THALES
Building a future we can all trust

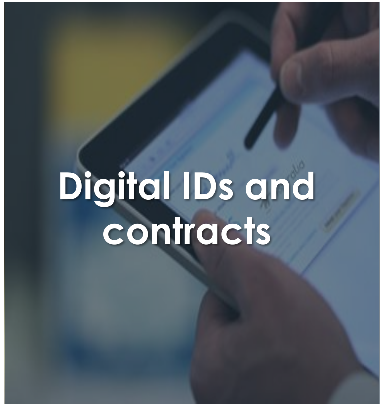
Accelerate Government Transformation by Reducing Risk, Complexity, and Cost

eBook

Government services benefit dramatically from innovation and transformation

Digitalization of services and adoption of new platforms are reinventing government services and public administration:

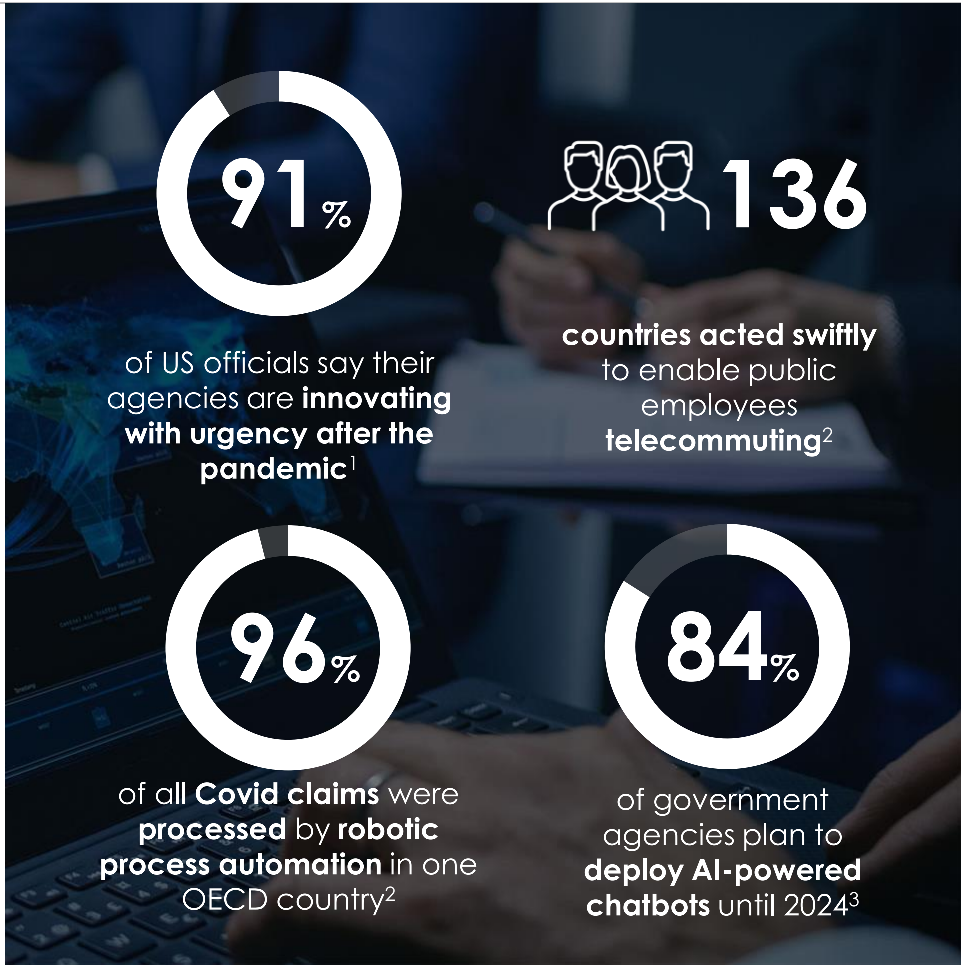
- **Digital citizen services** with improved and convenient experience are replacing long trips to government agencies.
- **Digital IDs and contracts** are enabling remote government interactions with high assurance and security.
- **Smart Cities** are using thousands of IoT devices and real-time insights to re-imagine public administration.
- **Artificial Intelligence (AI)** and **Big Data** insights are transforming governance, making it more effective, faster, and cheaper.
- **Open government & transparency** is becoming a reality by making more data public and available for collaboration and providing better accountability.
- **Remote work, cloud collaboration** and other platforms and practices common in the private sector are quickly being adopted by government agencies.



