Application-Level Data Protection Simplified

U.S. DISA Technical Exchange Meeting (TEM)

EncryptRIGHT® Overview

Established 1981

Securing an open and collaborative digital world

Software Solutions for

- Data Security
- Payments Security
- EDI Security

DISA Strategic Plan FY2022-2024 Alignment

Line of Effort #2: Drive Force Readiness Through Innovation
Speed to Capability / Emerging Technology

Line of Effort #3: Leverage Data as a Center of Gravity
Data Centric Security Architecture

Line of Effort #4: Harmonize Cybersecurity & the User Experience
Contextualize Data Security and Privacy by User

Where We Must Protect Data Has Changed

Historically

Today

Encrypt Data at Rest in Storage

Must Protect Data Everywhere

"The majority of successful attackers are exploiting the higher, more accessible and exposed, application layers to conduct attacks,
and regardless of their methods, they are most often interested in obtaining data."

~ Gartner

Security of Applications and Data Primer for 2019, February 2019

How We Must Protect Data Has Evolved

Historically

Encrypt Data

Today

“Data Protection” Means More

- Encryption
- Tokenization
- Hashing
- Masking
- Redaction
- Digital Signing

Along with access controls, traceability, and alerting

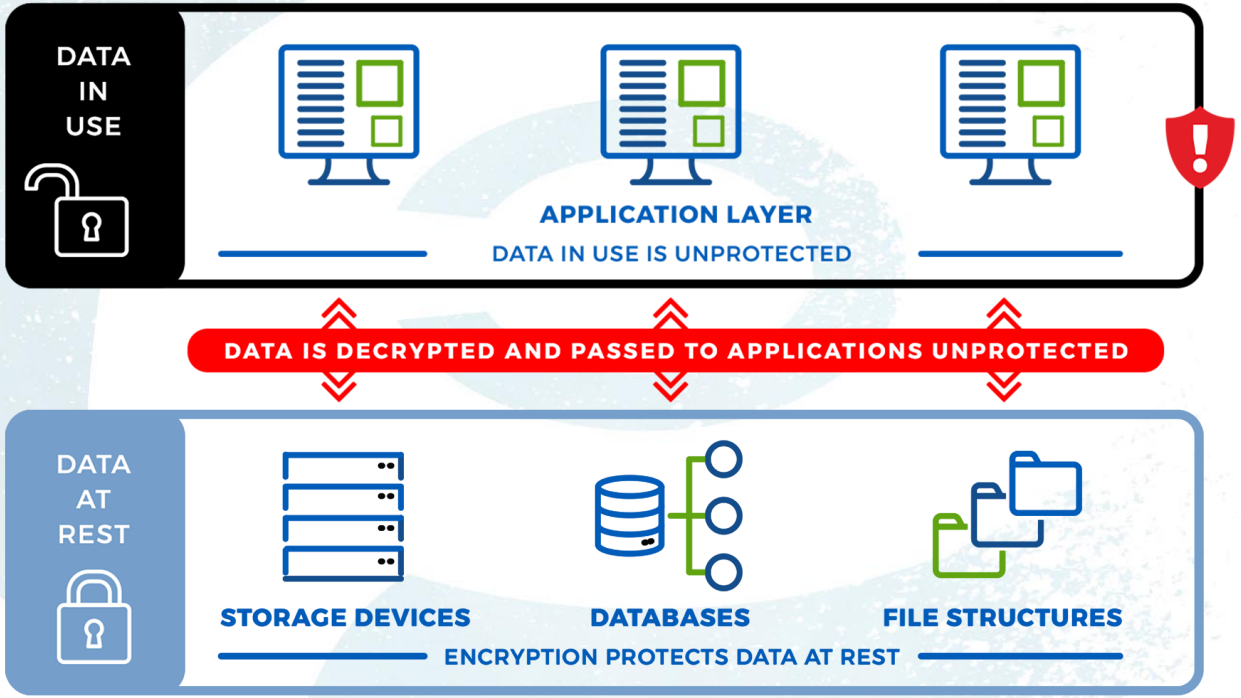
Modern Data Protection

Enterprises today must be able to Define & Enforce

- **how data is protected** (using whatever technique needed),
- **who is permitted to access specific data** and
- **what format the data takes** when access is granted

