comforte

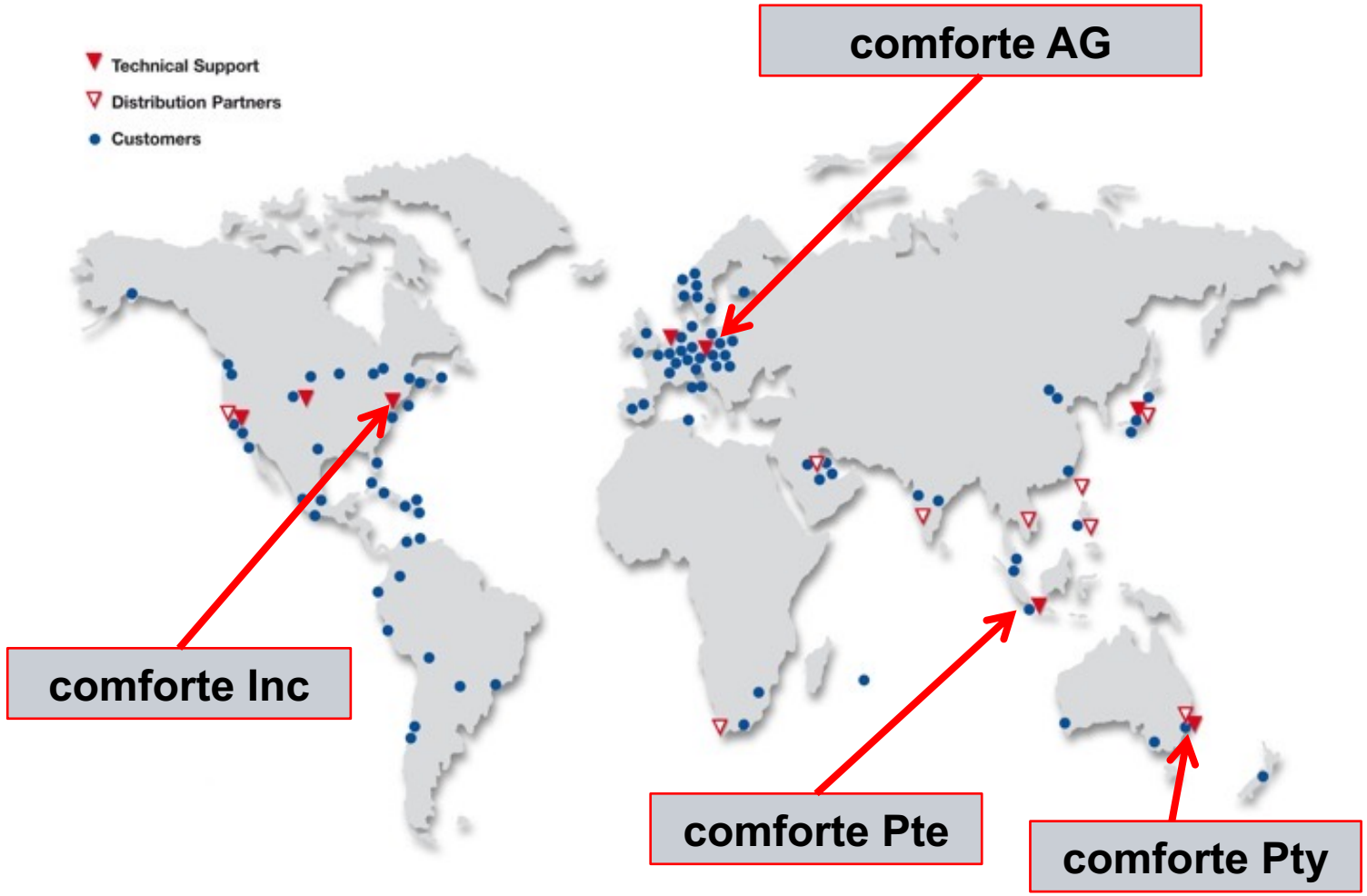
German NonStop User Group e.V.
Member of Connect Deutschland

