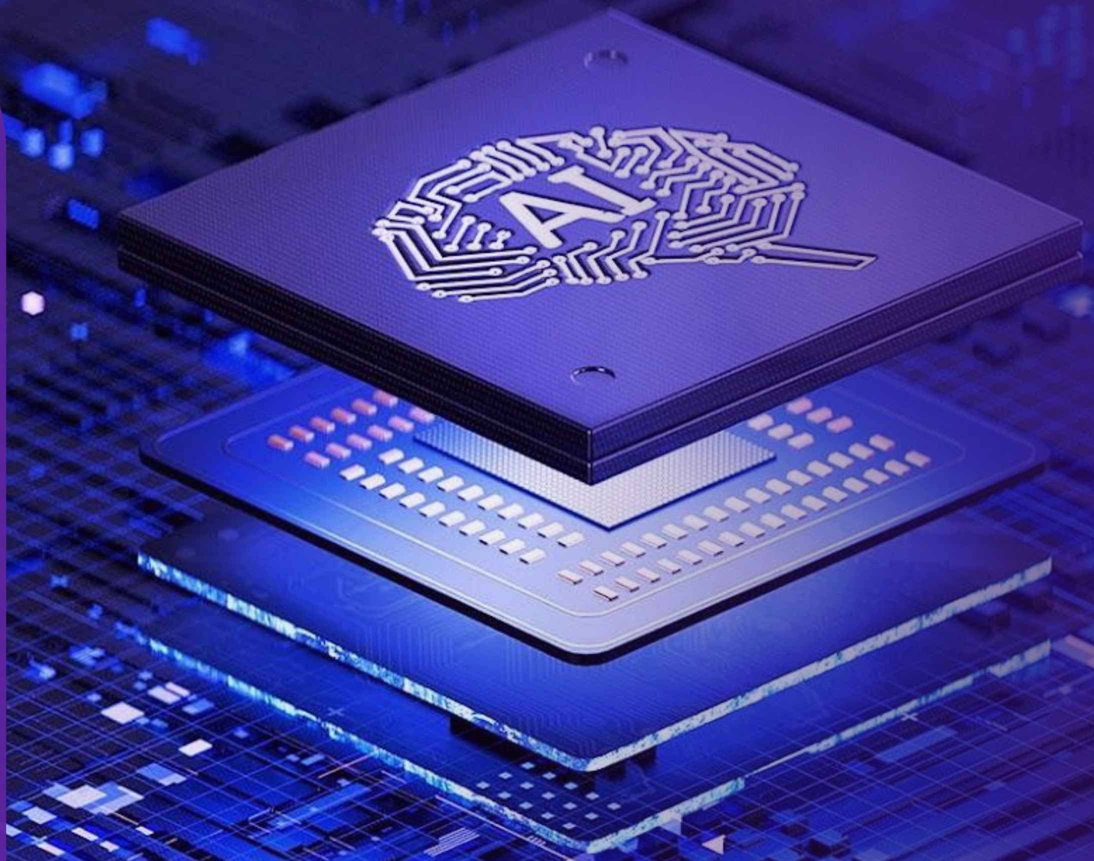
