clarence

NISDUC

May 19th 2026

Ensuring NIS2 Compliance with Clarence: The Sovereign Cloud Advantage

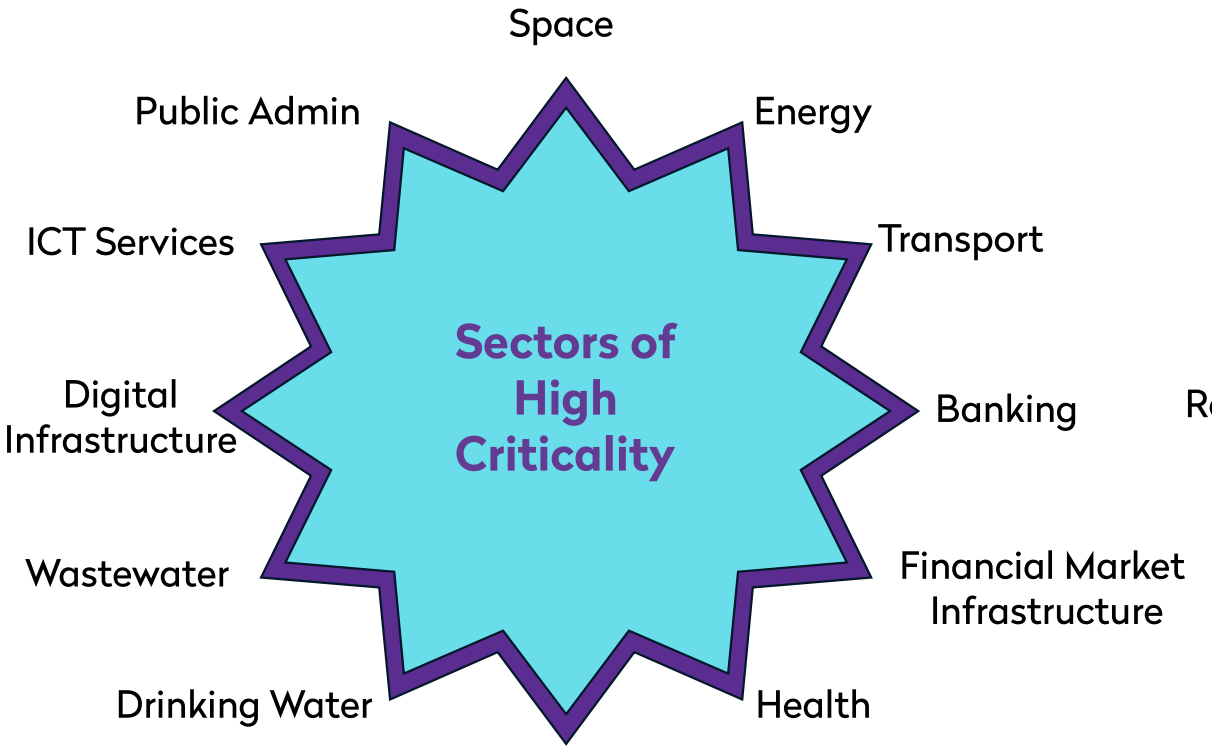
Jean-François TERMINAUX – Proximus NXT Luxembourg
Partner Manager – Disconnected Sovereign Cloud
jean.francois.terminaux@proximus.lu

