



Control the Device, Protect the People

Sovereignty, Security and Compliance in Digital Policing

In brief: Omnissa and GEMA



- 10 years of experience operating private clouds.
- 11 million devices under management.
- Trusted by public sector and regulated industries for data sovereignty across jurisdictions.



- 26,000+ customers worldwide, including 7 of the top 10 Fortune 500.
- Over 1 billion USD in annual recurring revenue (ARR).
- 4,000 employees worldwide.

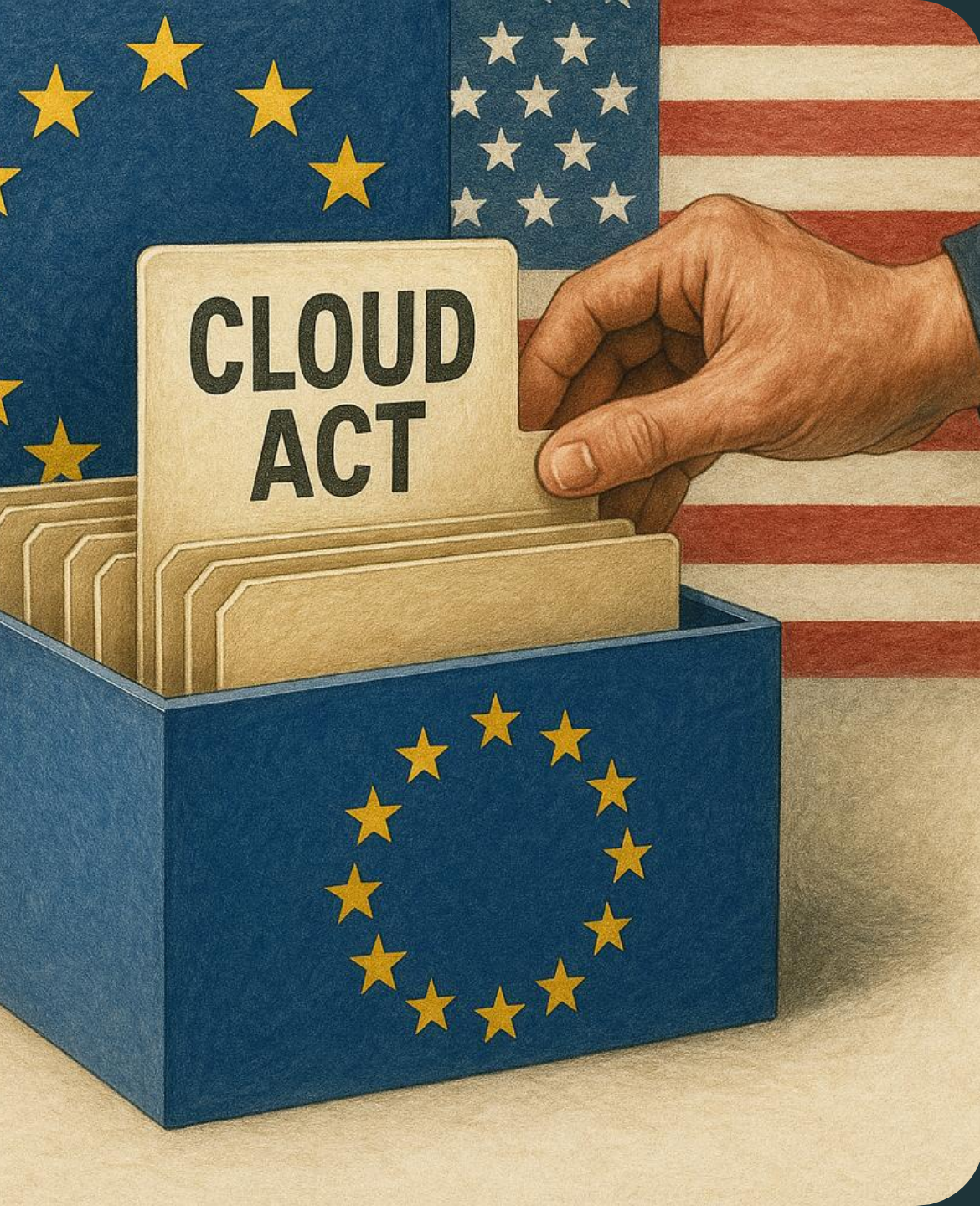


Why Sovereignty Matters

Endpoint Devices in Policing

- Rugged tablets & smartphones
- Handheld digital radios
- Body-worn cameras
- Mobile data terminals/ laptops
- Barcode scanners
- ID/passport readers
- ANPR cameras
- Drones with cameras
- RFID/NFC readers





The need for **sovereignty**

The US CLOUD Act (Clarifying Lawful Overseas Use of Data Act) and similar legislation pose a serious risk to digital sovereignty, enabling potential foreign access to sensitive data and even the shutdown of critical services.