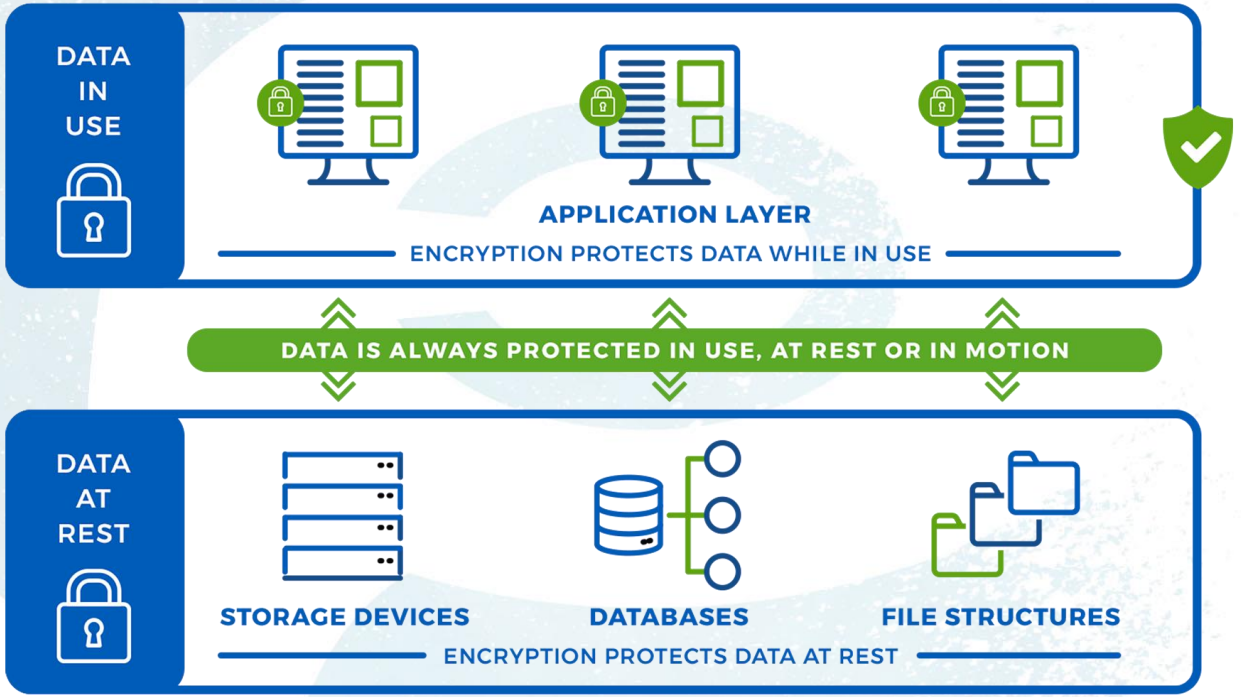
at the application layer, the moment data is created

Traditional Data Protection Solutions



Do not address protecting data in use

Application Level Data Protection

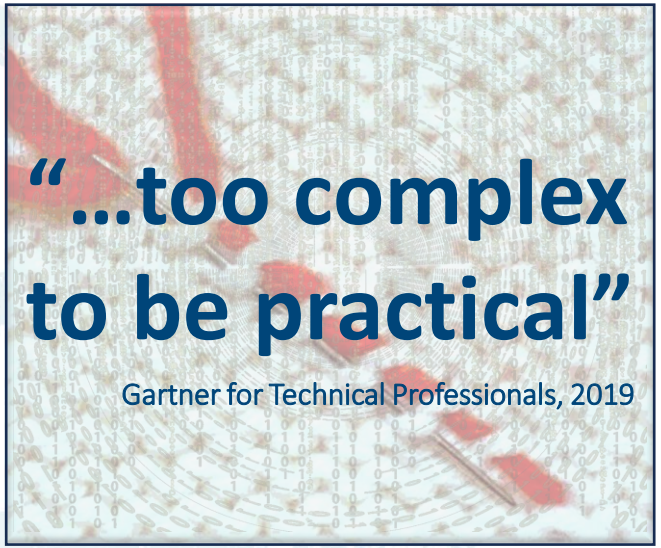


Protect Data Everywhere.

Protecting Data at the App Has Been Too Hard

Traditional SDK Approach:

- Data protection functionality interwoven into applications
- Months or years of costly custom integration
- Changes to security can require major rework



Application-Level Data Protection Simplified

EncryptRIGHT®

- Data Security Platform – a broad set of data protection functionality in a **single code base**
- Enterprise-level control over how data is protected, who can access it, and what form data takes when access is granted
- Drastically simplifies implementations:
  - Integrates in a fraction of the time of traditional SDKs
  - No Need for expensive professional services
  - No Need for developers to be crypto-experts

EncryptRIGHT® Data Protection Policies (DPPs)

