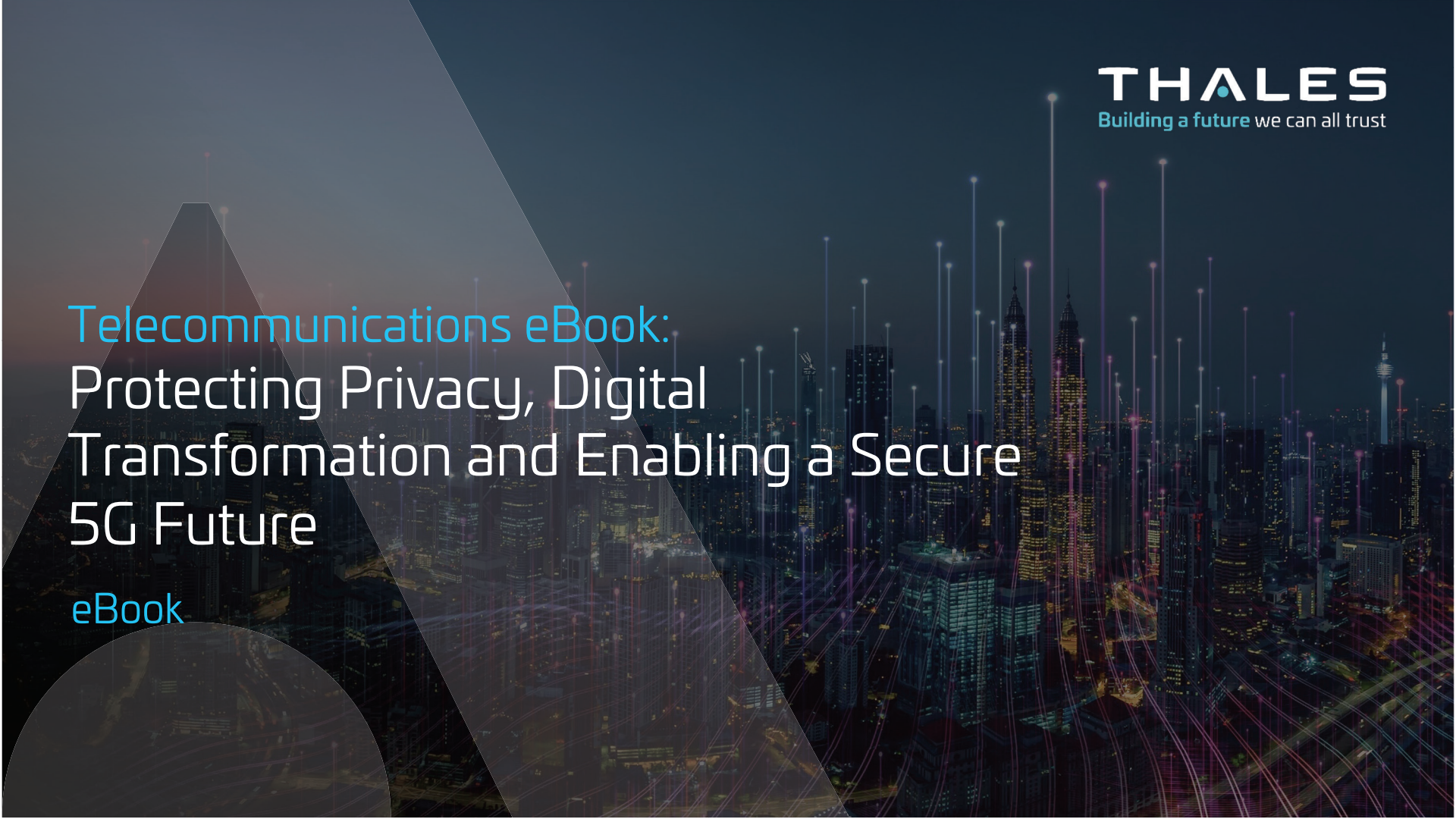

Telecommunications eBook: Protecting Privacy, Digital Transformation and Enabling a Secure 5G Future

eBook

Digital Transformation in Telecommunications

Telecommunications companies are adopting new platforms and environments at a fast pace, transforming their infrastructure and enhancing their capabilities.

