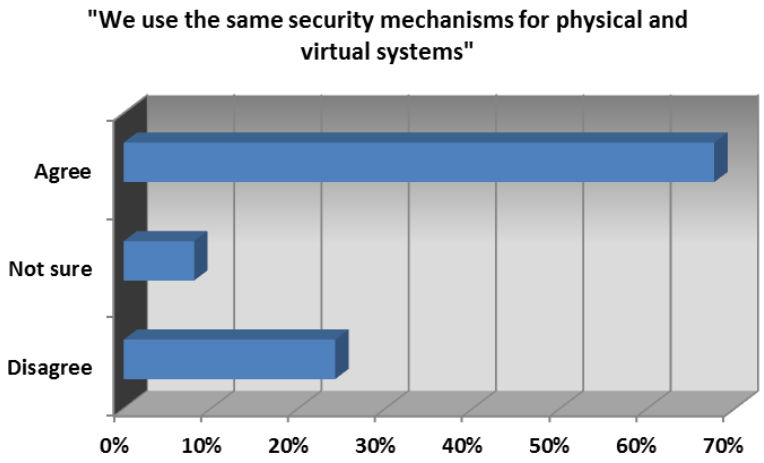
2011 Data Center Security Survey: Virtualization & Clouds

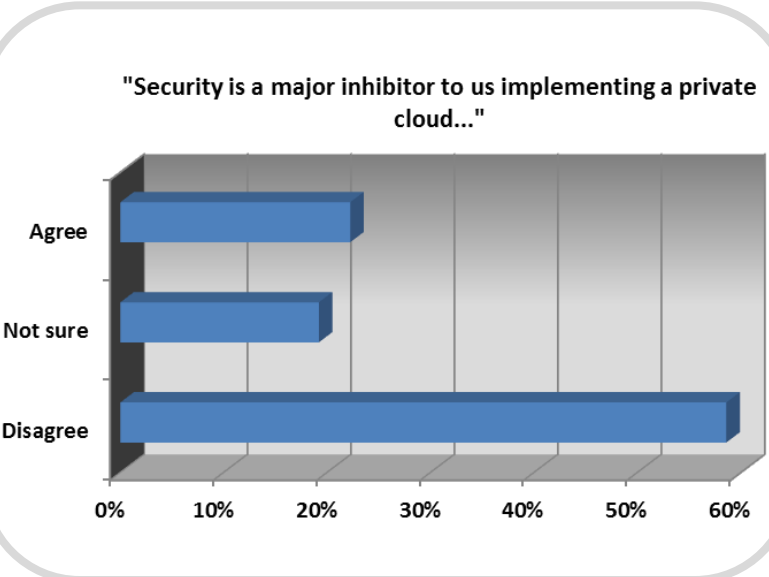
Virtualization and Cloud Computing have become part of every IT industry conversation. Virtualization is now standard operating procedure in many data centers. In the most forward-looking organizations, private clouds are being formed. Public clouds are receiving massive attention, but many data center folks remain skeptical of deploying important workloads onto public clouds due to security and other concerns.

We devoted part of our **2011 Data Center Security Survey** (demographics here) to finding out about the security implications of virtualization and cloud computing. We asked customers how they are securing their virtualized systems in general, and then inquired specifically about potential security concerns surrounding private and public cloud use.