Covid 19 dramatically accelerates digital government initiatives

The adoption of new technologies and platforms moved into high gear during the Covid 19 pandemic across all industries, and that was especially true in government:

- **Innovating with urgency** after the pandemic was the response by 91% of government agency officials in the United States when asked about digital transformation.
- **Enabling public employees to telecommute** was a priority for 136 countries that were able to act swiftly by making work rules more flexible and implementing technological upgrades.
- **Robotic process automation** was used by one OECD country to process 96% of all Covid-related unemployment claims, with each claim being processed in 36 seconds instead of 20 minutes in the previous manual process.
- **AI-powered chatbots** were implemented around the world to handle pandemic-related inquiries. By 2025, Gartner estimates that 84% of government agencies globally will have deployed AI-powered chatbots.



91% of US officials say their agencies are **innovating with urgency after the pandemic**[1]

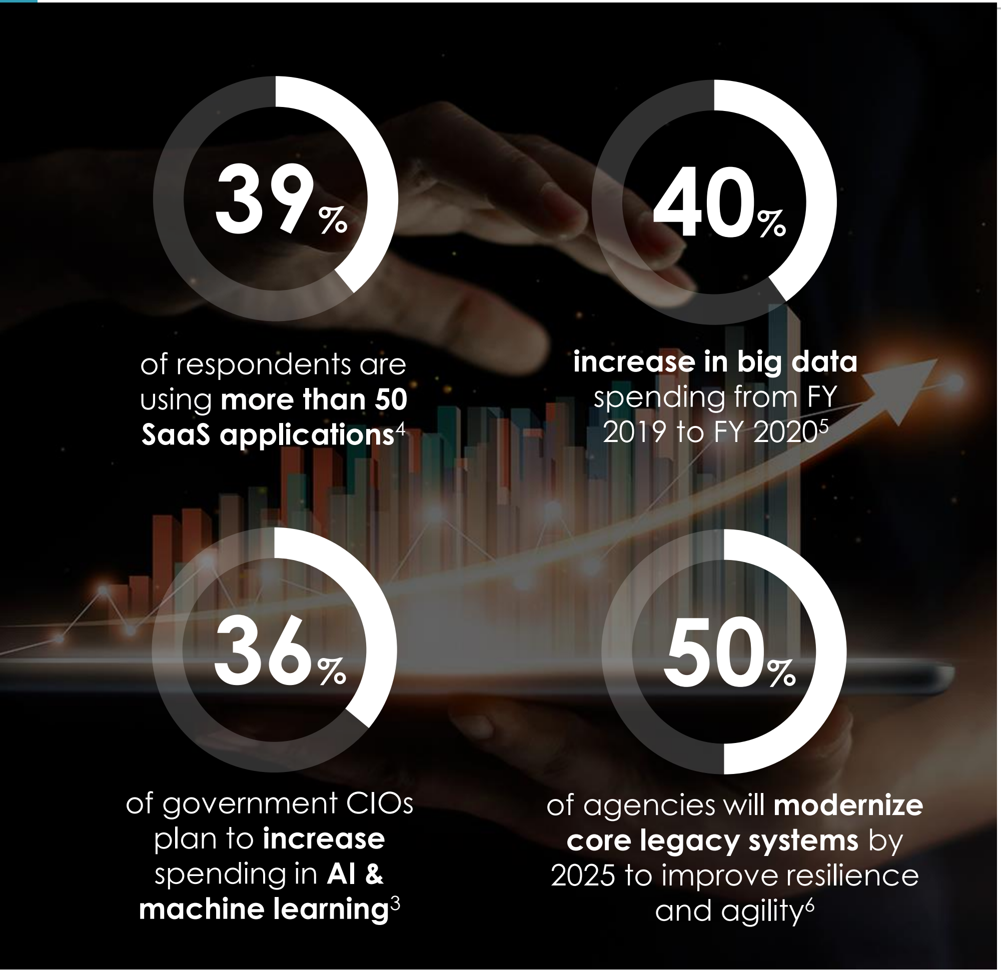
136 **countries acted swiftly** to enable public employees **telecommuting**[2]

