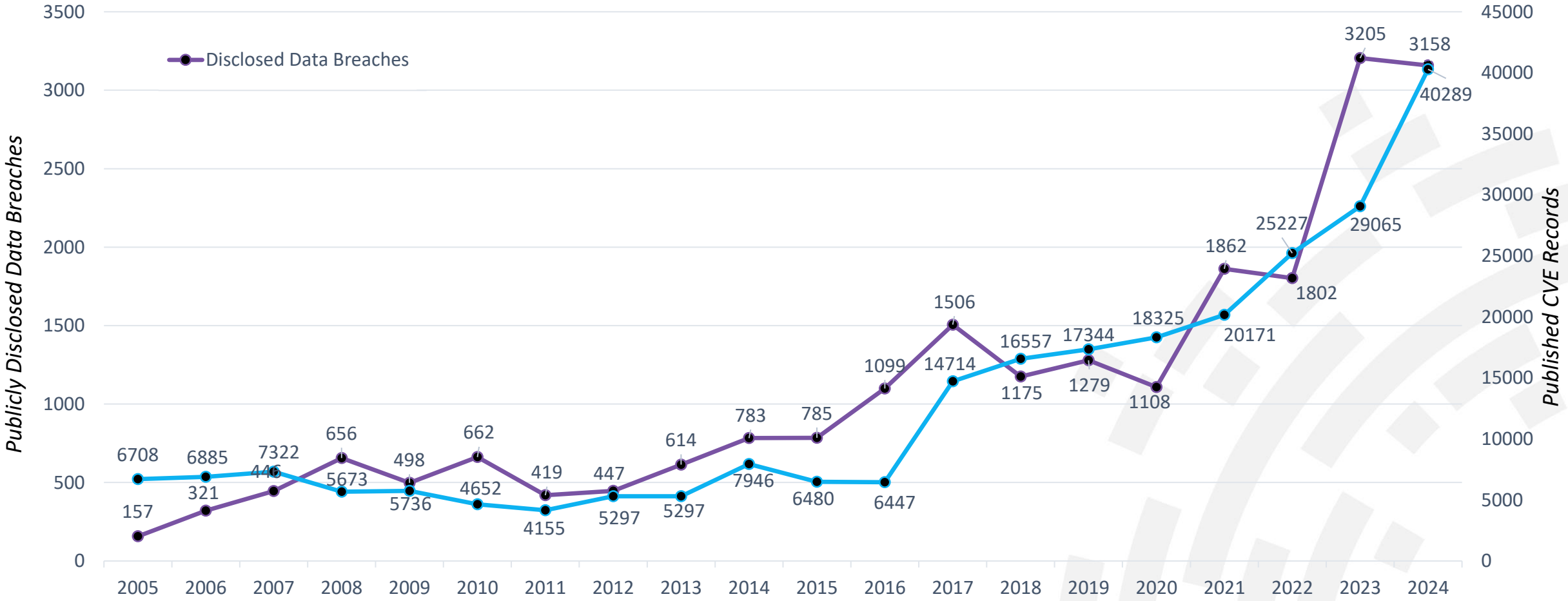
CY4

DATA LABS

Always Encrypted. Never At Risk.

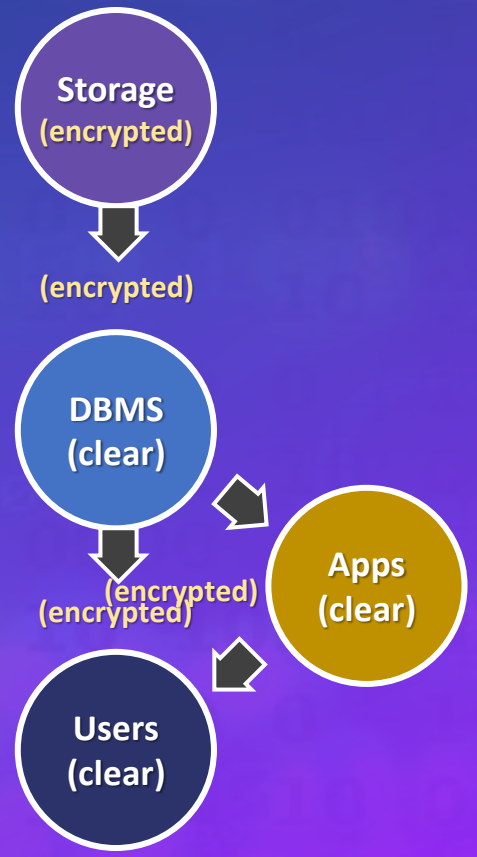
Data Breach Dilemma



https://www.cve.org/About/Metrics

The Flaw: Databases Operate in the Clear

- Databases (DBMS) operate on clear data
  - DBMS queries return clear data
  - Storage returns clear data to DBMS
  - Data lands on the user systems in the clear
- Data driven applications have vulnerability gaps
  - Application servers operate in the clear
  - Web apps are susceptible to SQL injection attacks
  - Web apps are inherently leaky