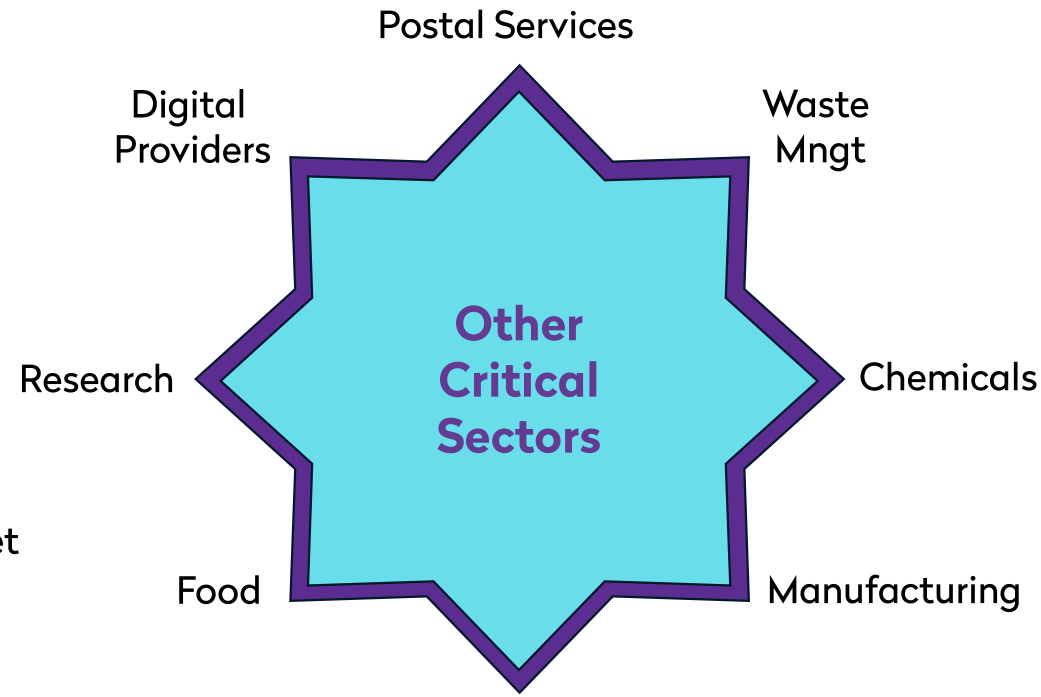
clarence

Clarence: The Sovereign Path to NIS2 Compliance

1

NIS2 Scope: 18 Key Sectors





NIS2 Main Objectives

Increasing Cyber Resilience

- **Risk Management:** Entities must implement technical, operational, and organizational measures to manage risks (e.g., incident handling, supply chain security, and cryptography).
- **Business Continuity**: Ensuring that if an attack happens, essential services (like water or electricity) can recover quickly without causing societal chaos.

Streamlining Reporting Obligations

NIS2 introduces strict, harmonized timelines to ensure the authorities can react in real-time to emerging threats.

- **The 24-Hour Rule:** Organizations must submit an "early warning" within 24 hours of becoming aware of a significant incident.
- **The 72-Hour Rule:** A full incident notification is required within 72 hours.

Strengthening Supply Chain Security

One of the biggest shifts in NIS2 : focus on the **Supply Chain.**

Recognizing that hackers often enter through smaller, less-secure vendors, the directive requires "Essential" and "Important" entities to vet the security practices of their direct suppliers.

Enhancing Accountability and Sanctions

- **Management Liability:** Corporate bodies can be held personally liable for a failure to comply with cybersecurity risk-management measures.
- **Hefty Fines:** non-compliance can lead to massive fines—up to €10 million or 2% of total worldwide annual turnover for essential entities.

New AI and Analytics use cases are driving demand for air-gapped services in Public Sector & Regulated Industries

Public - Space Defence Sectors

- Train ML models on sensitive datasets e.g. Analyze sensitive economic data, RF signals or satellite imagery
- Run sensitive training exercises and simulations where personal need it
- Use vision AI to optimize natural disaster response, analyse infectious diseases or detect fraud
- Use OCR and translate on documents found in the field

Financial Services

- Meet regulatory requirements and protect sensitive information
- Build resilience against any interruption in the public cloud
- Run closer to legacy computing systems to reduce latency
- Process data that cannot be put in a public cloud environment.

