The Future of the Cloud is Local, Sovereign, and High-Performance

Strategic Update 2026

6WIND

Cloud Networking for AI

www.6wind.com

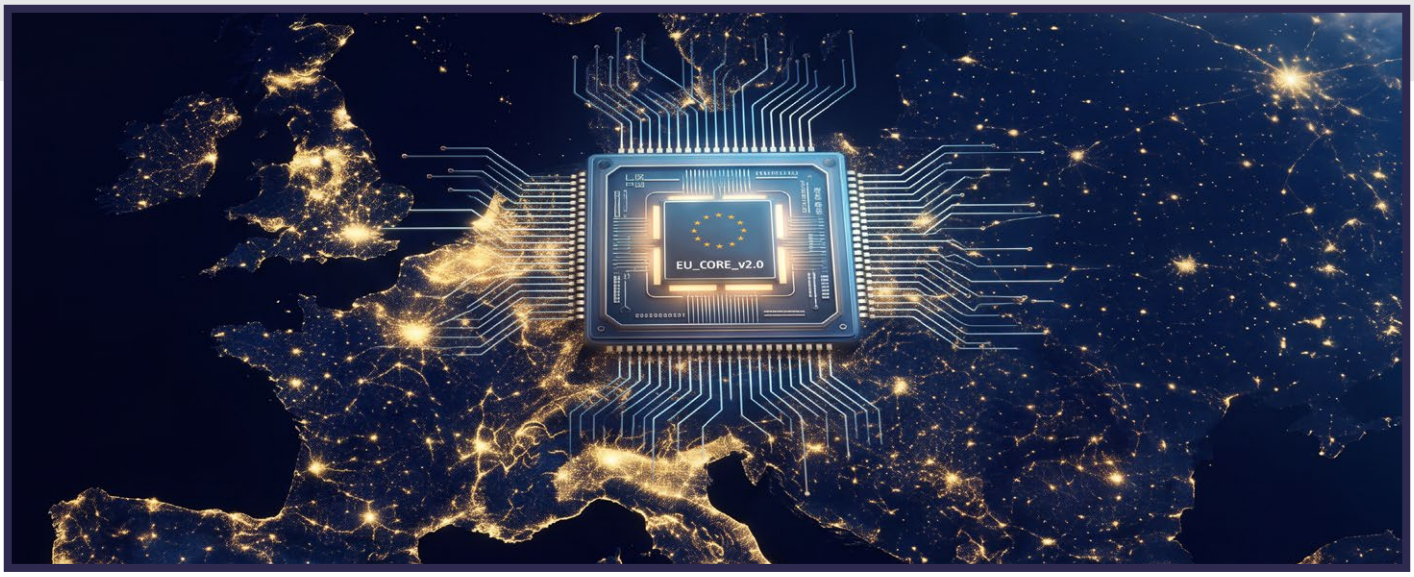

Table of Content

Notices & Disclaimers: Performance benchmarks vary by configuration and other factors. Performance results are based on the testing environment described in the testbed description section.

Market Context
The “AI Cloud” Wake-up Call

As of 2026, the global cloud market continues to experience strong annual growth, driven by AI adoption, enterprise modernization, and rising demand for scalable digital infrastructure. But the cloud market is no longer simply “growing”, it is transforming.

Across regions, buying criteria are shifting beyond price and service breadth toward trust, jurisdictional control, resilience, and secure data processing. This structural shift is most visible in the European Union, where sovereignty has moved from a niche concern to a mainstream enterprise requirement, and especially in Germany, Europe’s largest economy and one of its most strategic cloud markets.

The real momentum now lies in the Sovereign Cloud segment, projected to grow at approximately 26% annually, significantly outpacing traditional public cloud adoption. In parallel, the broader German cloud market is expected to expand from USD 65 billion in 2026 to more than USD 131 billion by 2031, underlining both scale and urgency.

By 2028, an estimated 60% of sensitive cloud workloads in Germany are expected to run in encrypted runtime or confidential computing environments, making sovereignty and runtime protection standard market expectations rather than specialist requirements.

The demand for sovereign solutions in Germany and in the EU has shifted from a “nice-to-have” for the paranoid to a legal mandate for the masses. According to the research Navigating Digital Resilience, nearly all enterprises (98%) say digital sovereignty is a priority, yet only 52% are taking action.