Our Motivations and Objectives

Threat Model-Driven Design

- Personal Information/PHI data
- Insider/Bad Actor breaches
- Data alterations/integrity
- SQL Injection, Logs & Snapshot leaks
- Decrypt to Share
- Data Breach ransomware
- PQC's Q-Day threat

Continuous Data Protection

- Any Database type
- Any DB backed application or SaaS
- First order "No Schema changes"
- Second order "In Situ Encryption"
- 100% Brownfield deployable
- Near zero performance impact
- Scalable data access management

CY4 SECURE

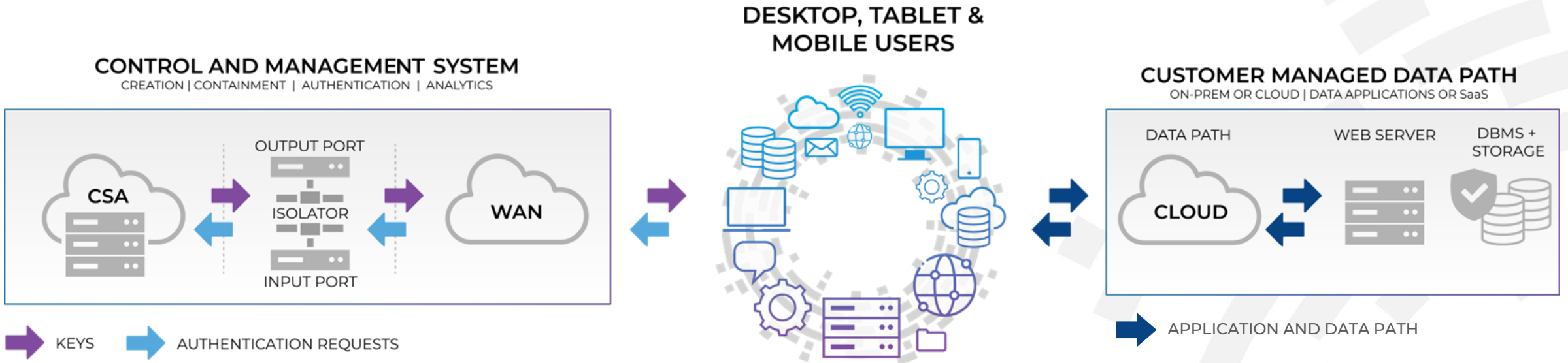
YESTERDAY'S ONLY OPTION

- Encrypting data At-Rest and In-Transit
- Application access control
- Perimeter based Defenses
- Single Domain Operating Theater

NOW WITH CY4

- In-Use Encryption
- Access Control Down to a Single Field
- Operates at the Data Layer
- Nomadic Data Protection

Cy4Secure Architecture



Cy4Secure's **"Data-In-Use"** Encryption

WebApp (UI) receives search fields

First	Last	City	State	Max Results
	Smith	Dallas	TX	100

Cy4Secure called to fetch keys and encrypt protected fields

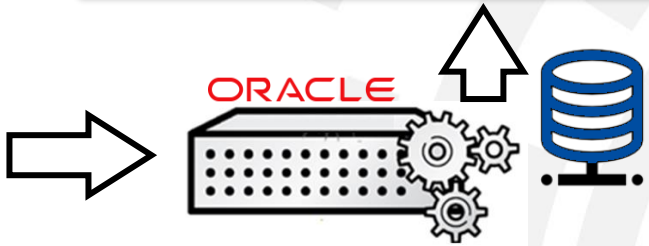
CLE Key #1	CLE Key #2	CLE Key #3
	00e6e4fb1923…	17eae1e12aef

Query is formed and sent to DBMS

SELECT record_id, first_name, last_name, city, comments_2 AS comments, credit_rating, state, salary, liabilities, key_id, ssn_key_id FROM ADMIN.demo_contacts WHERE last_name LIKE 'x00e6e4f1923%' AND city LIKE 'x17eae1e12aef%' AND state = 'TX' FETCH FIRST 100 ROWS ONLY

