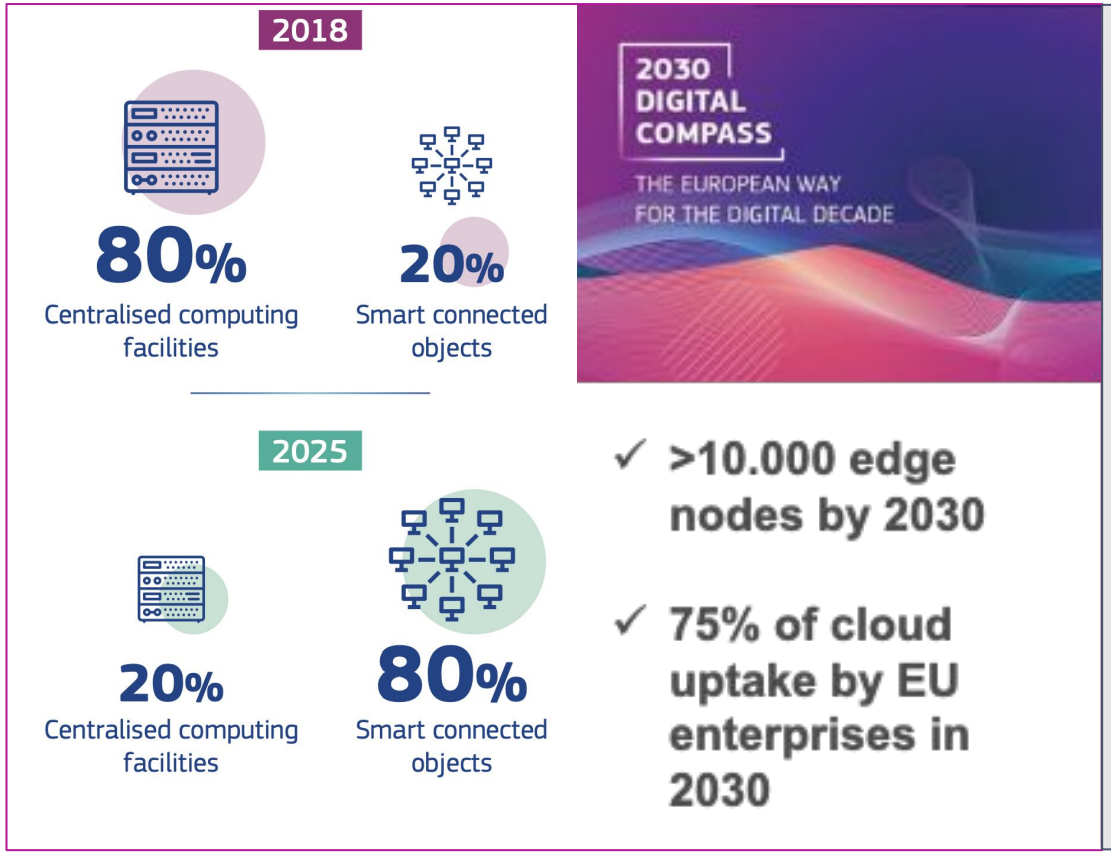
Cloud / Edge Security Challenges

Full Stack Confidential Computing

@jordiguijarro - OpenNebula Systems - 12 November 2024

Edge Computing Opportunities

Opening up **new opportunities** while **disrupting current business models**



Source: EU Data Strategy

✓ >10.000 edge nodes by 2030

✓ 75% of cloud uptake by EU enterprises in 2030

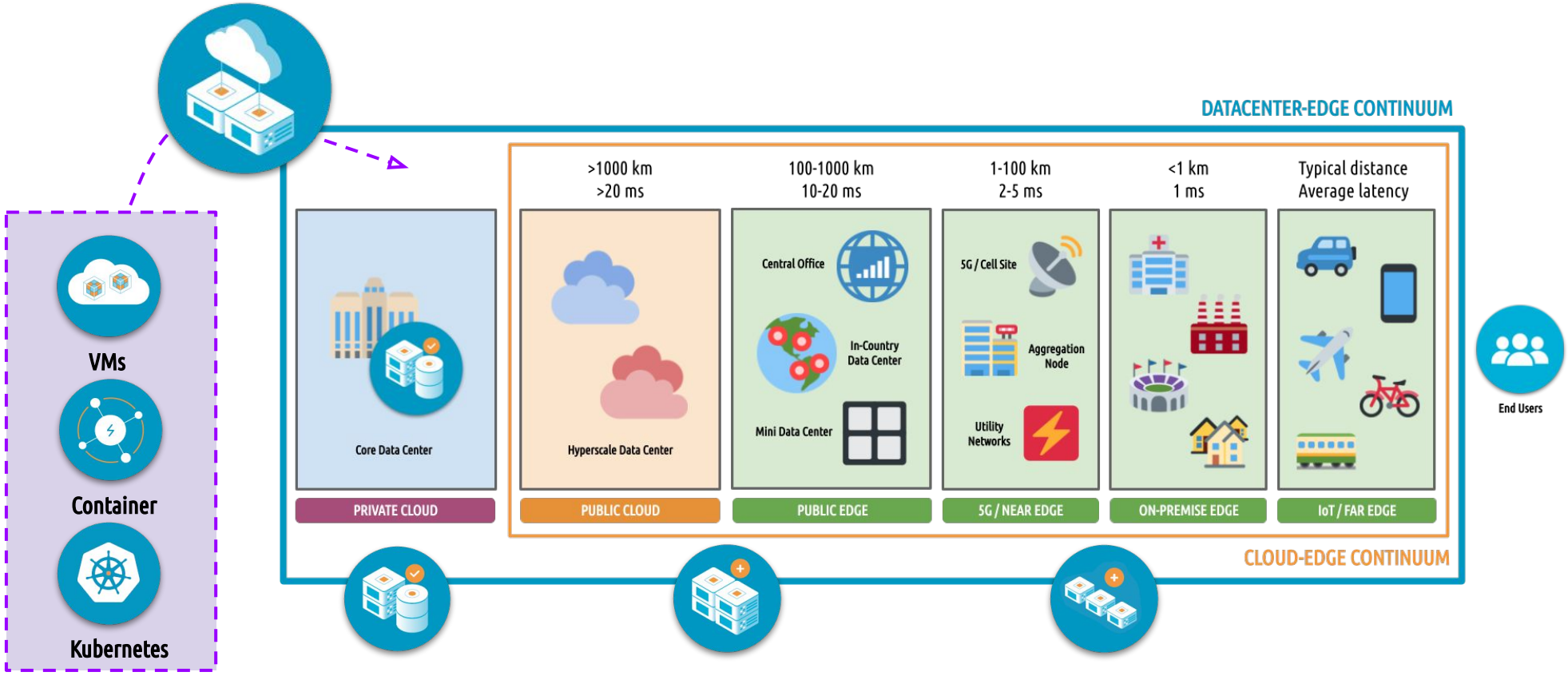
Source: EU Digital Compass

Europe's strengths in Industrial Internet of Things, 5G networks, and telco-cloud solutions

Source: EU Industrial Strategy

Cloud-Edge Computing Continuum

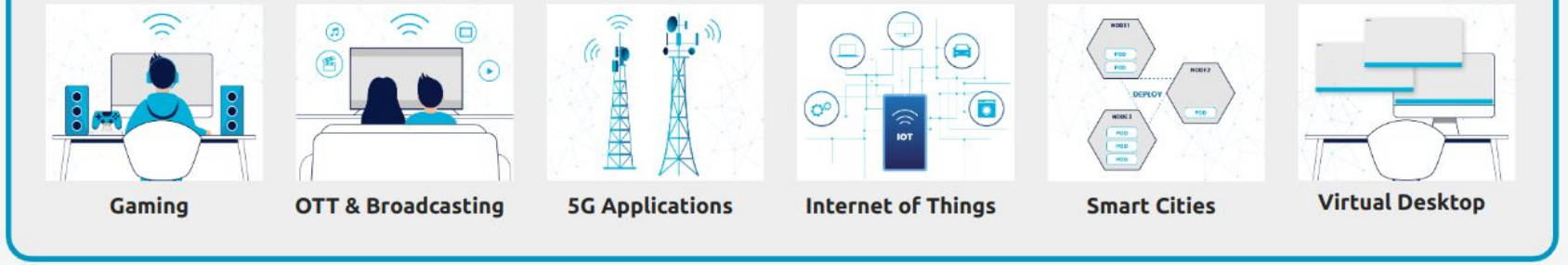
Opening up **new opportunities** while **disrupting current business models**



https://digital-strategy.ec.europa.eu/en/policies/edge-observatory

Cloud-Edge Computing Use Cases

Opening up **new opportunities** while **disrupting current business models**



- 🚀 Deploy (Ultra-) Low-Latency Applications
- 🚀 Improve User Experience
- 🚀 Expand Service Availability
- 🚀 Reduce Data Transfers and Security Risks
- 🚀 Reduce Energy Consumption
- 🚀 Minimize Vendor Dependency
- 🚀 Foster Ecosystem of New Infra Providers

Cloud-Edge Computing Continuum

Technological priorities

ECCO
European Cybersecurity COmmunity

STATE OF THE ART

Cloud-Edge Hybrid Architectures