Comprehensively Define How Data is Secured and Accessed

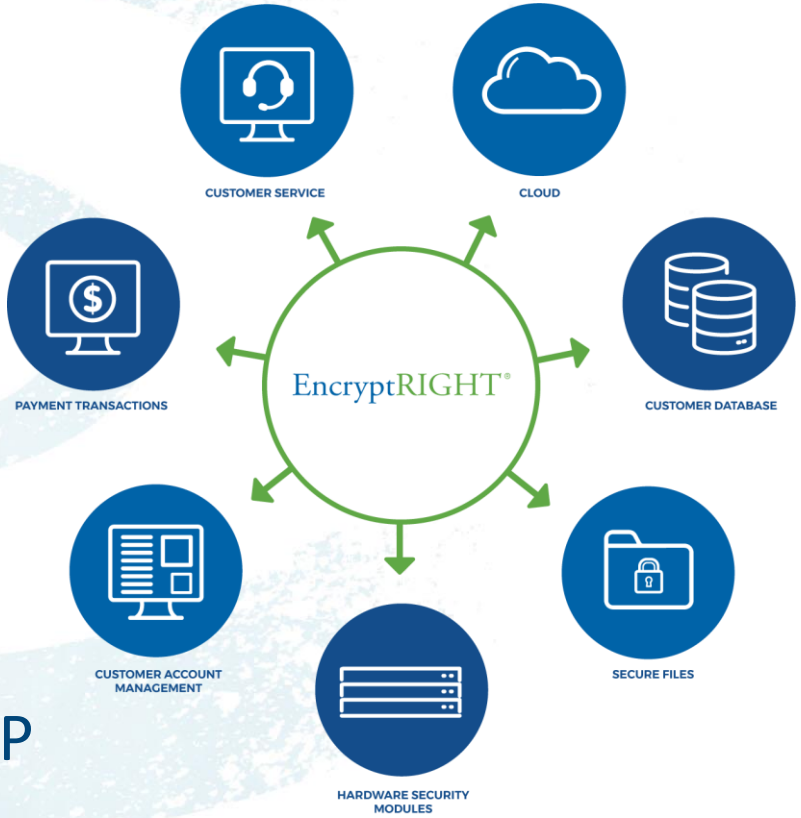
Data	Describe Data to be Protected & How It Will Be Protected
Encryption	Specific Encryption Techniques / Algorithm Types to Protect Data
Tokenization	Generation Techniques / Format Preserving or Format Targeting
Key Management	Generate, Exchange, Distribute, Store, Rotate, Suspend, Revoke, Destroy
Users	Who is Authorized to Access Data, to What Degree (Clear, Partial, or No Access)
Data Masking	Dynamic Data Masks Applied Based on Specific User Privileges
Versioning	DPP Name & Version Number for Change Management & Traceability

Applying Data Protection Policies

Any authorized application can simply protect any type of data:

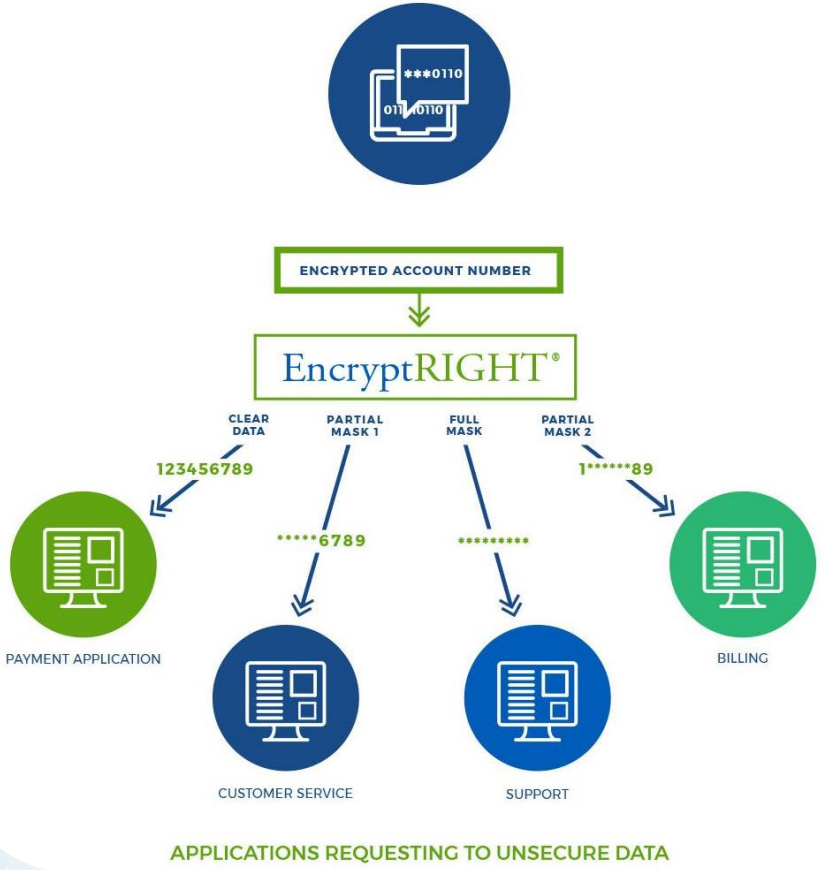
- Call EncryptRIGHT
- Give the Policy Name
- Ask to “Secure” (or Unsecure)

