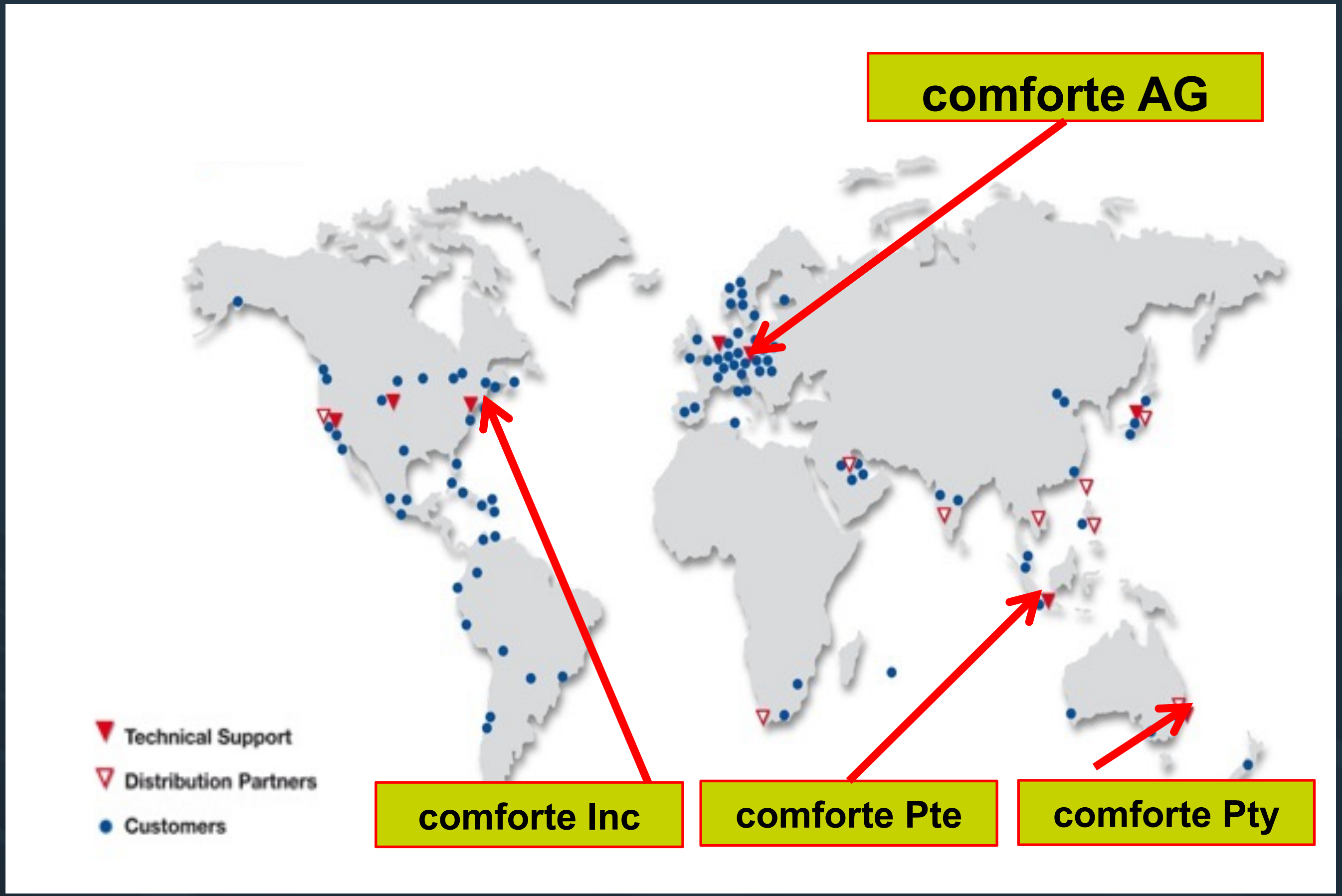
How to Securely Release the Value of Your Data From the HPE NonStop

Andreas Lutz & David Lock

Comforte

- Headquarters in Germany, offices in the USA, Australia & Singapore
- Privately owned – employs 160+ people around the world
- More than 25 years software provider for digital enablement & security on mission critical systems
- Over 600 enterprises worldwide rely on comforte solutions
- comforte AG protects approx. 60% of the worldwide credit card transaction business
- HPE Partnership since 2004 OEM security
- IBM Partnership since 2015 OEM middleware
- Help-Desk Support in English, Spanish and German



Hewlett Packard Enterprise

PCI Security Standards Council

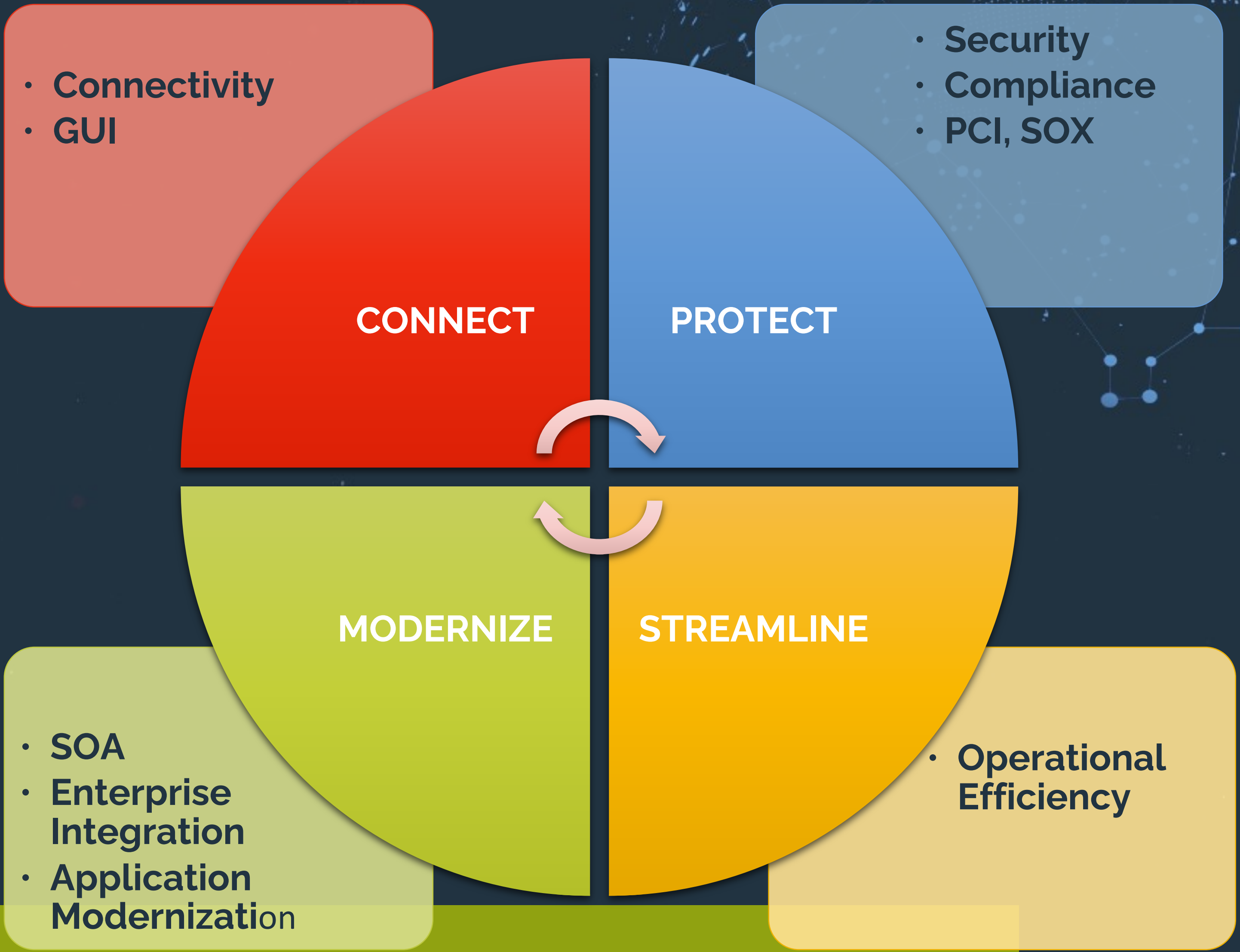
Accredited Standards Committee X9 Inc. Financial Industry Standards