However transitioning to a sovereign model isn’t as simple as flipping a switch, it presents a “Real Challenge” because of:

- The Feature Gap: Many regional providers have historically struggled to match the breadth of services, automation maturity, and developer ecosystems offered by global hyperscalers;
- The Sovereign Premium: Dedicated infrastructure, compliance controls, and specialized European operations can create costs 15–25% higher than standard hyperscale regions;
- Integration Complexity: Splitting workloads and AI across sovereign zones can significantly increase architecture and integration costs as enterprises navigate secure data “airlocks” between global and local environments.

For regional Carriers, MSPs, and cloud operators, the window for relevance is narrowing. To capture the European Enterprise opportunity, the market must evolve from defensive compliance positioning toward offensive innovation through cloud platforms that combine global-class performance with local trust, regulatory certainty, and European value creation.

Our Proposal for Europe

The Digital Sovereignty & Confidential Compute Blueprint

A "European Stack" built on the **Sovereign Cloud and Confidential Computing Principles** is our powerful response to these challenges, serving as a **global seal of trust**. While global hyperscalers focus on "scale at cost," the European Stack prioritizes sovereignty and confidentiality.

A **European Stack** doesn't just offer a place to store data; it offers a standardized blueprint that ensures:

- **Regulatory "Invulnerability":** Since the full implementation of NIS2 and the EU Data Act, sovereignty is no longer a "nice-to-have"! It is a matter of legal survival.
- **Interoperability & Open Standards:** The stack eliminates "vendor lock-in" by utilizing standardized, Kubernetes based open blueprints. This ensures the European Community can seamlessly move AI and sensitive cloud workloads between local providers, maintaining full operational flexibility. Thanks to Kubernetes, every line of code in the Sovereign Cloud Stack is auditable. This creates a level of security that "Black Box" systems can never match.
- **A Practical Path for Economic Sovereignty:** From Unpredictable Licensing to a Transparent, Open Approach. Don't let shifting proprietary strategies dictate your IT budget. As legacy vendors introduce unpredictable pricing models and deepen vendor lock-in, the European Stack provides a transparent, fully open approach built on interoperable technologies that preserve your freedom of choice, eliminate dependency on any single vendor, and deliver long-term financial predictability.
- **Technological Parity and AI Readiness:** European Service Providers are now delivering the first sovereign AI and Telco Clouds, on track to reach feature parity with global hyperscalers by the end of 2026. AI Training models require access to highly sensitive data with Intellectual Property. The fear that this intellectual property will "leak" into global models is the biggest brake on innovation for the European Community.
- **Cultural Alignment:** It is precisely tailored to federal structures and the specific security needs of the European Market (e.g., multi-tenancy, local support chains).
- **The repeatable Blueprint Effect:** By defining a horizontal, automated infrastructure, this solution creates a repeatable model for digital independence. This "European Stack" serves as a Gaia-X-compliant blueprint that not only Germany but the European Community can adopt to build secure, high-performance sovereign AI-ready platforms.

The **European Stack** is the definitive strategic answer to 2026's digital dependencies.

By bringing together a validated ecosystem of **Supermicro, SUSE, Scontain**, and **6WIND**, this blueprint demonstrates how local proximity can match and exceed global performance for Cloud, AI, and Telco applications, while providing a practical path away from proprietary platforms toward greater economic sovereignty and freedom from vendor lock-in.

This secure-by-design environment ensures sensitive data remains technically inaccessible to providers, at rest, in transit, and during active processing. By shielding Intellectual Property via hardware-based Confidential Computing on a NIS2-compliant foundation, we turn defensive compliance into a high-performance market offensive.

The Fast-Track to Sovereignty

Stop reacting to unpredictable proprietary licensing and start your transition to a risk-free European alternative.

- **Sovereign Readiness Assessment:** Launch a 4-week evaluation of your current proprietary, closed legacy footprint.
- **The Goal:** Receive a detailed migration blueprint to execute your local Sovereign Confidential Compute leadership.

Supermicro & Scontain

Sovereign AI Infrastructure & Trust Layer

The fear of intellectual property leakage is currently the biggest brake on European innovation. While standard public clouds typically offer encryption “at rest” or “in transit”, our platform also guarantees security “in use”. By combining Supermicro’s hardware systems, featuring Intel® TDX and AMD SEV-SNP technology with Scontain’s “Confidential Enclaves,” your data remains encrypted even during processing. This ensures that your sensitive AI models and IP are technically inaccessible to everyone—including the cloud provider’s administrators.