Secure any data, in any app, in any environment, as defined by the DPP



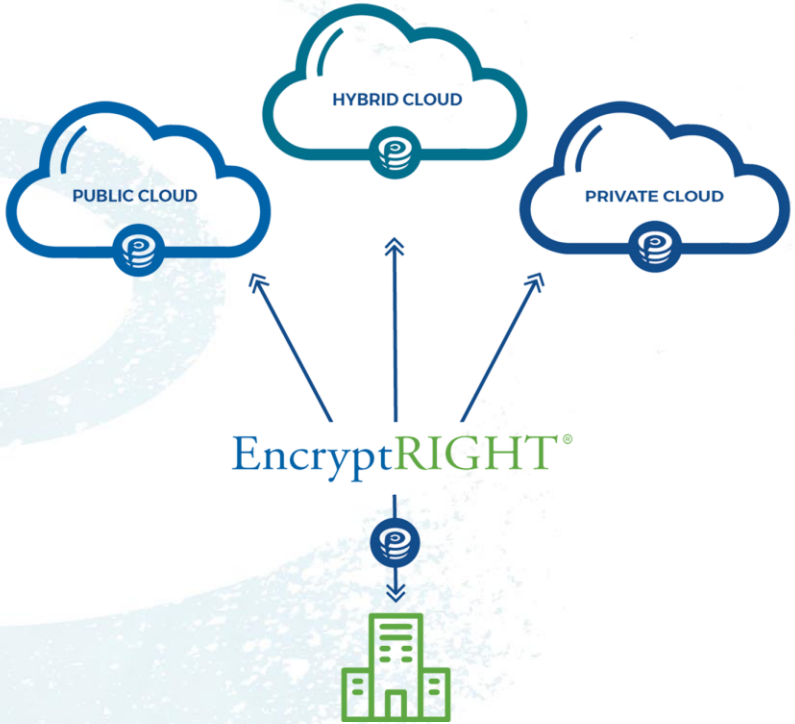
Accessing Secured Data

- Any application can request EncryptRIGHT to unsecure data
- Secured data is revealed exactly how it is permitted in the policy based on the user or application
- Data security/privacy is always enforced in accordance with the centralized policy
- Developers need to know nothing about the actual cryptography to enforce data privacy and protect PII