- Mostly based on **proprietary**, **complex** technologies, leading to **vendor lock-in**.
- **Centralized cloud structures** that assume highly **homogeneous** datacenters.

Multi-provider Interoperability and Portability

- **Low adoption of standards**, with **abstraction layers** based on containers with **reduced security** (i.e. K8s).
- Storage and network model **not well suited for the highly distributed** cloud-edge continuum.
- **Partial use of automation techniques** (e.g. IaC) for infrastructure provisioning automation.
- **Lack of specific edge node architectures** able to meet the needs of HPC and 5G/telco environments.

Multicloud Management and Orchestration

- Lack of **AI used to optimize and automate** cloud/edge infrastructure management.
- Centralized control planes that **do not allow the federation** of cloud and edge infrastructures.
- Limited support for **optimized orchestration**, **energy efficiency,** and enforcement of **security policies**.

Use Cases

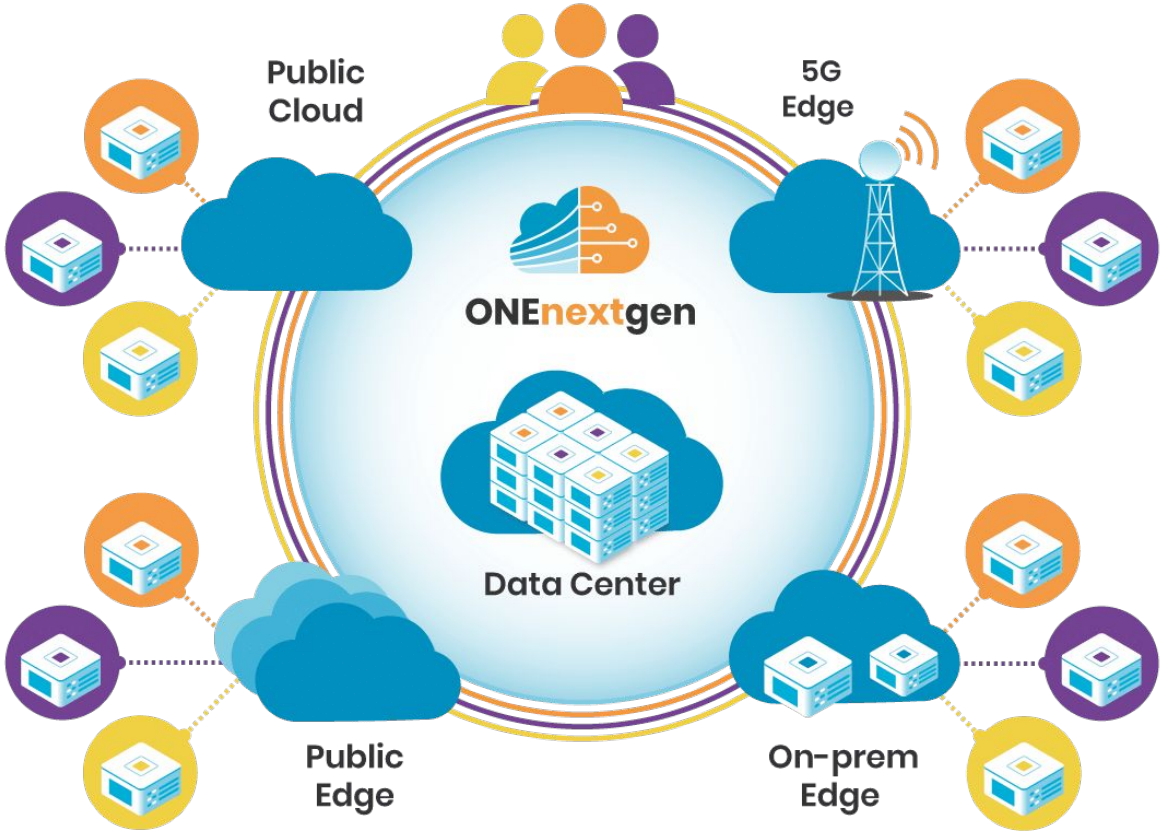
- Deployed as **static solutions** on a **case-by-case basis,** lacking automation, interoperability and portability.
- Creating **silos in strategic sectors** based on different technological stacks and ad hoc implementations.
- **Jeopardizes the consolidation of a cloud-edge continuum** and an associated industry ecosystem.