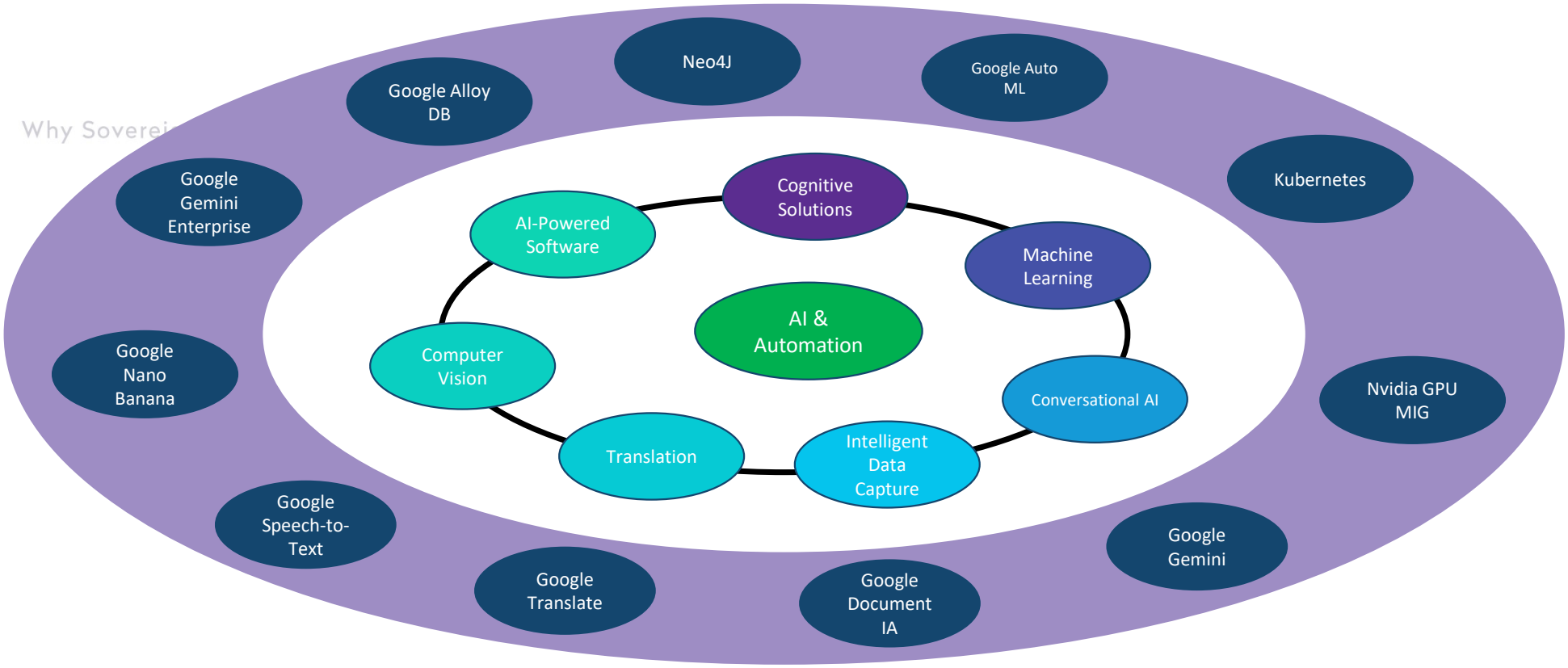
Manufacturing and Utilities

- Ensure operations will not go offline or be disrupted
- Run AI against proprietary data not in the public cloud
- Need low latency to process industrial device data in their facility
- Secure systems running national infrastructure and support remote environments.

Healthcare

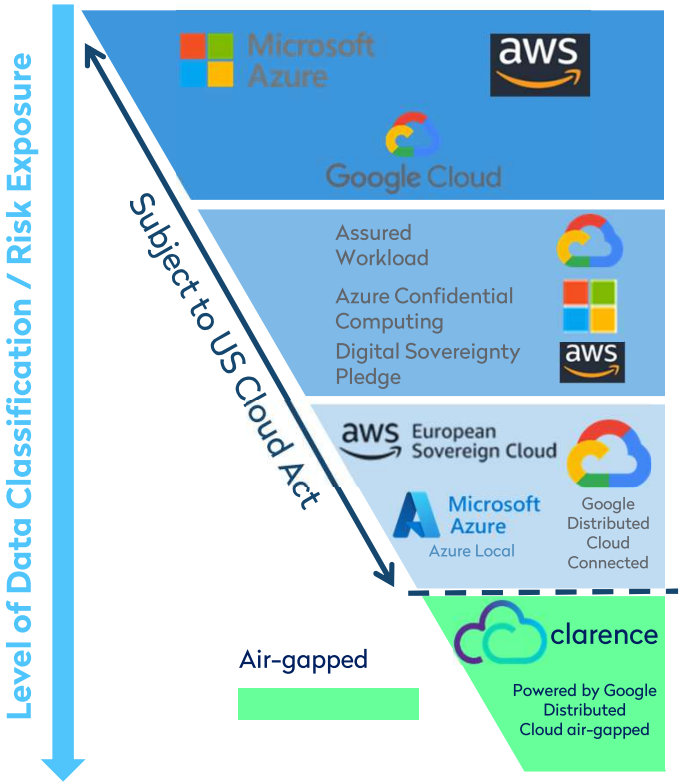
- Improve latency for the local operation of medical equipment
- Development and protection of sensitive clinical trial data
- Secure storage capabilities to process sensitive data, including patient and disease registries