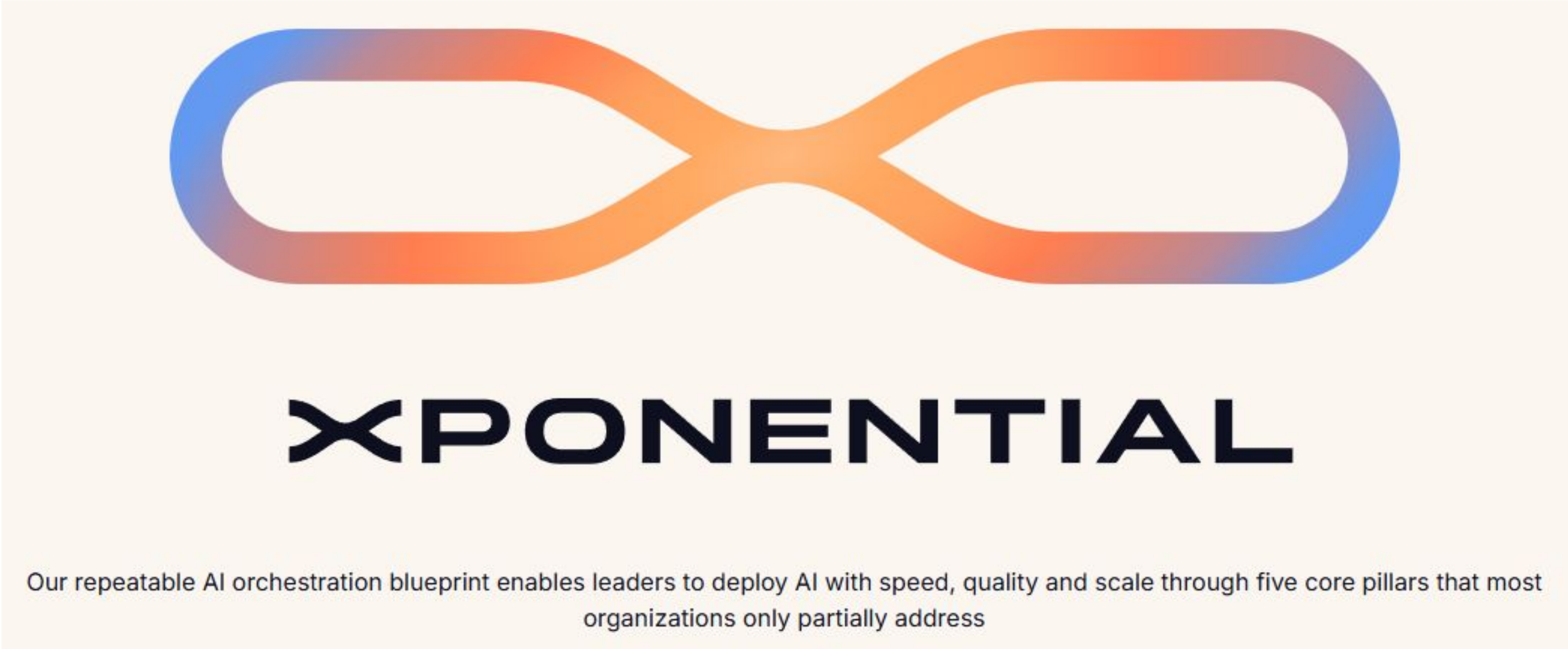
Vesmírna AI (ESA)