FUTURE CHALLENGES

- Increasing number of **edge providers** in the market.
- Emergence of **tens of thousands** of geographically distributed edge nodes.
- Need for complete **automation** of cloud edge operations.
- New **security threats** and larger impact of vulnerabilities.
- Preference for **energy-efficient** nodes.
- Tendency to platform **heterogeneity**.
- Infrastructure **dynamicity** and **volatile** devices.
- Dependency on **general-purpose**, **public** networks.
- Widely **distributed** environments.

OpenNebula

OpenNebula *Next Generation*



Funded by the European Union
NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

MAIN GEO-STRATEGIC CHALLENGES:

Coordination Failure

Lack of **coordination to deliver a suitable edge** computing offering

Concentrated Market Power

Market structure dominated by a few **non-EU providers**

Vendor **lock-in** practices

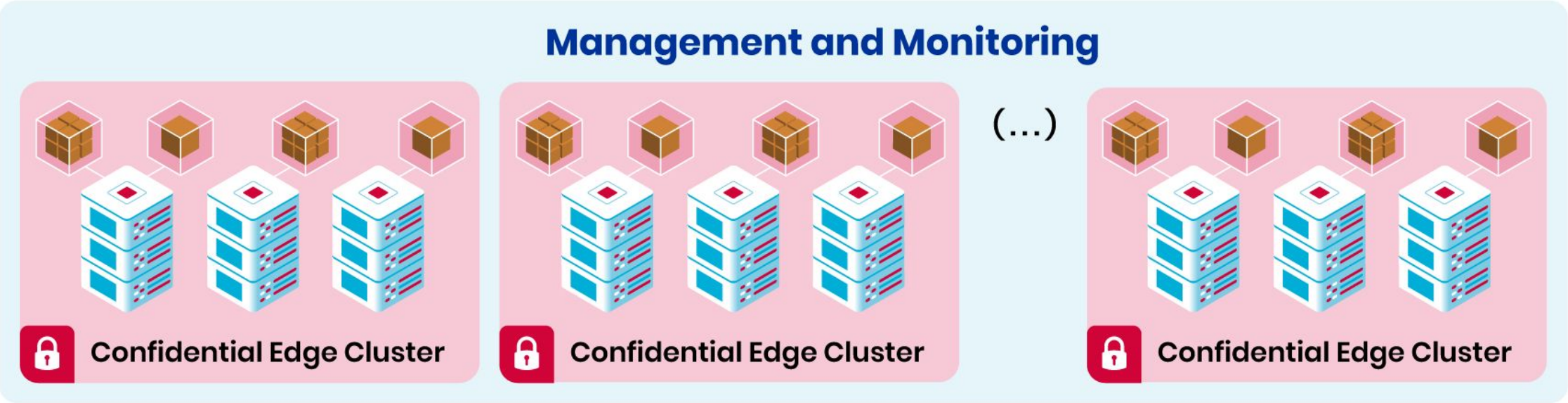
High barriers to entry for new cloud and edge providers