Beyond Sovereignty, powerful AI Toolbox is required*



** Available services depend on Clarence stack version and may require deployment of related solutions or BOYL model.*

Clarence brings both Full Sovereignty and AI Power



Use cases	Solution	Workload
Majority of commercial and regulated data	Public Cloud	Core access, encryption, and residency controls with transparency into operations
Sensitive, controlled and unclassified information	Sovereign controls, additional partner managed key operations	Sovereign control over encryption keys, admin access, service deployment location, partner services (log reviews, BYOID)
Highly regulated markets with strict on-rem requirements	Google Distributed Cloud Connected	On-premise data and processing. Fully managed and operated by Hyperscaler or local partner.
Critical, Sensitive, Classified, Secret, Top Secret, Localized	Google Distributed Cloud Air-Gapped	Air-gapped operations. Disconnected: Fully isolated from Google & the Internet. Operated by partner (Clarence). Survivability and full segregation.

Addressable Markets

Who is Clarence?

2

Clarence – First Strategic Partnership to Deliver Google Distributed Cloud air-gapped

Combining Truly Sovereign Cloud hosted and operated in Luxembourg

&

Powerful innovation and AI toolbox

based on Google Distributed Cloud air-gapped technology

LUX CONNECT 60 %

proximus 40 %

Google Cloud

Technology partner

Launch of Clarence - October 25th 2023

Clarence Go Live : November 15th 2024

Clarence 1st onboarded customer: December 1st 2024

Clarence
Powered by Google
Distributed Cloud air-gapped

3

Google Distributed Cloud Technology Stack

Management & Operations

air-gapped
Fully air-gapped local stack delivered As “operations rack” : You operate your dedicated sovereign environment while We ensure its functionality