Risk: Third-party access through dependencies

The New York Times

Europe's Growing Fear: How Trump Might Use U.S. Tech Dominance Against It

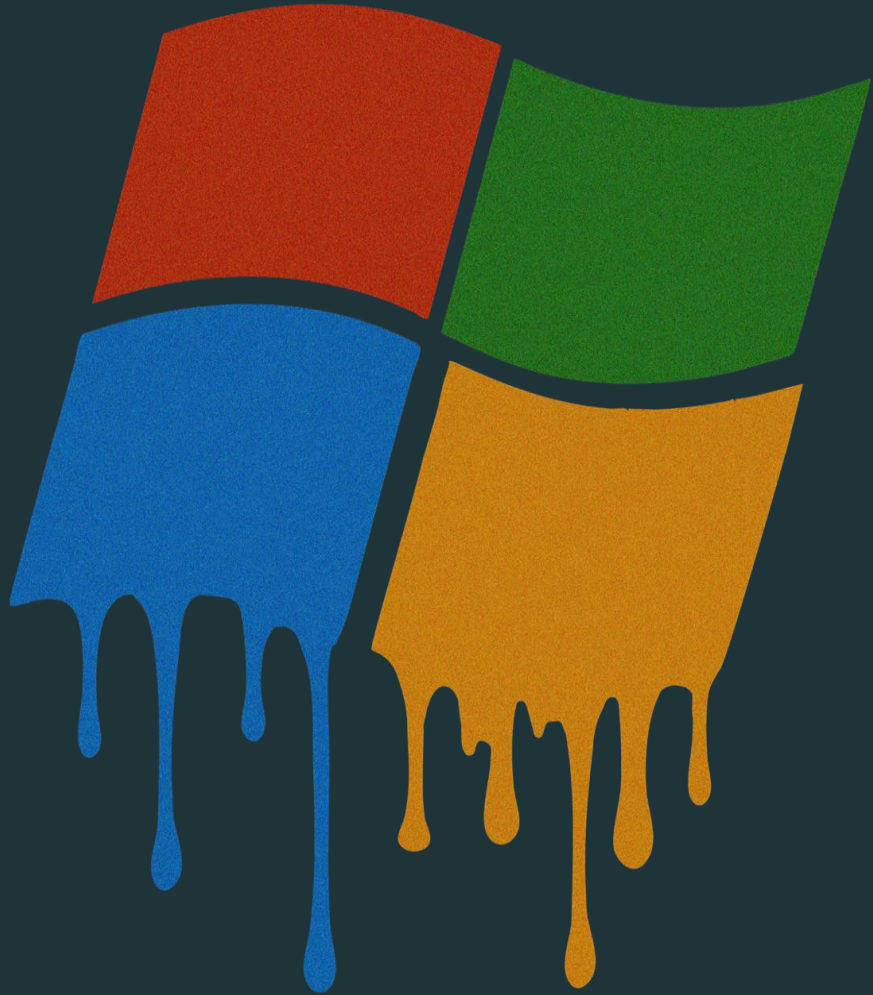
heise online

Criminal Court: Microsoft's email block a wake-up call for digital sovereignty

Forbes

Microsoft Can't Keep EU Data Safe From US Authorities

Sov-washing



During a hearing in front of the French Senate, the Chief Legal Officer of Microsoft France acknowledged that there is no assurance that EU data will not be disclosed to the U.S. government.

Requirements for Sovereign Solutions

Data Protection

- Protection of sensitive data
- Access controls
- Encryption
- Compliance

Goal: Protection against data emigration

Data Residency

- Control over data flows
- Processing in one's own jurisdiction
- Protection against extraterritorial access

Goal: Control over data and legal area

Operational Security

- Management within the specified jurisdiction
- Certified partners and employees
- Audit and Compliance
- Restrictions within value chain