Multicloud world

Multicloud is a reality for Telecoms. The average number of Infrastructure-as-a-Service (IaaS) cloud providers per Telecom is 2.36 and 80% have two or more cloud providers.[1]

Massive 5G investments

Telecommunications companies are expected to invest more than $600 billion in 5G infrastructure between 2022–25.[2]

SaaS growth

The average number of Software-as-a-Service (SaaS) applications used by Telecom organizations is 113, compared to 97 for enterprises in general.[1]

Artificial Intelligence (AI)

The global artificial intelligence Telecoms market was valued at USD $679.0 million in 2019 and is expected to grow at a compound annual growth rate (CAGR) of 38.4% from 2020 to 2027.[3]

80%
of telecommunications companies **have 2 or more IaaS clouds**

$600B
Investment expected **in 5G infrastructure** between 2022–25

113
Is the **average number of SaaS apps** used by Telecoms

38%
Artificial Intelligence use in Telecoms to **grow** by 38% a year until 2027

1: 2023 Thales Data Threat Report Telecommunications Edition
2: Straits Research: Telecom Analytics Market Size is projected to reach USD 13.76 Billion by 2031, growing at a CAGR of 14.2%
3: Grand View Research: Artificial Intelligence in Telecommunication Market Size, Share & Trends Analysis Report, 2020

THALES

Complexity of New Infrastructure Creates Security Vulnerabilities

Digital transformation at telecommunications organizations increases the complexity of hybrid IT infrastructure and both cybersecurity and compliance risks.

Key management complexities

57% of telecoms reported having five or more key management solutions, increasing complexity and making it cumbersome (and expensive) to manage.[1]

Lack of control over keys

Only 14% of telecoms said that they controlled all their encryption keys in their cloud environments.[1]

Lack of protection for sensitive data

Only 13% of telecoms reported that 60% or more of their sensitive data stored in the cloud is encrypted.[1]

Exponential data sprawl

Only 17% telecoms have complete knowledge where all their data is stored and only 24% indicated they could classify a majority of their data.[1]

1: 2023 Thales Data Threat Report Telecommunications Edition

THALES

5G concerns in Telecom, Governments and Enterprises

Concerns about the security of 5G infrastructure is widespread among telecommunications companies, governments, and the broader enterprise market.

Telecommunications

81%

81% of telecommunications companies are concerned about the potential security threats that can arise from new 5G Networks.[1]

Governments

76%

76% of governments and public sector agencies are concerned about the potential security threats that can arise from new 5G Networks.[1]

Enterprises

77%

77% of enterprises are concerned about the potential security threats that can arise from new 5G Networks.[1]

1: 2023 Thales Data Threat Report Telecommunications Edition

3 Key Areas of Concern About 5G Cybersecurity

Telecommunication companies, global enterprises, and governments are concerned about 3 key pillars of 5G Infrastructure.

Identities & Privacy

75%

Protection of identities of people and devices connecting to 5G networks is a top concern for 75% of organizations.[1]

Data in Motion

66%

Security of data moving across 5G networks is a top concern for 66% of organizations.[1]

Applications and Infrastructure

62%

Security of applications, infrastructure, and sensitive data on 5G networks is a top concern for 62% of organizations.[1]

1: 2023 Thales Data Threat Report Telecommunications Edition

Thales 5G Cybersecurity Use Cases

Thales 5G security solutions deliver end-to-end encryption and authentication to help organizations protect data as it moves across IoT, radio access, edge, and the core network and data stores.

Protect PKI Infrastructure, Subscriber Identity and Privacy with Hardware Root of Trust

Achieve the performance, flexibility, and scalability needed to secure subscriber privacy and authentication from the data center to the edge.

Protect Data in Motion with High-Speed Encryption

Maximize 5G security without compromising performance, encrypting all control plane traffic in the core, MEC, and RAN.

Protect Sensitive Data Across Hybrid IT with Encryption & Key Management

Protect sensitive data across containers, on-premises, cloud, or hybrid storage from a single pane of glass.

Protect PKI Infrastructure, Subscriber Identity, Privacy and Authentication with Hardware Root of Trust

Luna Network Hardware Security Modules (HSMs) provide a Post-Quantum Cryptography (PQC) ready solution that meets the performance, flexibility, scalability, and high availability needed to help MNOs and NEPs.

Thales Luna HSM 5G Use Cases

Subscriber Identities: Generate encryption keys, store home network private keys, and perform crypto operations to de-conceal SUCI within the Luna HSM to ensure subscriber identities and privacy, including the SUPI, are protected with a hardware root of trust.

Subscriber Authentication Vector Generation: Store master keys and run authentication algorithms within the secure confines of the Luna HSM to protect authentication related keys during the authentication execution process.

Subscriber Key Provisioning: Secure authentication-related keys during SIM personalization and provisioning by storing encryption keys for provisioning and storage systems and performing encryption/decryption of provisioning and storage system keys.