On-premise Environment

ISV + 3P Software

Security & Compliance

AI Everywhere

Cloud-Native Runtime (GKEE) Container / VM

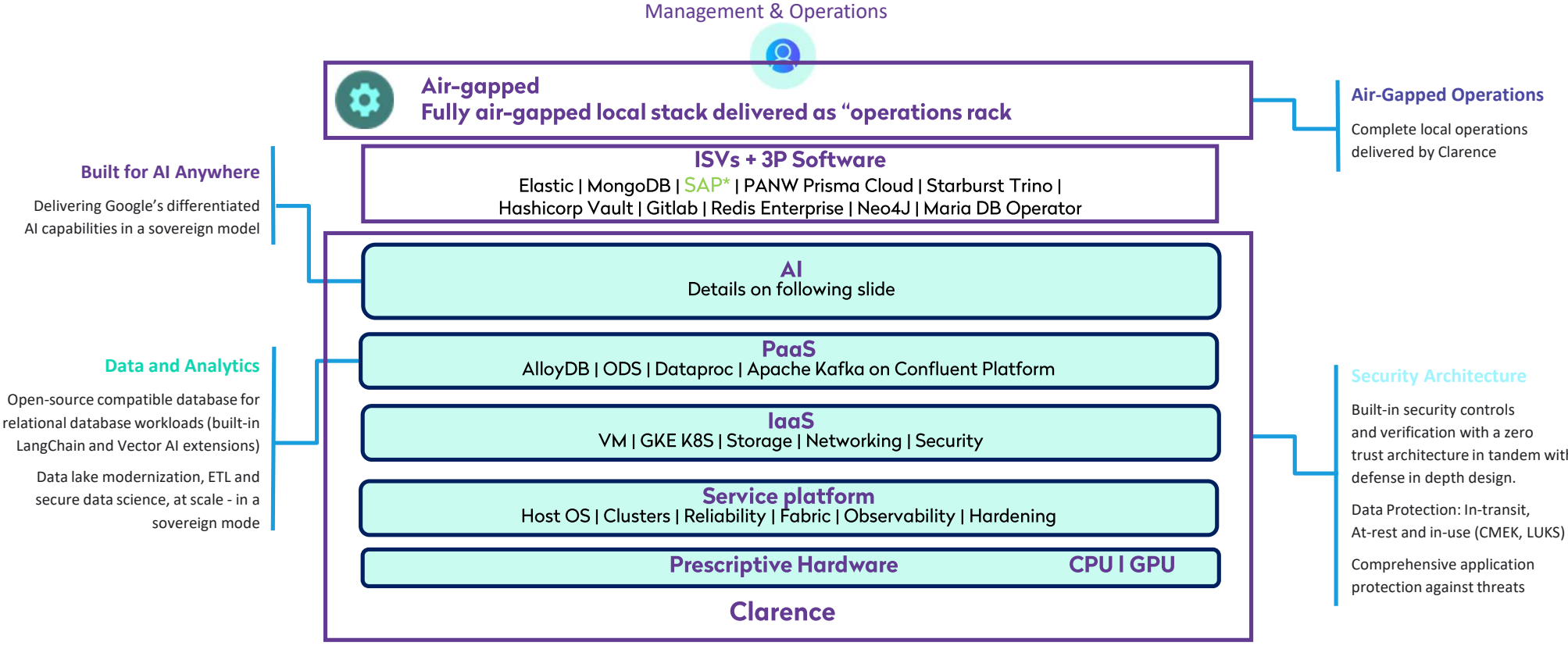
Host OS

Prescriptive Hardware CPU | GPU | SSD

Your on-premise cloud
Build once,
Run anywhere
With Google Distributed Cloud air-gapped