Negative Externality

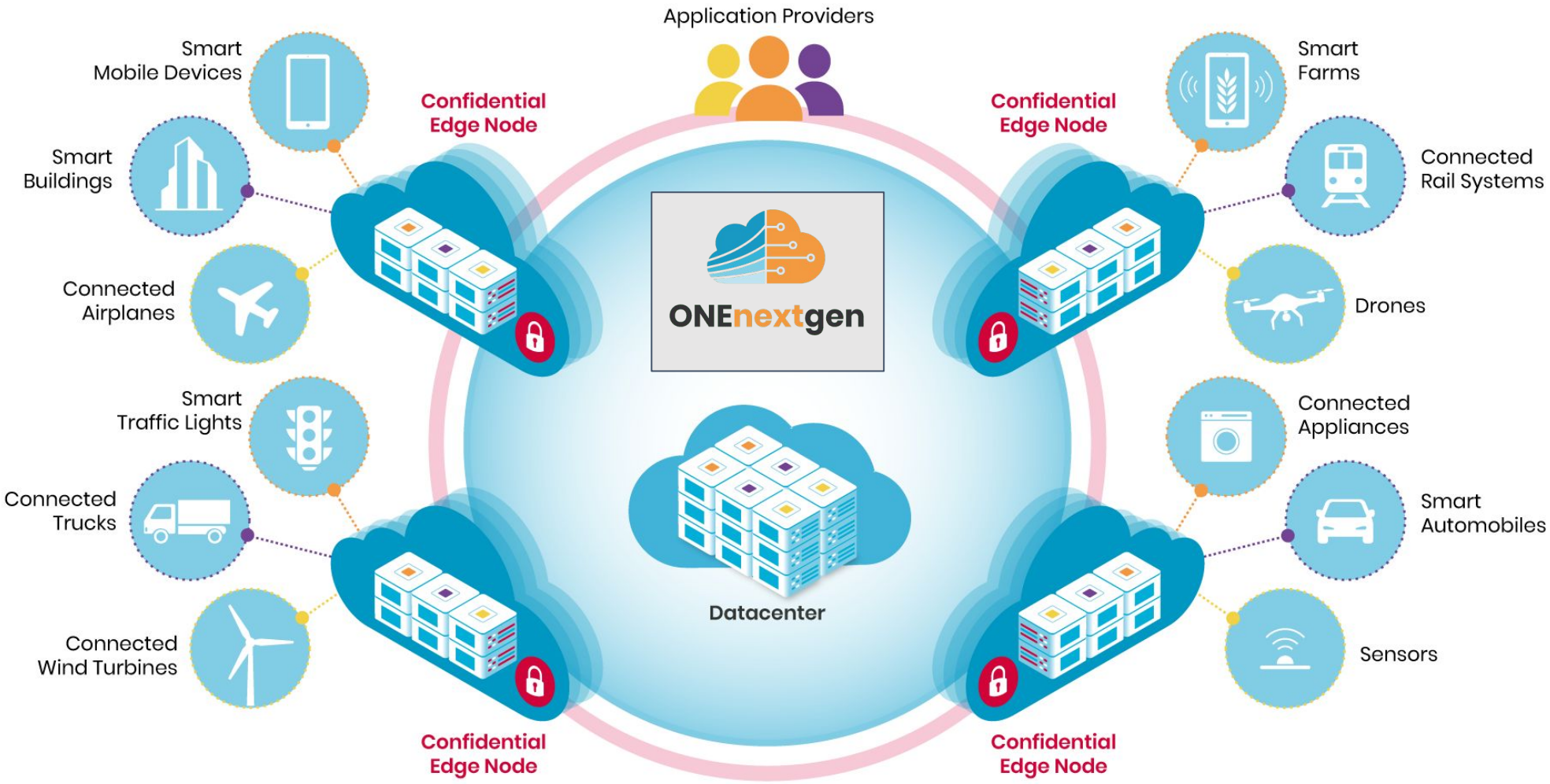
Excessive **energy consumption and pollution** from rapidly-expanding cloud infrastructure

OpenNebula.io/IPCEI-CIS

The Confidential Continuum Architecture will Adopt a Disaggregated Management Model



ONEnextgen Architecture Overview



Management Framework

- **Isolation**: Load a VM into the Continuum.
- **Measurement**: measure the entire image.
- **Secrecy**: accepting and storing.
- **Attestation**: Trust with other VM.

Confidential VMs

- Control of data in Public Clouds.
- Cryptographic isolation in Multi-Tenant environment.
- **All clouds will be confidential-clouds in 10 years.**

Expectations

- Orgs will have complete control.
- Framework that will enable end-to-end confidential computing on a highly-distributed continuum.
- Bring confidentiality to the entire data lifecycle.
- Enabling a multi-provider, vendor neutral cloud-edge confidential computing.

ONEnextgen

IPCEI-CIS

Next-Generation European Platform for the Datacenter-Cloud-Edge Continuum

Initiative supported by the Spanish *Ministerio para la Transformación Digital y de la Función Pública* through the **ONEnextgen Project: Next-Generation European Platform for the Datacenter-Cloud-Edge Continuum** (UNICO IPCEI-2023-003) and co-funded by the European Union's NextGenerationEU instrument through the Recovery and Resilience Facility (RRF).

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

UNICO IPCEI

OpenNebula.io/IPCEI-CIS

Full Stack Confidential Computing

Jörg Rödel - Confidential Computing Architect @ SUSE

What is Confidential Computing?

What is Confidential Computing?

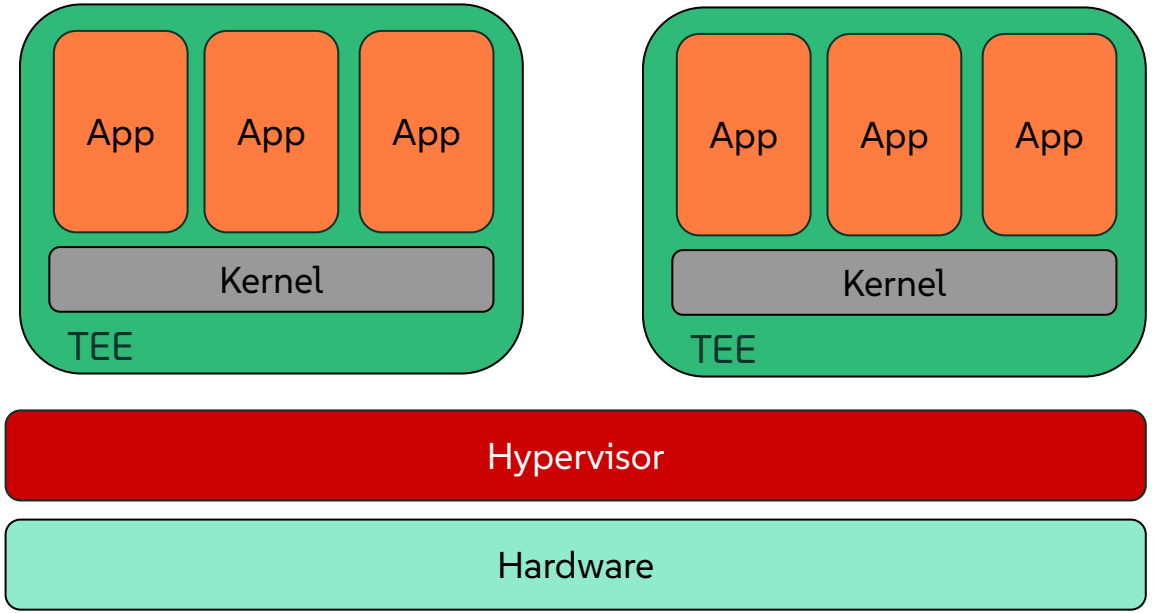
Confidential Computing is the protection of data in use by performing computation in a hardware-based, attested Trusted Execution Environment.

