privatecore

NEWS RELEASE

FOR IMMEDIATE DISTRIBUTION

PrivateCore Locks Down OpenStack Servers

vCage Software Establishes Trust and Protects Servers from Persistent Malware and Insider Threats

PALO ALTO, CA – February 11, 2014 – PrivateCore, the private computing company, today announced the general availability of its vCage software which audits platform integrity and protects OpenStack clusters from persistent malware, malicious hardware devices and insider threats. vCage validates the integrity of OpenStack infrastructure and protects servers using memory encryption to secure data in use across private, public, and hybrid clouds.

Click to tweet: .@PrivateCore vCage software now generally available, delivers trusted computing for #openstack http://bit.ly/11tMi78

OpenStack environments can contain thousands of compute nodes spread across geographic boundaries and in remote locations. Compromising or misconfiguring one node can jeopardize the security of the entire infrastructure. PrivateCore vCage validates trustworthiness to avoid misconfiguration and protects OpenStack servers and applications from persistent threats.

"What we have learned through our beta process is that enterprises and service providers have no easy way of verifying that their OpenStack compute nodes are running trustworthy configurations and have not been compromised," said Oded Horovitz, CEO of PrivateCore. "PrivateCore vCage provides a flexible way of protecting OpenStack-based environments by validating the integrity of the compute nodes, hardening the underlying hypervisor, and using full memory encryption to protect data in use where necessary."

vCage Solution Elements
PrivateCore's vCage solution consists of vCage Manager and vCage Host. vCage Manager provides security provisioning, attestation, management and reporting for OpenStack clouds. For servers requiring maximum security, PrivateCore vCage Host provides additional levels of server security.

vCage Manager: Server Auditing and Validation
Server security starts with visibility into the software and hardware comprising a server platform. Organizations need to verify that each server is in a known good state before trusting the server with any sensitive information, and they need validate that state from the server hardware layer through the hypervisor to the operating system. PrivateCore

vCage supports Intel® Trusted Execution Technology (TXT) hardware-based root of trust technology to validate the entire platform environment. Enterprises and service providers can create trusted computing pools in the cloud knowing that they are running on servers for which the integrity of the server firmware, BIOS, hypervisor and operating system code has been verified.

PrivateCore vCage provides simple administration with fine-grained control over the OpenStack environment, allowing enterprises to flexibly establish policies and adapt to infrastructure changes with a minimum of administration. PrivateCore's innovative approach to validating server integrity delivers powerful security while avoiding the complexity and policy bloat of prior solutions.

vCage Host: Server Hardening and Memory Encryption
vCage Host software provides an additional layer protection against and malicious local hardware devices attached to the host with a combination of hardening and memory encryption. vCage Host software provides additional security controls to prevent access to data while in-use on the server by physical intruders and malicious hardware devices. Leveraging security building blocks in the Intel CPU such as Intel VT-x, VT-d, AES-NI, Digital Random Number Generator (DRNG), Trusted Execution Technology (TXT) and the large Level 3 cache, vCage Host provide a secure environment for data processing within the CPU package, encrypting any information as it leaves the CPU cache and before it is stored in the server memory.

Availability and Pricing
PrivateCore vCage is available immediately from PrivateCore and its business partners worldwide to selected customers. The PrivateCore vCage Manager Starter Kit to manage a rack of servers is $495 per month.

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.

Media Contact:
Todd Thiemann
+1.650.352.3547
press@privatecore.com

###

PrivateCore and vCage are trademarks of PrivateCore, Inc. All other names mentioned are trademarks, registered trademarks or service marks of their respective owners.