NexaVM vs Huawei HHEE/FusionSphere: Competitive Battlecard

Executive Overview

NexaVM - The Secure Global Enterprise Solution

NexaVM delivers a comprehensive stack for enterprise virtualization and cloud, designed for mission-critical production environments. With many enterprise customers in 30+ countries and regions, NexaVM offers a complete solution for virtualization, cloud management, and hyperconvergence.

Huawei HHEE/FusionSphere - Security Risks and Geopolitical Limitations

Huawei FusionSphere with HHEE (Huawei Hypervisor Execution Environment) presents significant documented security risks, severe geopolitical limitations for international deployments, and architectural vulnerabilities that compromise enterprise security.

Critical Comparison: Why NexaVM is the Secure Choice vs Huawei

1. Security and Geopolitical Risks

☑ NexaVM - Transparent Enterprise Security

99% own code with complete security control

Zero backdoor policy

Swiss precision and trust, compliance guaranteed for European laws (GDPR, NIS2)

✕ Huawei - Documented Security Risks

Critical vulnerabilities unpatched for years

5000+ unsafe memory function calls in production code

Backdoor capabilities documented by Wall Street Journal

US/UK/Australia bans for national security risks

2. Security Architecture and Vulnerabilities

☑ NexaVM - Security by Design

Multi-layer security architecture

Secure hypervisor without known vulnerabilities

Encrypted communication for all components

Natively implementable zero-trust model

Integrated continuous security monitoring

✕ Huawei HHEE - Architectural Vulnerabilities

Memory corruption issues in HHEE security component

Logging system vulnerabilities allow privilege escalation

Hypervisor security bypass possible

Undocumented APIs with security implications

Critical Decision Factors

Enterprise MUST Choose NexaVM for:

- ✅ **International operations** in US/EU/UK/Australia
- ✅ **Government/Defense** contractors
- ✅ **Financial institutions** with regulatory compliance
- ✅ **Healthcare organizations** with patient data
- ✅ **Critical infrastructure** deployment
- ✅ **Public company** SOX compliance
- ✅ **Long-term strategic** investment protection

Huawei UNACCEPTABLE for:

- ❌ **Any US operations** (banned)
- ❌ **UK critical infrastructure** (banned)
- ❌ **Australian deployment** (banned)
- ❌ **EU telecoms/critical** (increasing restrictions)
- ❌ **Defense contractors** (security clearance risk)
- ❌ **Banking/finance** (regulatory prohibition)
- ❌ **Healthcare** (HIPAA/GDPR compliance risk)