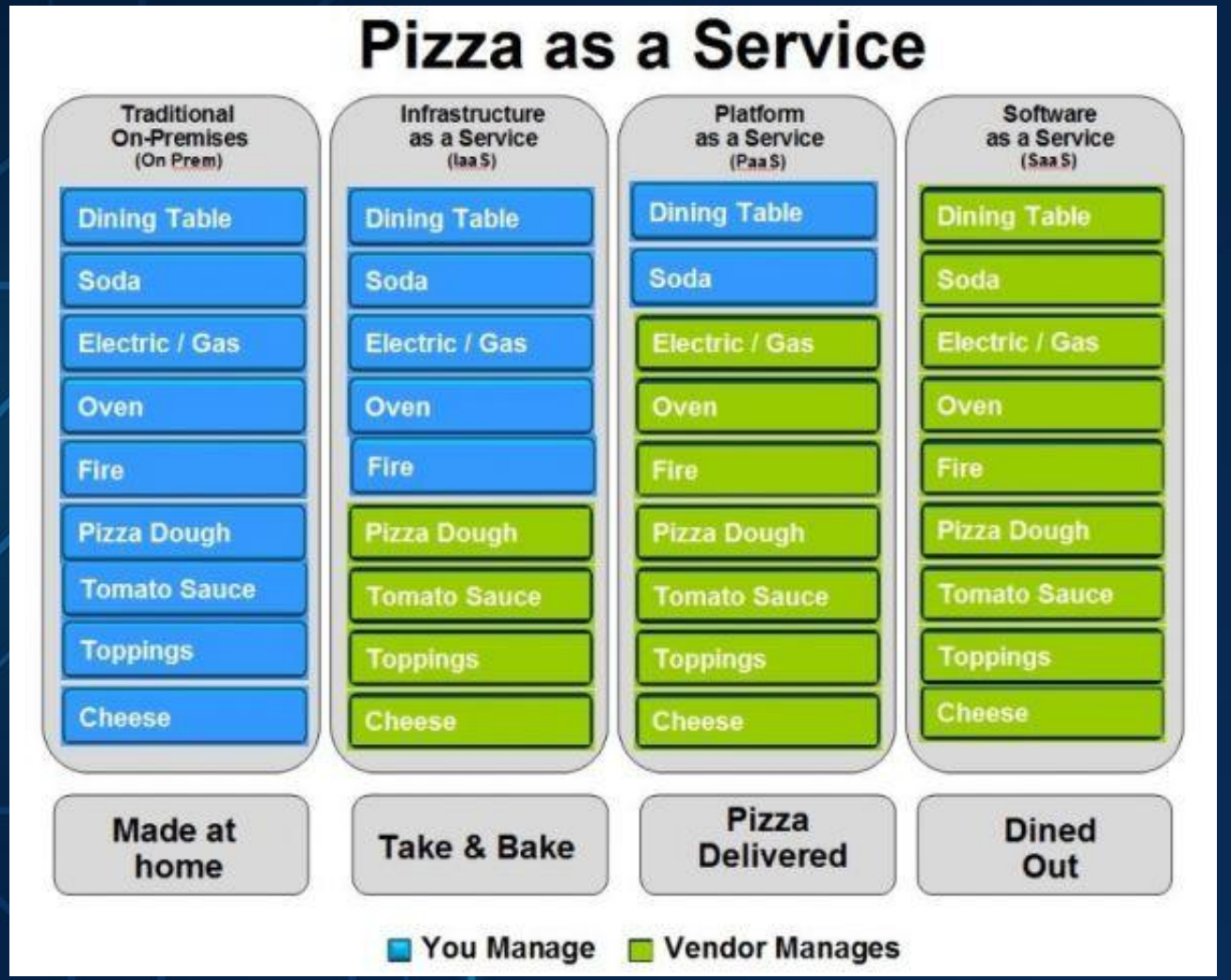
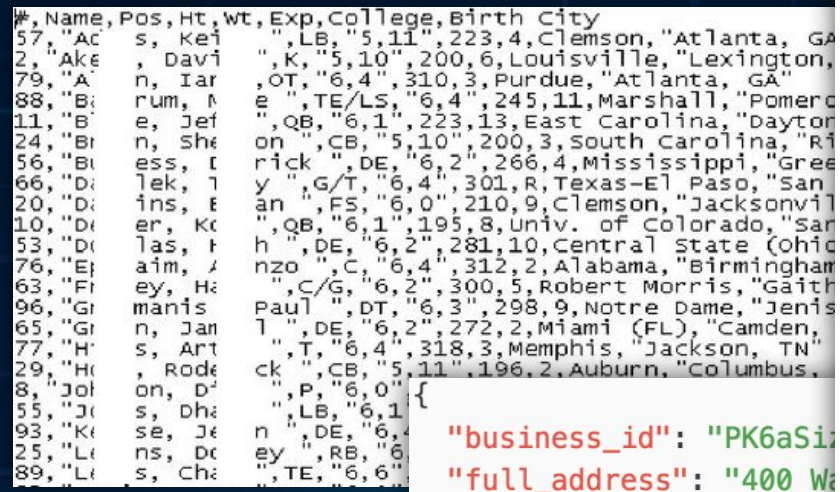