IBM

comforte
19
98
25
20
23
YEARS OF SERVICE
★★★★★

comforte NonStop Product Suite

- MR-Win6530
- J6530
- JPath
- uLinga



- Connectivity
- GUI

CONNECT

- Security
- Compliance
- PCI, SOX

PROTECT

MODERNIZE

- SOA
- Enterprise Integration
- Application Modernization

STREAMLINE

- Operational Efficiency

- PANfinder
- SafePoint
- SecurDPS
- SecurLib
- SecurSSO
- SecurTape
- SecurTN

- CSL
- Escort SQL
- JPath

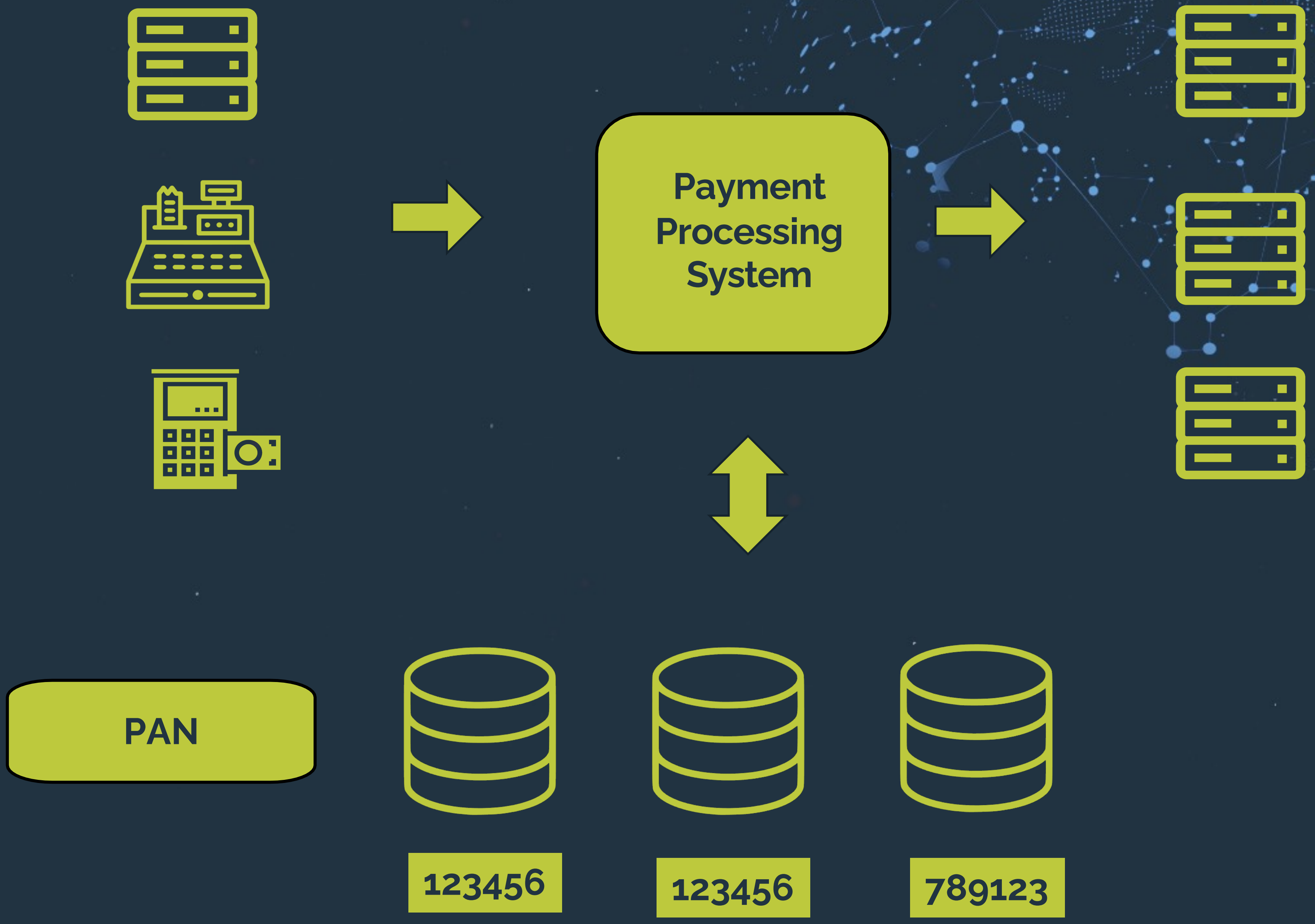
- Spool EmPower
- TOP

comforte

How to Securely Release the Value of Your Data From the HPE NonStop

Andreas Lutz & David Lock

Unprotected Data



Payment Processing System

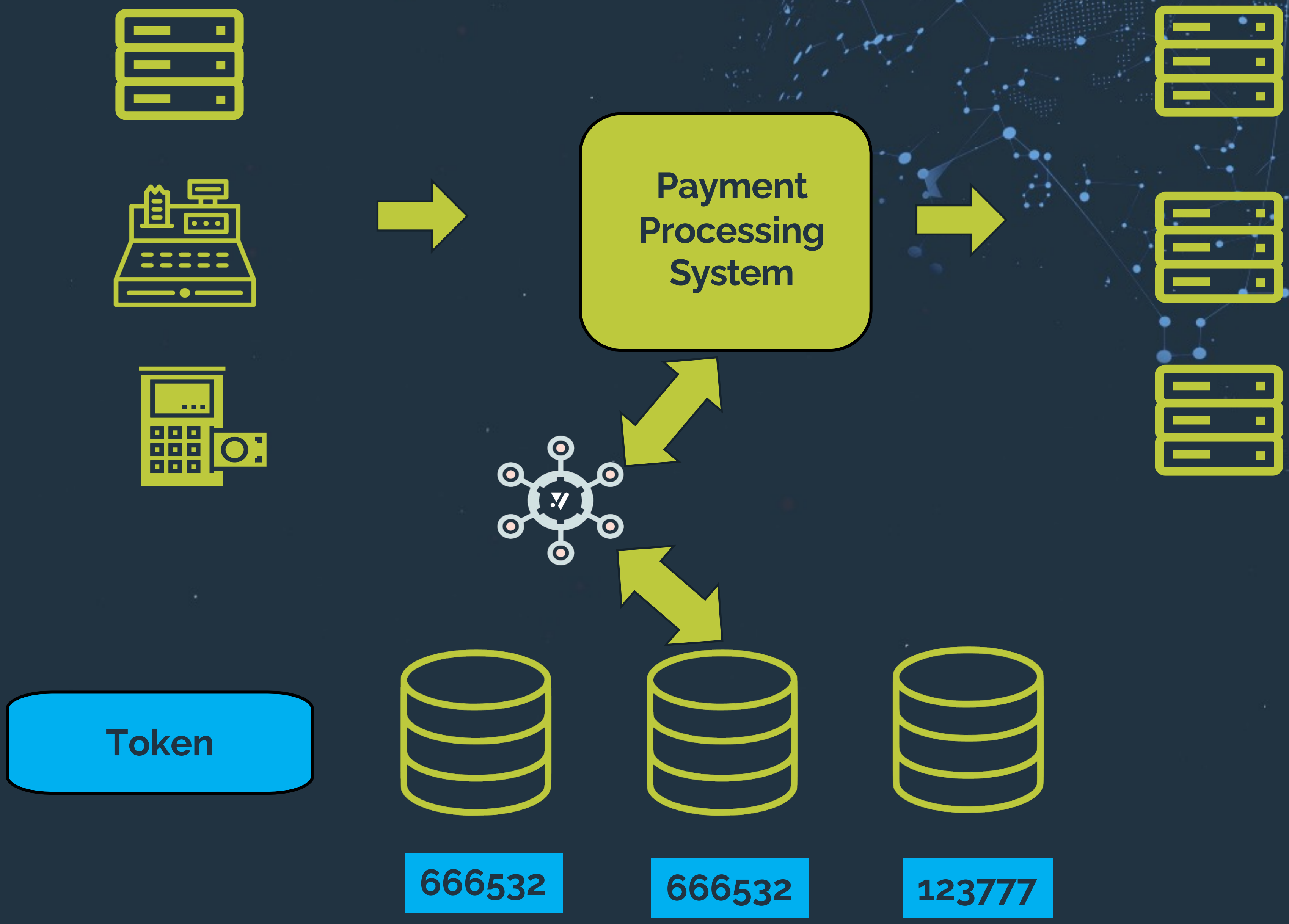
PAN

123456

123456

789123

Protected Data



Data Protection Methods

Clear

First	Last	Tax-ID	PAN	Phone	DOB
John	Smith	308-848-8163	4950 6997 2371 6503	982-824-9983	6/27/19

Loss of format, no usability, key rotation

Classic Encryption

First	Last	Tax ID	PAN	Phone	DOB
1TMVOHe%Pcx[...]	W1c9MLa9/zm[...]	:joN7dOG2rfyg[...]	kLtojCtlNJGkurBBdwwea3qd[...]	1TMVOoHePcx[...]	P5avCRZsL

Irreversible, not end-to-end, no utility

Data Masking

First	Last	Tax ID	PAN	Phone	DOB
XXXX	**XXXXX**	**XXX-XXX-**8163	4950 69**XX XXXX** 6503	**XXX-XXX-XXXX**	**X/XX/**1997

Tokenization

First	Last	Tax ID	PAN	Phone	DOB
Lkoiwey	Wuhrcghow	909-130-2983	4950 69**55 3333** 6503	622-978-8813	9/1/1965

Format preserving
Replace live data in apps, data stores and files

Reduce data exposure significantly
Operate on tokens while retaining data utility.

Reduce complexity
No key management required

Reduce cost of operation
Tokenize only where data is captured and where live data is interchanged. Everything else operates on tokens.

SecurDPS and PCI DSS

Objective	Requirements	SecurDPS direct impact