96% of all **Covid claims** were **processed** by **robotic process automation** in one OECD country[2]

84% of government agencies plan to **deploy AI-powered chatbots** until 2024[3]

[1] Accenture: Five trends for post-pandemic leadership
[2] Deloitte: 2021 Government Trends
[3] Gartner: Gartner Says Government Organizations Are Increasing Investment in AI

Driving major growth in digital transformation



39% of respondents are using **more than 50 SaaS applications**[4]

40% **increase in big data** spending from FY 2019 to FY 2020[5]

36% of government CIOs plan to **increase** spending in **AI & machine learning**[3]

50% of agencies will **modernize core legacy systems** by 2025 to improve resilience and agility[6]

Digital government initiatives are driving the adoption of a wide range of new technologies and platforms that completely change the existing IT infrastructure of agencies at the federal, state, and local level:

- **Cloud adoption** is widespread and growing fast. In the Data Threat Report 2021, 451 Research found that 39% of US federal agencies use 50 or more SaaS applications, and 83% store more than 30% of all their data in the cloud.
- **Spending in Big Data** is increasing around the world, in 2020 alone it grew by 40% across federal agencies in the United States**.**
- **Artificial Intelligence and Machine Learning** are a priority for most government CIOs. Gartner reported that 36% plan to increase spending on AI and machine learning, and 85% want to implement data-mining supported by machine learning until 2024.
- **Modernization of core legacy systems** is essential for an industry that is known for its reliance on legacy applications. Gartner reports 50% of agencies plan to do that by 2025 to improve resilience and agility.

3: Gartner: Gartner Says Government Organizations Are Increasing Investment in AI
4: Thales: Data Threat Report 2021
5: Gov Win: COVID-19 Influences Upward Trend in Big Data Contract Spending
6: Gartner: Gartner Identifies Top 10 Government Technology Trends for 2021

While making cyber-attacks an even bigger challenge

The digitalization of government services and processes make the growing incidence of cyber-attacks an even bigger challenge for agencies around the world:

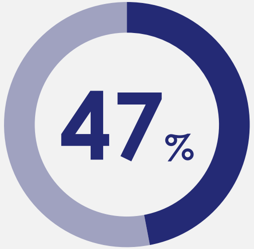
- **The number of cyber incidents** at government agencies around the world reached 3,236 in 2020, and of these 885 were confirmed data breaches that impacted federal, state, or local agencies, according to the Verizon Data Breach Investigations Report.
- **Ransomware attacks** struck 246 federal, state and local agencies in the United States in the last 3 years and are estimated to have impacted 173 million people.
- **An increase in the volume, severity and scope** of cyberattacks was reported by 47% of government respondents of the Data Threat Report of 2021.

3,236

cyber incidents at government **agencies across the world** in 2020[7]

246

government agencies impacted by **ransomware** in the US in the past 3 years[8]



govenrment respondents reported an **increase in volume, severity** or **scope** of **cyberattacks** in 2020[4]

173 million

people affected by **attacks** on US **government agencies** between 2018 and 2020[9]

4: Thales: Data Threat Report 2021
7: Verizon: 2021 Data Breach Investigations Report
8: Emisoft: The State of Ransomware in the US 2020
9 American City & County: Ransomware attacks cost local and state governments over $18 billion in 2020

Stricter cybersecurity mandates and legislation add urgency

The growth of cyber incidents at government agencies and critical infrastructure has led to unprecedented executive and legislative action:

- **The Executive Order to Improve the Nation's Cybersecurity** and protect federal government networks was signed by President Biden in 2021. The order helps move the US federal government 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.
- **Because of the convergence of existing privacy, sovereignty, and data protection** regulations, such as GDPR and PCI-DSS; federal standards, such as fedRAMP and FIPS; and global standards, such as ISO 27001, agencies are faced with an all-encompassing set of rules and standards that make compliance much more complex and challenging.

