Written by Marco Attard
16 June 2011

Gartner suggests the adoption of Systematic Workload Reprovisioning (SWR) to counter advanced threats compromising the host OS at deep level, particularly when it comes to dealing with high-risk workloads.

SWR is relatively straightforward-- it involves the periodic rebuilding and reprovisioning of server and desktop workloads from a high-assurance base image file library. Through workload restoration to a high-assurance state, security professionals can proactively remove deeply rooted malware, making sure undetected intrusions don't continue to persist within the system.

This is by no means a new concept-- what's new is the proactive and systematic workload reprovisioning. With SWR, workload restoration process becomes the norm as an automated process.

Gartner says now is the time for SWR strategy adoption, thanks to the uptake of server and desktop virtualisation techniques at both OS and application levels.

The analyst predicts more than 20% of enterprises will adopt a SWR strategy for their high-risk server-based workloads by 2016, while 60% will adopt a SWR strategy for their hosted virtual desktop workloads.

Thus, through a SWR strategy workloads in production are not trusted, but considered compromised-- a change in mindset required in this age of advanced threat management.

Go Systematic Workload Reprovisioning Will Become Increasingly Prevalent