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components	
Protect Account Data	3. Protect stored account data	✓
	4. Protect cardholder data with strong cryptography during transmission over open, public networks	✓
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software	
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data	
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data	✓
	11. Test security of systems and networks regularly	
Maintain an Information Security Policy	12. Support information security with organizational policies and programs	

Secure, future-proof technology

Stateless / Vault-less tokenization

ANSI X9.119-2 tokenization standard

Patented technology

Validated by independent cryptologists

Highly performant

Quantum-safe

WHITE PAPER

COMFORTE AG
SECUREDPS

PCI DSS TECHNICAL ASSESSMENT

LYLE MILLER | CISA, CISSP, QSA, PA-QSA,
PCI SSLCA, PCI SSA
NICK TRENC | PCI SSLCA, PCI SSA, CISSP, CISA,
QSA (P2PE), PA-QSA (P2PE), QPA, CCSK

On Practical Provably-Secure FPE Schemes

Viet Tung Hoang

Dept. of Computer Science, Florida State University, USA

July 14, 2019

1 Summary

The goal of this report is to design practical Format-Preserving Encryption (FPE) schemes with

Analysis of comForte 21 Tokenization Algo

Dr Carlos Cid and Prof Fred Piper
Codes & Ciphers Ltd.

14 October 2014
version 2.0

1 Introduction

comForte 21 GmbH have commissioned Codes & Ciphers
uation of the company's proposed tokenization mechanis
mechanism is to produce a replacement string (a "token")
a Primary Account Number (PAN) string, but potential

FAST: Secure and High Performance Format Preserving Encryption and Tokenization

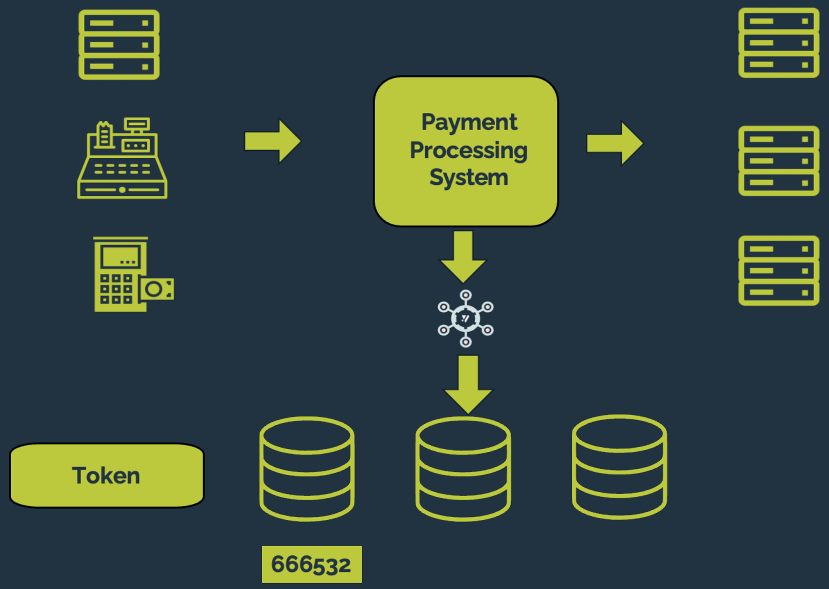
F. Betül Durak[1], Henning Horst[2], Michael Horst[2], and Serge Vaudenay[3]