Supermicro serves as the infrastructure enabler of the Sovereign Provider Platform, delivering a high-performance, secure, and energy-efficient hardware foundation for sovereign AI and cloud deployments. In close collaboration with SUSE, Scontain, and 6WIND, Supermicro provides an integrated Sovereign AI development platform tailored to the needs of European service providers, enterprises, and the public sector.

Supermicro’s scalable COTS server and GPU-accelerated systems form the physical backbone of the platform, optimized for AI training and inference as well as telco and cloud-native workloads. SUSE contributes an open, cloud-native software stack, including SUSE Rancher Prime and SUSE Virtualization, that enables flexible, vendor-neutral cloud operations. Scontain enhances the platform with confidential computing capabilities, leveraging hardware-based security features such as Intel TDX and AMD SEV-SNP to ensure that sensitive data remains protected during processing.

The collaboration with 6WIND adds high-performance, software-defined networking and security capabilities. Solutions such as the Virtual Service Router (VSR), Virtual Security Gateway, vHost Network Accelerator, and virtual Broadband Network Gateway enable scalable, automated, and secure connectivity for cloud and telco environments. These technologies provide carrier-grade networking performance, integrated IPsec encryption, and support for quantum-safe security, making the platform suitable for next-generation 5G, future 6G, and other services.

A key differentiator is Supermicro’s strong European footprint. With manufacturing, system integration, and logistics capabilities in Den Bosch, the Netherlands, Supermicro ensures local value creation, reduced delivery times, and enhanced supply chain resilience. This regional presence, combined with Supermicro’s vertically integrated supply chain, enables rapid deployment while maintaining independence from global supply uncertainties—an essential element of digital sovereignty in Europe.

Together, Supermicro, SUSE, Scontain, and 6WIND deliver a fully integrated, sovereign European solution that combines high-performance infrastructure, open, cloud-native software, confidential computing, and carrier-grade networking. This Sovereign AI development infrastructure empowers **organizations** to design, implement, and scale AI and telco applications while maintaining full control over data, infrastructure, and operations.

6WIND

High-Performance Networking & Quantum-Safe Security

French-based 6WIND delivers world-class software-defined network **performance**, now reinforced by **cutting-edge encryption** and **architectural isolation**.

By replacing hardware-heavy legacy systems with high-velocity software, 6WIND provides the agility required for the German AI-ready Cloud.

- **VSR (Virtual Service Router) – Performance & Multi-tenancy:** Manages North-South traffic with industry-leading throughput and provides essential VPC services, including NAT and policy controls. Its advanced **multi-tenancy** capabilities allow Managed Service Providers (MSPs) to securely host hundreds of independent customers on a single physical footprint without cross-talk or performance degradation.
- **vHNA (Host Network Accelerator) – Isolation & Micro-segmentation:** 6WIND vHNA transforms standard Kubernetes networking into a high-performance, enterprise-grade network platform. Fully integrated with Kubernetes, vHNA delivers advanced routing, multi-tenancy, **micro-segmentation**, and workload **isolation** through **declarative policies** and **end-to-end automation**. Its **hardware-agnostic** architecture enables consistent network and security controls across any infrastructure, while allowing each tenant, namespace, or application to operate in its own securely isolated environment.
- **Virtual BNG (vBNG) – Scalable Multi-tenancy:** Enables the delivery of broadband services through PPPoE/IPoE and LNS termination. Optimized for the Mittelstand, it allows carriers to scale subscriber management with high-density **multi-tenancy**, ensuring that every connection is treated as a secure, individual “tenant” lane.
- **Automation – Agile Performance:** These functions are fully automated via the Kubernetes VSR operator. This removes the “human bottleneck,” enabling agile, error-free provisioning of ISP services. Automation ensures that **performance** profiles and security policies are applied instantly and consistently across the entire cloud fabric.
- **Quantum-Ready Secure Integration – Future-Proof Security:** 6WIND offers quantum-safe IPsec VPNs. This technology secures data connections against “harvest now, decrypt later” threats posed by future quantum computers. It provides a level of **security** that exceeds current global hyperscaler standards, making the “European Stack” a global benchmark for long-term data integrity.

In response to unpredictable market pricing for proprietary solutions, this stack offers a transparent and powerful “VMware Exit” Network Stack.

SUSE

Cloud-Native Modernization

SUSE provides the operating system and management layer that orchestrates Supermicro's hardware, 6WIND's networking, and Scontain's encryption into a high-performance, sovereign solution.