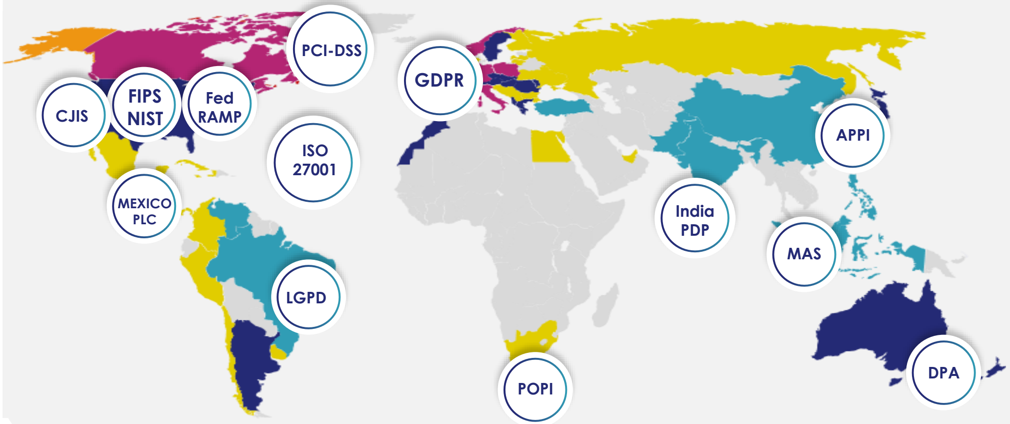
New mandates and legislation complement…

THE WHITE HOUSE
WASHINGTON

White House Cybersecurity Executive Order

European Union Cybersecurity Act

…existing data security and privacy regulations



How Thales Cloud Protection and Licensing can help

Thales enables government agencies to offer better services
by accelerating digital transformation while reducing risk, complexity, and cost.

Accelerate digital transformation

Adopt innovations, such as **cloud, Big Data, AI, and IoT** faster with a framework for a zero-trust world

Scale security across hybrid IT

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

Reduce risk and complexity

Simplify compliance with **centralized data governance** and de-identified sensitive data

THALES

Accelerate digital transformation

Digital Records and Signatures

Multi-cloud

Smart Cities & IoT

Artificial intelligence

Big Data

Adopt innovations such as digital signatures, multi-cloud environments, Smart Cities & IoT, 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 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**

Secure agility and flexibility of Court's digital transformation in LATAM

Centralized data security and access management across Hybrid IT

Challenge

The **Court of Auditors** of the state of Mato Grosso in Brazil does highly **confidential investigations** with privileged access to **regulated sensitive data** on the accounts of **870 public entities.**

Digitalization and **modernization** of IT systems made the Court more efficient, but also made it a priority to **protect data against cyberattacks.**

The Court sought a **security solution** focused on **cryptography as well as access controls.**

Solution

CipherTrust Transparent Encryption in conjunction with **CipherTrust Manager** was implemented to protect unstructured sensitive data and **CipherTrust Tokenization** with **Dynamic Data Masking** was implemented to protect structured data in databases.

The Court also incorporated Thales's **Safenet Trusted Access** to ensure secure access management with **multi-factor authentication (MFA)** combined with access policies.

Results

Quick and seamless deployment secured sensitive assets and enforced compliance with regulations **in a matter of days.**

Protected confidential information in files and servers and **set granular policies** for data access.