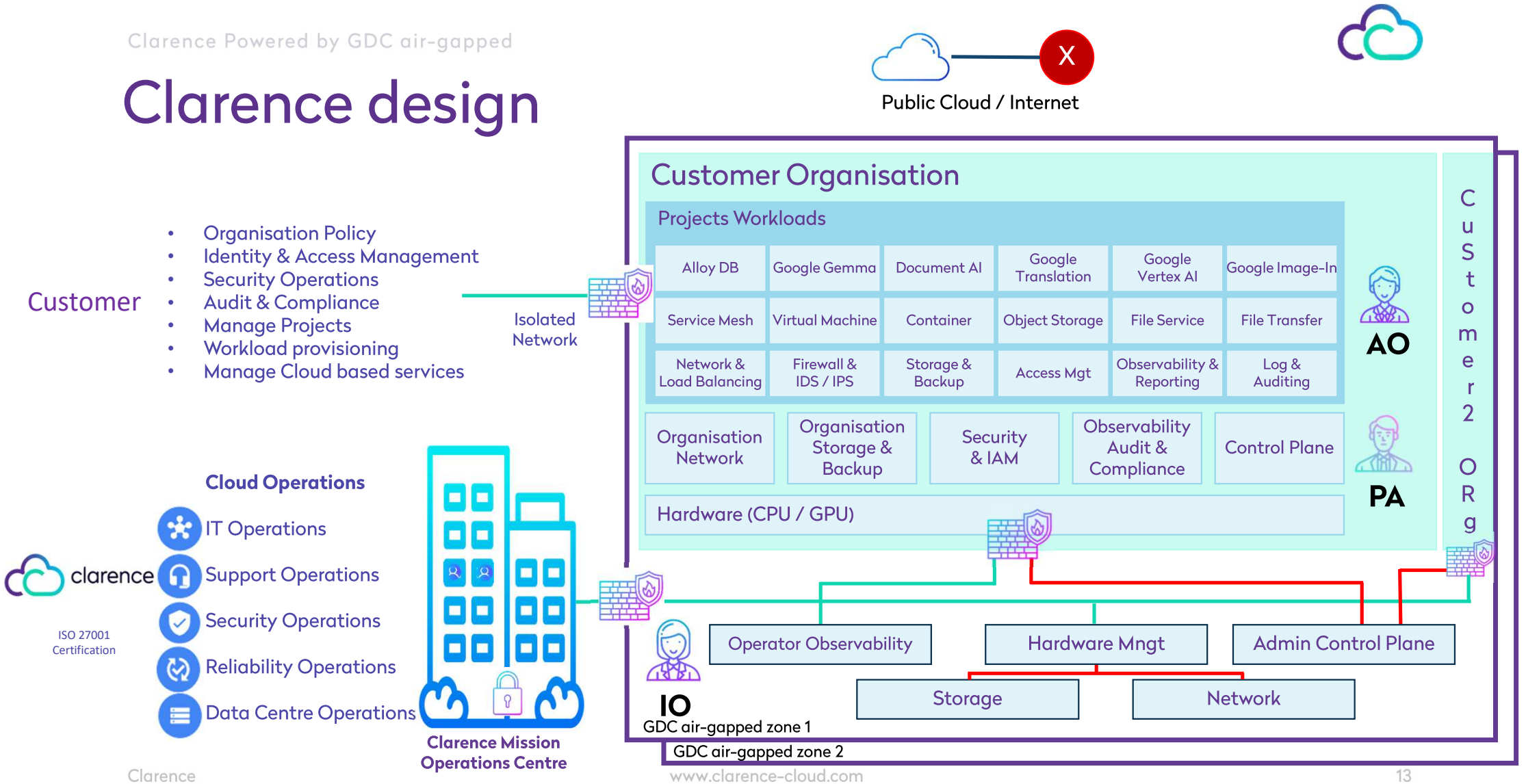
Clarence Air-Gapped configuration*

Fully air-gapped local stack delivered as "operations rack"



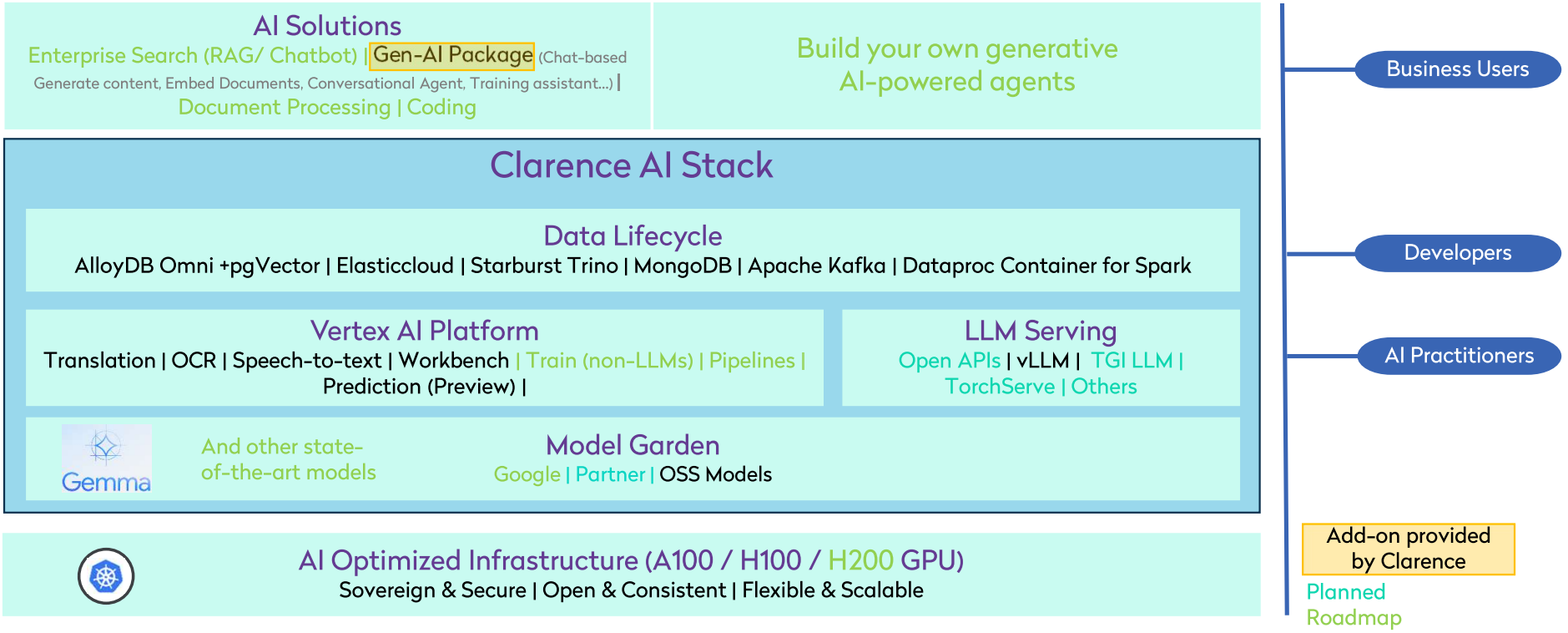
** Available services depend on Clarence stack version and may require customer's deployment of related solutions.*

