

By: February 2008 Technology News Editor

[Download Free Hardware Virtualization-Based Windows Rootkit Detector](#)

The Hypersight Rootkit Detector is in beta stage at this point in time

Hypersight Rootkit Detector is a hardware virtualization-based rootkit detector for the Windows operating system. The Hypervisor based-security solution has hit public beta at the end of 2007, and comes with support just for Windows 2000, Windows XP, and Windows Server 2003. The anti-rootkit is also limited to running Intel Core 2 CPUs, for the time being, as it functions exclusively based on hardware virtualization. [North Security Labs](#), the makers of the Hypersight Rootkit Detector, promised to add support for AMD processors, as the product's development will evolve. "Hypersight Rootkit Detector employs the innovative hardware virtualization technology implemented by Intel in their latest CPUs. The Intel VT-x technology works as a hypervisor on supported Intel CPUs, encapsulating the entire operating system into a virtual machine. All sensitive events are handled by Hypersight Rootkit Detector, which allows the product to detect, intercept and notify the user about actions that are inherent to rootkit operation," reads an excerpt of the Hypersight Rootkit Detector's official description. While in beta, the Hypersight Rootkit Detector is available for download at no charge. Once the anti-rootkit will evolve past pre-release stage, it will also no longer be free. But North Security Labs says that the product will be worth every penny. According to the anti-rootkit maker, Hypersight Rootkit Detector has bested similar products from heavyweight players on the security market, including Rootkit Unhooker 3.31.150.420, Panda Anti-Rootkit v1.08.00, Norton Antitbot 2.02, McAfee Rootkit Detective 1.0, IceSword 1.22en version for 2000/xp/2003/vista, GMER 1.0.12 and AVZ 4.25. The tests were run using samples of the Rustock.A and Unreal.A rootkits. "Hypersight Rootkit Detector intercepts and blocks attempts of software programs to run in an exclusively privileged hypervisor mode. This type of activities is inherent to rootkits that use hardware virtualization, e.g. Blue Pill or Vitriol. Hypersight Rootkit Detector also intercepts operations with memory page table as well as GDT and IDT, which in turn allows it to detect rootkits implementing stealth technologies to hide themselves in the memory of the PC (e.g. Shadow Walker)," North Security Labs added in the description of the Hypersight Rootkit Detector. Hypersight Rootkit Detector is available for download [here](#).