Pseudonymized and anonymized sensitive information in databases while maintaining the ability to analyze aggregate data.

Enabled secure single sign-on access to multiple applications, whether **in the cloud** or the Court's **internal networks**.

Securing access to digital government services in North America

Luna HSMs protect PKI keys for citizen digital identities

Challenge

“**The Secure Channel**” is a **Canadian government network** that allows citizens and businesses to **access a range of services electronically**, from paying taxes to applying for benefits.

As part of the country’s **largest technology undertaking to date** all transactions needed to remain **private** and **secure**.

The security solution had to **protect** the **encryption keys** used to encrypt **digital certificates** and **authenticate** users, and **ensure availability** at anytime from anywhere.

Solution

Thales Luna Hardware Security Modules (HSMs) were deployed to control and protect the government root signing **PKI keys**.

Luna HSMs meet the **Canadian Government’s stringent standards** and specifications for hardware security by being validated to **FIPS 140-2 level 3** and **Common Criteria** standards.

Luna HSMs are available **on-premises, in the cloud, as a service** on Thales Data Protection on Demand (DPoD), and also **in hybrid environments**.

Results

Ensured security of digital transactions including filing **tax returns**, **passport renewals** and checking **employment records.**

Luna HSMs provided the **high performance** and **24/7 availability** of the solution and consequent successful digital services.

Maintained the **trust of citizens** and the Canadian government’s position as a **leader in eGovernment initiatives.**

Thales solutions are now in widespread use **throughout the Canadian** government.

Scale security across enterprise Hybrid IT

SaaS, PaaS, IaaS services

On-premises systems

File repositories and databases

External 3rd party collaboration

Remote IoT devices

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 o**n-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.

Responding to Covid 19 while improving privacy and security in APAC

Encryption security with virtually no impact on system performance

Challenge

Responding to the **outbreak of Covid19, Cheonan City in Korea** needed to establish a system for **citizens to apply for emergency aid on its website**.

The City needed to **quickly install a stable encryption solution** to protect sensitive information it would be gathering from applicants.

The system needed to be **compatible with other solutions** in the web infrastructure and **expandable to other sensitive data,** such as **voice, image,** and **text**.

Solution

CipherTrust Transparent Encryption was implemented to protect **structured** and **unstructured** sensitive data.

Unlike other encryption solutions, **CipherTrust Transparent Encryption** provided **excellent performance** for both encryption and decryption.

Common Criteria and **FIPS 140-2** certification eased implementation and compliance with local regulations.

Results

Transparently protected sensitive data on web-based COVID19 emergency support application while maintaining application availability.

Ensured compatibility with the City's existing **security solutions, data storage** and **processing platforms**.

First foreign solution to be certified by the **Korean National Intelligence Service**.

Cheonan City is considering an **expansion of this data protection** to include the sensitive data of more citizens in more use cases.

Securing remote access with cost savings and efficiency in EMEA

Securing access to cloud and on-premises systems while reducing costs

Challenge

Dudley Metropolitan Borough Council, a local governing board in the UK, was providing **remote access for over a thousand users**, but wanted to increase that number to **save on office space and help improve service quality**.

However, its **aging secure remote access infrastructure** was **costly** and **demanded a high degree** of attention from technical staff.

Solution

The Council switched to **Thales SafeNet Trusted Access**, which delivers **fully-automated, highly secure, strong authentication** with flexible token options tailored to unique organizational needs.

The service enables a **quick migration to multi-tier and multi-tenant cloud environments** and protects cloud-based and on-premises applications and data as well as corporate networks, identities, and devices.

Results

Achieved immediate cost effectiveness with SaaS model SafeNet Trusted Access service **no up-front expenses**.

Lowered total cost of ownership by reducing work-load on support staff and associated costs **by 25-30%** and **reducing** key fob purchase **costs by 10%.**

Increased remote user satisfaction of **5,000** desktop and **1,200** laptop users.

The Council is considering **expanding its remote access offering** to further reduce operational costs.

