

Improve retail competitiveness  
by accelerating transformation  
while reducing risks and cost

eBook



# Retailers upgrade their technology infrastructure to compete and deliver better value to consumers

Technological innovation is changing the face of retail, from omni-channel and e-commerce to hyper-personalization and automation. Retailers face a competitive landscape where innovation is key.



## Supply and fulfillment management

Optimize supply chain by acting on insights quickly, increasing efficiency, and lowering cost.

## Hyper-personalization

Provide the fulfilling, convenient, and secure personalized service that consumers expect.

## Omni-channel experience

Deliver a seamless and secure shipping experience through mobile, self-service, or any other channels consumers use to shop.

## Analytics and intelligence

Analyze consumer data in big data repositories and leverage artificial intelligence (AI) to power better decision making.

## Merchandizing and cost optimization

Understand demand better, respond to trends faster, and increase sales, satisfaction and retention.

## Hybrid workforce

Enable a hybrid workforce with employees that can provide customer service, operational, and technical support from anywhere.



# Retail industry going through major digital transformation

Retailer organizations of all kinds are adopting new platforms and environments at a fast pace, transforming their infrastructure and enhancing their capabilities.

## Cloud adoption



The spending on cloud services by the retail industry is expected to reach \$39 billion by 2026, exhibiting a CAGR of 16% during 2019-2026.<sup>1</sup>

## Spending on Internet of Things (IoT)



The global market size of internet of things in retail is expected to reach \$182 billion by 2028, registering a CAGR of 26%.<sup>2</sup>

## Big Data



The big data analytics market in retail is estimated to reach \$26 billion by 2028, witnessing a CAGR of 23%.<sup>3</sup>

## Artificial Intelligence (AI)



Global Artificial Intelligence in the retail market is estimated to reach \$17 billion by 2028, powered by application and chatbot adoption for a (CAGR) of 34%.<sup>4</sup>

**\$39B**

Spending on **Cloud services** by retailers to reach \$39 Billion by 2026

**26%**

Spending on **IoT** will grow by 26% a year in the retail sector by 2028



**\$26B**

Spending on **Big Data** in retail to reach \$25 Billion by 2028

**34%**

**Artificial Intelligence** use in retail to grow by 34% a year until 2028

1: Fortune Business Insights: Retail Cloud Market Size, Share & Industry Analysis, Forecast 2019-2026

2: Research and Markets: The "Global Internet Of Things In Retail Market Size, Share & Trends Analysis Report, Dec 2021.

3: Allied Market Research: Big Data Analytics in Retail Market to Reach \$25.56 Billion by 2028: June 2021

4: Vantage Market Research: Artificial Intelligence (AI) in Retail Market Size to Reach 17,086.54 USD Million by 2028, March 2022



# Transformation increases complexity challenges

Digital transformation at retail organizations increases the complexity of hybrid IT infrastructure and the risk of data breach.

## A challenging multi-cloud world



66% of global retailers have more than 25 Software-as-a-Service (SaaS) providers, and 68% have more than one Infrastructure-as-a-Service (IaaS) provider.<sup>5</sup>

## Key management complexities



59% of retailers reported having five or more key management solutions, increasing complexity and making it cumbersome (and expensive) to manage.<sup>5</sup>

## Exponential data sprawl



Only 46% of retailers felt they had very good knowledge of where their data is stored and 53% indicated they could classify a majority of their data.<sup>5</sup>

## Lack of protection of sensitive data



Only 18% of retailers reported that 60% or more of their sensitive data stored in the cloud is encrypted.<sup>5</sup>

# Hacker groups target weaknesses in the new retail hybrid IT infrastructure

Cyber criminal organizations continue to target retailers and their suppliers for financial gain.

## Cyber attacks in retail on the rise



44% of retail industry respondents reported increases in the volume, severity, and/or scope of cyberattacks in the past 12 months.<sup>5</sup>

## IoT cyber attacks skyrocket



The first half of 2021 saw 1.5 billion attacks on IoT devices, with attackers looking to steal data, disrupt operations, mine cryptocurrency, or build botnets.<sup>6</sup>

## Malware and ransomware on top



Malware was the top threat to 65% of retailers in 2022 in a stacked ranked survey, with ransomware coming in second at 52%.<sup>5</sup>

## Rising cost of cyber attacks on retail



The average cost of cyber attacks in the retail sector reached \$3.27 million, according to the Ponemon Institute cost of data breach report.<sup>7</sup>

44%

of retailers reported **increases in volume, severity, and scope of attacks** in the past 12 months

1.5B

**attacks on IoT devices** were registered in the first half of 2021



65%

of retailers identified **malware** as the main cybersecurity threat.