[1] Robert Bosch LLC Research and Technology Center, Pittsburgh, USA
[2] Comforte AG, Germany
[3] EPFL, Lausanne, Switzerland

Abstract. We propose a new construction for format preserving data protection. Our design provides the flexibility for use in format preserving encryption (FPE) and for static table driven tokenization. Our algorithm is a substitution-permutation network based on random Sboxes. Using pseudorandom generators and pseudorandom functions, we prove a strong adaptive security based on the super-pseudorandom permutation assumption of our core design. We obtain empirical parameters to reach this assumption. We suggest parameters for quantum security. Our design accommodates very small domains, with a radix a from 4 to the Unicode alphabet size and a block length ℓ starting 2. The number of Sbox applications is asymptotically $\ell^{\frac{3}{2}}$, which is also the number of bytes we need to generate using AES in CTR mode. For instance, we tokenize 10 decimal digits using 27 (parallel) AES computations to be done only once, when the tweak changes.

Summary

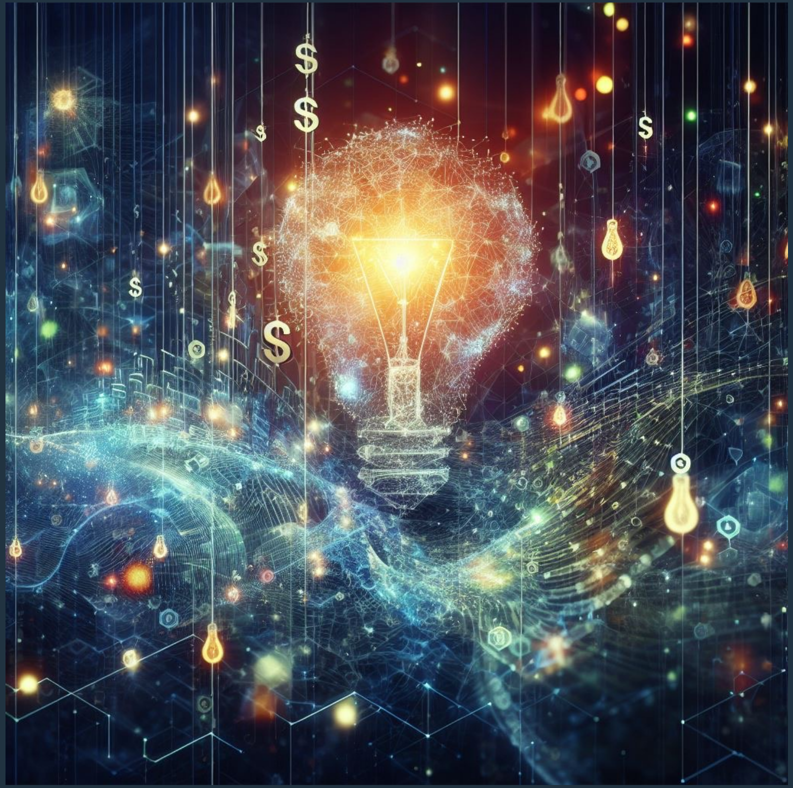
- SecurDPS can provide a native NonStop solution for Tokenisation of all data – Including PAN
- It does not change the overall architecture
- Protects data as default – only used when required
- Provides a solution for all applications
- Easy implementation
- Can be extended to enterprise solution
- Only solution for PCI 4.0



The Value of Data

"The value of data refers to the benefits and advantages that organizations can derive from their data assets, such as innovations, services, security measures, improved decision-making, better customer experiences, increased operational efficiency, and new revenue streams.."