Goal: Ensuring operational controllability

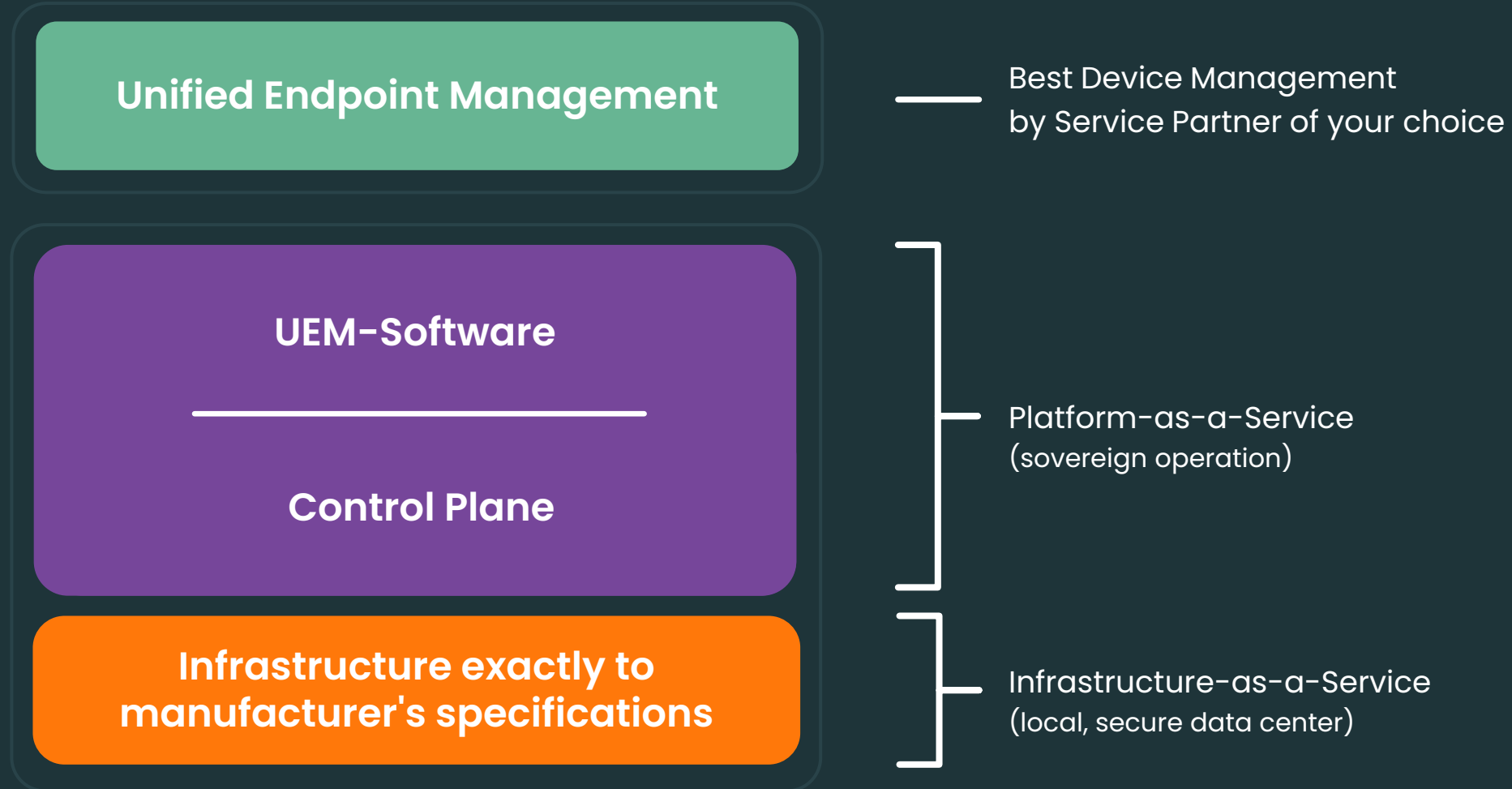
Support

- Strict user controls
- User certification
- Policy-based access and control

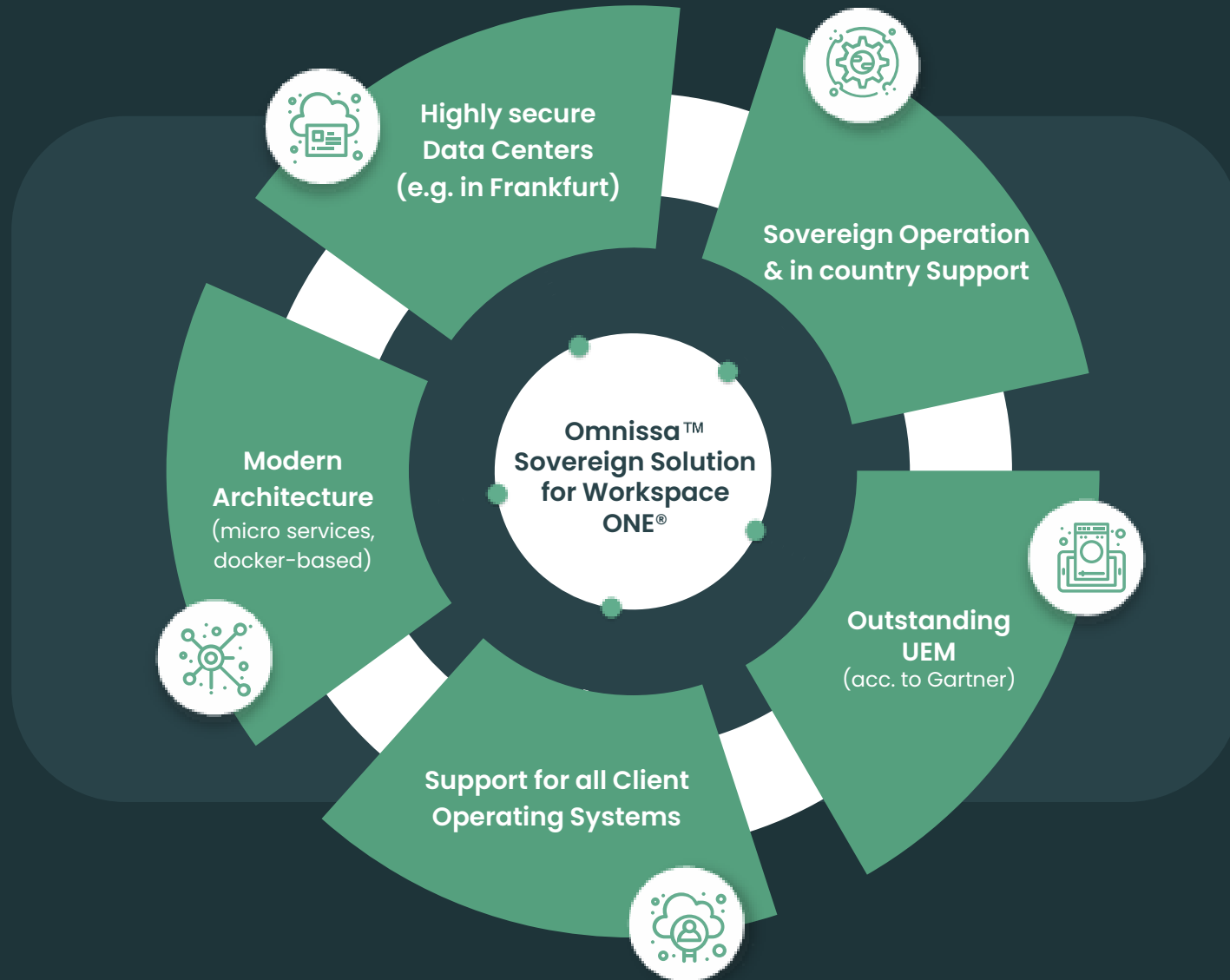
Goal: Compliance with European Regulatory Requirements, incl. Support



Architecture Overview: Separation of Powers



The sovereign path to a resilient workplace



Architecture Checklist



Protection

Control Architecture:

- Administrative Control
- Control Plane Sovereignty
- Cryptographic Control
- Policy and Compliance Control



Residency

Data Sovereignty:

- Data Classification
- Data Processing
- Legal Area and Operator Structure
- Tenant Separation



Resilience

Operational Security:

- Operation without Manufacturer
- Exit Strategies
- Operating Model
- Emergency and Restart Concepts

West Midlands Police

From Downtime to Operational Readiness



Before: Operational disruption

- Officers on patrol had to leave the scene and drive back to the station for device issues
- Losing hours per shift

Change: Workspace ONE deployed

- Centralized device management
- Officers stay operational in the field

Impact: Measurable outcomes

- More than 1.8 million hours saved
- Reduced in-person visits for technical support

“ 80% adoption, and the support-to-feature request ratio flipped from 80:20 to 20:80.

– Gregg Hudson, Mobility & Automation Manager



Spencer Pitts | Omnissa



Heiko Friedrich | GEMA International

Contact us

✉ oss@de.thegema.com

☎ +41 415 510 024

Sovereign Endpoint Management in
Mission-Critical Contexts



omnissa™



omnissa™