Zero Trust and Data Centric Security

The Misunderstood ‘Pillar’ of Zero Trust

Helmut Bernhard
Senior Solutions Architect EMEA
comforte AG
27th April 2022

COMFORTE AS A COMPANY

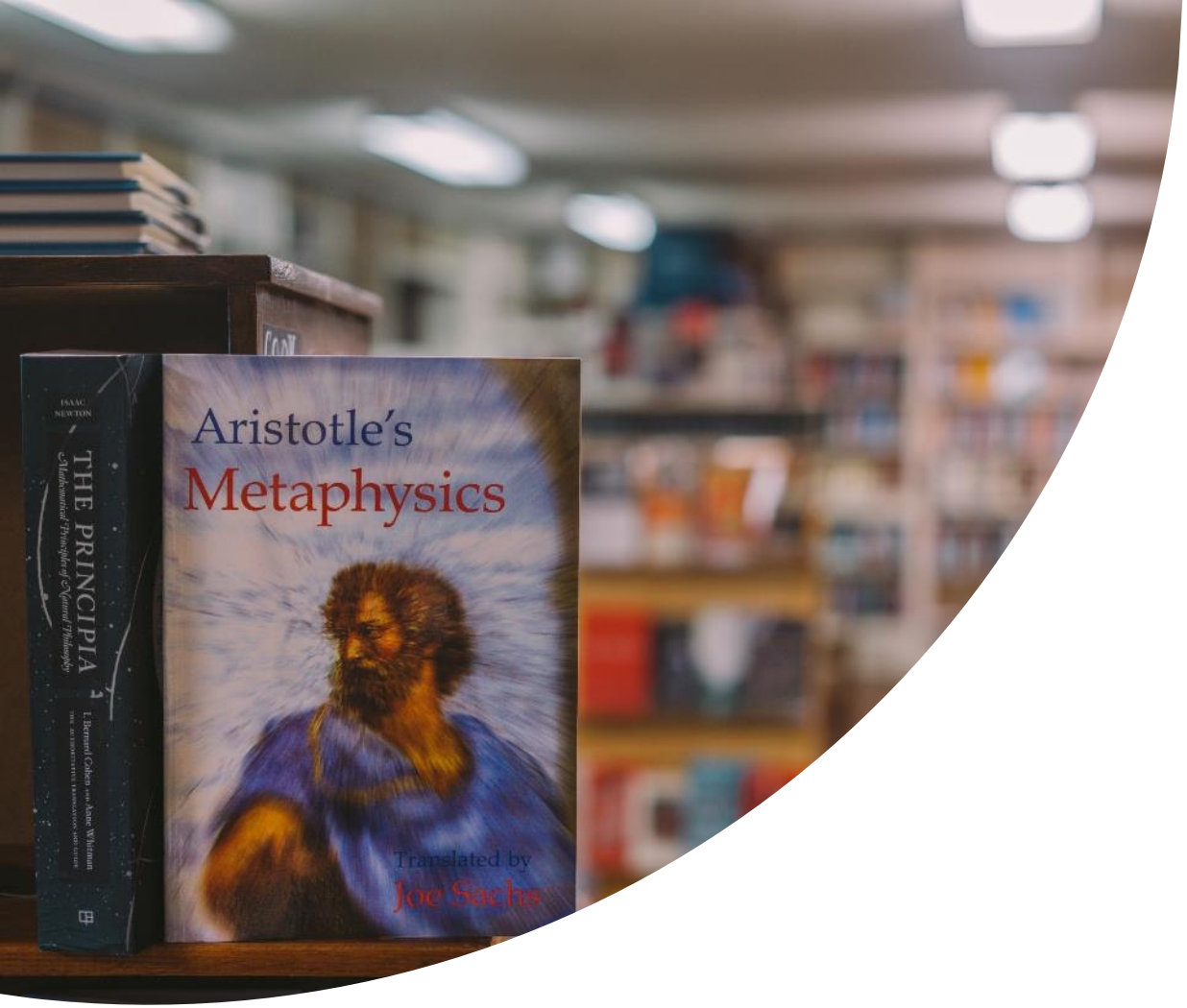


- Headquarter in Germany, offices in the USA, Australia & Singapore
- More than 30 years support for Tandem and HPE NonStop
- Public Company – employs 150+ people around the world
- Over 500 enterprises worldwide rely on comforte solutions
- Market leader for data security and cloud-native tokenization using our own patented methodology
- Internationally recognised cryptologists core members of our team
- Secure billions of identity records, payments and other secret information across our customer base around the world
- 24x7 Help-Desk Support in English, Spanish and German

Hewlett Packard Enterprise

PCI Security Standards Council

Accredited Standards Committee X9 Inc.
Financial Industry Standards



“

ZT is a dramatic shift in philosophy of how we secure our infrastructure, networks, and data

US DoD

Is This Zero Trust?

- Overused
- Misunderstood
- Marketing-speak
- Practical
- Complex

Drivers for a security framework like ZT

Attack surfaces
Distributed remote workforce and increased mobile devices

High-profile breaches
Attacks against supply chains and infrastructures

Cloud architectures
Companies continue to shift more data to cloud resources

Legacy systems/tools & methods
Too focused on borders and perimeters around data

Borders and perimeters will always be compromised

What threat actors want:

1. Compromise/breach a data environment
2. Apprehend data of value
3. Leverage/monetize/weaponize stolen data

“A ZT approach is primarily focused on **data** and **service** protection

NIST

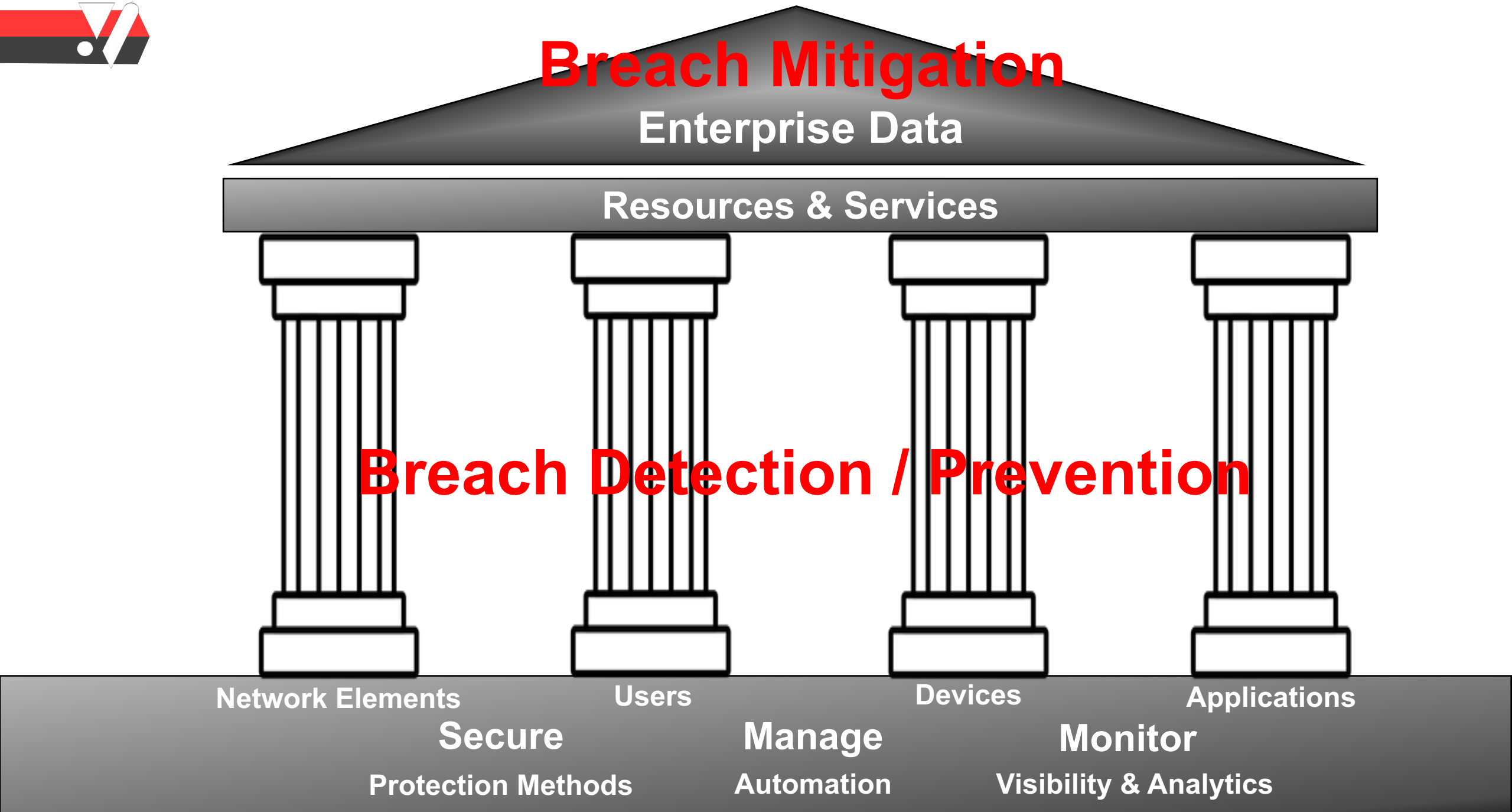
“Successful organisations can significantly facilitate the utilisation and value of their data by transitioning from siloed data security offerings to data security platforms.

This enables simpler, consistent end-to-end data security. A DSP solution delivers and protects this future state.

Gartner approved citation

Gartner 2022 Strategic Roadmap for Data Security Platform Convergence,Joerg Fritsch, Brian Lowans, David Mahdi,28th September 2021

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.