THALES

Reduce risk and complexity

Accelerate time to compliance with centralized data and **identity security governance**

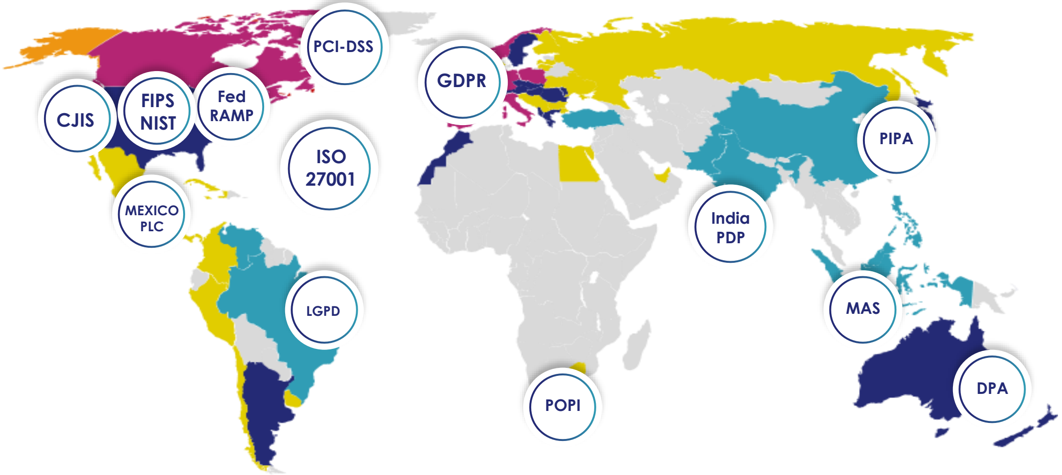
Discover and classify data across **hybrid IT** according to sensitivity to **specific** legislation requirements.

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**.

White House Cybersecurity Executive Order

European Union Cybersecurity Act



THALES

Securing transparent citizen access to government data in Hawaii

Secure data access and compliance with legislation though encryption

Challenge

The **State of Hawaii** is increasingly making more of its **data accessible to the public** under the **open government initiative**.

The State needed to **implement just-in-time access to sensitive data**, maintaining the data encrypted at all times and only decrypting it when an authorized user needed it.

The State also wanted to offer this "**encryption-as-a-service**" **offering to all State departments** that wished to better secure their data.

Solution

The State chose **CipherTrust Transparent Encryption** to protect a wide variety of file formats and data states.

Granular controls allowed only **specific data to be decrypted** when needed by authorized user while maintaining **data encrypted at all times** in the servers, maximizing security against data breaches.

Results

Achieved secure just in time **access to sensitive data by thousands of users** across multiple departments and facilities.

Addressed requirements of relevant regulations such as Accountability Act (**HIPAA**), Fair Information Practice Principles (**FIPPs**), and Federal Information Security Management Act (**FISMA**).

Enabled availability of **encryption-as-a-service across the State** and the standardization of Ciphertrust Transparent Encryption as the **data protection platform** for **Hawaii**'s Office of Enterprise Technology Service.

High-performance security for defense department in EMEA

High Speed Encryptors protect data in motion & comply with defense requirements

Challenge

A European Ministry of Defense needed to replace an end-of-life encryption solution that allowed **secure communication between command centers and field bases** through a field service pack.

The customer was looking for a **FIPS certified, high-performance** solution with **small form-factor**.

The Ministry wanted to **add layer 2 encryption** to their existing layer 3 encryption to **increase bandwidth and performance**.

Solution

Thales deployed **Thales CN4010 High Speed Encryptors** at both **command center** and at **field bases** through a field service pack.

The triple-certified solution with **FIPS 140-2 Level 3, Common Criteria and CAPS** CN4010 provided high speed communication in **small form-factor** to fit **field service packs**.

Results

Achieved highest security and compliance with **defense department** requirements for data in motion protection.

