

By: Apurva Ganga, Technology News Editor

[Secure by Default - Windows, Linux and Mac OS X](#)

Also Secure by Design and Secure in Deployment

The correlation between the ubiquity of the Windows operating system and the volume of attacks targeting the product, together with the platform's ill reputation for protecting end users have forced Microsoft to step up its security game. As a consequence, the Redmond company has adopted new models, strategies and best practices of building software including Secure by Design, Secure by Default, and Secure in Deployment (SD3), the Defense-in-Depth and the Security Development Lifecycle. Vulnerability statistics for Windows Vista in comparison to its predecessors revealed that the added security mitigation and the new development process are functioning in reducing the attack area on Windows. Microsoft wants now to extend its vision of security to the Internet with End to End Trust, a part of which is focused on bulletproofing platforms, from Windows to Linux and Mac OS X. "The operating system must be verifiable based upon keys stored in the hardware (e.g., 'trusted boot'). This allows the device to claim that the operating system has not been tampered with to bad effect. Note that there are other things that must be done to increase trust in the operating system. Robust implementation of SD3 remains necessary since 'trusted boot' does not by itself mean the operating system will be free from unintentionally introduced vulnerabilities," Microsoft [stated](#). A more trusted, user-oriented Internet experience with enhanced privacy is the goal of Microsoft's End to End Trust. And in this context operating systems play a critical role in the tiered architecture that connects the end user to the Internet. The Redmond company is of course not referring exclusively to Windows, or any of the desktop operating systems for that matter, but to all platforms, as users are capable more than ever to connect online via a continually growing diversity of devices. Microsoft said that in addition to OS hardware integrity checks "operating system development organizations must take steps to prevent insertion of malicious code by members of the development community. To the extent that End to End Trust has been realized, robust authentication may limit opportunities for the insertion of malware by restricting access to code bases, and auditing of internal business activities should permit the provenance of bad code to be determined, thus allowing for a more robust response process."