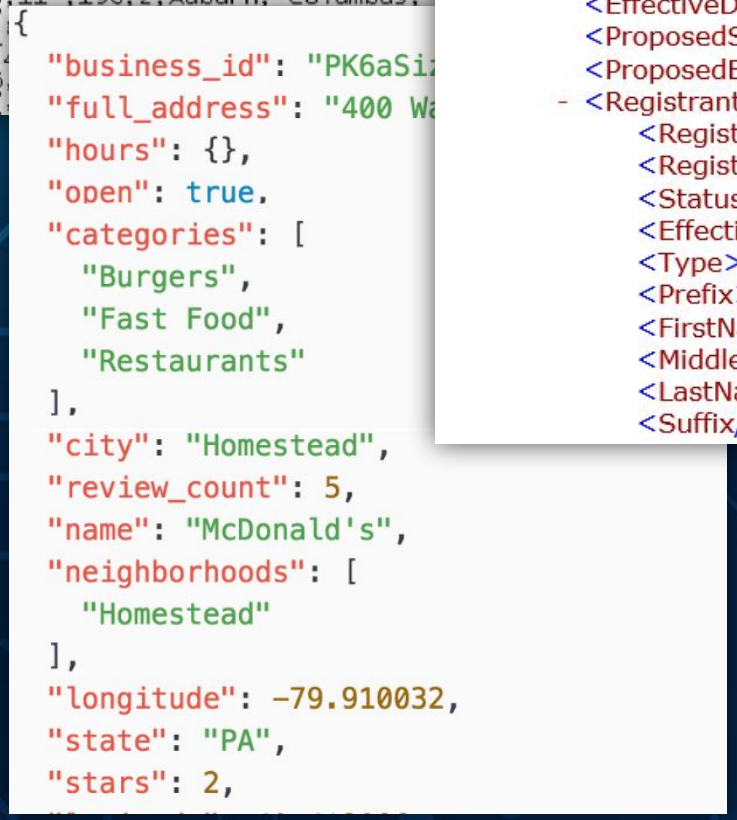
Image source: medium.com


123.548
150.128
238.727
283.026
314.036
380.485
411.495
52.669
322.896
269.736
34.949
318.466
353.906
83.678
274.166
371.625
247.587
221.007
181.137
229.867
57.099
105.828
21.659
345.046
79.248
74.818
216.577
358.336
145.698
198.857
194.427
252.017
212.147
88.108
260.877
367.195
154.558
376.055
30.519
132.408