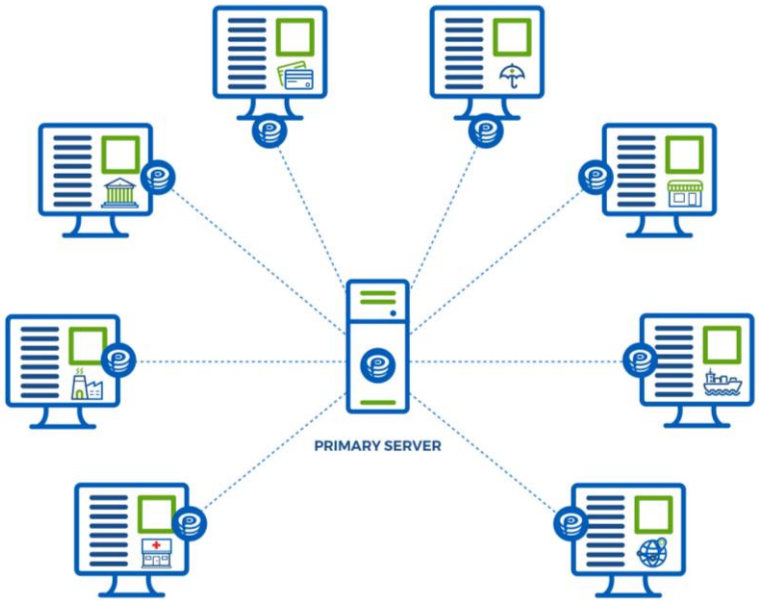


On-Premises and In the Cloud

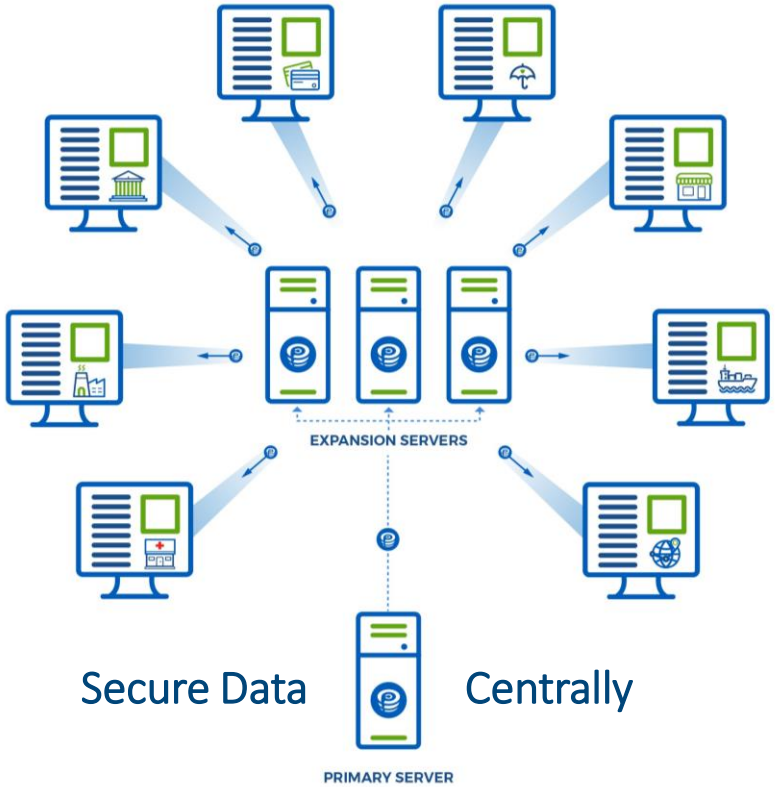
- Deploys in the cloud, on-premises, or in hybrid environments
- Protects any type of data from applications running in any environment



Built to Scale



Secure Data Locally



Secure Data Centrally

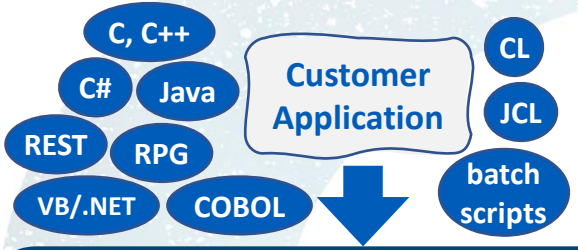
Why EncryptRIGHT®

- Simple & Flexible Solution – Easy to Deploy, Integrate and Control
- Scalability from a Single Application to Thousands of Applications
- Broad Data Protection with Granularity of Control
- Works on every common operating system – OUT OF THE BOX!

Better Protection • Less Programming • More Flexibility • Quicker Deployments
ALWAYS protecting data where it's most exposed and susceptible to breach

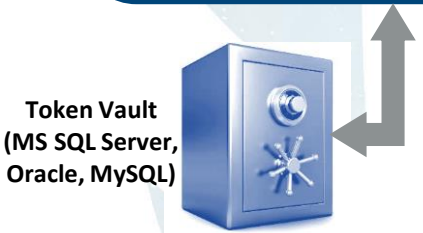
Technical Overview

EncryptRIGHT Features and Capabilities



EncryptRIGHT

- API Library
- Command Line Interface / Batch
- Secure / Unsecure Data
  - Encryption
  - Tokenization
  - Data Masking
  - OpenPGP
- EncryptRIGHT Security File
- Configuration and Administration
  - Key Management
  - Data Protection Policies
  - Access and Permissions
  - Audit Log and Reports

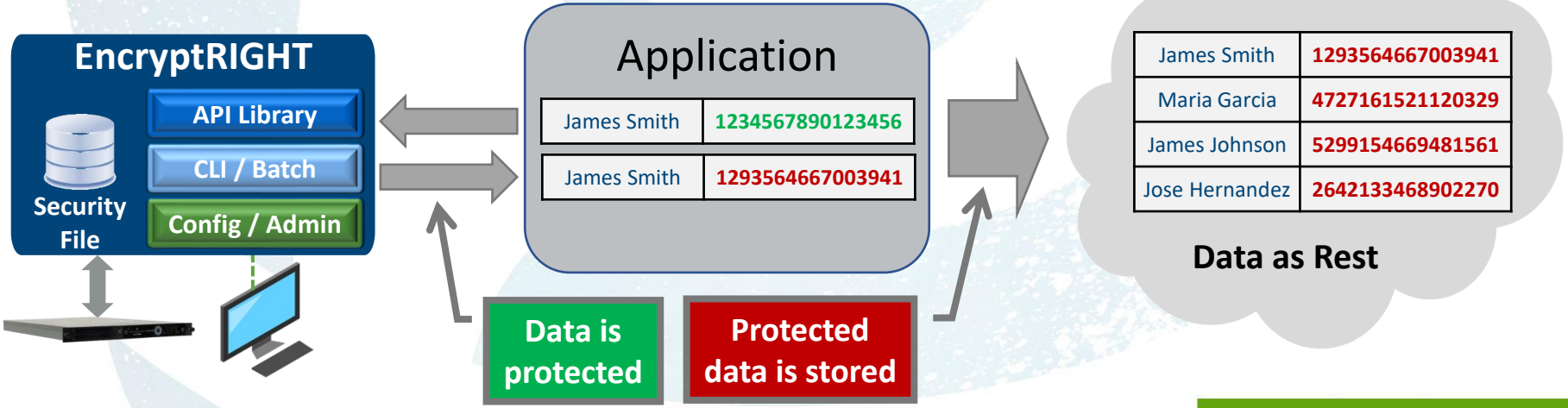


z/OS | AIX | Linux | IBM i (OS/400) | Solaris | Windows

Optional (PKCS#11)