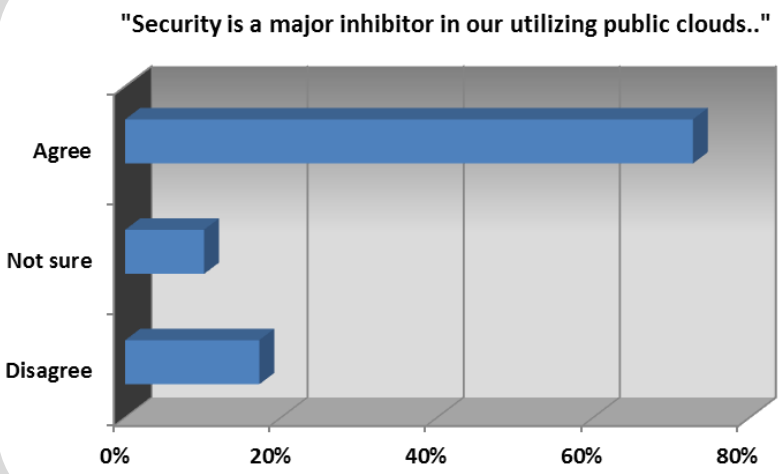
A large majority of customers were using the same tools to secure both physical and virtualized systems. Of course, not many security suites are optimized for virtualized systems.

Most of the security software in the data center has been modified to work on virtualized systems rather than designed (or re-designed) from the ground up with virtualization in mind. While our respondents didn't cite this as a problem, we'd think that there must be some virtualization features (like partition mobility) that need special treatment from a security perspective.



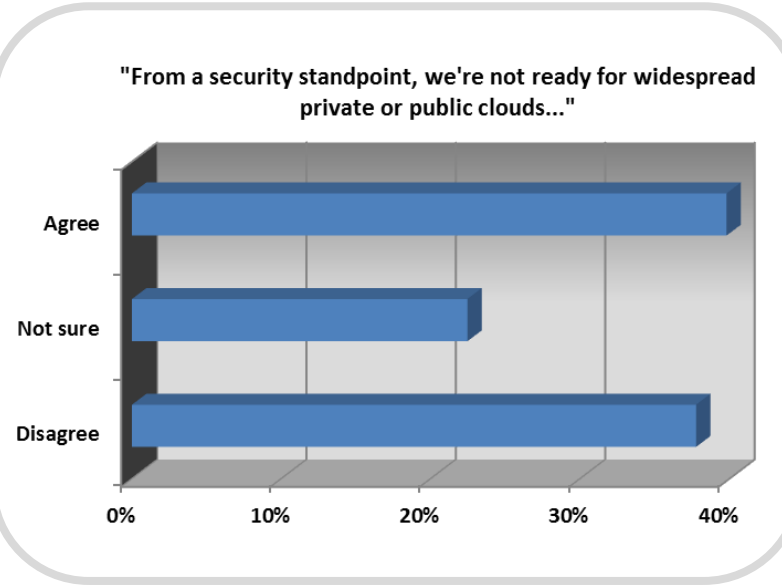
Most of our respondents (close to 60%) don't see much problem with securing private clouds. This isn't surprising; by definition, private clouds are at least somewhat secure since they live behind the organizational firewall.

This isn't to say that private clouds don't present security challenges – they do, particularly when workloads can be easily moved from system to system. Mechanisms need to be in place that will prevent a sensitive VM from being moved to a physical system that doesn't have an appropriate level of security.



Security concerns are the biggest factor keeping corporate customers from embracing public clouds. Some believe that public clouds are, by their very nature, insecure. But even customers who are more trustful of the technology feel that the cloud providers don't have any "skin in the game" when it comes to security and also availability.

In some cases, they also see public clouds as more attractive targets for hackers and other bad guys as opposed to their own data centers.



It's interesting to note the almost equal split on this question: a very slight majority agree that their security isn't ready for widespread cloud utilization.

Most of the customer doubt is due to our inclusion of public clouds in this question. Respondents made it clear that their major concern about cloud computing is that they simply don't trust public clouds right now.

From a security standpoint, virtualization and private clouds aren't seen as too big a challenge by our security survey respondents, but public cloud utilization is quite a different story. In our next report, we're going to take a look at the impact of security breaches on both the business and IT sides of our respondents' organizations. You can find that report here.

If you're interested in finding out more about this survey and seeing more results (demographics, expanded results, detailed GCG analysis), click here.

Gabriel
CONSULTING GROUP

www.GabrielConsultingGroup.com
gcginfo@GabrielConsultingGroup.com
(503) 372-9389