



NexaVM vs Huawei HHEE/FusionSphere: Battlecard di Confronto

Panoramica Esecutiva

NexaVM - La Soluzione Enterprise Sicura e Globale

NexaVM offre uno stack completo di virtualizzazione e cloud enterprise, progettata per ambienti di produzione mission-critical. Con molti clienti enterprise in 30+ paesi e regioni, NexaVM offre una soluzione completa per virtualizzazione, cloud management e iperconvergenza.

Huawei HHEE/FusionSphere - Rischi di Sicurezza e Limitazioni Geopolitiche

Huawei FusionSphere con HHEE (Huawei Hypervisor Execution Environment) presenta significativi rischi di sicurezza documentati, limitazioni geopolitiche severe per deployment internazionali, e vulnerabilità architetturali che compromettono la sicurezza enterprise.

Confronto Critico: Perché NexaVM è la Scelta Sicura vs Huawei

1. Sicurezza e Rischi Geopolitici

✓ NexaVM - Sicurezza Enterprise Trasparente

99% codice proprietario con controlli di sicurezza rigidi e periodici

Zero backdoor policy

Precisione e affidabilità Svizzera, compliance assicurata alle normative europee (GDPR, NIS2)

✗ Huawei - Rischi di Sicurezza Documentati

Vulnerabilità critiche non patchate per anni
5000+ unsafe memory function calls in codice di produzione
Backdoor capabilities documentate dal Wall Street Journal
US/UK/Australia ban per rischi di sicurezza nazionali

2. Architettura Security e Vulnerabilità

✓ NexaVM - Security by Design

Multi-layer security architecture
Secure hypervisor senza vulnerabilità note
Encrypted communication per tutti i componenti
Zero-trust model implementabile nativamente
Continuous security monitoring integrato

✗ Huawei HHEE - Vulnerabilità Architetture

Memory corruption issues in HHEE security component
Logging system vulnerabilities permettono privilege escalation
Hypervisor security bypass possibile
Undocumented APIs con security implications



Critical Decision Factors

Enterprise **MUST** Choose NexaVM for:

- ✓ **International operations** in US/EU/UK/Australia
- ✓ **Government/Defense** contractors
- ✓ **Financial institutions** con regulatory compliance
- ✓ **Healthcare organizations** con 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)