Provided maximum throughput with zero protocol overhead, **zero latency**, and **increased performance** from **10Mb to 1Gb** in the most demanding environments.

Ensured flexibility with quick **in-field upgrades** to meet the range of use cases.

Successful and easy deployment, added to network with ease, and once deployed, "**set and forget**".

Thales Cloud Protection & Licensing

Our Solutions

Data Protection

Access Management & Authentication

Software Monetization

#1
Worldwide in general purpose HSMs

#1
Worldwide in payment HSMs

#1
Worldwide in cloud HSMs

#1
Worldwide in data encryption

#1
Worldwide in key management

#2
Worldwide in cloud authentication

#1
Worldwide in software protection

#1
Worldwide in software licensing

Over **2,600** employees

25 Countries Presence

750 Engineers Worldwide

30,000 Customers Worldwide

The people we all rely on to secure their privacy – they rely on Thales

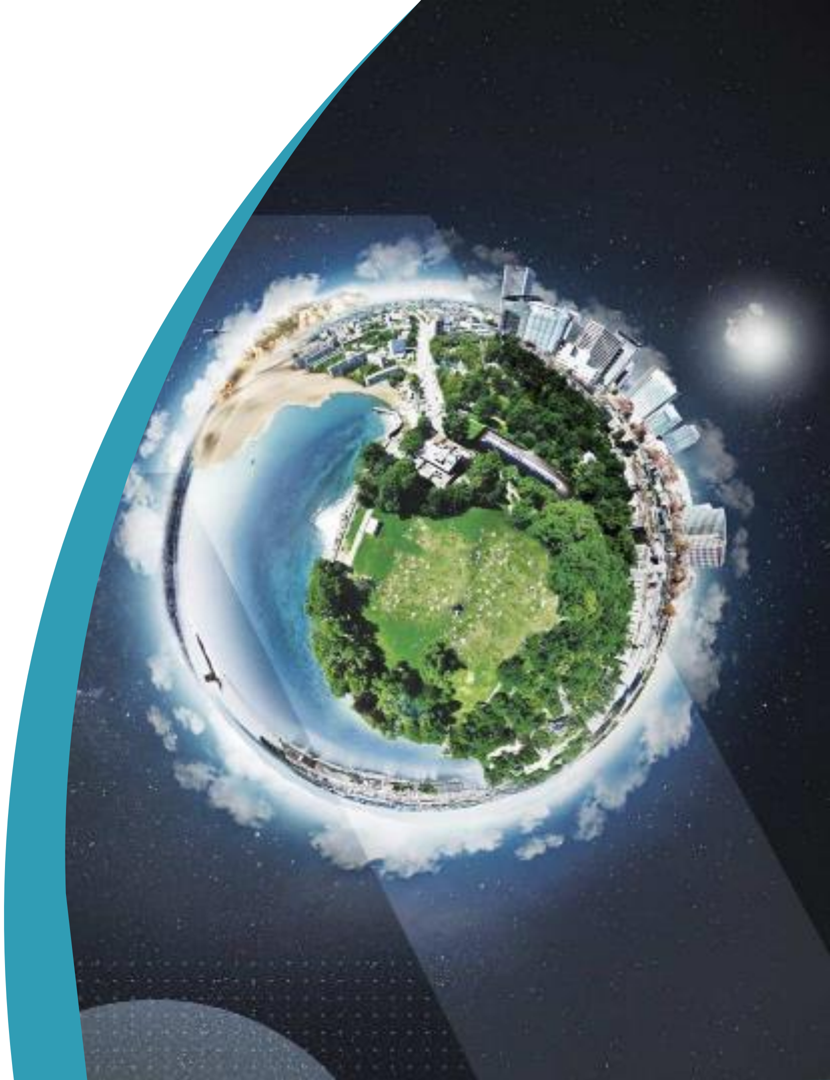
*Thales's technologies and services help secure **more than 80%** of the world's payment transactions and the most valuable corporate and government information*

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.

Thank you!



cpl.thalesgroup.com