ITAPA 9.12.2025

Marián Možucha, DXC Technology

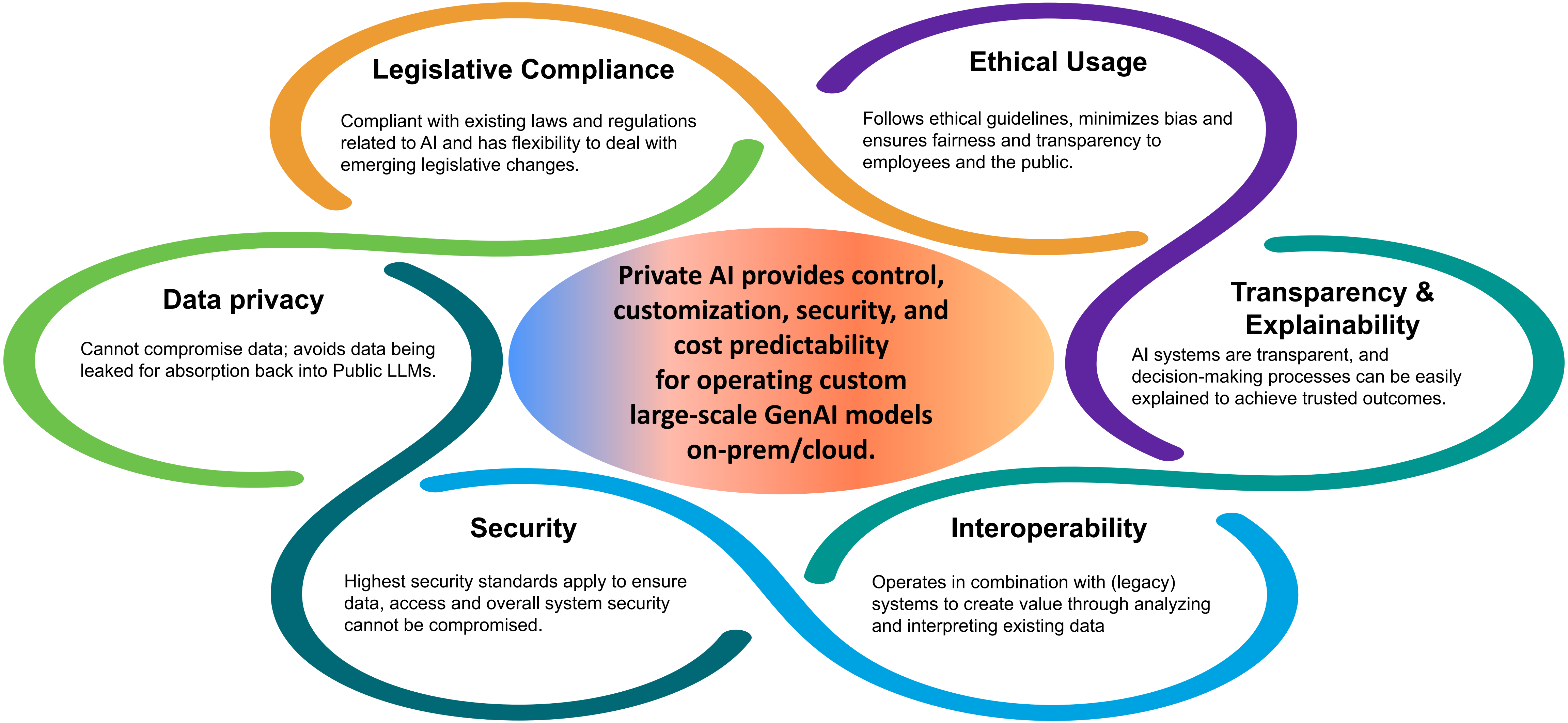




XPONENTIAL

Our repeatable AI orchestration blueprint enables leaders to deploy AI with speed, quality and scale through five core pillars that most organizations only partially address

DXC Secure Sovereign AI (Private AI)



Legislative Compliance

Compliant with existing laws and regulations related to AI and has flexibility to deal with emerging legislative changes.

Ethical Usage

Follows ethical guidelines, minimizes bias and ensures fairness and transparency to employees and the public.

Data privacy

Cannot compromise data; avoids data being leaked for absorption back into Public LLMs.

Private AI provides control, customization, security, and cost predictability for operating custom large-scale GenAI models on-prem/cloud.

Transparency & Explainability

AI systems are transparent, and decision-making processes can be easily explained to achieve trusted outcomes.

Security

Highest security standards apply to ensure data, access and overall system security cannot be compromised.