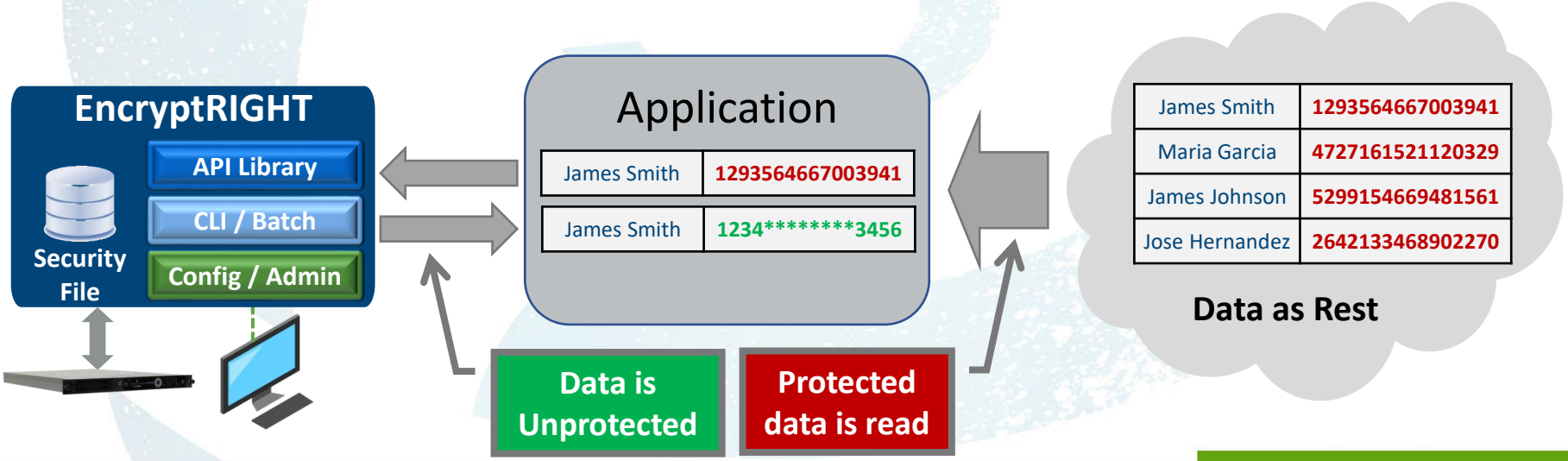
EncryptRIGHT Application-Level Data Protection

- Sensitive data is protected by an application by calling EncryptRIGHT before it is stored or sent anywhere