Data Dimensions - Structured vs Unstructured



```
#,Name,Pos,Ht,Wt,Exp,College,Birth City
57,"Ac   s, Kei    ",LB,"5,11",223,4,Clemson,"Atlanta, GA
2,"Ake   , Davi   ",K,"5,10",200,6,Louisville,"Lexington,
79,"A    n, Iar   ",OT,"6,4",310,3,Purdue,"Atlanta, GA"
88,"B    rum, M   e  ",TE/LS,"6,4",245,11,Marshall,"Pomero
11,"B    e, Jef   ",QB,"6,1",223,13,East Carolina,"Dayton
24,"Br   n, She   on ",CB,"5,10",200,3,South Carolina,"Ri
56,"Bu   ess, D   rick ",DE,"6,2",266,4,Mississippi,"Gree
66,"Da   lek, J   y  ",G/T,"6,4",301,R,Texas-El Paso,"San
20,"Da   ins, E   an  ",FS,"6,0",210,9,Clemson,"Jacksonvil
10,"De   er, Ke   ",QB,"6,1",195,8,Univ. of Colorado,"San
53,"De   las, H   h  ",DE,"6,2",281,10,Central State (Ohio
76,"Ep   aim, A   nzo ",C,"6,4",312,2,Alabama,"Birmingham
63,"Fr   ey, Ha    ",C/G,"6,2",300,5,Robert Morris,"Gaith
96,"Gr   manis    Paul ",DT,"6,3",298,9,Notre Dame,"Jenis
65,"Gr   n, Jam   l  ",DE,"6,2",272,2,Miami (FL),"Camden,
77,"Hi   s, Art    ",T,"6,4",318,3,Memphis,"Jackson, TN"
29,"Ho   , Rode   ck ",CB,"5,11",196,2,Auburn,"Columbus,
8,"Joh   on, D    ",P,"6,0"
55,"Jo   s, Dha    ",LB,"6,1
93,"Ke   se, Je   n  ",DE,"6,4
25,"Le   ns, Do   ey ",RB,"6,
89,"Le   s, Cha   ",TE,"6,6"
```



```
{
  "business_id": "PK6aSiz
  "full_address": "400 Wa
  "hours": {},
  "open": true,
  "categories": [
    "Burgers",
    "Fast Food",
    "Restaurants"
  ],
  "city": "Homestead",
  "review_count": 5,
  "name": "McDonald's",
  "neighborhoods": [
    "Homestead"
  ],
  "longitude": -79.910032,
  "state": "PA",
  "stars": 2,
```

```
<?xml version="1.0"?>
- <ROWSET>
  - <ROW>
      <SMNumber>SM12232</SMNumber>
      <Status>Active</Status>
      <Type>In-house</Type>
      <SubjectMatter>Grants/Funding</SubjectMatter>
      <Particulars>City Partners sin
        funding with To pedestria
        provide the community w
        years+.</Particulars>
      <InitialApprovalDate>2008-09-
      <EffectiveDate>2012-01-18</
      <ProposedStartDate/>
      <ProposedEndDate/>
    - <Registrant>
        <RegistrationNUmber>1252
        <RegistrationNUmberWithSc
        <Status>Active</Status>
        <EffectiveDate>2012-06-0
        <Type>In-house</Type>
        <Prefix>Ms.</Prefix>
        <FirstName>Christa</First
        <MiddleInitials/>
        <LastName>Kroboth</Last
        <Suffix/>
```



```
name:
  '#title': 'Your Name'
  '#type': textfield
  '#required': true
  '#default_value': '[current-user:display-name]'
email:
  '#title': 'Your Email'
  '#type': email
  '#required': true
  '#default_value': '[current-user:mail]'
subject:
  '#title': 'Subject'
  '#type': textfield
  '#required': true
  '#test': 'Testing contact form from [site:name]'
message:
  '#title': 'Message'
```

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Data Dimensions - Structured vs Unstructured

It's on
it com
regior
just s

Image source: twitter.com/kareem_carr, soundcloud.com

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Data Dimensions - Logical vs Physical Medium

- **Object level**
  - Managed by an application
  - Custom metadata
- **File level**
  - Managed by an operating system
  - Fixed file-system attributes
- **Block level**
  - Managed by an operating system
  - Fixed system attributes

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Data Dimensions - Logical vs Physical Medium

Non-Volatile

- Hard Drive
- Flash Drive
- DVD

Volatile

- Random Access Memory
- Processor Registers

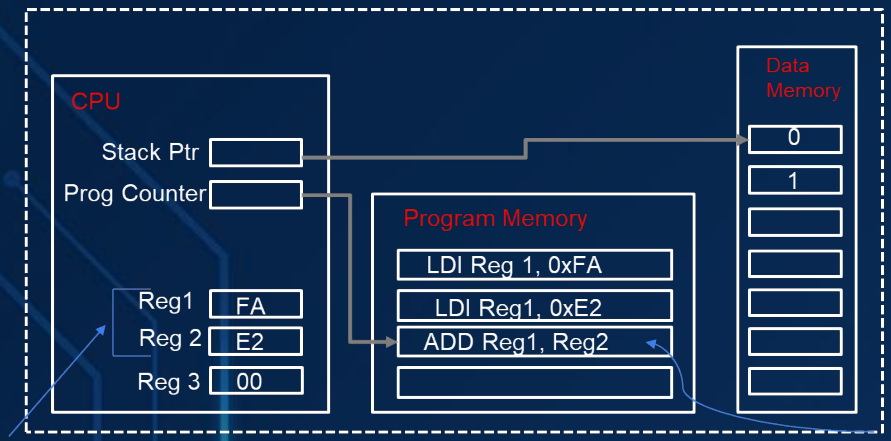


Image source: shutterstock.com, medium.com

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Data Dimensions - On-Premises vs Cloud

On-Premises

Image source: planetgeek.ch

Cloud

?