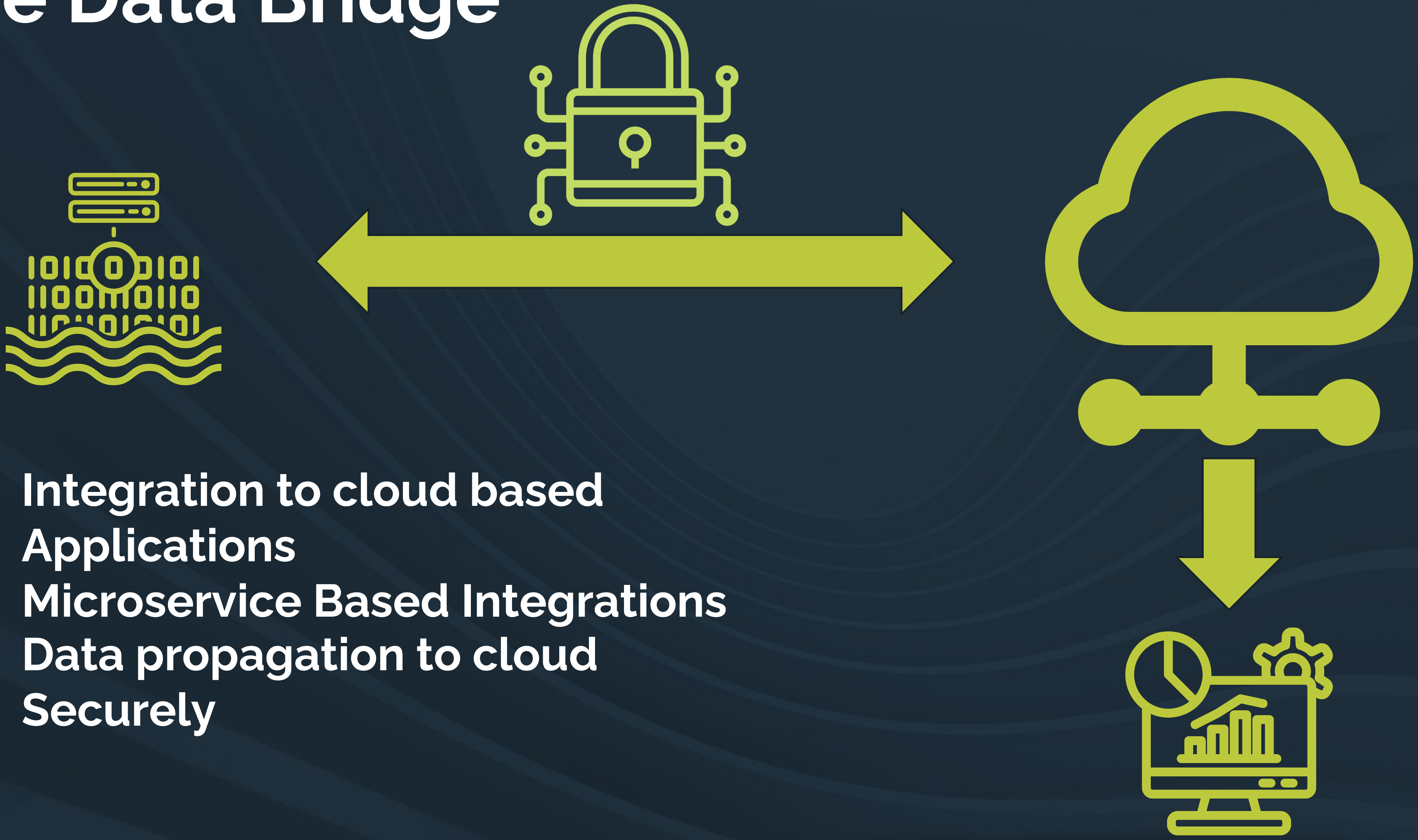
HPE



12

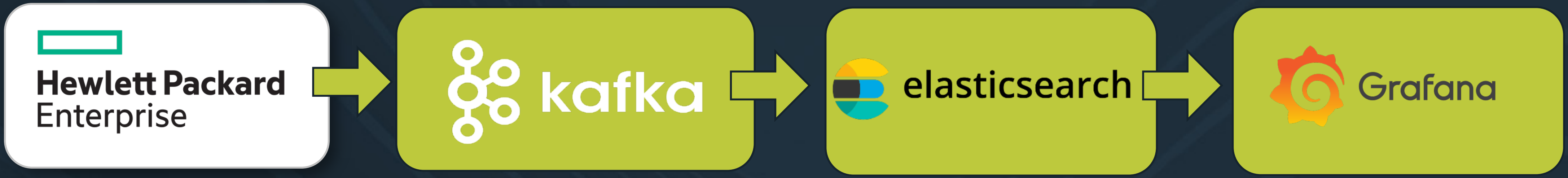
The Data Pond in NonStop

The Data Bridge

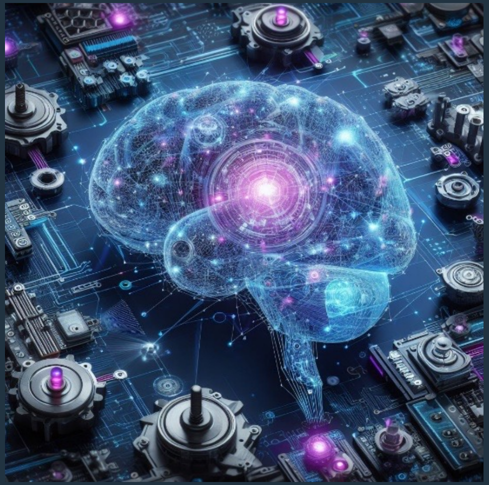


- Integration to cloud based Applications
- Microservice Based Integrations
- Data propagation to cloud
- Securely

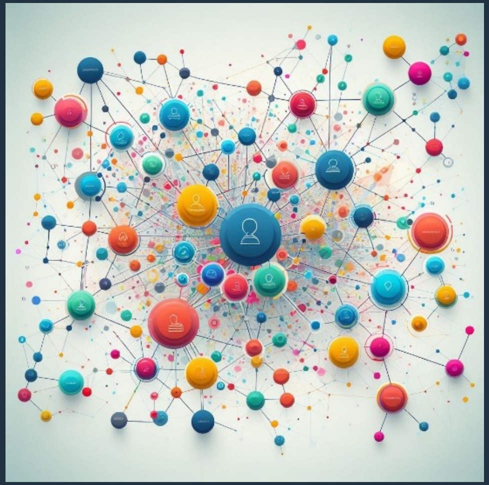
A Potential Pipeline



Some Opportunities Of Opening up the Data Pond With SecurDPS and Ulinga for Kafka