Interoperability

Operates in combination with (legacy) systems to create value through analyzing and interpreting existing data

DXC Secure Sovereign AI

Addressing regulatory and security compliance challenges

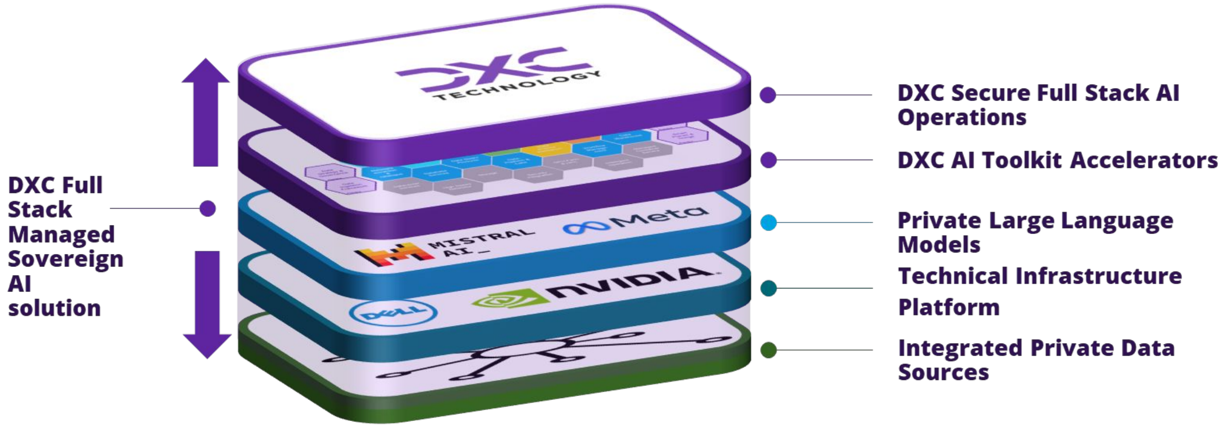
AI presents huge opportunity for A&D organizations that includes quality improvement, smart scheduling, safety improvements, predictive maintenance and many more use cases.

However, this needs to overcome the inertia many organizations are facing that is inhibiting the opportunity:

- Regulatory and security compliance
- Data classification and privacy needs
- Ability to navigate the options and identify a viable solution for their needs

DXC Capability

DXC provides a full-stack, fully-integrated end-to-end AI solution across multiple Secure AI deployment options.



DXC Full Stack Managed Sovereign AI solution

DXC Secure Full Stack AI Operations

DXC AI Toolkit Accelerators

Private Large Language Models

Technical Infrastructure Platform

Integrated Private Data Sources

Case Study: ASK ESA Project

- **Background:** The European Space Agency (ESA) awarded DXC Technology a contract to develop "Ask ESA," an AI platform to enhance efficiency and knowledge sharing.
- **Project Overview:**
- **Technology:** Built by DXC, using NVIDIA and Mistral AI's generative AI.
- **Functionality:** Modular platform for accessing documents, deploying AI applications, and ensuring data privacy.
- **Impact:** Increased efficiency, innovation boost
- **Efficiency:** Enhances ESA's ability to deploy AI solutions quickly.
- **Partnership:** Builds on a 15-year collaboration between ESA and DXC.

European Space Agency

ESA's challenge in Secure Sovereign AI (Private AI) setup

RAG-as-a-Service

Business need:

- One Go-To-Chatbot for all space scientists and engineers
- Customizable chat solution for individual directorates – e.g. Rocket propulsion, fuel
- Anyone can upload any document and interact with it
- Enhanced analytics, monitoring and scaling across ESA entities

4,000+
Users – rocket scientists, engineers, IT staffs, business users, and more

100%
On-premise solution using open-source technologies and models

ASK ESA – Enterprise Platform & Application

Business need:

- Develop Scalable Platform for hosting AI and GenAI solutions
- Setup customization GenAI Application layer adaptable to need and scalability
- Custom UI and portal application for serving users and leadership and external vendors

Scalable Platform to serve users need

Application layer hosting GenAI, LLMs, or AI Agents

Enterprise ChatGPT

Business need:

- Create a secure, private "ChatGPT"
- Boost productivity and augmented day-to-day tasks
- Gradually rolling out to the entire enterprise

11,000
Augmented staff

30%
Productivity gains on average

Ideation & Feasibility	Data Strategy & Sourcing	Data & Platform Engineering	Model Development & Integration	Governance, Ethics & Guardrails	Scaling & Operationalizing	Security & Maintenance	Model Training & Fine-tuning (LLMOps)

DXC Helps European Space Agency Launch GenAI Agents

esa

Accelerated by NVIDIA infrastructure and designed and built by DXC, the new platform is based on Mistral AI and will allow the Agency to efficiently access high volumes of documents and data.