Clarence design



AI on Clarence*

Bringing a unified, open, and secure infrastructure for Data and AI workloads where you need it

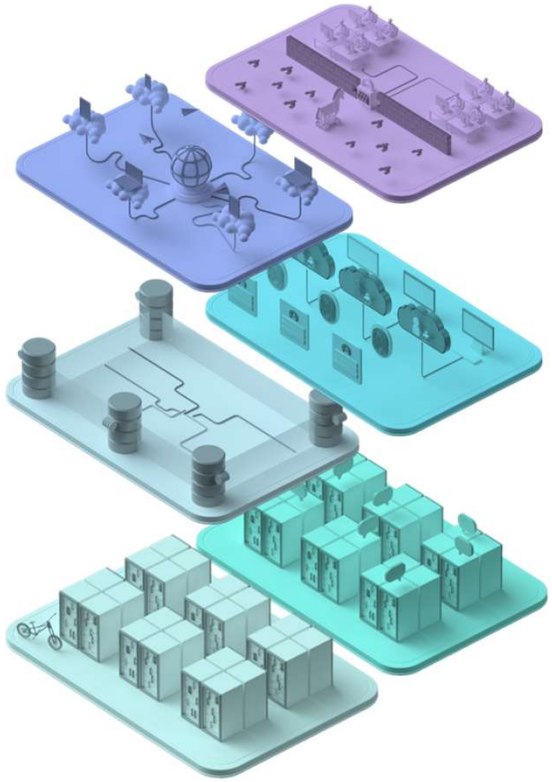


** Available services depend on Clarence Stack version and may require customer's deployment of related solutions.*

Clarence: Zero Trust Strategy

4

Strong Security by Design



Security as a Service
IPS / KMS / more…

Compliance

Security Operations

Reliability Operations

Cryptography
PKI / KMS / Encryption

IAM

Host/Node Security
Data At-Rest

Application Security
Data In-Use

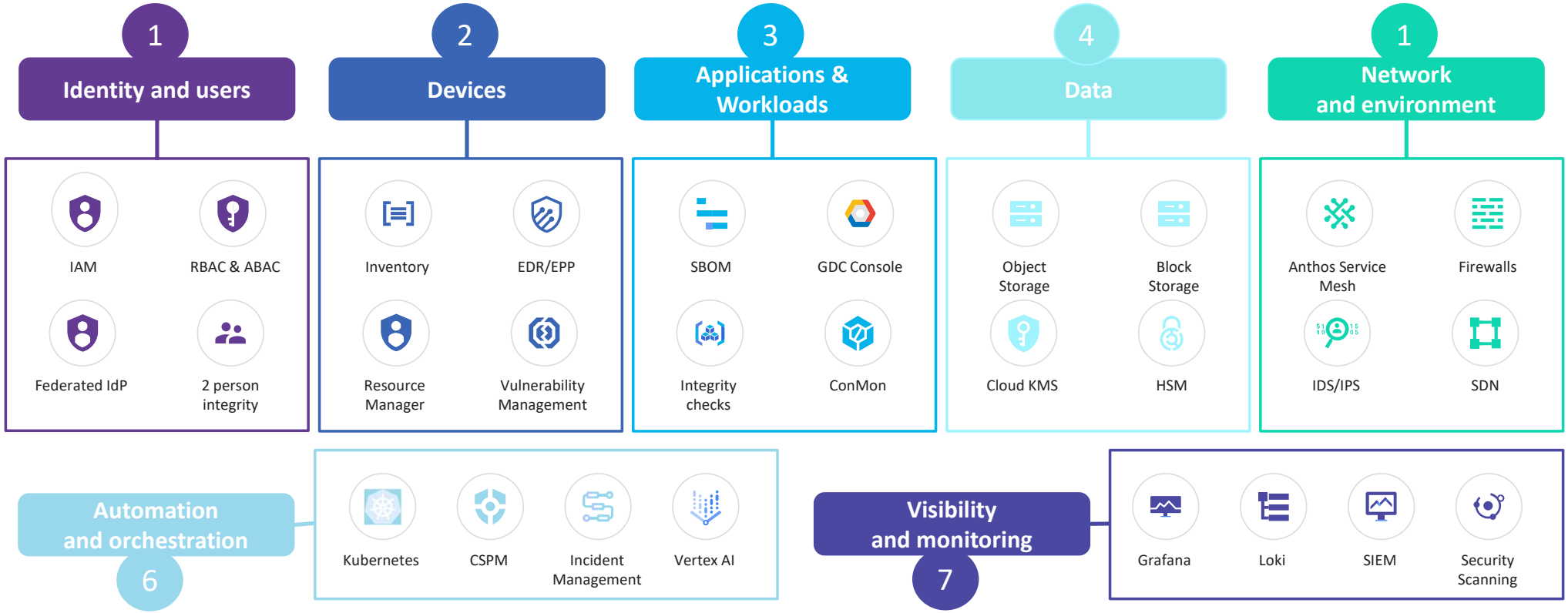
Network Security
Data In-Transit

Hardware Security

Facility Security

Native Zero Trust Architecture

Innovations Meets Sovereignty. Secure Cloud for Sensitive Workloads. Thanks to Google Technology, Clarence aligns to the core components of Zero Trust and National Security Memorandum 8 (NSM-8)



GDC air-gapped Supportable Regulatory Standards

- Digital Operational Resilience Act
- Network & Information Systems Directive 2
- SOC II
- FedRAMP High
  FedRAMP+ IL6
- ISO 27001
- AICPA SOC
- SecNumCloud
- BSI C5:2020
- ISO 27017
- Cyber Essentials
- ANSSI- ii901
- NIST Risk Management Framework
- NIST 800-53
- VS-NfD

clarence

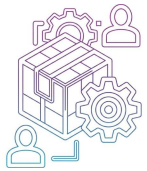
How Clarence Automates NIS2 Obligations

5

Achieving NIS2 Compliance via Clarence

Risk Management & Governance

- **Total Sovereignty:** Clarence gives you full control over the hardware and software stack. There is no link to the hyperscaler, satisfying request of digital sovereignty & risk mitigation.
- **Zero Trust Architecture:** Clarence uses a built-in Zero Trust model This addresses NIS2's push for "state-of-the-art" security controls.
