Protecting Edge Network Servers

Articulating Edge Network Use Case to service providers and enterprises

PrivateCore vCage Secures Edge Network Servers

Enterprises and solution providers are reducing latency and accelerating application performance by moving compute power to the edges of their networks. Such "edge" data caches reduce bandwidth costs, improve performance, and increase global availability of content for locations such as branch offices, manufacturing facilities, and retail locations. Edge networks frequently process sensitive information including:

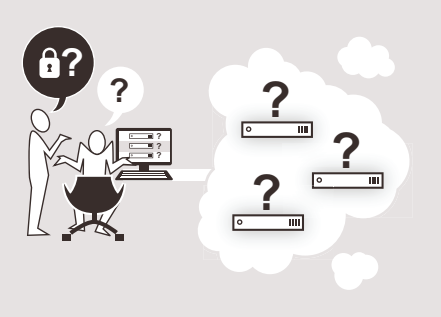
- **Encryption keys:** Stealing of encryption keys in memory can enable hackers to decipher and access the underlying encrypted information.
- **Personally identifiable information (PII):** Loss of PII can trigger state data breach laws or national data protection laws.
- **Certificates:** Increasing use of Transport Layer Security (TLS), commonly referred to as Secure Socket Layer (SSL), to ensure secure communication between browsers and the edge server has resulted in increased SSL deployments to edge network servers. SSL certificates contained in edge servers are valuable material that, in the hands of hackers, enable spoofing of legitimate websites.

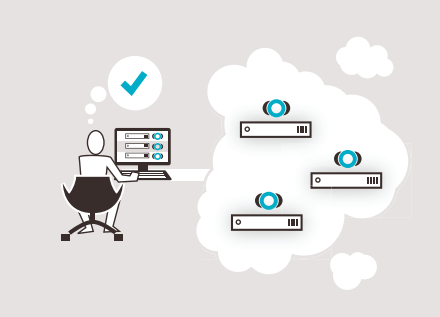
The compromise of edge server data can lead to significant financial and brand damage.

Key Benefits

- **Increased Revenue:** More servers processing sensitive information closer to the end user speeds business and generates more revenue
- **Improved Deployment Models:** Businesses can deploy servers to improve performance in locations previously deemed too insecure for sensitive information while minimizing costs by avoiding the cost of physical security
- **Reduced Risk Profile:** Improved edge protection reduces the security risk, minimizing the possibility of a costly data breach

privatecore





The Edge Network Security Challenge

Maintaining physical security for a distributed edge "Point of Presence" (PoP) network environment can be costly and include the burden of physical infrastructure security such as locks, cameras, and server cages in potentially hostile geographic locations. Businesses deploying edge networks have historically had to consider tradeoffs between security and business drivers, including application performance and revenue. Limiting the number of nodes containing secure information minimizes the security risk of information being compromised. However, such an approach may hinder network performance and limit revenue.

Businesses can also be concerned about the possibility of information being accessed via legal subpoenas issued to access data in foreign jurisdictions. While encryption for data at rest provides a measure of control, sensitive information including encryption keys may still be available and accessible in memory. If servers are located in hosted or co-location environments, information could be accessed without the information owner's knowledge.

The PrivateCore vCage Solution

PrivateCore vCage protects sensitive information located on the edge network, enabling service providers and enterprises to securely deploy more PoPs and avoid the expense of hardware security. The PrivateCore software-only security solution encrypts all memory contents, mitigating against the possibility of memory compromise. vCage memory encryption enables service providers and enterprises to safely deploy more nodes, even in environments previously considered too risky to contain sensitive information.

"The number-one concern of IT professionals is a lack of controls to enable them to effectively limit access to data and services to authorized users."

— Intel Corporation, "Peer Research: What's Holding Back the Cloud?", page 8, May 2012

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