Breach Mitigation
Enterprise Data
Resources & Services
Breach Detection / Prevention
Network Elements
Users
Devices
Applications
Secure
Protection Methods
Manage
Automation
Monitor
Visibility & Analytics

Data-Centric Security: Classic Encryption

First	Last	Tax ID	P-ID	PAN	EXP	Phone	DOB
Chandra	Lagharinan	308-848-8163	A726	4950 6997 2371 6503	02/25	982-824-9983	6/27/1997

First	Last	Tax ID	P-ID	PAN	EXP	Phone	DOB
1TMVOHe%Pcx[...]	W1c9MLa9/zm[...]	:joN7dOG2rfyg[...]	GuywuJH[...]	kLtojCtlNJGkurBBdwwea3qd[...]	*Jwiow[...]	1TMVOoHePcx[...]	P5avCRZsLbbY[...]

Not format preserving
Requires app & schema changes

Live data exposure in systems
De-protection required for processing.
Keys must be present at all times.

Complex key management and operation
Backup, re-encryption of data over key change

High cost of operation
must be on every system, always on.

Data-Centric Security: Tokenization

First	Last	Tax ID	P-ID	PAN	EXP	Phone	DOB
Chandra	Lagharinan	308-848-8163	A726	4950 6997 2371 6503	02/25	982-824-9983	6/27/1997

First	Last	Tax ID	P-ID	PAN	EXP	Phone	DOB
Lkoiwey	Wuhrcghow	909-13-2983	P423	4950 69**AY HHIW** 6503	12/26	622-978-8813	9/1/1965

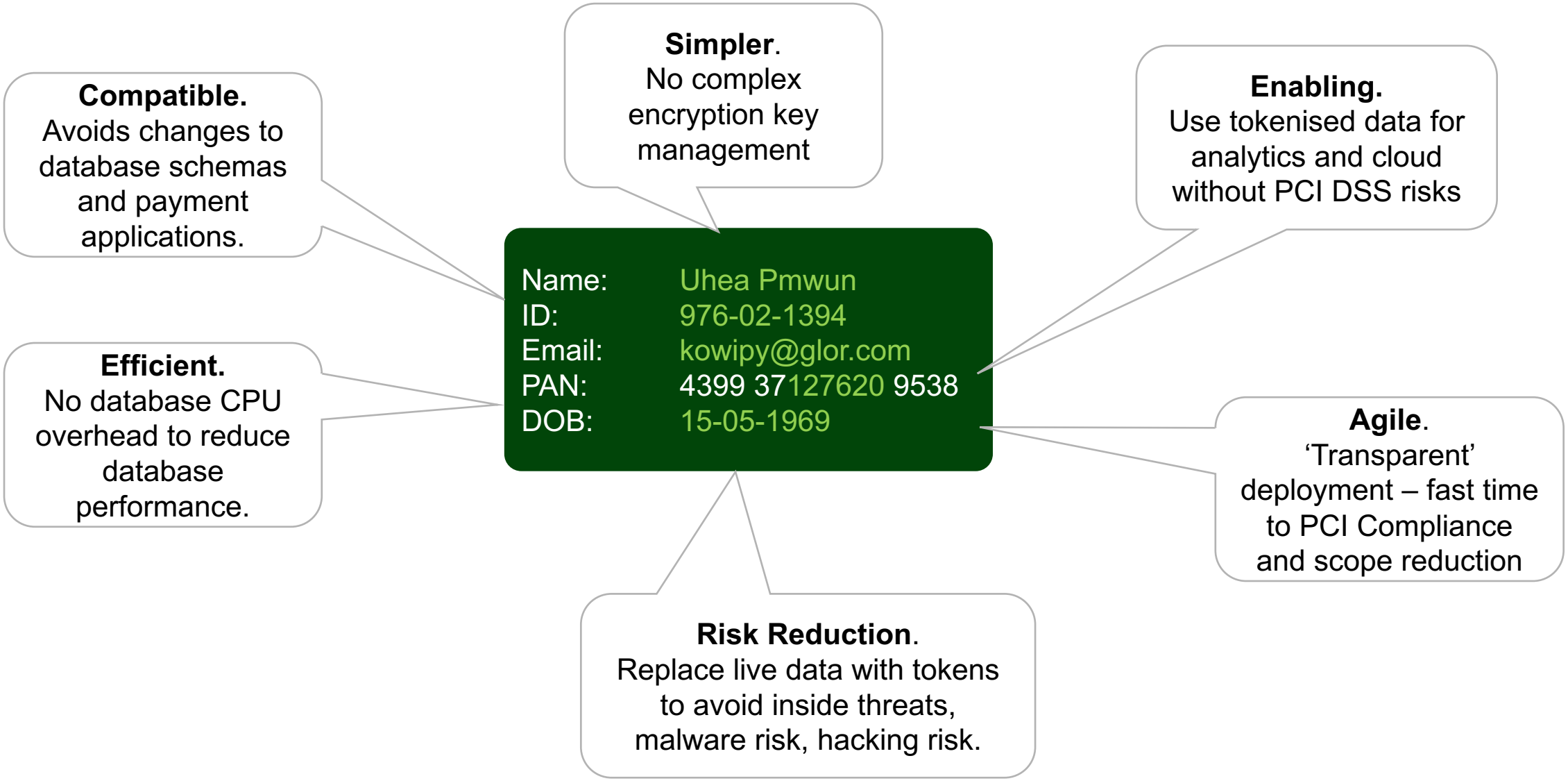
Format preserving
Replace live data in apps, data stores and files

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.

