Secure Virtual Appliances

Articulating the use case to harden virtual appliances with vCage

PrivateCore vCage Secures Virtual Appliances

Virtual appliances are becoming the preferred method for software and hardware vendors to distribute their technology for enterprise customers requiring an on-premise solution. Virtual appliances are virtual machine images designed to run in a virtualization platform. The recent industry trend has been for technology vendors to migrate to a virtual appliance form factor as it is cost-effective and easier for customers to deploy and manage.

Virtual appliances enable technology vendors to increase revenues by distributing technology in a format desired customers demand as well as opening up market opportunities through easier technology trials ("try before you buy") that are not possible with hardware appliances. Virtual appliances also lower costs by reducing or eliminating hardware engineering, support and logistics. Technology providers can avoid the burden of hardware logistics and navigating complex import/export regulations for such specialized hardware appliances.

As technology vendors consider virtual appliances, they must also wrestle with how to secure the sensitive information that such virtual appliances can contain. Sensitive information in memory can be compromised and code reverse engineered. Virtual appliances can contain a variety of sensitive information including:

- Intellectual Property (software algorithms, design information, etc)
- Cryptographic Keys
- Digital Certificates
- Customer Data (personally identifiable information, etc)

privatecore

Key Benefits

- **Accelerating Sales Cycles and Revenues:** Secure virtual appliances speed sales cycles with faster product trials and deployment. Secure virtual appliances also increase revenues by ensuring enforcement of product licensing requirements.
- **Increasing Revenues in New Regions:** Technology providers can reach a broader market by selling and deploying software products in previously prohibited geographic locations
- **Expanding Deployment Options:** Secure virtual appliances open up new market opportunities by meeting the needs of customers who lack physical space to install hardware appliances.
- **Maintaining Competitive Advantage:** PrivateCore vCage creates tamper-proof and leak-proof virtual appliances, protecting intellectual property in memory so it cannot be compromised and reverse engineered.
- **Reducing Costs:** Replacing hardware appliances with secure virtual appliances reduces development and support costs while avoiding the expense of hardware and hardware support logistics. Virtual appliances also reduce enterprise IT administration requirements.

Compromising virtual appliance information can lead to lost revenue for technology vendors through pirated technology and copycat products. Without adequate protection for intellectual property, technology providers face the prospect of a customer becoming a competitor.

Both technology vendors and enterprises can be harmed if virtual appliances containing sensitive enterprise data is compromised. Damage can include tarnished reputations, monetary damage, and data breach reporting costs.

The Virtual Appliance Security Conundrum

Technology providers, both hardware and software, are offering virtual appliances to their customers as a way of increasing revenues and decreasing costs. However, technology providers also need to protect their intellectual property and sensitive information. The legacy hardware approach to appliance security relied on creating a self-contained "black box" with costly to operate features such as tamper-evident seals to ensure that hardware was not compromised.

While it is possible to secure sensitive information with encryption when it is stored on disk (data at rest), such information is unprotected and open to compromise when it is in memory (data in use). Memory can be copied by a hypervisor administrator or via physical access and subsequently parsed to extract valuable secrets. For example, encryption keys for data at rest are typically kept in memory. Attackers can obtain a copy of memory, parse that memory to extract encryption keys, and then unlock the sensitive data at rest.

Tamper-proof Virtual Appliances with PrivateCore vCage

PrivateCore vCage enables software providers to secure their intellectual property, avoid the burden of hardware appliances, and protect customer data. PrivateCore vCage protects the contents of data in use with memory encryption, enabling technology providers to protect and control sensitive data. With vCage from PrivateCore, enterprises can now increase revenues by selling products containing valuable intellectual property in locations previously considered to be too risky.

About PrivateCore

PrivateCore is the private computing company. Its innovative vCage software is the first product to transparently protect any application while in use on commodity x86 servers. Founded by security industry veterans from VMware and Google in 2011, PrivateCore is based in Palo Alto, California. The company received venture funding from Foundation Capital in 2012. For more information, please visit www.privatecore.com.

> "U.S. networks are built on inherently insecure architectures with increasing use of foreign-built components"
>
> — US Department of Defense, Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, Page 1, January 2013

privatecore

PrivateCore, Inc.
555 Bryant #821
Palo Alto CA 94301
+1 (650) 427-9784
sales@privatecore.com
www.privatecore.com