\$3.27M

was the **average cost of cyber attacks** in the retail sector in 2021

5: 2022 Thales Data Threat Report Retail Edition  
6: Internet of Things News Kaspersky: Attacks on IoT devices double in a year  
7: IBM & Ponemon Institute: Cost of Data Breach Report 2021

# Stricter cybersecurity mandates and legislation add urgency

The growth of cyber incidents has led to unprecedented executive and legislative action:



White House Cybersecurity  
Executive Order



European Union  
Cybersecurity Act

**The Executive Order to Improve the Nation's Cybersecurity** and protect federal government networks and the nation's infrastructure was signed by President Biden in 2021. The order helps move organizations to secure cloud services and a zero-trust architecture and mandates deployment of multi-factor authentication and encryption.

**The European Union's Cybersecurity Act** passed in 2019 gives ENISA, the EU Agency for Network and Information Security, a permanent mandate. It also establishes a European cyber security certification framework for information and communications technology products and services. It calls for up-to-date software and hardware with mechanisms for secure updates leveraging code signing.

**The convergence of existing privacy, sovereignty, and data protection regulations**, such as GDPR and PCI-DSS; federal standards, and global standards, such as ISO 27001; mean that retailer organizations are faced with a comprehensive set of rules that make compliance much more complex and challenging.

# How Thales can help

Thales enables retailers to improve competitive advantages by accelerating transformation while reducing risk of data breach, complexity, and cost.

Improve  
security and resilience



Automate and streamline data protection and key management across cloud, hybrid, and on-premises systems

Reduce risk, complexity  
and cost



Simplify compliance and minimize reputational and operational risk with centralized data security governance

Accelerate  
digital transformation



Increase customer satisfaction by adopting innovations, such as IoT, cloud, and Big Data, faster with a framework for a zero-trust world



# Increase security and resilience across enterprise Hybrid IT

Automate and streamline data and identity protection with scalable solutions for multiple use cases

**Centralize key management** for third-party security solutions across cloud, hybrid, and on-premises environments

**Minimize the threat of data breach** by de-identifying all sensitive data in all new environments and legacy platforms, including partners and suppliers

**Centralize access management** and multi-factor authentication with single sign on to all IaaS, PaaS, SaaS, and on-premises platforms



SaaS, PaaS, IaaS services



On-premises systems



File repositories and databases



External 3rd party collaboration

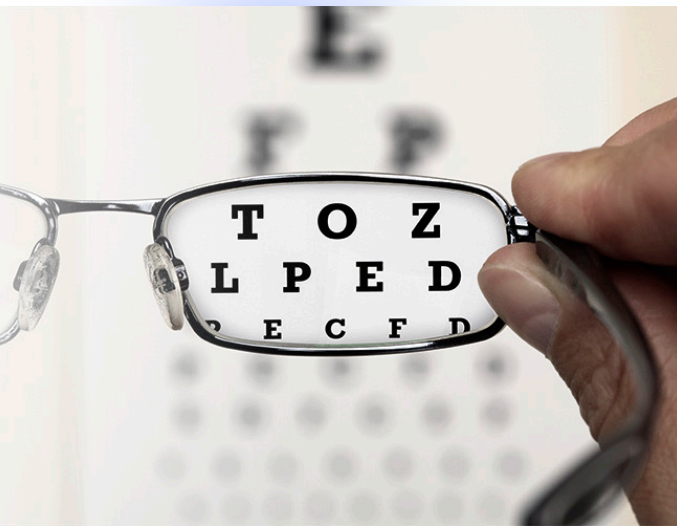


Internet of things (IoT)



# Specsavers secures access to corporate applications with low cost and scalability

Multi-Factor Authentication for large European retailer



## Challenge

- **Specsavers is a UK-based eyewear retailer** with more than 1,300 branches and 26,000 staff across Europe.
- The company wanted to secure access of hundreds of remote workers to a range of central resources such as email, web applications, and financial resources.
- Required a scalable and flexible solution able to cope with new applications and growth in staff levels across existing and new markets.



## Solution

- **Thales Safenet Trusted Access was deployed** to enable Multi-Factor Authentication (MFA) remote access to their internal applications and databases.
- Specsavers chose a mix of token formats -- hardware, software, and SMS -- to meet various end user needs.
- The tokens, combined with a unique PIN code, deliver a one-time password with letters, numbers, and characters, offering the most secure OTPs on the market.



## Results

- **Achieved scalability and empowerment** by empowering local offices to instantly allocate and retract tokens without the assistance of central IT department.
- **Lowered total cost of ownership** with OPEX model and simple annual subscription fee, which includes the service's software components and applications.
- **Increased usability and service longevity** with a mix of hard, soft, and SMS tokens that fit the needs of multiple user groups.

# Major grocery chain stops leaks of sensitive data with Thales

High speed encryption to protect sensitive data in motion



## Challenge

- **A large grocery chain** was concerned with the ongoing leaks of product pricing and time-sensitive offers to competitors.
- The retailer wanted to implement the highest level of security to protect the internet connection between major offices from eavesdropping.
- Required high performance end-to-end encryption of data in motion.



