The security of our VANTAGEO Products is a top priority. We undertake all necessary measures to safeguard the operation of your enterprise servers and storage systems. As servers and storage solutions become more versatile and complex, the focus for robust security increases.

Given the evolving nature of security threats, we acknowledge the importance of implementing strong defense mechanisms to protect both users and customers. Our goal is to maintain industry-leading security practices to ensure the highest level of protection.

Customers expect products that meet rigorous security standards, and we are committed to delivering solutions designed with advanced security features. To further enhance protection, we recommend following security best practices, such as:

- Regularly updating your operating system.
- Ensuring that firmware and all software are kept up to date.

By adhering to these practices, it ensures that the systems remain secure and resilient against emerging threats.

Secured Product Protection

- Sourcing : Trusted sourcing and rigorous testing define Vantageo's commitment to quality.
- Manufacturing : Resilient Manufacturing. Process oriented assembly.
- Run Time Security : Root of Trust , Cryptographically signed firmware’s , Strong credentials
- Life cycle Management : Recycle Process , E-Waste management, HDD retention services.
- Protect : Protect asset of life cycle, including BIOS, firmware, data, and physical hardware.
- Detect : Detect malicious cyberattacks and unapproved changes.
- Recover: Recover BIOS, firmware, and operating system to a known good state.

Product Security Standards

Hardware

- Silicon Root of Trust
- Chassis Intrusion Protection
- Trusted Platform Module (TPM)
- Intel Boot Guard
- Intel SGX
- AMD SME
- AMD Secure Processor
- Secure Encrypted Virtualization.
- Anticounterfeit/Approved components

BIOS/BMC

- Secure Boot
- Secure Drive Erase
- Secure Flash
- Secure Firmware Upgrades
- Cryptographically signed firmware
- Password Security
- Secure API
- Firmware Recovery
- Anti Rollback
- Runtime BMC Protection
- System Lockdown
- Supply chain security

Security Feature Descriptions

Silicon Root of Trust : Silicon Root of Trust (RoT) is a firmware technology that adds security and protection to the hardware level of a server. RoT starts a chain of trust that validates that the server is booted with legitimate firmware

Trusted Platform Module (TPM) 2.0 : Trusted Platform Module (TPM) technology is designed to provide hardware-based, security functions. TPM is a dedicated chip designed to secure hardware via cryptographic keys.

Cryptographically Signed Firmware : firmware image is signed with a private key. This "signed firmware" guarantees that the firmware update has not been modified or corrupted.

Secure Boot : The secure boot process is designed to ensure that the server starts safely and securely by preventing unauthorized software from taking control at boot-up.

Secure Firmware Updates : Use of cryptographically signed firmware. All BMC, BIOS, firmware updates happen securely via the BMC which checks for signatures and roll-back ids before updating the firmware.

Automatic Recovery : RoT design reduces the downtime of servers with its secure recovery feature. RoT automatically recovers servers during the firmware boot process from corrupt images caused due to malicious attacks, illegal or incomplete operations, and significantly. In case

of suspicious activity or unexpected results in existing firmware, the user can manually initiate BIOS or BMC recovery from backup images.

System Lockdown : System Lockdown is a security feature that prevents all system configuration changes including firmware updates.

Encrypted Data Storage : Support for SED.

WWW. VANTAGEO.COM

Toll Free: 1800 266 9898

Contact: wecare@vantageo.com