Machine Learning



Data Visualisation

Alerting

Cross Selling

SIEM

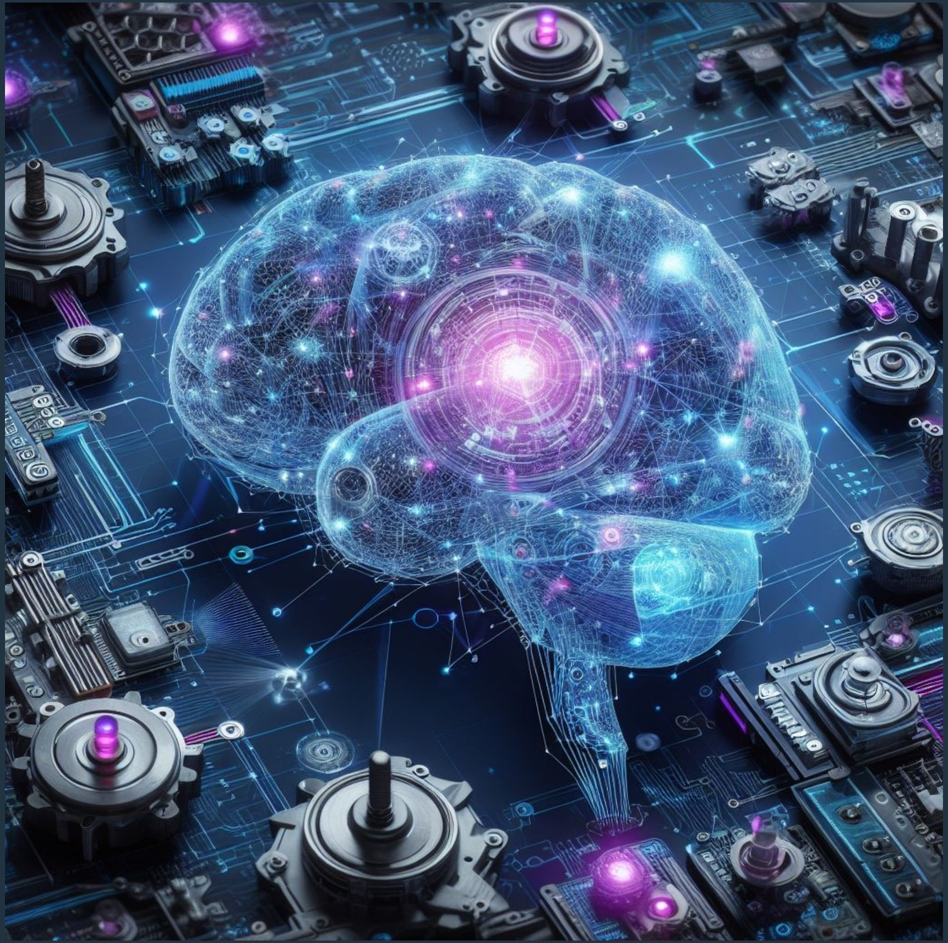
Forensic Data

* Images produced by Dall-E 3

Machine Learning and AI

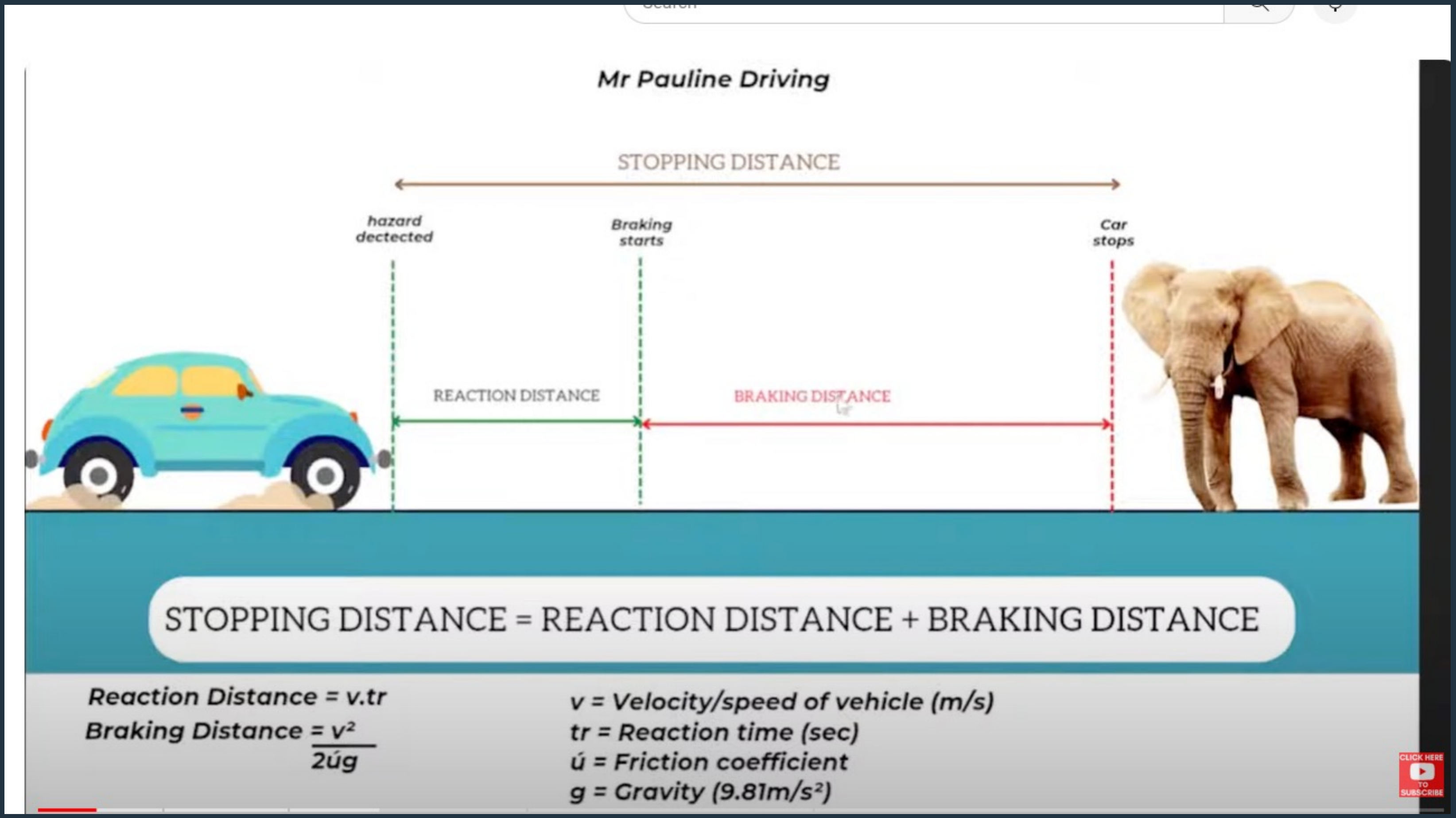
Some Examples

Fraud
Predictive Maintenance
Cash prediction



* Images produced by Dall-E 3

Fraud – Stopping Distance



STOPPING DISTANCE = REACTION DISTANCE + BRAKING DISTANCE

Reaction Distance = v.tr

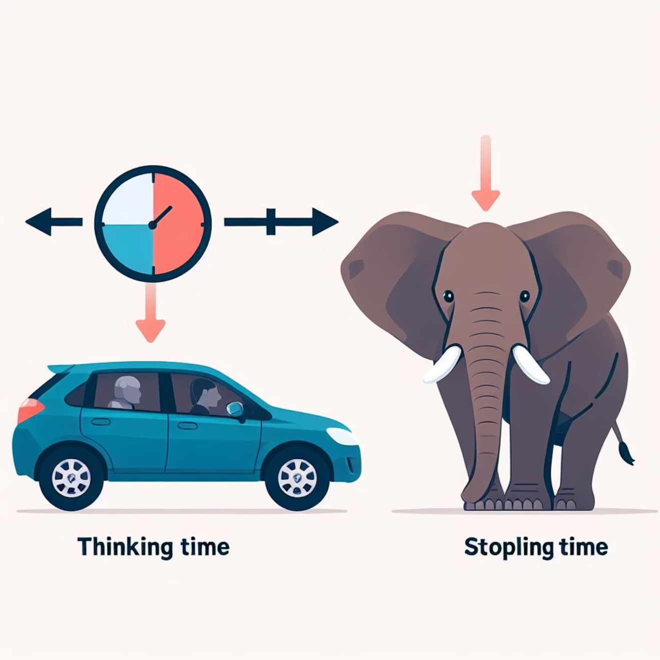
Braking Distance = $\frac{v^2}{2úg}$

v = Velocity/speed of vehicle (m/s)

tr = Reaction time (sec)

ú = Friction coefficient

g = Gravity (9.81m/s²)



* Images produced by Dall-E 3

Cash Prediction

- Major cost of running ATM network
- Predicting cash model – multi million cost
- Using H2o models getting ‘similar’ results
- Also predict cash out if a run on cash
  - Competitors ATM fails