## Solution

- **Thales High Speed Encryptors** were deployed to provide end-to-end protection for data in motion between main offices.
- The FIPS 140-2 Level 3 and Common Criteria certified appliance provided high speed communication with the highest levels of standards-based security.
- **Thales Luna Hardware Security Modules** were deployed later to provide root-of-trust for encryption keys and PKI-based use cases.



## Results

- **Stopped leaks of pricing and offer data** by protecting sensitive and confidential data flowing between its main offices.
- **Optimized network performance** with zero-overhead protocol with no impact on latency and ensured maximum performance.
- **Enabled fast, easy deployment** with seamless 'bump-in-the-wire' integration and easy scalability from 1Gbs solution to 10Gbs solution after a few years.

# Reduce risk and complexity

Accelerate time to compliance  
with centralized data and identity  
security governance



White House Cybersecurity  
Executive Order



European Union  
Cybersecurity Act

**Discover and classify data** across hybrid IT environments  
according to sensitivity to specific legislation requirements

**Automate data protection** with centralized policy-based  
enforcement from a single pane of glass

**Apply data privacy and sovereignty rules** through granular  
data and access security controls with MFA authentication

# Major retailer group complies with PCI and establishes security best practices

Luna HSMs protect PII, credit card data,  
and privileged access



## Challenge

- **A major North American grocery and pharmacy chain** wanted to implement data security and key management best practices to protect credit card and personally identifiable information (PII) data and comply with PCI.
- The retailer wanted to protect keys for important security platforms managing encryption of databases, privileged access control, and PKI use cases.



## Solution

- **Luna Hardware Security Modules (HSMs)** were deployed to protect encryption keys from multiple systems, including Oracle databases leveraging transparent data encryption and CyberArk Privileged Access Management.
- Luna HSMs centralized all key management in a single highly secure root-of-trust for encryption keys for all use cases.



## Results

- **Established security best practices for key management** based on Luna HSMs for the entire group including grocery, pharmacy, and retail bank.
- **Enhanced PCI compliance posture** by protecting essential encryption key material used in multiple use cases.
- **Successful scalability of solution to multiple new use cases** has ensured a long-term customer relationship for over 10 years.

# Accelerate digital transformation

Adopt innovations such as IoT and smart devices, multi-cloud environments, AI, and big data faster with a framework for a zero-trust world

**Secure digital identities, applications, IoT devices**, and cryptographic keys with a certified root of trust

**Protect data in, and moving across, multi-cloud environments** with BYOK, HYOK, BYOE, and centralized key lifecycle management

**Adopt a zero-trust posture** for all environments with MFA, intelligent SSO, and centralized access controls



Big data



Multi-cloud



IoT and smart devices



Artificial Intelligence



Digital records and signatures

**THALES**

# Protection of credit card and personal information for a major US retailer

PCI compliance and scalable security across environments



## Challenge

- A **major US retailer with operations in multiple countries** suffered a major data breach that exposed credit card data from millions of customers.
- The retailer wanted to protect credit card data across its systems, from stores to back-end processing, and achieve PCI compliance.
- The enterprise also wanted a scalable solution to protect personally identifiable information (PII) as well as new platforms and environments.



## Solution

- The **Ciphertrust Platform** was deployed to provide protection for credit card data captured at stores as well as in datacenters and databases in the back-end.
- **Ciphertrust Transparent Encryption** with centralized key management was deployed to protect PII data on key files and databases.
- **Thales Luna Hardware Security Modules provided** root-of-trust for encryption keys and PKI-based use cases.



## Results

- **Dramatically improved PCI compliance posture** by providing end-to-end security for credit card data from stores to back-end data stores, including Microsoft SQL.
- **Successful deployment and implementation** of the credit card use case enabled the expansion to protection of personally identifiable information (PII).
- **Scaled security** to new platforms, environments, and use cases.



# Thales Cloud Protection & Licensing

## Our Solutions

Data Protection

Access Management & Authentication

Software Monetization



Over **2,600**  
employees



**25** countries  
presence



**750** engineers  
worldwide



**30,000**  
customers worldwide

Thales's technologies and services help secure **more than 80%** of all global payment transactions and increasingly valuable corporate and government information.

The people we rely on to secure  
our privacy rely on Thales

#1

Worldwide in  
general-purpose  
HSMs

#1

Worldwide in data  
encryption

#1

Worldwide in  
payment HSMs

#1

Worldwide in key  
management

#1

Worldwide in  
cloud HSMs

#2

Worldwide in  
cloud  
authentication

#1

Worldwide in  
software  
protection

#1

Worldwide in  
software licensing

THALES




# About Thales

The people you rely on to protect your privacy rely on Thales to protect their data.



When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.



Decisive technology for decisive moments.



## Contact Us

For all office locations and contact information, please visit



[cpl.thalesgroup.com/contact-us](https://cpl.thalesgroup.com/contact-us)



[cpl.thalesgroup.com](https://cpl.thalesgroup.com)