Raw query results:


```
"results": [
    {
      "city": "x17eae1e12aef60de0",
       "credit_rating": "a9a7a8f78f1",
      "first_name": "x1af1e8f93ffd60de0",
      "key_id": "74d73c80-eac5-11e9-a763-b3ef662b17b5",
      "last_name": "x00e6e4f92363780",
      "liabilities": [
        "x12fef9e283730 x1fe4ece383730",
        "x15e2f5e82f63780 x1ee4fff92cfd4a4bafa90" ],
      "record_id": "8e0285e0-46be-4c47-bb6f-72e4424af17e",
      "salary": "9596adafabb0b1a96a3",
      "ssn_key_id": "803ae600-eac5-11e9-a2ce-7132abf58d74",
      "state": "TX"
       "comments":
"xfff02b18d0c2f46b3e5b075cae4edb5310d60055280c351577a11c2e307cd02e508
694c3dd556d507ad979c6f24352bfeae72d9b1ae05d08c5a66e591dfca27e454a50c
34fc0177bb6905a3028657c663851a3594baa1dc7150b4ff50d3e91c567165dfd7ec
8b357c7cd2c5feefd55f814536fec5c902ce8050c252020520757f2df5f2386ab5308b
927951be5d05a1475f4bf58d01ec209ee71a1a4a00ade1d2bdc85e926ac39968aeb
e2bbf49c19f0f8afe8090fece8a1c6d64523a9fdeb02c00a0eb570f607de87c3ba2c57
8a2afa82fdb0170c490ec0efee11facb46e97e26e64ae50743a55d9f5",},
```

More to “Data-in-Use” Encryption…

Interoperability

Performant

Data Analytics

Adjustable Encryption

Endpoint Inclusion

Multipoint Resiliency

Multiparty Control

Q-Day Protection

Deterministic Security

Protected Data Sharing

Key Lifecycle Management

Key and Encryption Integrity

Governing and Data Access

Insider Detection

Decryption Validation

Billions of Keys

Nomadic Data Protection

- “Data defined security”
- Encrypts masks, partials, and data
- Shareable across domains
- Exchange between DBs and apps
- Embed in application reports
- Prevent unauthorized changes
- Ensures valid decryptions
- Continuous data protection

Keys to the Kingdom

Stolen credentials and Bad actors…

- Zero-trust ML monitoring governs suspicious activity limiting key access
- Data access permissions is separate from authorization to obtain keys

Stolen or compromised end-point devices…

- Millions of keys need to be stolen to reveal the entire database
- Terminated/expired session deletes any cached keys
- Zero-day event detection governs and shuts off key access

Advanced Data Privacy controls…

- Ability to be forgotten
- Multiparty and fine grain access control
- Align security attributes with permission attributes

PQC Unbreakable – Perfect Secrecy

Perfect Crypto Rules

1. Key is random
2. Key equals length of data
3. Key is used on only one data

“In 1945, Claude Shannon proved One Time Pad is mathematically unbreakable.”

NIST, “the most secure type of encryption”

Quantum Proof/Safe/Resistant?

- Asymmetric keys today – NO
- 256 bits Symmetric Keys – YES

Breach today break tomorrow

- Nation States are the primary threat
- Low Qubit QC commercially available
- Q-Day is coming

First commercialized One-Time-Pad

- Field Level Encryptions
- Dedicated variable length keys
- Nanosecond operations

Cy4Secure Crypto Performance

Column based decryption test

- 1M rows of 128B field data
- ~128MB of data

Large data decryption test

- 1000 rows of 1MB images
- ~1GB of data

Single Field decryption test

- ~500K rows random word fields
- ~7.36MB of data

Benchmark Comparisons

Cipher	Column (sec)	Large (sec)	Single (sec)	vs AES256
Perfect Secrecy	0.17	0.32	0.03	250x
Stream800	3.01	6.86	1.07	12x
AES256 Block CTR	14.9	114.2	1.06	1x
AES256 Block CBC	14.9	114.0	1.05	1x

Cy4Data Labs keeps data encrypted everywhere—at rest, in motion, and in use—with zero performance trade-offs.

CY4

DATA LABS

QUESTIONS

“IT ONLY TAKES ONE EXPOSED PASSWORD”

“..the focus has shifted towards logging in rather than hacking in..”

*2023 Forgerock consumer identity breach report
**IBM X-Force Threat Intelligence Index 2024