What is Confidential Computing?

Confidential Computing is the protection of data in use by performing computation in a **hardware-based**, attested Trusted Execution Environment.

Hardware-Based Trusted Execution Environments

AMD SEV-SNP - Intel TDX - Arm CCA - IBM System Z Secure Execution - Risc-V CoVE



Hardware-Based Trusted Execution Environments

AMD SEV-SNP - Intel TDX - Arm CCA - IBM System Z Secure Execution - Risc-V CoVE

Memory Encryption ✅

Memory Safety ✅

Register Encryption ✅

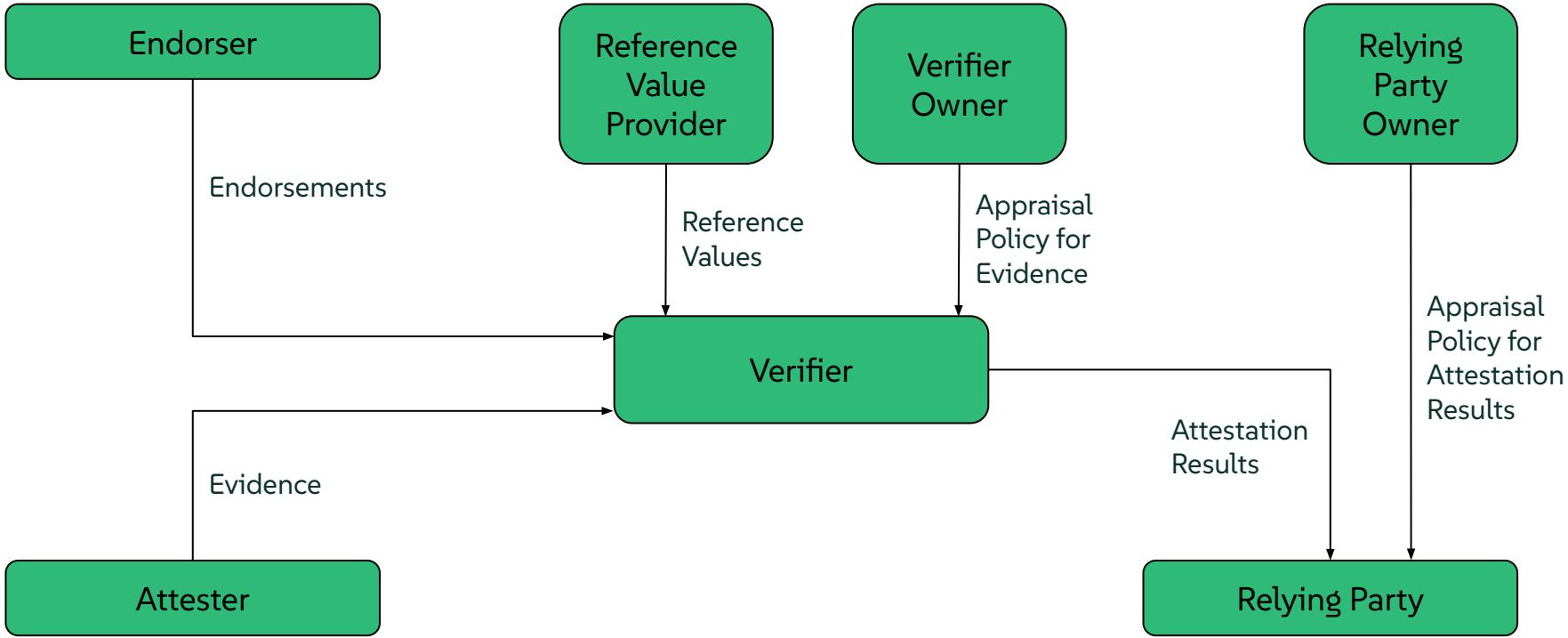
What is Confidential Computing?

Confidential Computing is the protection of data in use by performing computation in a hardware-based, **attested** Trusted Execution Environment.

Remote Attestation

Remote attestation is a process that allows a remote party (verifier) to gain confidence that a TEE is running in a secure and trusted environment, with its integrity intact.

RATS Architecture (IETF RFC 9334)



Confidential Computing Use-Cases

Confidential Computing in the Cloud

- Data is encrypted at rest, in transit, and in use.
- Protects against insider threats and unauthorized access.
- Retains data ownership in untrusted environments
- Enables secure collaboration on sensitive data.
- Maintains data confidentiality in multi-tenant environments.

Confidential Computing for the Edge

- Executing edge workloads in TEEs makes code and data integrity verifiable.
- Protects against unauthorized access and tampering.
- Ensures data confidentiality in shared edge environments.
- Maintains integrity of critical functions and applications.

Confidential Computing for AI

- Protects sensitive training data (e.g. personally identifiable information (PII))
- Secures valuable AI models (e.g. intellectual property)
- Safeguards the model training process from external interference and manipulation.
- Prevents unauthorized access to the model's internal workings.
- Protects against model inversion attacks.
- Helps meet compliance requirements.

Confidential Computing for Secure Multi-Party Computation

- TEE derives results from multiple data sets.
- Data set confidentiality guaranteed by Confidential Computing.
- Enables secure collaboration on sensitive data.
- Each party remains owner of its data.
- Attestation is critical!