Business Advantages of Tokenisation



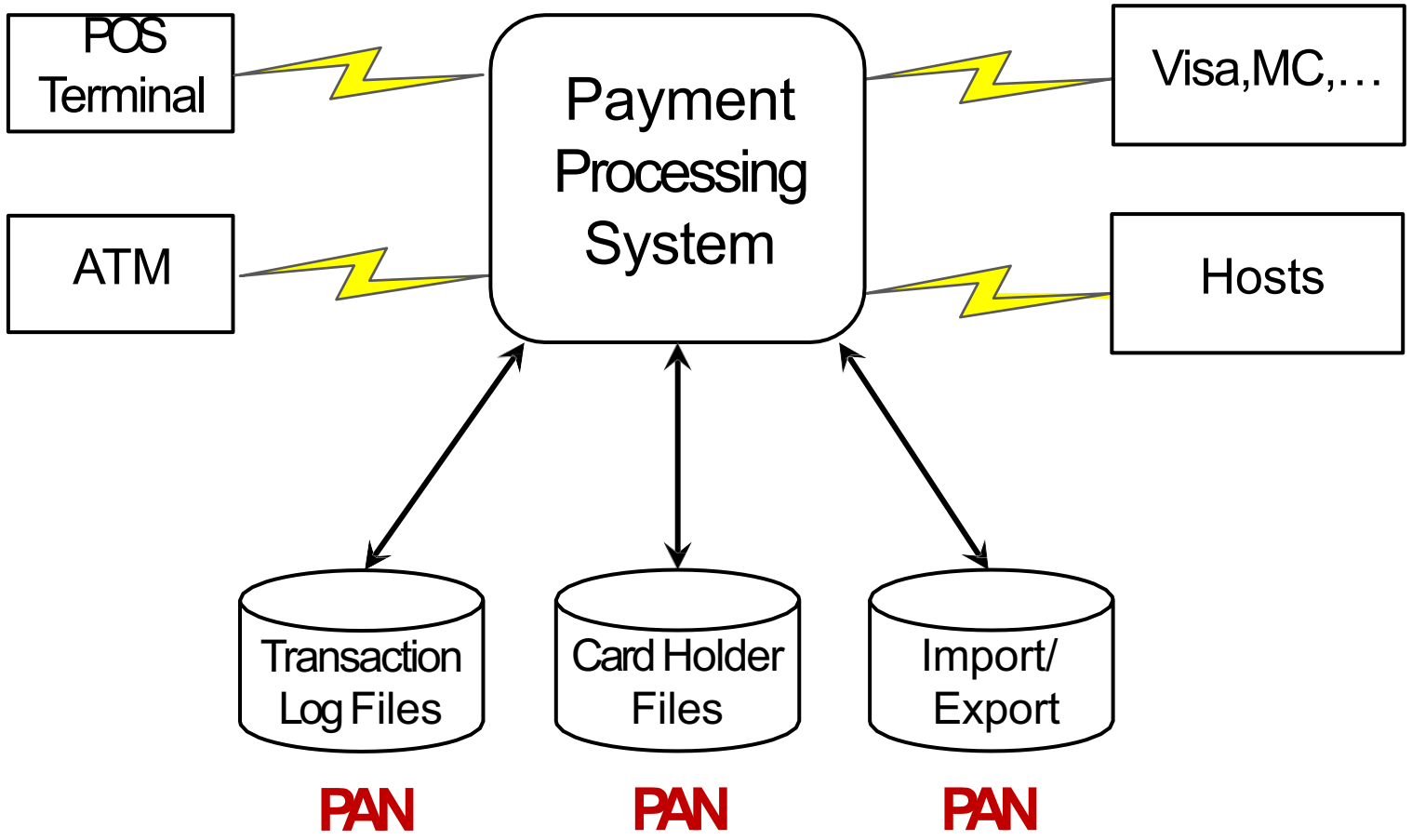
Major Fashion Retailer

- Spent $5.5M USD deploying data-centric protections for stores
- Saved $13M avoiding back-to-back firewall deployments
- Saved millions more on auditing & PCI compliance
- Reduced infrastructure complexity & monitoring costs

NB: Typical customer projects start at approx. €200k, dependent on size and complexity of the customer environment

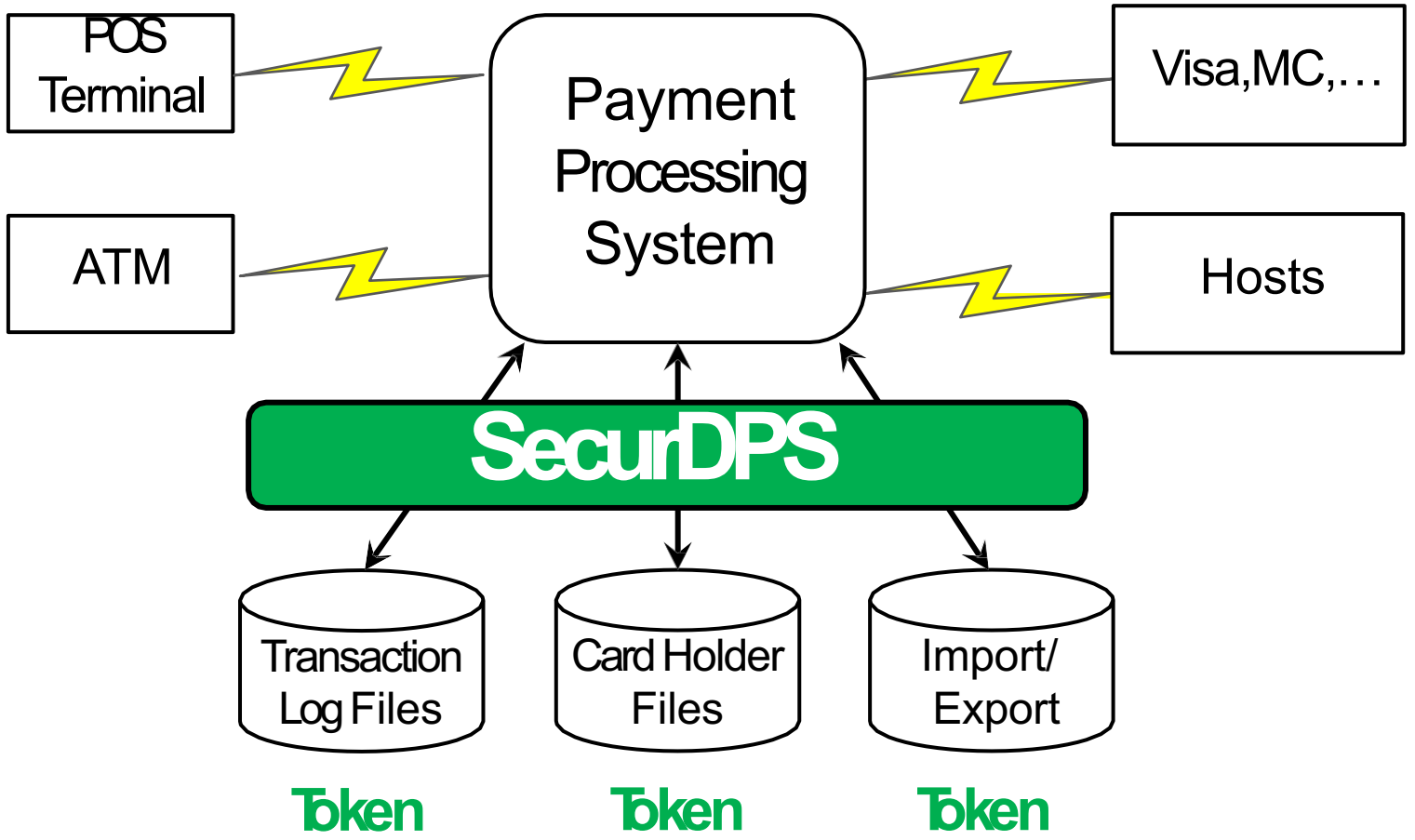
High Level View on a typical Payment System