> “By working with DXC and applying agile methodology, we quickly evolved from a prototype experiment to corporate production maturity with a robust and scalable solution.”

Charles Antoine Poncet
IT Portfolio Manager & AI Leader at ESA

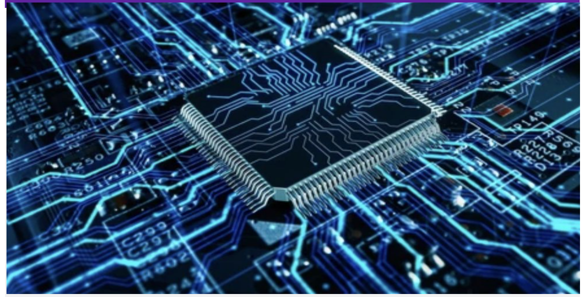
DXC's Secure Sovereign AI Value:

Full Stack Integration

DXC delivers Secure AI as a **fully integrated, end-to-end stack**—from infrastructure to inference—designed to slot into complex environments.

This means **faster deployment**, **less disruption,** and seamless alignment with existing platforms and data

Defense Grade Security



With air-gapped options, **confidential computing**, and **zero-trust** architecture, DXC's Secure AI meets the **highest standards for data sovereignty**, encryption, and tenant isolation.

It's built for classified workloads and mission-critical operations

Accelerated Adoption

DXC's platform accelerators, modular frameworks, and proven delivery models help defence clients **move from pilot to production quickly**.

We bring **pre-integrated toolkits**, agentic workflows, and scalable infrastructure to reduce time-to-value

Trusted Expertise

With decades of experience across secure domains and over 280 government clients, **DXC is a trusted partner in defence**.

We take full-stack accountability and offer deep consulting on governance, compliance, and operational readiness

Guaranteeing Confidentiality

Data Encryption

- We use encryption to maintain strict data confidentiality for data at rest, in transit, and optionally in use.
- Data at rest is always encrypted with industry-standard methods, allowing customers to control their encryption keys via BYOK options and HSMs, which remain inaccessible to the service partner.
- Data in transit is secured through TLS 1.3 with Perfect Forward Security and authenticated using Mutual TLS.
- For data in use, we may implement Confidential Computing within Trusted Execution Environments, using Intel TDX, AMD SEV, or NVIDIA Confidential Compute on supported hardware, along with the NVIDIA GPU Operator and secure boot measures.
- Customers can manage their encryption keys through KMS integrations or dedicated HSM appliances.

Access Controls

- Our team adheres to legal NDAs and confidentiality agreements, lacking access to customer data unless explicitly permitted in a controlled and audited manner. We utilize multi-factor authentication (MFA) and just-in-time (JIT) access managed by a privileged access management (PAM) system. Customers oversee their users and identities via federated identity providers, maintaining full control over authentication and authorization. Role-based access control (RBAC) is implemented at all levels.

- Service-level workload identities are linked with the Istio service mesh for secure service authentication. Administrative tasks are automated and run in isolated pathways. For debugging and support, our staff only accesses non-production environments that mimic customer setups, using only synthetic or anonymized data to ensure customer confidentiality during operations.

Modification for CONFIDENTIAL classified information

- Dedicated hardware for each customer, utilizing customer-owned HSMs only.
- Physically isolated network, power, and racks, with no public internet access.
- Service personnel must be nationals with security clearance and complete background checks.
- Optional use of air-gapped environments or one-way firewalls for controlled data output.