As a company founded in Germany, **SUSE** bridges the gap between traditional IT and modern cloud-native environments. Its role is central to the management and modernization of the sovereign infrastructure.

Cloud-Native Software Stack & Orchestration

SUSE provides the open, cloud-native software foundation required for flexible and vendor-neutral cloud operations.

- **Centralized Management via SUSE Rancher Prime:** This platform enables control of multi-cluster environments, allowing providers to manage complex Kubernetes landscapes efficiently.
- **Interoperability:** By adhering to open standards, SUSE prevents "vendor lock-in". This enables the German Mittelstand (SMEs) to move workloads seamlessly between different local providers.

Bridging Virtualization and Containers (HCI)

SUSE offers a path to modernize legacy systems by unifying traditional and modern workloads.

- **Hyper Converged Infrastructure (HCI):** Through SUSE Virtualization, Managed Service Providers (MSPs) can manage virtual machines (VMs) and container workloads on a single, 100% open-source platform.
- **Cost Efficiency:** This approach reduces reliance on expensive, proprietary SAN or HCI hardware. This is crucial for taming the "Sovereign Premium"—the historically higher cost of local sovereign solutions.

Role in the "Sovereign AI" Ecosystem

In collaboration with partners like Supermicro and Scontain, SUSE contributes to an integrated Sovereign AI development platform.

- **Optimized Performance:** The stack is optimized for AI training, inference, and cloud-native workloads.
- **Auditability and Trust:** Since the Sovereign Cloud Stack is open-source, every line of code is auditable. This provides a level of security that proprietary "Black Box" systems cannot match.

A Strategic Open Approach

SUSE is a core component of a transparent alternative to proprietary solutions with unpredictable pricing.

- **Kubernetes-Native Operations:** Using Custom Resource Definitions (CRDs) and Operators, SUSE enables a single, GitOps-ready control plane.
- **European Sovereignty:** As a European vendor, SUSE ensures no dependence on US-based entities, thereby fulfilling strict legal and sovereignty requirements.

https://www.suse.com/navigating-digital-resilience-2026/

Scontain

Confidential Cloud-Native Applications

Scontain GmbH develops the **SCONE platform**, a production-ready solution for running secure and trustworthy applications in untrusted environments. SCONE enables organizations to transform existing cloud-native workloads into confidential applications with minimal changes, while enforcing strong, policy-driven security guarantees across the entire lifecycle—from build to deployment to runtime—without sacrificing performance or operational usability.

- **SCONE Platform:** The SCONE platform enforces a comprehensive, policy-based security model that protects data at rest, in transit, and in use, ensuring end-to-end confidentiality even during processing. It achieves strong isolation with high efficiency by leveraging node-level confidential virtual machines (CVMs) rather than spawning a CVM per pod, resulting in significantly improved cost-effectiveness and scalability. At the same time, SCONE provides excellent diagnosability, enabling operations teams to retain sufficient visibility for monitoring and debugging without compromising the confidentiality guarantees of applications.
- **SCONE-TD-BUILD:** SCONE-TD-BUILD transforms existing containerized applications into confidential workloads without requiring code changes, preserving full compatibility with standard Kubernetes applications, CI/CD pipelines, and deployment practices. It ensures that configurations and secrets are provisioned securely by releasing them only to workloads that successfully pass hardware-based attestation, thereby eliminating manual key management and solving the key bootstrap problem while maintaining a seamless developer experience.
- **SCONE CAS:** SCONE's Configuration and Attestation Service provides continuous trust assurance by transparently attesting and verifying applications and their dependent services at startup, ensuring that only approved, untampered components are executed. It also automatically checks the trusted execution environment for known vulnerabilities, preventing workloads from running on insecure platforms, and extends this verification capability to include application-level vulnerability checks, thereby strengthening protection across the entire software supply chain.
- **Provider Exclusion:** SCONE enforces a strong provider-exclusion model that protects application code and data at rest, in transit, and in use, even from privileged infrastructure operators, such as cloud providers. Through cryptographic isolation and attestation-based access control, SCONE ensures that no party managing the hypervisor, confidential virtual machines, Kubernetes cluster, or host and guest operating systems can access, modify, or exfiltrate application code, data, keys, or configurations in the clear, thereby enabling true zero-trust deployments and supporting strict data sovereignty requirements.

6WIND

Cloud Networking for AI

2026 The Future of the Cloud is Local, Sovereign, and High-Performance

www.6wind.com