Example



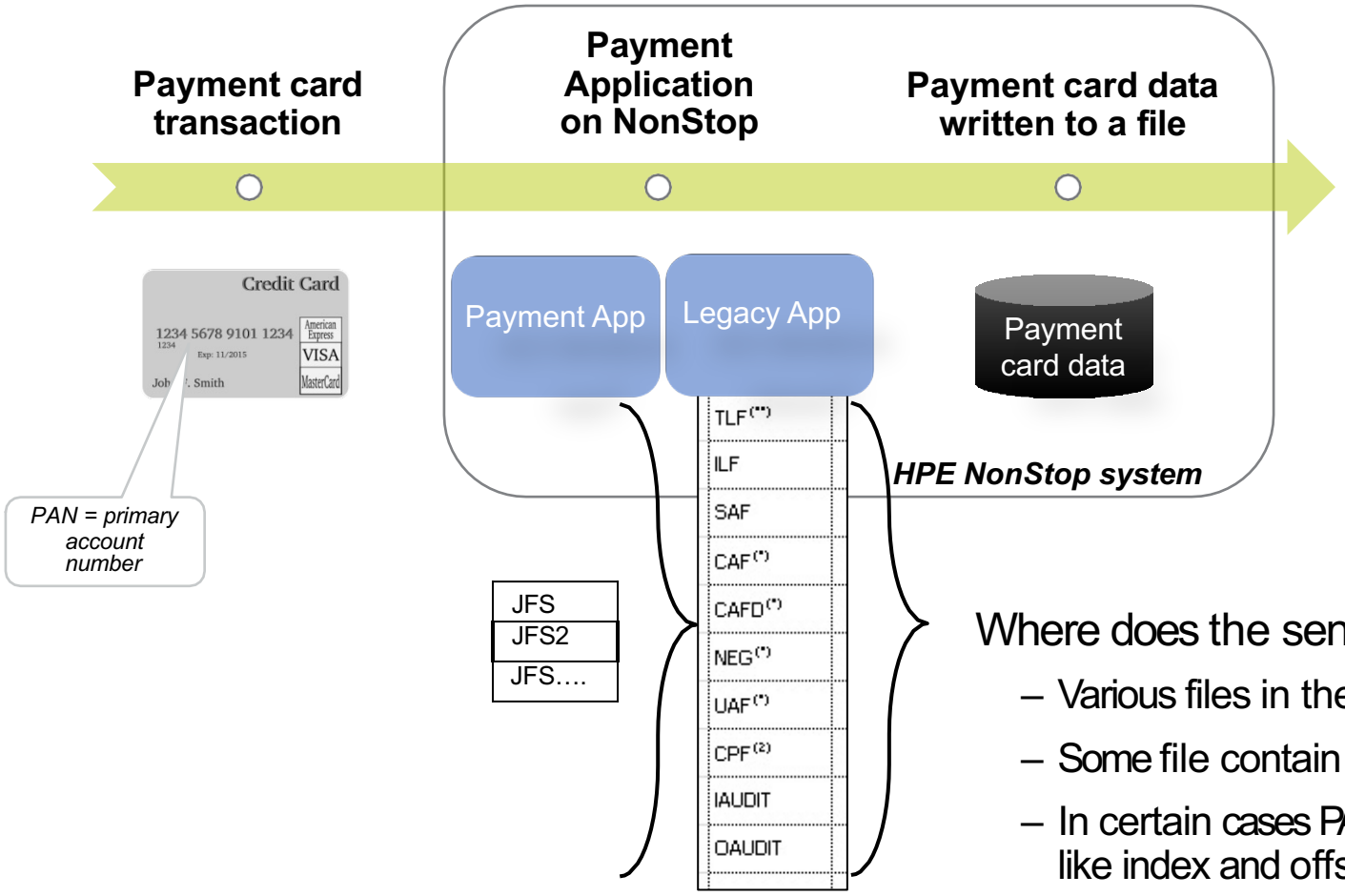
Introducing Data Centric Security Platform comforte securDPS

Example PSP



LOCATING SENSITIVE DATA

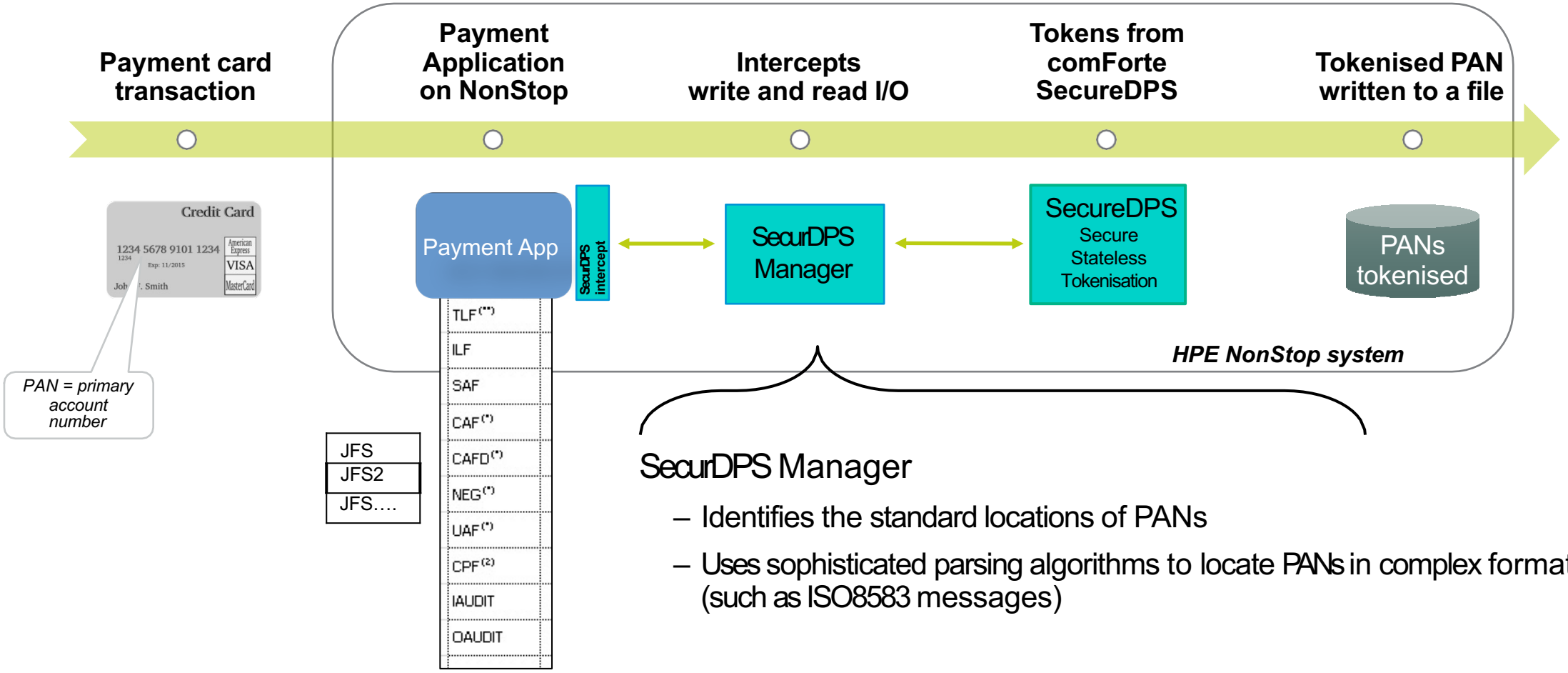
Example PSP



Where does the sensitive data (PAN) exist?