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Key Data Security Challenges in The Cloud

Image source giphy.com/animalsfacingleft:

Key Data Security Challenges in Cloud

Direct

- Data Leakage Detection and Prevention in Cloud
- Data Segregation and Protection
- Threat and Vulnerability Management
- Identity and Access Management
- Application Security
- Physical & Personnel Security

Source: "Data Security Challenges and Its Solutions in Cloud Computing Article" by R. Velumadhava Rao and K. Selvamani, 2015

Key Data Security Challenges in Cloud

Direct

- Data Leakage Detection and Prevention in Cloud
- Data Segregation and Protection
- Threat and Vulnerability Management
- Identity and Access Management
- Application Security
- Physical & Personnel Security

Indirect

- Ability to Support BCP & DR Requirements Securely
- Availability of Services and Data in the Cloud
- Incident Response Arrangements

Source: "Data Security Challenges and Its Solutions in Cloud Computing Article" by R. Velumadhava Rao and K. Selvamani, 2015


BOOKING HOLDINGS
CENTERS OF EXCELLENCE

Data Truncation

Shorten an object / datum so it wouldn’t disclose any sensitive information

Pros

- ✔ Full protection
- ✔ Relatively easy
- ✔ Negligible performance impact

Cons

- x You can’t retrieve the full piece of data
- x Uniqueness isn’t preserved deterministically

Data Hashing

Map arbitrary size value to fixed-size value

Pros

- ✔ (Highly) impossible to retrieve the original data from the hash value
- ✔ (Highly) injective (preserve uniqueness)
- ✔ Low performance impact

Cons

- x You can’t retrieve the cleartext data from the hash value

Data Tokenization

Turning a piece of data to a random unique string, and use a dictionary to bind them

Pros

- ✔ Tokenized data is completely random, meaningless, and doesn't provide even a small hint about the original data or it's tokenization algorithm
- ✔ Helps to reduce the regulatory scope
- ✔ Token can be format preserving