Strong Foundation of Trust: Secure the entire PKI-based telco infrastructure, digital certificates and signatures by storing and managing the private keys used in code signing applications in a Luna HSM. Luna HSMs can also be used as a root of trust for Thales CipherTrust Manager to secure 5G cloud infrastructure (databases, file servers, TLS/SSL keys, virtual machines and containers).

Compliance and Quantum Readiness: Luna HSMs provide a FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified crypto agile solution, enabling quantum safe algorithms to secure users and data today and into the future.

Thales Luna HSMs (Hardware Security Modules)

5G

Provide a foundation of digital trust for PKI and address security concerns around **subscriber privacy** (SUCI/SUPI), **identities** and **authentication** vector generation, as well as subscriber **key provisioning**.

Protect Data in Motion with High-Speed Encryption

Thales High Speed Encryptors (HSEs) help network equipment providers (NEPs) and mobile network operators (MNOs) address data in motion security challenges and are PQC-ready.

Thales High Speed Encryptors (HSE) 5G Use Cases

Increased Performance: 5G promises remarkable speeds and larger data transfer potential with substantially less wait time. Thales High Speed Encryptors (HSEs) are built for modern networks like 5G that demand enhanced security capabilities for data-in-motion protection, such as encrypting all control plane traffic in the core, MEC, and RAN.

More Flexibility: A multi-point solution, HSE hardware and virtual appliances support a wide range of network requirements, such as network slicing. Thales network encryption solutions are equipped with Transport Independent Mode (TIM), which allows for concurrent encryption over network Layers 2, 3, and 4, eliminating transport constraints and providing for optimum performance at the highest standards of network security.

Compliance & Quantum Readiness: Thales HSEs are certified by NIST, FIPS 140-2 Level 3, and by ANSSI, Common Criteria EAL 4+, and have been vetted by the US Department of Defense Information Systems Agency, NATO, and others. Thales HSEs uphold security best practices, such as authenticated end-to-end encryption, automated key generation and updates, and controlled access (separation of duties). With quantum computing on the horizon, Thales HSEs are quantum ready and support all four NIST PQ algorithm finalists.

Thales High-Speed Encryptors (HSE)

5G

Secure sensitive data in motion/transit to protect network links without compromising performance. Provides low latency, near-zero jitter, and high throughput.

Protect Sensitive Data Across Hybrid IT with Encryption, Key Management, and Secrets Management Solutions

Strong encryption, combined with key management, provides consistent protection for sensitive data and secrets across containers, on-premises, cloud, or hybrid environments.

CipherTrust Data Security Platform Use Cases

Encrypt Sensitive Data Across All Environments: CipherTrust Transparent Encryption provides consistent data-at-rest encryption with granular access control across cloud and on-premises environments regardless of 5G network configurations or virtual network functions. This solution encrypts data generated from containerized applications without any change to application business logic.

Centralized Key Management: CipherTrust Manager centralizes cryptographic key management across multiple cloud vendors and hardware storage providers.

DevOps, Secrets, and Kubernetes Security: Secure, deploy and run cloud-native workloads across environments by transparently protecting sensitive data with RESTful calls, protecting secrets, and establish strong safeguards around data stored in Kubernetes environments.

Strong Access Controls and Auditability: The solution provides strict access controls and the capability to audit all file operation/access events to protected data. Users can monitor usage via SIEMs to better understand who is accessing the information.

5G

Thales CipherTrust Data Security Platform

Protect sensitive virtualized data across containers, on-premises, cloud and hybrid IT environments with encryption, key management and secrets management solutions.


THALES
Building a future we can all trust
Telecommunications Case Studies

Case Study

Global MNO Deploys Thales Solutions as Centralized Data Security Solution for Enterprise

Encryption, Key Management, Code-Signing, and Transaction Security

Challenge

- **A global MNO** wanted to revamp its cyber security posture and implement best-in-class security to improve compliance and reduce the risk of a data breach.
- After assessing its Hybrid IT security needs, the MNO decided to implement a centrally-managed data security solution that could be tapped by several business units.

Solution

- **CipherTrust Data Security Platform** was selected to simplify data security administration and accelerate time to compliance:
  - **Transparent Encryption** protects file systems on-premises and in the cloud.
  - **Cloud Key Manager** centralizes and automates key lifecycle management across the enterprise's AWS, Google Cloud, and Microsoft Azure environments.
  - **Tokenization with Dynamic Data Masking** protects structured data in databases.
- **Luna Hardware Security Modules (HSM)** protect private keys and associated certificates used in code-signing and business apps.
- **payShield HSMs** protect in-store payment transactions at thousands of locations.