- Various files in the applications requiring data protection
- Some file contain complex records (e.g. ISO8583 message format)
- In certain cases PANs cannot be found with simple locating mechanisms like index and offset

Localizing sensitive data and tokenizing/detokenizing it



SecurDPS Manager

- Identifies the standard locations of PANs
- Uses sophisticated parsing algorithms to locate PANs in complex formats (such as ISO8583 messages)

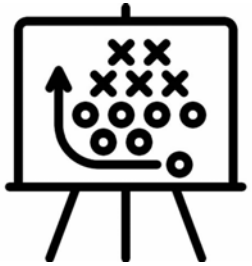
FLEXIBLE DATA PROTECTION WITH SIMPLE CONFIGURATION

- Comforte's powerful and flexible data protection engine is configured by one simple file – called the **SDF**

  The SDF also configures application authentication and authorisation rules, logging, and all other aspects of the SecurDPS solution

- In the SDF, administrators configure the Data Protection solution via two basic concepts:
- **Non-DB-Vaults**
  - Defines static objects controlling the translation of plain to protected data and vice versa
  - Commonly referred to as the "token table" but does **not** store or manage any data you protect – it's a vault in the sense of tightly protected secrets used to make tokens
  - Configures the desired character set "alphabet" for clear/protected data using predefined groupings, specified custom character lists, or codepoint definitions

- **Strategies**
  - Specifies how SecurDPS should perform data protection operations and ACLs
  - Multiple strategies can share a single vault or use dedicated vaults as desired
  - Defines format of protected data, including type, length, preserved characters, suffix/prefix, distinguishment, and token translation



COMMON EXAMPLES OF SECURDPS CONFIGURATIONS

SDF VAULT

- **Specifies character set of all numbers and upper/lower case while ignoring any other characters – ideal for e-mail addresses**
- **Clear:** h.bernhard@comforte.com
- **Protected:** n.je6dlj2H@NbwGq7k0.SOb

```
vaults:
  EMAIL-VAULT1:
    store: vault3
    alphabet:
"012…789abc…xyzABC…XYZ“
    ignore-unsupported-chars: yes
```

SDF STRATEGY

- **Protects NUMERIC data while generating easily distinguishable ALPHA tokens while preserving the first 4 and last 4 characters – ideal for numeric / ID data**
- **Clear:** 6011001330186059
- **Protected:** 601100**INJCFT**6059

```
strategies:
  PAN:
    vault: PAN-VAULT1
    format: NUMERIC
    distinguish-method: ALPHA
    preserve-first: 6
    preserve-last: 4
```

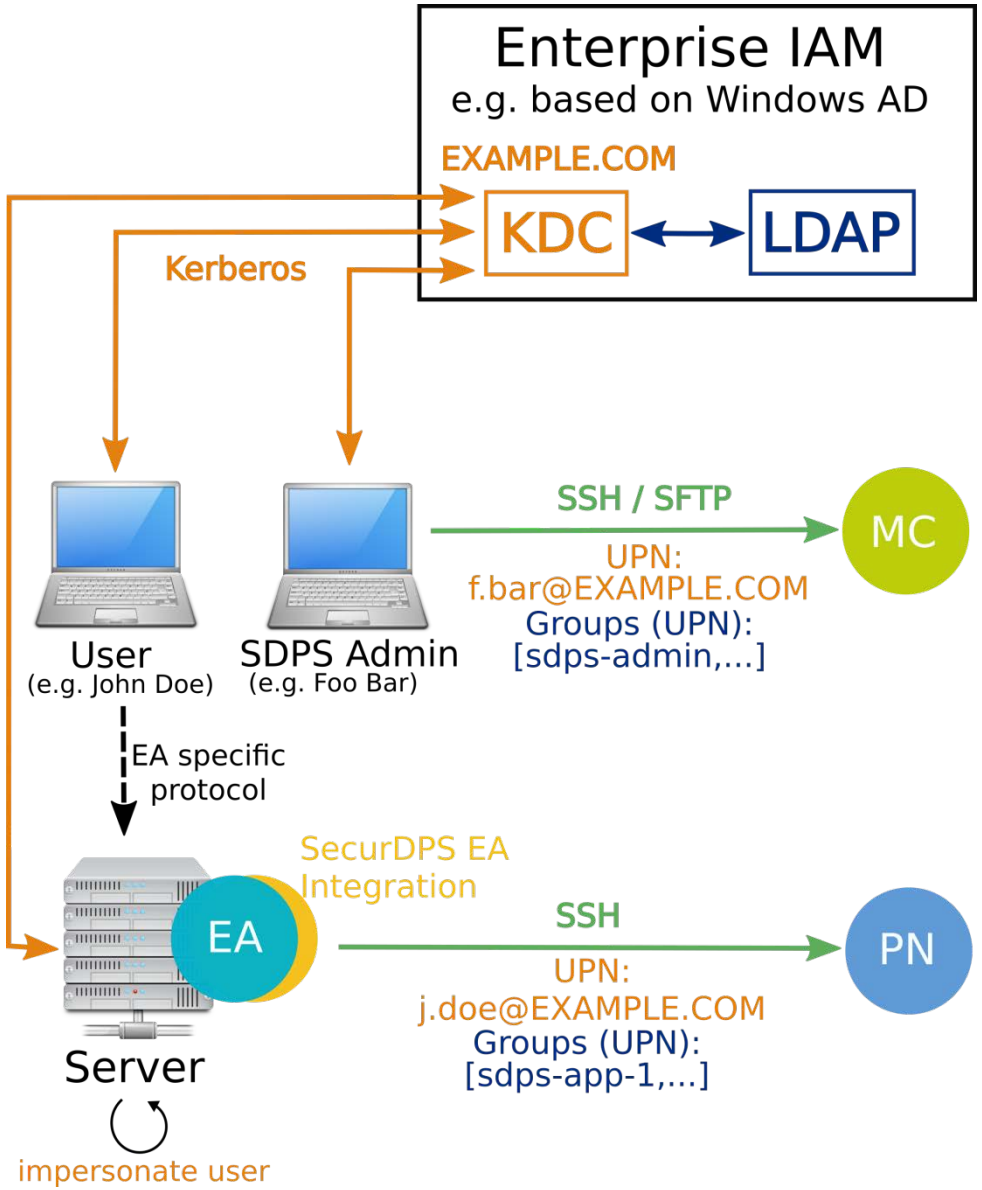
APPLICATION AUTHENTICATION OPTIONS - IAM INTEGRATION

Multiple options to fit any authentication and authorisation scheme – all managed by a single pane of glass on the SecurDPS Management Console

- **Pre-shared SSH Keys:**
  - Application maintains private key
  - Protection Cluster has public complement

- **Kerberos:**
  - Secure authentication of actual user
  - True SSO and inheriting any MFA done before