Cons

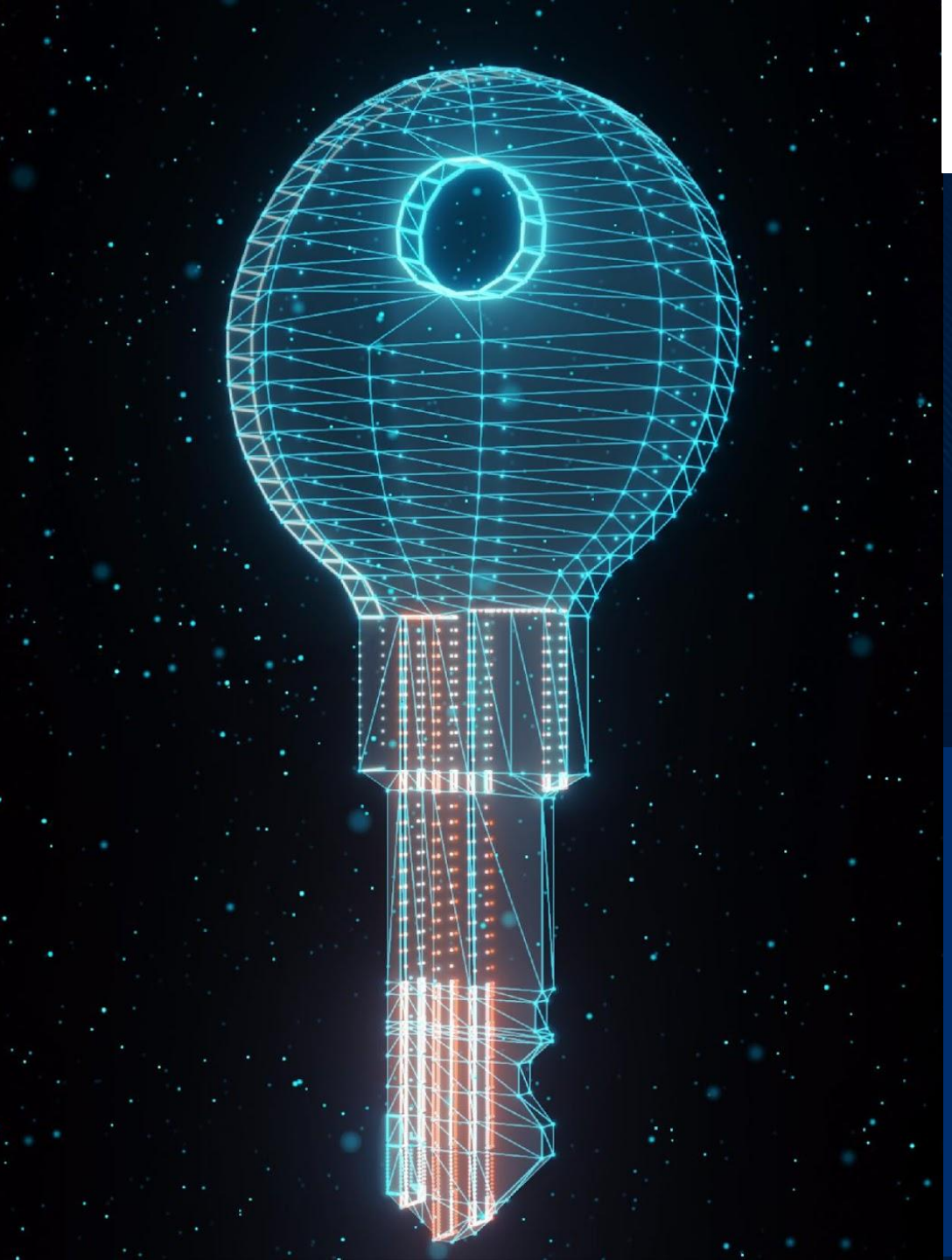
- ✔ Extra measures to protect the token dictionary
- ✔ High maintenance / performance impact with organizations dealing with huge sets of sensitive data
- ✔ Partial incompatibility due to the usage of non-standard algorithm to tokenize

Data Encryption

Turning a piece of data to a random unique string, and being able to retrieve the original data only with a key

There are various dimensions which we need to take into consideration while choosing data encryption as a data protection strategy:

- Symmetric vs Asymmetric
- Transparent vs Payload
- Mode of Operation
- Encryption Algorithm
- Key Management
- Key Architecture
- Single vs Dual Control
- Hardware Security Modules



DATA SECURITY SOLUTIONS - DATA ENCRYPTION

Symmetric

Pros

- Low performance impact

Cons

- A single key for both encryption and decryption
- Higher risk (Length / Excessive privileges)
- High maintenance

Asymmetric

Pros

- Encryption key is public knowledge
- No need for extra controls if you only need to encrypt

Cons

- High performance impact

BOOKING HOLDINGS
CENTERS OF EXCELLENCE

DATA SECURITY SOLUTIONS - DATA ENCRYPTION

Transparent

Pros

- Low performance impact
- Easy to implement
- No modifications need to be done on client side
- Effective low-level protection

Cons

- Ineffective for most attack scenarios
- Not applicable for all platforms
- Ineffective for OS level without TPM

BOOKING HOLDINGS
CENTERS OF EXCELLENCE
BPOPK

Payload

Pros

- Effective for most attack scenarios

Cons

- Mid-High performance impact
- Requires modification on client-side at most scenarios
- For most of the 3rd party solutions, not supported by-product

Data Encryption

Turning a piece of data to a random unique string, and being able to retrieve the original data only with a key

There are various dimensions which we need to take into consideration while choosing data encryption as a data protection strategy:

- Symmetric vs Asymmetric
- Transparent vs Payload
- Mode of Operation
- Encryption Algorithm
- Key Management
- Key Architecture
- Single vs Dual Control
- Hardware Security Modules

Conclusions and Takeaways

- **From data security perspective, On-Prem and Cloud are different - both on the attack vector level, and the type of solution which needs to be effective**
- **There are different motivations for data protection**
  - Complying with any regulation or standard
  - Having the right security maturity level to engage with specific partners or customers
  - Different Constraints to consider
- **Don’t use an ineffective “checking-the-mark” solutions**


Thank You