http://www.eweek.com/cloud/cloud-security-viewed-as-vital-but-effective-solutions-lacking.html

Cloud Security Viewed as Vital, but Effective Solutions Lacking

By Wayne Rash | Posted 2014-03-29

NEWS ANALYSIS: One of today's most important IT challenges is how to make cloud security more robust. But there was little agreement among experts at the Cloud Innovation Summit on how to do this.

SARATOGA, Calif.—There's a saying that's been making its way around the IT business for a long time that asserts that "when the only tool you have is a hammer, everything looks like a nail."

This saying was proven true at the NetEvents Cloud Innovation Summit in Saratoga, Calif., where a number of vendors presented what they claimed were innovative but were remarkably similar to their existing security products. So appliance vendors suggested appliances, server vendors suggested server software, and so forth.

Fortunately, some new workable ideas also surfaced. One in particular is potentially standards-based and could actually work. Martin Casado, the inventor of OpenFlow, proposed an answer to cloud security that exists outside any individual server operating system.

Instead, it would reside in a separate layer, within, or perhaps virtually next to, the hypervisor. While Casado now works for VMware, he made it clear that such a security layer should exist with any hypervisor, not just VMware.

Casado, borrowing a concept from the Space Science Laboratory at the University of California, Berkeley and NASA, said that such a layer would effectively exist in the cloud's "Goldilocks Zone." He said that one problem with security systems that run as a guest process in a virtualized system is that once the operating system in that process is fully locked down, you lose visibility to network resources. But when you gain visibility, you lose security, he noted.

The Goldilocks Zone would be a place where both visibility and security are possible—in other words, a location that's not too visible or not too inaccessible, but is just right. Such a layer in the hypervisor would work because it's outside of any one virtualized server, but can observe server operations in detail.

As a spokesperson for VMware told me later, the first thing that malware invading a server tries to do is to block the operations of any anti-malware software. But since a process on a virtualized server has no way to reach the hypervisor, then the security layer that's working with the hypervisor can take action to prevent damage. -