Protecting CDN Network Nodes

PrivateCore vCage for Content Delivery Network Node Protection

Content Delivery Networks (CDNs) rely on points of presence (PoP) around the world to ensure that data streams as quickly as possible to users requesting data. Such "edge" data caches reduce bandwidth costs, improve page load times, and increase global availability of content so that consumers can use more data and generate more revenue. The number of nodes and servers can reach thousands of nodes with tens of thousands of servers scattered among many remote points of presence. The increasing use of Transport Layer Security (TLS), commonly referred to as the Secure Socket Layer (SSL) protocol, to ensure secure communication between the consumer and the CDN node has resulted in increased SSL deployments, including edge networks. SSL certificates contained in CDN PoPs are valuable material that, in the hands of hackers, enable spoofing of legitimate websites. A breach of a CDN node could prove damaging to the brands of both the CDN operator and the CDN operator's customer.

The CDN Security Challenge

Maintaining physical security for a distributed CDN PoP environment can be costly and include the burden of physical infrastructure security such as locks, cameras, and server cages in potentially hostile geographic environments. CDN operators have historically had to consider tradeoffs between security and business drivers, including network performance and revenue. Limiting the number of nodes containing secure information minimizes the security risk of nodes and SSL certificates within those nodes being compromised. However, such an approach hinders network performance and limits revenue.

Key Benefits

- **Increased Revenue:** More secure nodes containing sensitive information generate more revenue
- **Improved Deployment Models:** CDNs can deploy nodes 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 to both CDN and CDN customer brands

privatecore

The PrivateCore vCage Solution

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

"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/

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