* Images produced by Dall-E 3

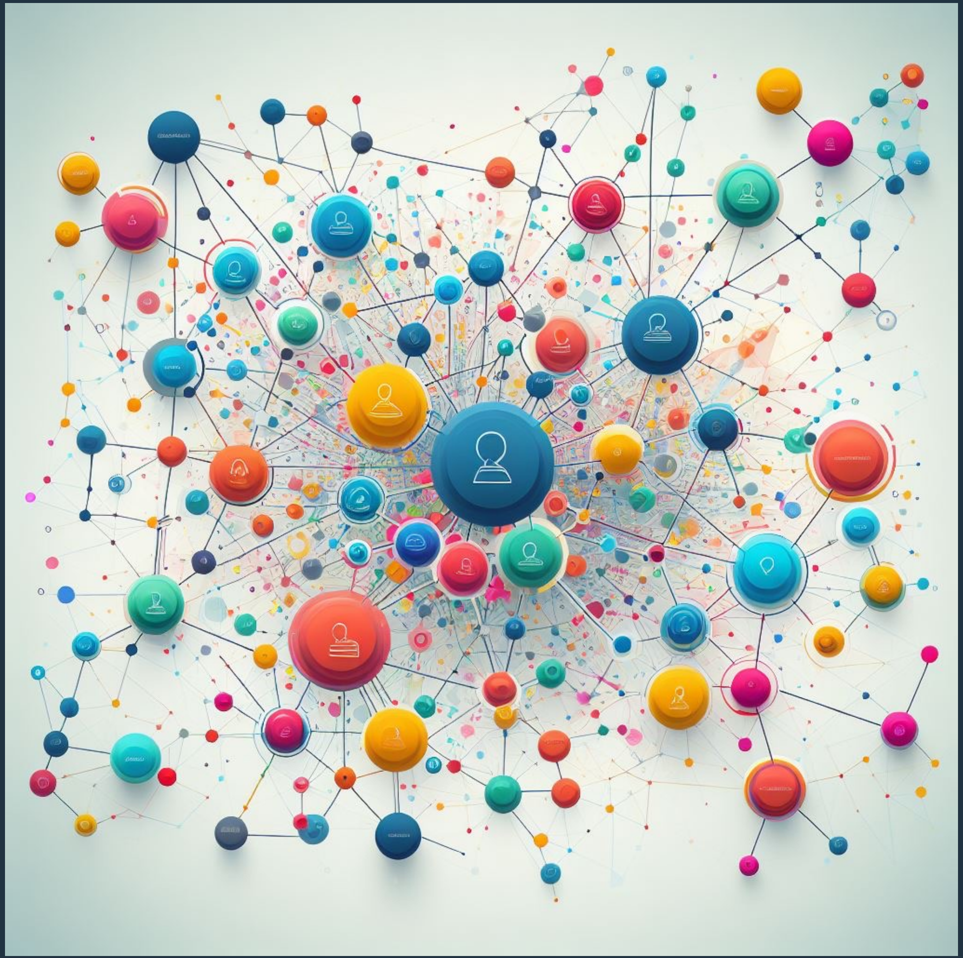
Preventive Maintenance

- Analysing errors and delays
- Can predict if machine will have problem
- Allow replacements etc. to provide continuous availability

* Images produced by Dall-E 3

Data Visualisation

A Picture is worth a thousand words
Even more if it's Real Time



* Images produced by Dall-E 3

Examples

- Areas of Device Estate Available
- Liquidity Positions
- Endpoint Profitability
- Card use splits and drill down
- Country code usage

Alerting

* Images produced by Dall-E 3

Intelligent monitoring based on previous activity

Unusual patterns – e.g. by BIN

Messages from logs

SIEM Functions

<u>Consolidation is key</u>

Security ‘Islands’ are huge weaknesses

Ability to send Log data for EMS

Log data for SecurDPS

* Images produced by Dall-E 3

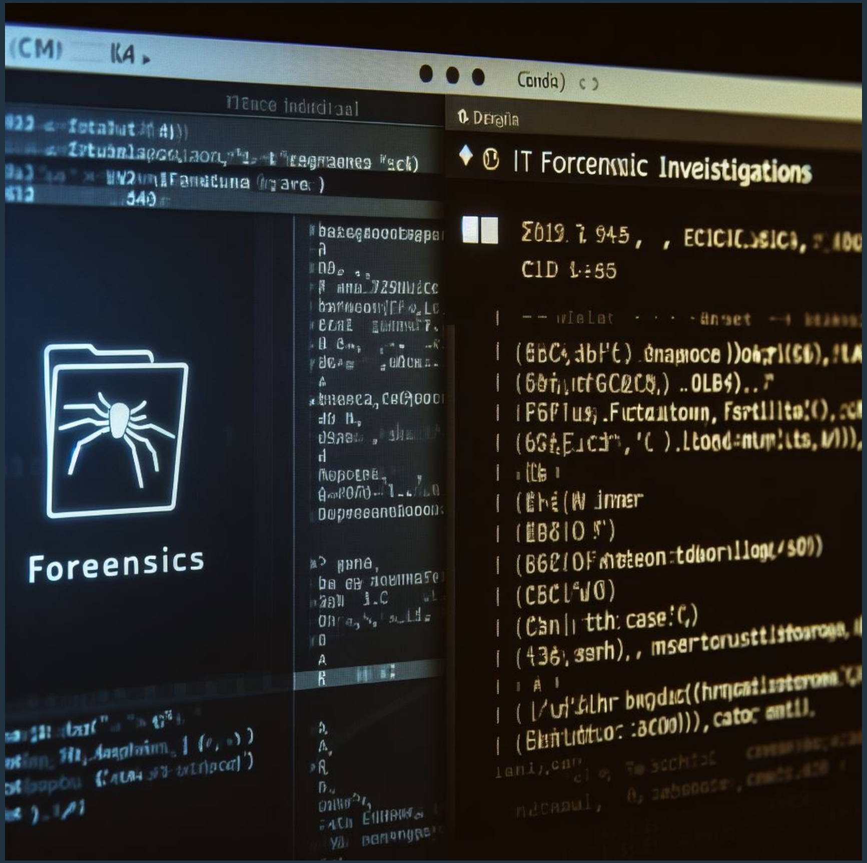
Forensic Investigations

Real time vs historic

Full text search

Reviewing historical patterns

Looking for ‘clusters’



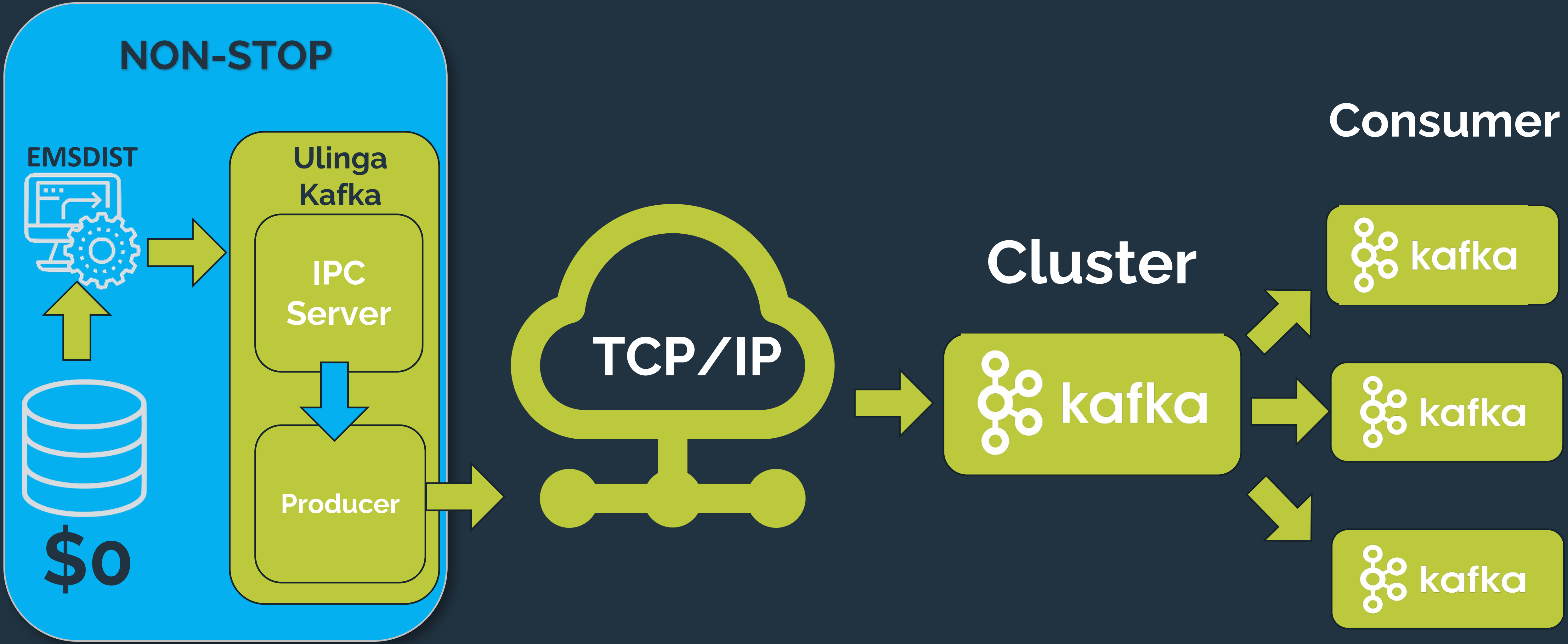
* Images produced by Dall-E 3

What are the Benefits?

