NIST Special Publication 800-53 Revision 4: Implementing Essential Security Controls with PrivateCore vCage Manager

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides guidance for the selection of security and privacy controls for federal information systems and organizations. Revision 4 is the most comprehensive update since the initial publication. Major changes include new security controls and control enhancements to address advanced persistent threats (APTs), insider threats, and system assurance.

The recommended security controls in NIST SP 800-53 can help organizations to comply with applicable federal laws, regulations, and standards such as the Federal Information Security Management Act (FISMA). NIST SP 800-53 makes recommendations regarding a full range of controls.

This document provides organizations with an understanding of how PrivateCore vCage Manager software helps meet NIST SP 800-53 Revision 4 requirements as they apply to Linux x86 servers and OpenStack cloud environments.

Number	Priority	Control	How does PrivateCore vCage Manager help?
Family: Configuration Management			
CM-2	P1	CONFIGURATION MANAGEMENT Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	PrivateCore vCage Manager maintains a parameterized whitelist of known good values for x86 Linux servers beneath the virtual machine (VM) layer. The server stack (elements below the hypervisor) is validated at bootup and only servers having a known, good configuration would be admitted for use. In an OpenStack environment, only attested servers would be admitted to create a “trusted computing pool”.
CM-3	P1	CONFIGURATION CHANGE CONTROL Control: The organization: • Determines the types of changes	PrivateCore vCage Manager provides a point of change control by maintaining a whitelist for x86 Linux servers of known good values and an

www.privatecore.com
Email: sales@privatecore.com

		to the information system that are configuration-controlled; ● Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; ● Documents configuration change decisions associated with the information system; ● Implements approved configuration-controlled changes to the information system; ● Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; ● Audits and reviews activities associated with configuration-controlled changes to the information system; and ● Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	audit trail of any changes to the whitelist values. Any changes to that whitelist would be logged and can be audited. In the context of a cloud based on OpenStack, a server attempting to join an OpenStack cluster without a whitelisted configuration would be denied admission.
CM-6	P1	CONFIGURATION SETTINGS Control: The organization: ● Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; ● Implements the configuration settings; ● Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system	PrivateCore vCage Manager controls X86 server settings via a whitelist of known, good values for x86 Linux servers that provide an audit trail for any changes to the whitelist values. This list includes firmware, BIOS, hypervisor and the commands used to invoke the hypervisor. Any change to the whitelist is logged. Any server without an approved, whitelisted configuration would fail attestation and would not be available. Any new, valid configurations or deviations would need to be entered into vCage Manager.

www.privatecore.com
Email: sales@privatecore.com

		components] based on [Assignment: organization-defined operational requirements]; and ● Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	
Family: Contingency Planning			
CP-10	P1	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	PrivateCore vCage Manager attests the integrity of Linux servers from the hardware layer up to and including the hypervisor. This granular attestation includes BIOS, firmware, hypervisor and command line arguments invoking the hypervisor. By leveraging Intel® Trusted Execution Technology (Intel® TXT) and a server's Trusted Platform Module (TPM) chip, PrivateCore vCage Manager can verify that X86 Linux servers are in a known, good state at boot-time. Following a disruption, compromise or failure, vCage Manager can ensure that Linux servers return to a known, good state.
Family: System and Services Acquisition			
SA-12	P1	SUPPLY CHAIN PROTECTION Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.	PrivateCore vCage Manager enables organizations to attest that their server firmware are in a known, good state at boot-time and that the firmware has not been tampered with. PrivateCore vCage Manager maintains a whitelist of known, good firmware values and validates that x86 Linux server firmware is in validate state at boot-time.
SA-13	P0	TRUSTWORTHINESS Control: The organization: ● Describes the trustworthiness required in the [Assignment: organization-defined information system, information system component, or information system service] supporting its critical missions/business functions; and ● Implements [Assignment: organization-defined assurance overlay] to achieve such	PrivateCore vCage uses Intel Trusted Execution Technology (Intel TXT) and an x86 servers Trusted Platform Module (TPM) to ensure that servers are in a known, good state at boot-time and can be trusted. This can be used to validate server infrastructure and create "trusted computing pools" within an OpenStack infrastructure.

		trustworthiness.	
SA-18	P0	TAMPER RESISTANCE AND PROTECTION Control: The organization implements a tamper protection program for the information system, system component, or information system service.	vCage Manager validates that the system elements below the virtual machine (VM) are in a known good state and free of tampering. Any tampering with system components such as firmware, software and configuration below the VM layer would be evident.
Family: System and Information Integrity			
SI-14	P0	NON-PERSISTENCE Control: The organization implements non-persistent [Assignment: organization-defined information system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization- defined frequency]].	PrivateCore vCage Manager protects system elements below the virtual machine layer to ensure that system elements are in a known, good state at boot-time. This protects against potential modification of system elements including the server BIOS, firmware, hypervisor, and command line arguments invoking the hypervisor.

About PrivateCore

PrivateCore is the private computing company. PrivateCore vCage software validates the integrity of OpenStack servers and secures against persistent malware, malicious hardware devices, and insider threats. PrivateCore was founded in 2011 by security industry veterans from the IDF, VMware and Google. The company is based in Palo Alto, California and has received venture funding from Foundation Capital. For more information, please visit www.privatecore.com.