Confidential Computing Challenges

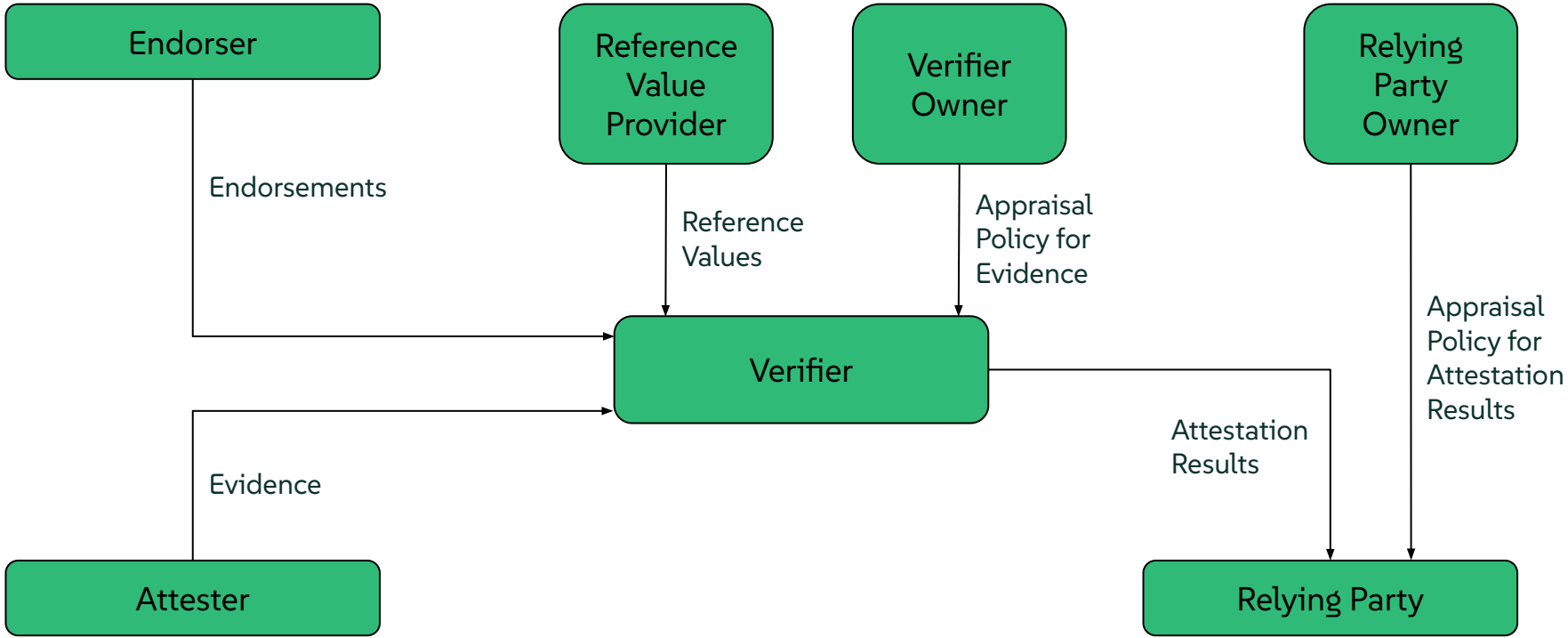
Open Source Hardware Enablement

- Linux virtualisation stack slow in adopting hardware-based TEE features.
- AMD SEV-SNP is supported now with kernel 6.11.
- Intel TDX and Arm CCA host environments remain unsupported
- Problem for on-prem confidential computing providers with an upstream-first policy

Full-VM Remote Attestation

- Running full Linux OS in TEE makes a big TCB.
- Every executable, library, and configuration file needs verification.
- Big data set for evidence.
- How to gather reference values?
- With regular updates it can get very complex.

Full-VM Remote Attestation



Full-VM Remote Attestation

- No widely used standards yet for:
  - Providing reference values
  - Appraisal and attestation result policies
  - Verifier implementations
  - Key broker services


SUSE

ECCO
European Cybersecurity COmmunity

Addressing challenges in Cloud Security Certification: COBALT & EMERALD

Cloud / Edge Security Challenges, Webinar

12th of November 2024

Jesus Luna (Bosch) / Juncal Alonso (TECNALIA)

Challenges in Cloud Security Certification

Complex IT ecosystems, infrastructure (virtual & heterogeneous) , application code (data, AI, MMLs) , business processes.

The upcoming demand for automated certification is not yet finally addressed and it remains unclear how the **"continuous assessment concept"** will be realized by stakeholders

Some solutions are available at technology level, but **interoperability, complete support** of the underlying certification processes, and **practical experiences** are still **missing**.

Cybersecurity is *per se* **"highly-regulated"** in the EU, and this is getting more and more intense within the standardization and legislation landscape (EUCS, AI Act, CRA, NIS2, …).

https://cybersecuritycertcluster.eu/

European Cluster for Cybersecurity Certification:

COBALT, EMERALD, CUSTODES, **CERTIFAI,** SYNAPSE

EMERALD: Evidence Management for Continuous Certification as a Service in the Cloud

The overall objective of EMERALD is to pave the road towards **Certification-as-a-Service (CaaS)** for continuous certification of harmonized cybersecurity schemes, like the European Cybersecurity Certification Scheme for Cloud Services (EUCS).

Cybersecurity **Evidence management at different levels** (resources, application, processes)

Lean re-certification / **multi-certification** (optimized cybersec metrics – compliance to multiple controls)

Audit suite covering the needs of the different stakeholders of the ecosystem

This project has received funding from the European Union's Horizon Europe programme under grant agreement No 101120688

Addressing the challenges in cloud security certification with EMERALD

Next-generation evidence gathering tools based on a knowledge graph approach

- Knowledge extraction on various layers of the cloud service (infrastructure, code, business processes) and prepare suitable evidence based on them.
- A graph-based structure to consolidate all necessary information of the service and to make it easily query-able, linking heterogeneous information extracted from different evidence sources.

Reduce complexity in multi-scheme Cloud certifications by assisted metric mapping

- An intelligent system to select an optimized set of metrics that can be measured to demonstrate compliance to the selected certification scheme.
- A tool to assess chosen metrics based on information stored in the certification graph and to evaluate the final certificate decision.
- A proof of concept (PoC) on how to scale the CaaS approach to cloud-based AI systems.

Addressing the challenges in cloud security certification with EMERALD

Seamless user experience of continuos auditing for auditors and auditees

- User interaction concept and conducted studies to show what information each user needs in an audit process

Increased interoperability between frameworks, security assessment tools and repositories

- Interoperability layer among the trustworthy systems, assessment results and catalogue data. Standardized formats such as OSCAL (Open Security Controls Assessment Language) will be used to mitigate the impact of changes in the security schemes.