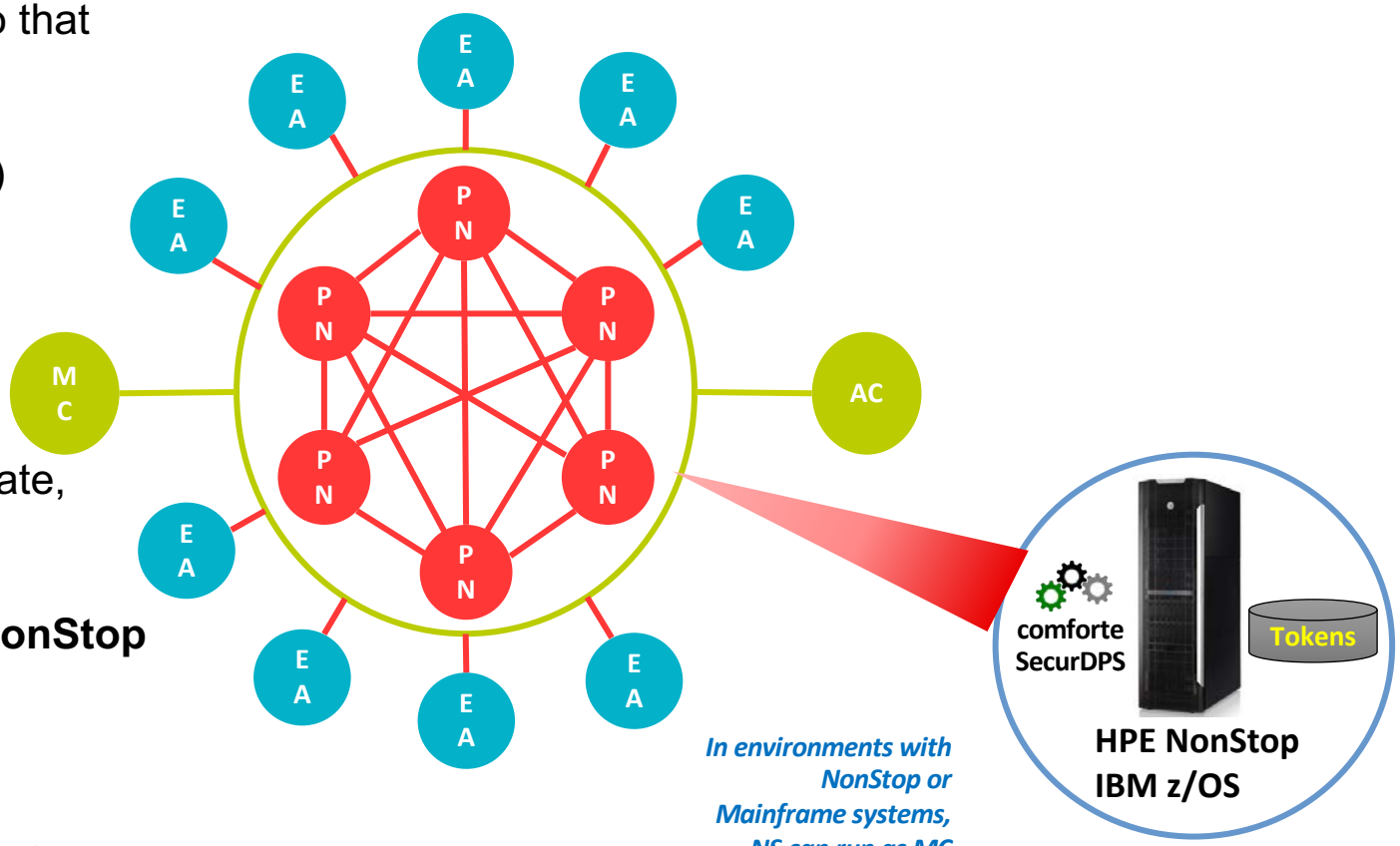
- **LDAP:**
  - RBAC to SecurDPS *service user account* based on group membership of user account



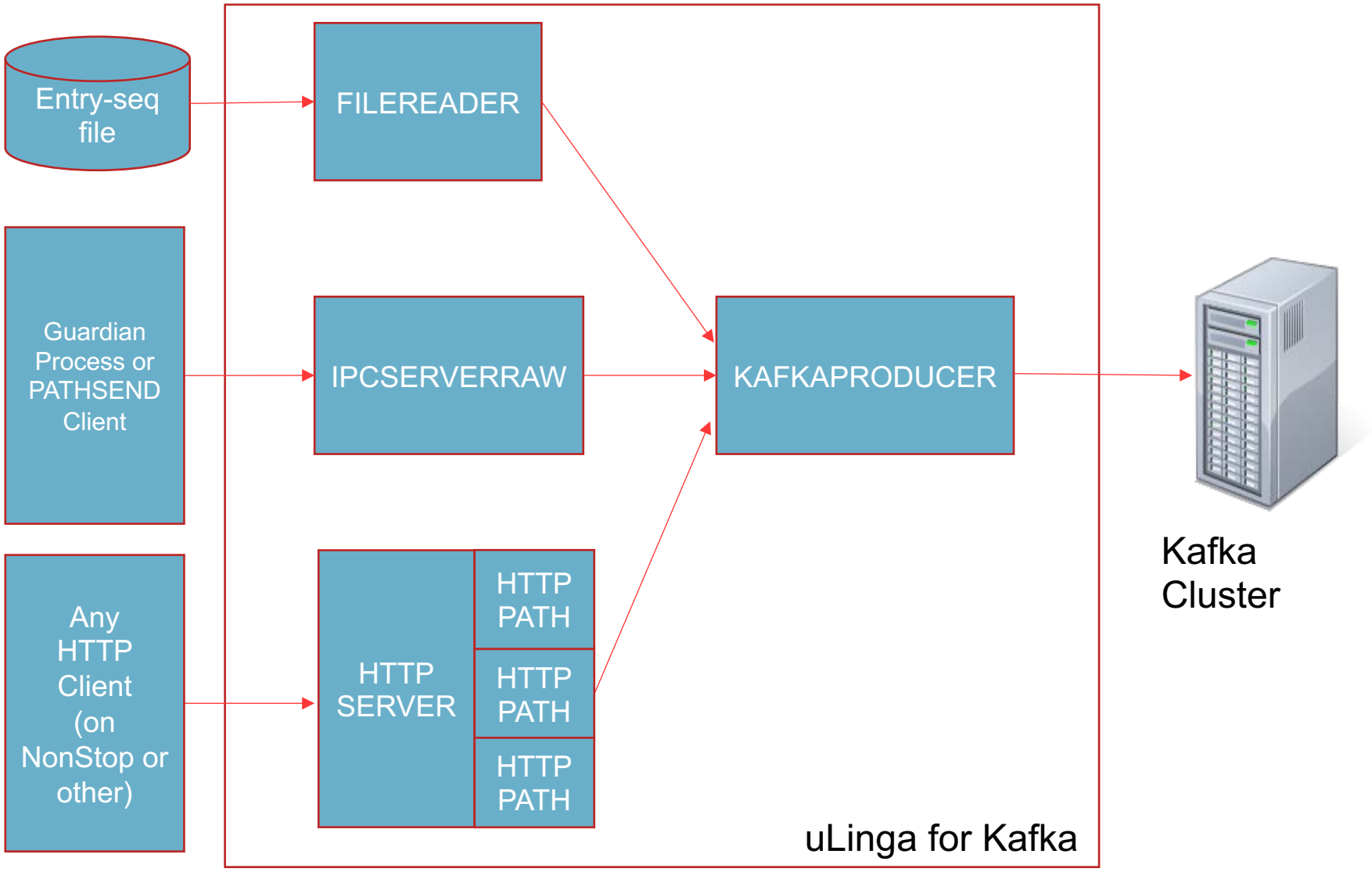
SECURDPS KEY FEATURES FOR NONSTOP

Summary

1. **Intercepts DB I/O calls**
   - The intercept approach is similar to that used in other solutions (Golden Gate E/R, Escort SQL, …)
   - Control is passed to the SecurDPS Manager via intra CPU IPC
2. **No code changes need to be made**
3. **Plays well with others** (e.g., Golden Gate, ShadowBase, HPE-RDF …)
4. **Proven with NonStop Enscribe and NonStop SQL MP/MX**
5. **Passive deployment**
   - bind with application at next normal QA cycle but activate tokenisation later
6. **API- and JSON/Rest-IF are also available**



