

26 May 2008

By: Marius Oiaga, Technology News Editor

Security  
Microsoft

## [If There's One Vista Feature with a Bad Rap, It's UAC](#)

### *Claims Microsoft*

If there's one Windows Vista feature deeply misunderstood and with a bad reputation, it's User Account Control. Microsoft confirmed officially that UAC has a bad rap but, at the same time, the software giant's perspective over the matter is that UAC deserves better if not, at least, a second chance. The Redmond company compared Vista with UAC disabled with a house with no locks, and warned end users not to trade off security for easy access. This because, in the end, although it does not act as a security boundary, UAC does provide an extra mitigation adding a layer of protection for end users. "One reason this feature is misunderstood is because UAC isn't a single feature; it's a set of technologies to help end users run with standard user privileges, and reserves Local Administrator privileges for IT staff or limited specific circumstances," Microsoft revealed. The User Account Control has been set in place as a watchdog for any code, application, user, process, malicious in nature or genuine that attempts to manipulate key aspects of the operating system from the registry to the file system, and to kernel layers. "Part of the advantage of UAC is precisely the difference between standard and administrator privileges, such that any action that cannot be handled by a standard user must be handled by a user with administrator rights," Microsoft added. "A key goal of UAC in Windows Vista is to help nudge Independent Software Vendors towards designing applications that function in standard user mode." Unlike Windows XP, which was generally run with administrative privileges even for standard users, Vista and UAC limit admin rights effectively, reducing the impact surface of potential attacks by locking them out of the critical areas of the platform. And believe it or not, the UAC has actually proved it's worth the trouble in a recent benchmark involving anti-rootkit solutions performed by [AV-Test](#). A total of six rootkits were able to infect Windows Vista, but not until the User Account Control had been taken out of the equation. "The review on Windows Vista included just six samples which run well on Vista, covering [two versions of the Sony rootkit (XCP/First4Internet rootkit) found on CDs and one copy of the Alpha DVD (Settec) rootkit used on the German DVD Mr. and Mrs. Smith], two versions of Hacker Defender, as well as one copy of NT-Illusion and a copy of Vanquish. These rootkits are a little older, but still work well on Vista as long as User Account Control (UAC) has been switched," AV-Test representatives Andreas Marx and Maik Morgenstern [explained](#).