Experimentation in diverse use cases

- Category I: Certification of public Cloud Services (IaaS, PaaS, SaaS)
- Category II: Certification of hybrid cloud-edge environments for the financial sector

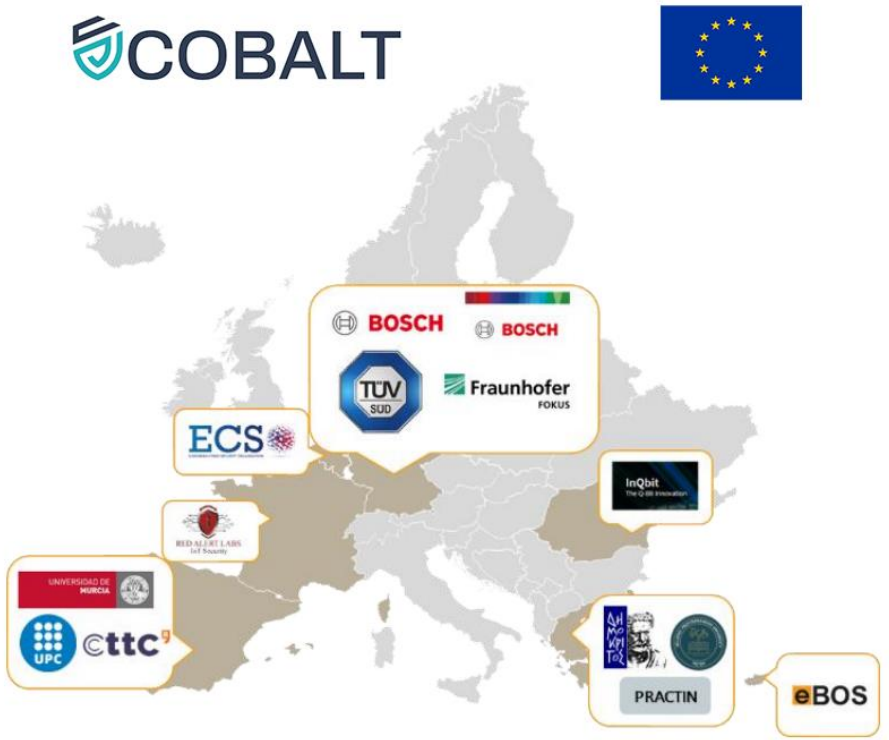
EMERALD will **enhance the user experience of continuous auditing** for auditors and auditees through a **CaaS process**, supported by user-tailored tools for complexity reduction in **multi-scheme cloud certifications,** including **next-generation evidence gathering tools** based on a **knowledge graph approach** and **assisted metric mapping tools**.

Scan me!

www.emerald-he.eu

EU-funded COBALT Project (2023-2026)
Certification for Cybersecurity in EU ICT using Decentralized Digital Twinning

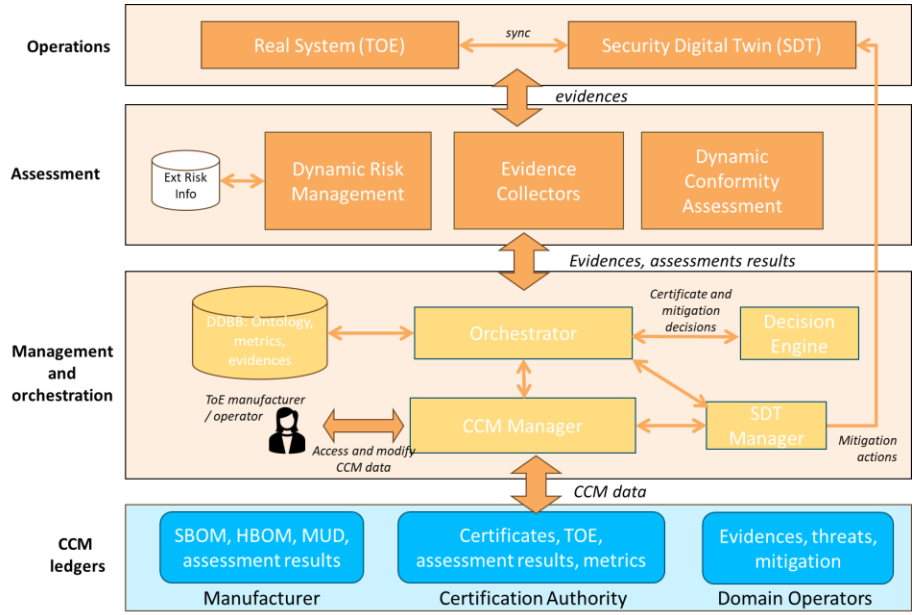
- COBALT aims to contribute an innovative framework for supporting cyber security certification with automation and digital twins.
- Main approaches:
  - Specification of compliance metrics.
  - Security Digital Twin.
  - Management of justified audit evidence.
  - Dynamic risk assessment.
  - Certificate's life-cycle management.
  - Standards and interoperability.
- Use cases:
  - Artificial Intelligence Systems (AI Act).
  - Quantum Computing.



See https://horizon-cobalt.eu/

Addressing the challenges in cybersecurity certification with COBALT

- Expected results:
  - ✓ Framework for supporting cybersecurity certification of ICT processes and services.
  - ✓ Auditor's toolbox comprised of certification enablers (e.g., evidence collectors and compliance metrics) and dynamic risk assessment techniques.
  - ✓ Security Digital Twin (SDT) to model, analyze, and certify ICT processes and services.
  - ✓ Validation scenarios addressing specific certification challenges of HPC and AI.
  - ✓ Impact maximization measures including standardization, dissemination, and exploitation.
- Progress to date:
  - Reference architecture v1.0
  - Draft GenAI cybersecurity controls
  - Initial SDT tests
  - Contributions to ISO/IEC, ENISA, NIST OSCAL



Threat / Anomaly Monitoring

ECCO – European Cybersecurity Community
Pedro De Castro – Prowler – 12 November 2024

PROWLER

contact: pedro.dc@prowler.com

Contents

- Edge challenges
- Cloud challenges
- Detection
- Response
- How Prowler helps

Edge challenges

- Each environment (cloud and edge) has different levels and tools for security.
- Maintaining security in an environment with interdependencies and constantly moving data.
- Achieve efficient and agile detection in limited and diverse environments.
- Different providers have different attack vectors and possible vulnerabilities.

