Vantageo Enterprise Servers - Product Security Datasheet

Overview

Vantageo Enterprise Servers are engineered with a comprehensive, multi-layered security architecture to safeguard customer environments from supply-chain to runtime operations. Our design philosophy embeds **“security by design”**, ensuring hardware, firmware, and software integrity throughout the product lifecycle.

Security Philosophy

- **Built-in Trust:** Hardware-anchored security from the silicon up.
- **Proactive Defense:** Continuous detection and recovery from unauthorized changes.
- **Sustainable Security:** Lifecycle controls including secure recycling and e-waste management.
- **Compliance Ready:** Meets global security standards and MSME audit requirements.

Secure Product Protection Lifecycle

Stage	Security Assurance
Sourcing	Trusted suppliers, physical inspection, anti-counterfeit components
Manufacturing	Process-oriented assembly, controlled access, resilient manufacturing
Runtime Security	Root of Trust, signed firmware, strong credentials, role-based access
Lifecycle Management	HDD retention, secure firmware recovery, recycle & sanitization
Protect	BIOS, firmware, data, and physical hardware assets
Detect	Malicious or unauthorized changes during runtime
Recover	Restore BIOS, firmware, and OS to known-good state

Hardware Security Features

- Silicon Root of Trust (RoT)
- Trusted Platform Module (TPM) 2.0
- Intel® Boot Guard & SGX
- AMD Secure Processor, SME & SEV
- Chassis intrusion protection
- Anti-counterfeit/approved components

Firmware & BIOS Security

- Secure Boot & Measured Boot
- Cryptographically Signed Firmware
- Secure Firmware Updates with Anti-Rollback
- Secure Flash & BMC Runtime Protection
- Firmware Recovery & Drive Secure Erase
- Password Security and Role-Based Access
- Secure API & System Lockdown Mode

Key Security Technologies

Feature	Description
Silicon Root of Trust (RoT)	Hardware-anchored verification of firmware integrity at power-on.
TPM 2.0	Cryptographic chip for secure key storage and authentication.
Secure Boot	Prevents unauthorized software from executing during startup.

Feature	Description
Signed Firmware	Ensures firmware authenticity and integrity through digital signatures.
Automatic Recovery	Restores firmware from verified backup in case of corruption or attack.
System Lockdown	Prevents any configuration or firmware modification in production mode.
Secure Data Storage	Support for self-encrypting drives (SED) and secure wipe.

Compliance & Best Practices

- Adheres to global security standards (ISO/IEC 27001, NIST SP 800-193)
- MSME-registered supplier: compliant with Indian statutory disclosure and data protection mandates
- Recommended practices:
    - Keep firmware and OS updated
    - Apply latest security patches
    - Enforce strong authentication policies
    - Follow secure data disposal and retention procedures

Vantageo Commitment

Vantageo continues to innovate in hardware and firmware security, aligning with the highest standards of enterprise, government, and defense-grade cybersecurity. Our systems are Made in India, integrating global best practices for secure manufacturing and trusted computing.

VANTAGEO PRIVATE LIMITED

📍 Plot No. F7, Road No. 21, Wagle Industrial Estate, Thane (W), Maharashtra, India

🌐 www.vantageo.com ✉️ info@vantageo.com 📞 Toll Free 1800 266 9898