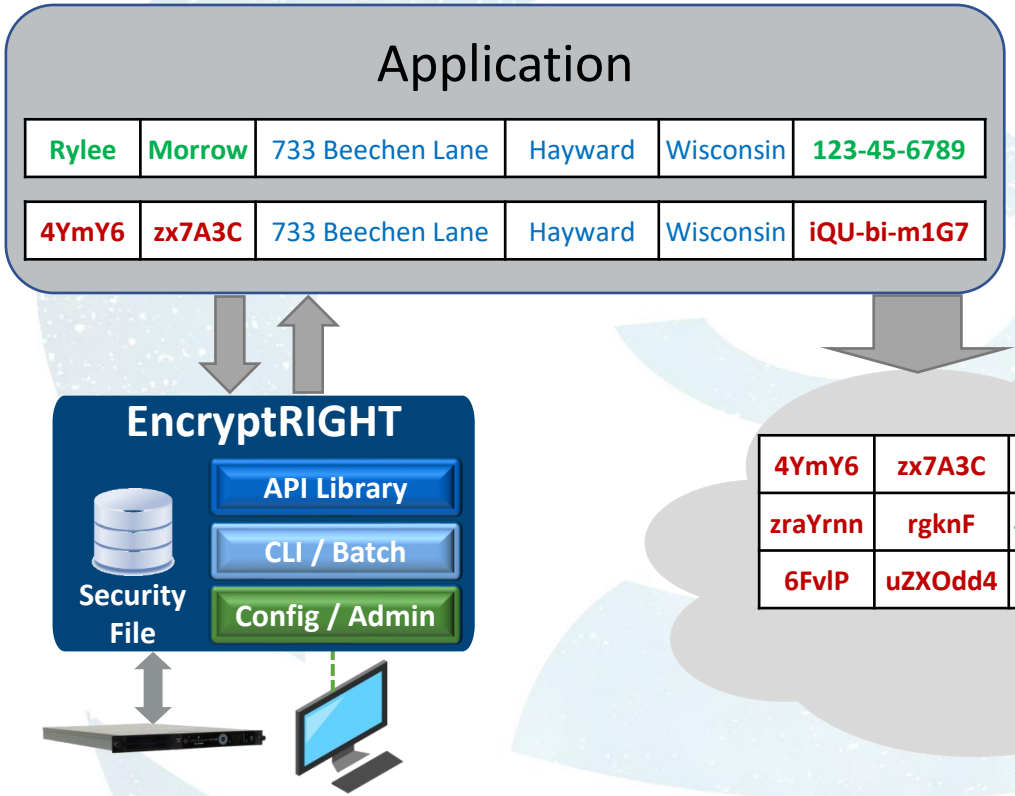


EncryptRIGHT Application-Level Data Protection

- An application obtaining any data will call EncryptRIGHT to unprotect the data based on its permissions



EncryptRIGHT Application-Level Data Protection

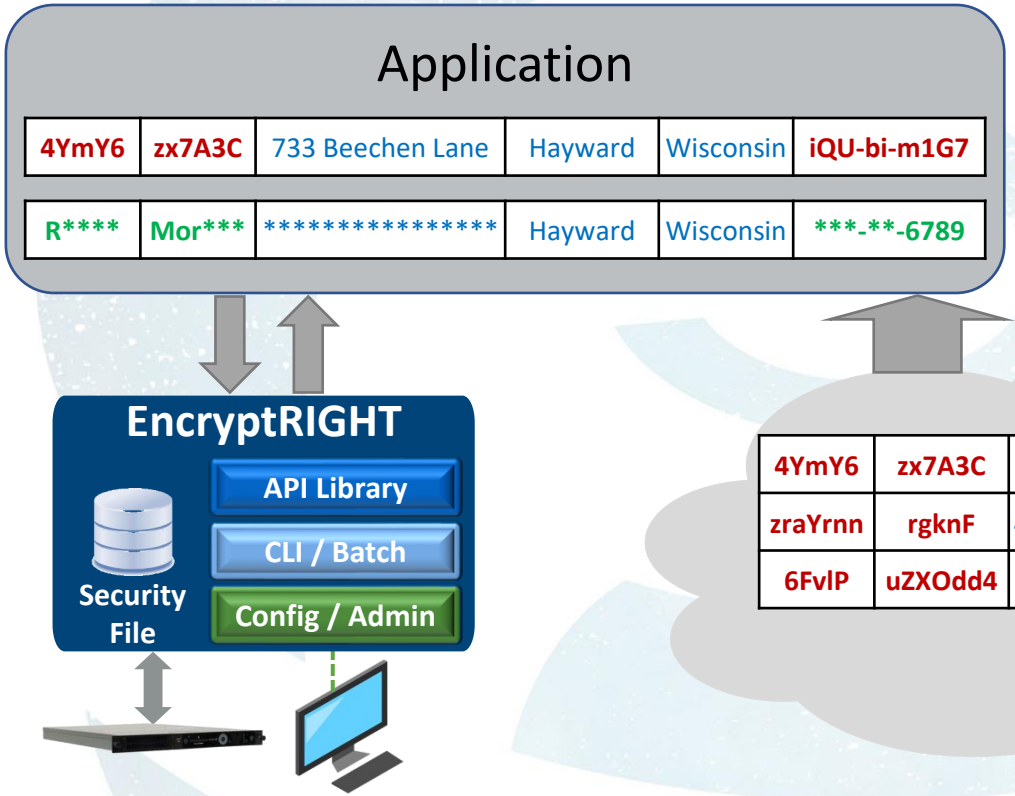


- DPPs can protect specific fields in data records with permissions to only unsecure designated fields

4YmY6	zx7A3C	733 Beechen Lane	Hayward	Wisconsin	iQU-bi-m1G7
zraYrnn	rgknF	4978 Canon Avenue	Fayetteville	Ohio	eEf-lG-s6Ce
6FvlP	uZXOdd4	7617 Pine Drive	Reno	Virginia	htC-bg-aPM6

Data as Rest

EncryptRIGHT Application-Level Data Protection



- DPPs can protect specific fields in data records with permissions to only unsecure designated fields

4YmY6	zx7A3C	733 Beechen Lane	Hayward	Wisconsin	iQU-bi-m1G7
zraYrnn	rgknF	4978 Canon Avenue	Fayetteville	Ohio	eEf-lG-s6Ce
6FvlP	uZXOdd4	7617 Pine Drive	Reno	Virginia	htC-bg-aPM6