Cloud challenges

- What do I have?
- Where is my data?
- Is it secure?
- What 3rd parties have access to to our information and cloud resources?
- What do I have to do/change immediately? And tomorrow? And in a week? In 3 months?
- Are we being attacked right now?

Detection

Continuous monitoring

1. Run on demand and scheduled scans
2. Deploy security at first
3. Visualize and report new findings

Configuration assessment

1. Checks database always updated
2. Checks customization
3. Easy to deploy new checks on-demand

Compliance

1. Compliance regulations are a safe-guard. Check your compliance status.

Response

Evaluate the risk

1. Reduce the noise. Evaluate real severity.

Remediation

2. Consider to remediate the findings at runtime.
3. Consider to remediate the miss configuration in your IaC stack (Terraform, CloudFormation..).

How Prowler helps

Community Adoption and Tracktion

STARS

10k+ stars with 1k m/m for last three months

WATCHERS

128 watchers on GitHub

DOWNLOADS

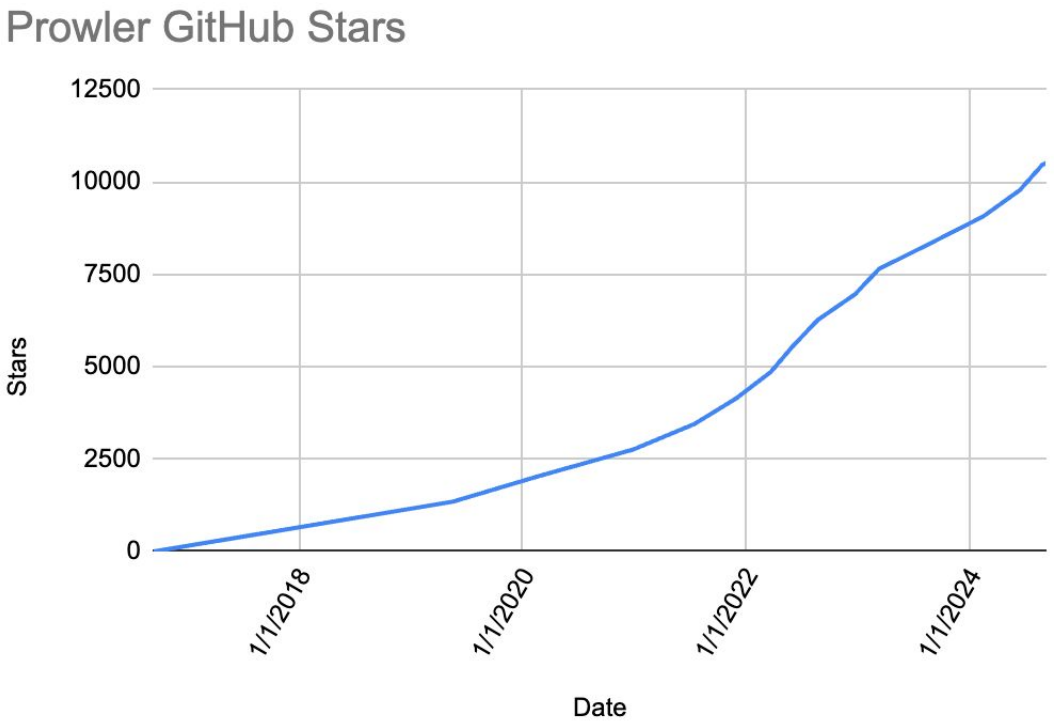
10M+ downloads -- 3M in the last 4 months

FORKS

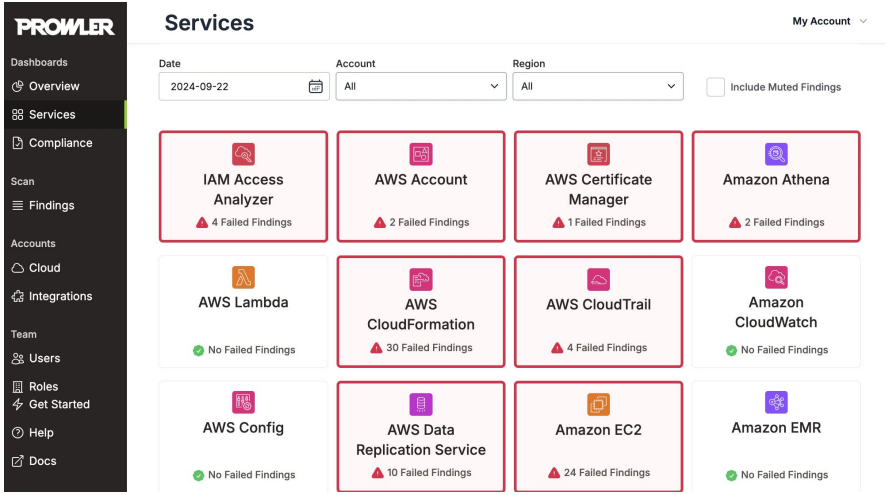
1.5k Forks to date

AND MORE

Sustainable, community-driven growth



- **Open Source:** Unparalleled transparency and customization in detection & remediation engineering
- **Community-Driven:** enabling seamless collaboration with a vast community of experts.
- **Not a Black Box:** with the majority of checks available out of the box, you gain immediate, actionable insights.
- **Multi-Provider:** No vendor lock-in. Same tool for different providers.
- **Developer Friendly:** Prowler provides developers with Open SDKs to tailor security checks, remediations, and alerts.
- **Compliance:** 39 available compliance frameworks.



Thank you

for attending