

Microsoft's NGSCB Integration Plans Should Simplify Security

Martin Reynolds

Microsoft's plans to integrate the Next-Generation Secure Computing Base (NGSCB) with the Longhorn operating system. This approach should make it easier to secure applications without modifications.

NEWS ANALYSIS

Event

On 4 May 2004, Microsoft announced changes to NGSCB that will integrate it closely with the forthcoming version of Windows, code-named Longhorn. This integration is designed to make NGSCB more accessible to applications without modification.

Analysis

NGSCB was originally designed to create a parallel, secured, sealed and trusted partition that ran alongside any operating system. This architecture isolated NGSCB from the Windows development process, but also required modifications to applications using NGSCB features.

Microsoft now plans to simplify implementation of NGSCB within the Longhorn infrastructure. Longhorn will provide scheduling, boot, advanced driver, and application programming interface (API) capabilities for NGSCB, simplifying the NGSCB nexus. This simplification makes it easier to develop the trusted code required by the nexus. The nexus may also be able to support Windows APIs, allowing the nexus agents to be more sophisticated, yet still be secured. The nexus maintains ultimate discipline over the secured memory partition feature to be introduced in NGSCB-capable processors, and will presumably be capable of offering strong isolation capabilities to the Longhorn kernel, further improving system security and stability.

NGSCB capability will now be potentially far more accessible to applications without modification. The more sophisticated NGSCB environment will open the door for a broad range of infrastructure components that need to be implemented in a secured environment. Network security and hard-drive encryption would, for example, be good candidates for Nexus implementation, because they cannot be compromised by a successful attack on Longhorn.

Recommendations: Gartner expects Longhorn to launch with NGSCB components that provide strong authentication without passwords — which will, for example, enable users to effectively secure laptop data. Gartner recommends that technology vendors and buyers continue to observe the progress of the Longhorn/NGSCB program and plan for availability in 2007.

Analytical Source: Martin Reynolds, Gartner Research

Recommended Reading and Related Research

- "Palladium Security's Brave New World" — NGSCB (formerly code-named Palladium) may finally deliver on the promise of a truly trusted environment inside the PC. **By Martin Reynolds**
- "How to Select a Client Operating System" — Choosing a client operating system can be difficult — and mistakes can be costly. **By Michael Silver**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509