Another use case….. uLinga for Kafka – Complete Scenario



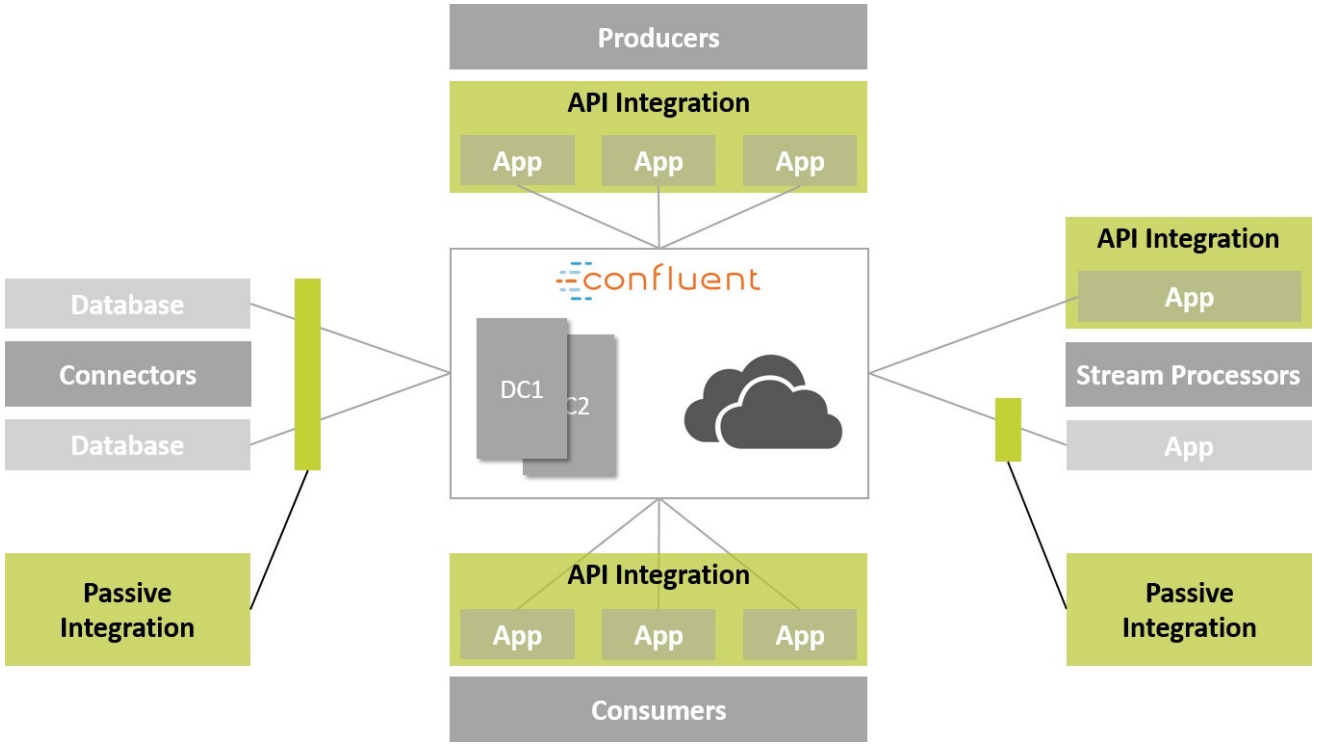
uLinga for Kafka - Summary

- uLinga for Kafka provides:
  - Excellent performance, written in C, with no additional components required
    - > 10,000 – 25,000 recs/second (real life measurements dependent on customer configurations)
    - All the advantages of other uLinga products:
      - Well-proven
      - NonStop process pair
      - Extensive tracing and diagnostics
      - WebCon browser-based user interface
- Variety of mechanisms to input data to uLinga, and from there to Kafka cluster:
    - FILEREADER for Enscribe files
    - IPC mechanism for Guardian/OSS $RECEIVE and Pathsend clients
    - HTTP mechanism to allow HTTP/REST clients to stream data

Kafka Security Integration Options with SecurDPS Enterprise

Recommended option

- For Kafka Producers and Consumers, SecurDPS integration can be performed using the SmartAPI.
- For Kafka Streams SecurDPS provides a dedicated “passive”/ transparent Kafka Streams Integration module out-of-the-box



{"ID":"42","CustomerName":"Arthur Dent","CustomerPAN":"424242EBAIFC4242"}
{"ID":"43","CustomerName":"Ford Prefect","CustomerPAN":"123456JHDCIA3456"}
{"ID":"44","CustomerName":"Zahod Beeble","CustomerPAN":"987654FIGABJ3456"}

Why comforte?

Partnering with the security ecosystem and industry leaders, e.g. Microsoft Research, École Polytechnique Fédérale de Lausanne, etc. to develop and enhance a future proven data-centric protection for the customer community

Cybersecurity Excellence Awards 2022
Best Data Security Company – Europe
Data Security Platform – Gold Winner
Security Platform – Gold Winner

Key Takeaways ZT & Data Centric Security & NonStop

- Change in thinking
- Eliminate implicit trust
- Data is the target
- Not a pillar but the pediment
- Data-centric security first

comforte

comforte

Secure Your Growth

Helmut Bernhard

Senior Solutions Architect

Tel: +43-676-4039-614
Email: h.bernhard@comforte.com

Germany
comforte AG
Abraham-Lincoln-Str. 22
65189 Wiesbaden, Germany
Phone: + 49 611 93199 00
Fax: + 49 611 93199 05
email: sales@comforte.com

Australia
comforte Pty Ltd.
Suite 20, 1 Rivett Road North Ryde
NSW 2113, Australia
Postal Address: PO Box 1710 Lane Cove
NSW 1595, Australia
Phone: +61 2 8197 0272
email: aussales@comforte.com

USA
comforte Inc.
4600 S. Syracuse St. #900
Denver, CO 80237, USA
Phone: +1 303-256-6257
Fax: +1 303-256-6205
email: ussales@comforte.com

Singapore
comforte Asia Pte Ltd
1 Raffles Place, #19-61 Tower 2,
Singapore 048616
Phone: +65 6808 5507
email: asiasales@comforte.com