Vantageo Enterprise Servers Product Security

Made In INDIA

vantageo™

www.vantageo.com

Overview

The security of our customers is a top priority; hence we ensure to put all measures in place to safeguard the operation of your Enterprise servers and storage systems. Servers and storage systems are becoming more versatile but more complex & with that it brings more need to be secured.
The new threat facets , there needs a defense mechanisms to protect users and customers and thus bring our security knowledge to the highest in the industry.

It's recognized that customers expect to deploy products that meet high-security standards; therefore, the products are designed for the highest level of protection.

Recommended that you follow security best practices, including keeping your operating system up-to-date and running the latest versions of firmware and all software.

Secured Product Protection Lifecycle

- **Sourcing**：Trusted Suppliers , Physical Inspections of components .
- **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

vantageo™

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.

THANK YOU!

Phone Numbers

Sales | (+91) 98339 86727

Support 1800 266 9898 (Toll Free)

Vantageo Proprietary & Confidential

Email ids

Sales | sales@vantageo.com

Service | support@vanatgeo.com