Protecting SaaS In-Memory Applications

Articulating SaaS In-memory database use case

PrivateCore vCage Protects SaaS Data for In-Memory Applications

Software-as-a-Service (SaaS) providers are growing revenues and gaining competitive advantage by processing increasing volumes of customer data more quickly. While traditional application architectures use disk storage to store data, moving data from relatively slow disk storage into memory offers exponentially faster application performance and scalability. This evolution to in-memory technology opens up additional revenue streams in a variety of ways - new applications, improved application performance, and more SaaS users processing larger volumes of data than was previously possible. However, such architectures also raise data security concerns that can inhibit SaaS customer adoption.

While in-memory processing improves performance and scalability, it also leaves large volumes of sensitive information unprotected and “in the clear”. SaaS customers have a security concern that their sensitive data in memory may be compromised and need assurance that such information is secured.

The Security Challenge

SaaS providers must inspire confidence in their customers that their data in the SaaS environment is secure. Ambiguity and uncertainty around data security inhibit the adoption of new services and can limit revenue growth for SaaS providers. Enterprises entrusting their sensitive data with a SaaS provider need assurance that sensitive information is secured at all stages of the information lifecycle.

privatecore

Key Benefits

- **Accelerating Revenues:** vCage enables SaaS providers to overcome customer security concerns and demonstrate security of sensitive in-memory data
- **New Service Offerings:** In-memory technology opens up new SaaS application opportunities that might not be accepted by SaaS customers without the in-memory data security provided by vCage
- **Competitive Differentiation:** Encrypting data in use with vCage allows SaaS providers to differentiate their services through superior data security
- **Auditable Security for In-memory Data:** SaaS customers can now see in a provable way that their sensitive data in RAM is secure
- **Rapid Operational Scaling:** SaaS providers can quickly scale operations to a broader array of hosting providers and locations without increasing physical or legal exposure risks.
- **Improved Security Posture:** Protect sensitive customer information from potentially compromised hardware in the supply chain.

In traditional compute architectures, the bulk of data stays in storage environments that are typically protected by some sort of data-at-rest encryption technology with a modest amount of data stays in memory. The advent of in-memory architectures move large volumes of sensitive data into persistent random access memory (RAM) and leave it vulnerable to well-documented attack strategies to extract and parse memory. As RAM becomes the "new disk", data in memory provides an appealing opportunity for hackers and SaaS providers need to demonstrate security for such an attractive target. Securing memory is a particular challenge because much of the SaaS hardware infrastructure is in colocation facilities or the public cloud, locations over which the SaaS provider has little control.

> "Attackers are increasingly using outsourced service providers as a means to gain access to their victims."
>
> — Mandiant Threat Report 2013, Mandiant, 13 March 2013, https://www.mandiant.com/resources/m-trends/

The PrivateCore vCage Solution

PrivateCore vCage enables service providers to secure compute memory while taking advantage of the performance benefits of in-memory database technology. PrivateCore vCage encrypts data in use and reduces the SaaS environment attack surface, enabling service providers to satisfy customer demands for rigorous protection of sensitive data.

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.

privatecore

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