- Your mileage will vary
- Tokenisation is a requirement for PCI
- Most banks will have a cloud infrastructure with NoSQL
- Combining those two elements can give huge returns
- Speed and agility of data

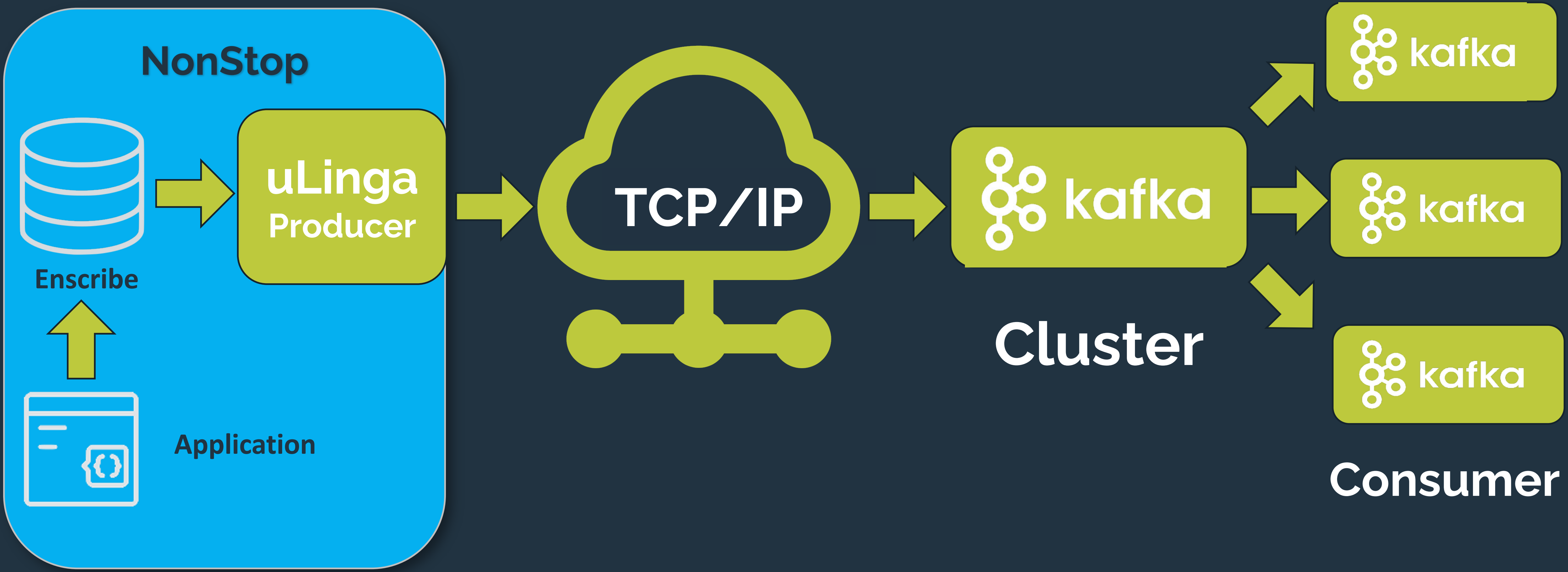
* Images produced by Dall-E 3

Streaming EMS Events to Kafka

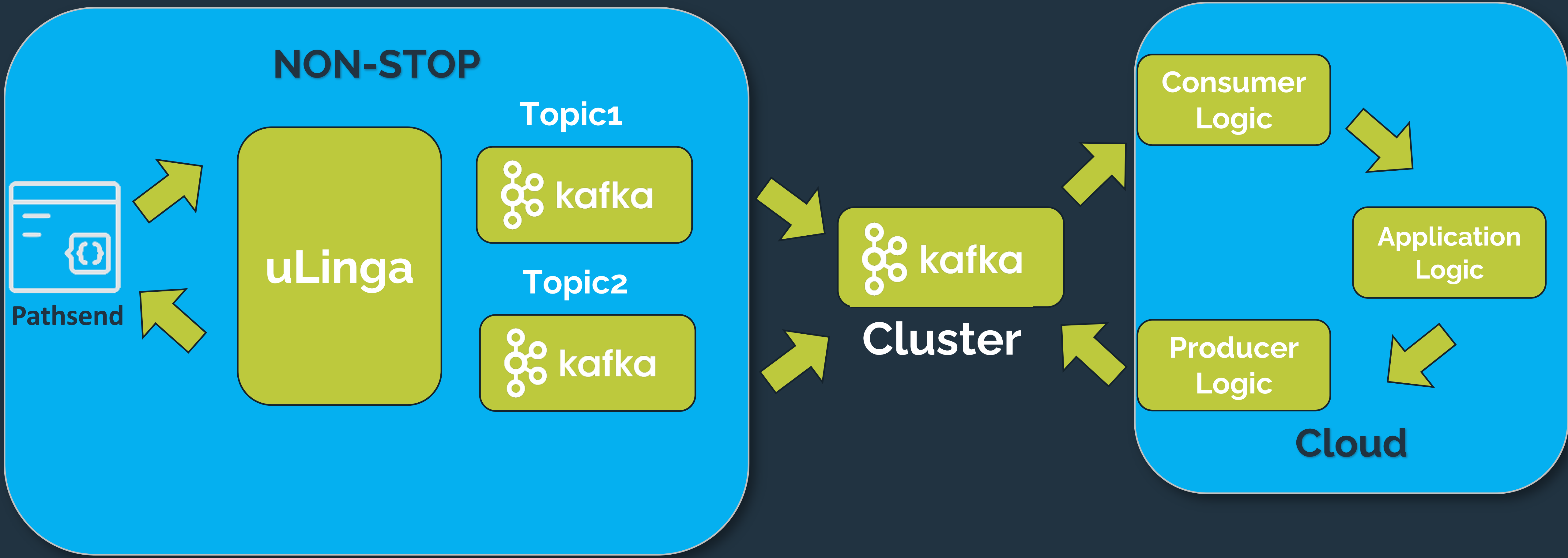


```
TACL> EMSDIST /NOWAIT/ COLLECTOR $0, TYPE PRINTING, TEXTOUT $ULKAF.#KAFKA1
```

Enscribe Support - Producer



Produce Consume - Example



NON-STOP

Topic1

Topic2

Pathsend

uLinga

kafka

kafka

kafka

Cluster

Consumer Logic

Application Logic

Producer Logic

Cloud

comforte

Summary

- Secure PCI compliant Integration to Cloud Based Applications
- Security ecosystem across all platforms
- Open up more actionable data for business benefit
- Enrich data for greater utilisation

comforte

SECURE YOUR GROWTH

www.comforte.com