- **Physical Isolation:** By being physically disconnected from the internet, you mitigate nearly all external network-based risks, which is the gold standard for "Essential Entities".



Supply Chain Security

- **Hardware Root of Trust:** It is achieved through hardened UEFI Secure Boot, local physical HSMs, and a verified supply chain.
- **Curated Marketplace:** You use a localized, Clarence marketplace. This ensures that any third-party software you run has been pre-vetted and "containerized" for security.
- **Limited Vendor Access:** Since the vendor has no remote access, the "vendor risk" of the cloud provider itself is structurally eliminated.

Incident Handling & Business Continuity

- **Integrated Monitoring:** Clarence includes embedded security layers (like Elastic) that provide kernel-level visibility and AI-driven defense without an internet connection.
- **Local Logging and Audit:** All audit logs are stored locally and are tamper-evident. This allows for rapid forensic analysis.
- **Immutable Backups:** Clarence offers local backup and disaster recovery services.

Cryptography & Access Control

- **Encryption by Default:** Data is encrypted at rest and in transit within the Clarence environment using FIPS 140-2/3 validated modules.
- **Mandatory MFA:** Clarence enforces MFA for privileged users and uses "least privilege" IAM roles by default.
- **Hardware Security Modules (HSM):** Physical control over the keys used to encrypt your data, ensuring that **no third party** can decrypt it.

clarence

Thank You

Jean-François TERMINAUX – Proximus NXT Luxembourg
Partner Manager – Disconnected Sovereign Cloud
jean.francois.terminaux@proximus.lu