Results

- **Centralized data security solution** with multiple capabilities available in a data security stack to address the specific use cases of all business units.
- **Reduced the risk of a data** breach by protecting all the most important systems that store or process sensitive data across the enterprise.
- **Quick time-to-compliance** with mandates, such as PCI, and regulations, such as FIPS.
- **Benefits of scale and lower cost** by replacing ineffective point solutions with a single solution for the entire enterprise.

THALES

EMEA Telecom 5G Implementation - HSM for PKI Root of Trust

Challenge:

- **A leading EMEA-based telecommunications company** providing mobile, fixed-line, broadband and IT services globally was implementing 5G infrastructure and wanted to ensure data security for sensitive data and compliance with GDPR.
- The customer wanted to execute cryptographic functions within a secure environment to ensure both the integrity and the confidentiality of the keys used to encrypt and decrypt data.

Solution:

- **Thales Luna Hardware Security Modules (HSMs)** were implemented to protect master key used in Hashicorp Vault certificate lifycycle management.
- Luna HSMs also supported the mTLS requirement for 5G Service-Based Architecture with Telco-operator PKI root of trust.

Results:

- **Achieved high level assurance in security** by protecting essential crypto graphic functions within a FIPS140-2 Level 3 security appliance.
- **Improved compliance posture** with regulations such as GDPR by reducing risk of data breach.
- **Ensured scalability** by adopting proven, tried, and tested Luna HSMs with flexible protection for multiple use cases.

Major MNO Protects Privacy of Millions of Subscribers

Data-at-rest encryption with separation of duties and granular access policies

Challenge

- **A major MNO** with operations in multiple countries experienced a continuous increase in the number of attempted cyber-attacks on its IT infrastructure.
- The organization wanted to implement a comprehensive data security solution to protect the sensitive data of millions of subscribers across its systems and to replace complex point solutions.

Solution

- **CipherTrust Transparent Encryption** was implemented to protect multiple file systems and databases, including hundreds of Oracle database servers.
- **CipherTrust Transparent Encryption** delivers data-at-rest encryption, centralized key management, privileged user access control, and complete separation of duties.
- **Thales Luna HSMs** were deployed to provide a secure root-of-trust for all encryption keys.

Results

- **Reduced the risk of a data breach** and ransomware attacks by protecting all the most important systems that store or process sensitive data across the enterprise.
- **Centralized management panel** enabled the MNO to understand the disposition of sensitive data, how each data set was protected, and who had access.
- **Had no impact on operations** and no reduction in performance of protected systems; authorized users and processes continue to leverage data for essential operations.

Telecom 5G Compliance with GDPR using HSM Root of Trust

Challenge:

- **A leading telecommunications company in the Nordics** provided mobile and fixed telephony, broadband, and TV services to both residential and business customers.
- The customer wanted to protect subscriber privacy and confidentiality to comply with regulations, such as GDPR and 3GPP, as it upgraded its infrastructure to 5G.

Solution:

- **Thales Luna Hardware Security Modules (HSMs)** were implemented to protect subscriber privacy and integrated with the Network Equipment Provider.
- Luna HSMs provided a secure and tamper-proof FIPS 140-2 Level 3 environment for storing and managing encryption keys.

Results:

- **Protected subscriber privacy** by protecting essential PKI cryptographic functions within a FIPS140-2 Level 3 security appliance.
- **Improved compliance** with regulations such as GDPR by reducing risk of data breach.
- **Ensured scalability** by adopting proven, tried and tested Luna HSMs with flexible protection for multiple use cases.

MNO Expands Cybersecurity Services Portfolio and Protects Customer Data

Cloud-based access management as managed service for enterprises

Challenge

- **A North American MNO** wanted to add advanced access management and Multi-Factor Authentication (MFA) to its growing enterprise cybersecurity services portfolio.
- This MNO has a large variety of enterprise customers of different sizes and in different industries and was looking for the most comprehensive and flexible solution available to protect access control in multiple use cases.

Solution

- **SafeNet Trusted Access** premium was adopted as a new cybersecurity managed service to protect an enterprise customer with over 20,000 users.
- SafeNet Trusted Access leveraged hardware and software multi-factor authentication (MFA) tokens to enable comprehensive access management to multiple cloud and on-premises environments, including integration with Azure AD and protection of Office 365.

Results

- **Seamless onboarding** of new service with multi-tier, multi-tenancy architecture, monthly billing, and easy user migration.
- **Single panel of glass** with simplified access management to a complex set of cloud and on-premises environments.
- **Robust MFA** options including phishing-resistant authentications based on FIDO and CBA.
- **Highly profitable service** with low operating costs based on 100% Software as a Service that is quick and easy to deploy and requires few resources to manage and maintain.

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.

THALES

Building a future we can all trust

Contact Us

For all office locations and contact information, please visit

cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com