Data as Rest

Live Demo

Q&A

Thank You

www.primefactors.com

Company Contact

Gene Paschall, Strategic Alliances

408-718-2955

gene.paschall@primefactors.com

Additional Contacts

Henry Cheli
President & CEO
henry.cheli@primefactors.com

Justin Teitt
COO & CMO
justin.teitt@primefactors.com

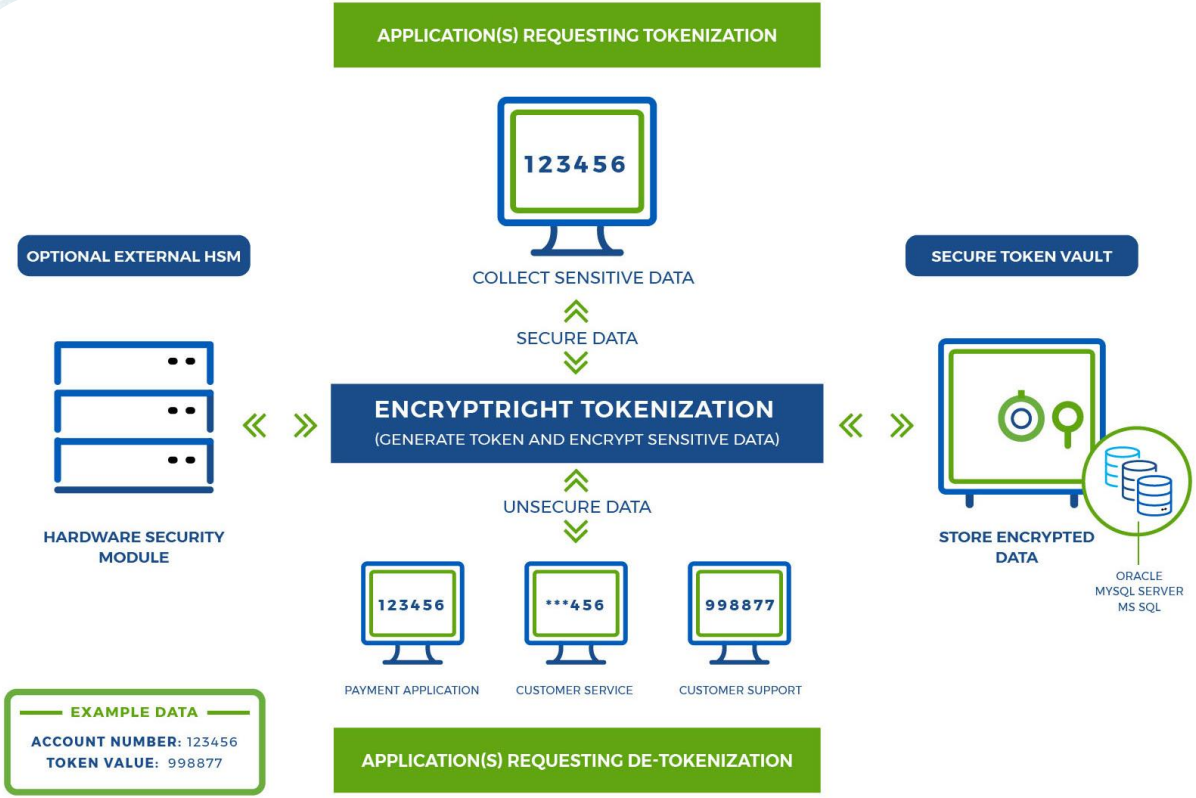
Jose Diaz
Vice President, Products and Services
jose.diaz@primefactors.com

Supplemental Material

Cryptographic Key Management

- Centralized Key Management for the data EncryptRIGHT touches
- Key Management lives independently of any given application
- Hardware or Software based cryptography capabilities

Tokenization



Analyst Coverage

Prime Factors Recognized in Gartner® Hype Cycle™ for Data Security, 2023

Prime Factors Recognized in 2023 Gartner® Security and Risk Management Summit Session, "Outlook for Data Security"

Prime Factors Recognized In 2023 Gartner® Market Guide™ for Data Masking

Prime Factors Recognized in 2022 Gartner® Hype Cycle™ for Privacy

Prime Factors Recognized in 2022 Gartner® Innovation Insight for Data Security Platforms

Prime Factors Recognized in 2021 Gartner® Hype Cycle™ for Privacy

Prime Factors Recognized in 2021 Gartner® Hype Cycle™ for Network Security

Prime Factors Named Among Eight Dynamic Data Masking Solutions Providers By Independent Research Firm

Prime Factors Recognized in 2021 Gartner® Hype Cycle™ for Data Security