

Symantec Norton 2010 Releases Offer 'Quorum' Security Approach

Neil MacDonald, Peter Firstbrook

Norton Internet Security 2010 and Norton AntiVirus 2010 will use "Quorum" technology, which focuses on the gray area between whitelisting and blacklisting strategies. This may supplement a global whitelisting effort.

NEWS ANALYSIS

Event

On 9 September 2009, Symantec released Norton Internet Security 2010 and Norton Antivirus 2010, which both leverage a security technology model code-named Quorum that helps identify newly generated malware. Symantec also stated that a netbook edition of its software would be available through its retail partners in select countries.

Analysis

In the face of increasingly sophisticated cybercrime, enterprises are finding that endpoint protection strategies based solely on signature-based blacklisting are often ineffective. Signatures can't keep up with the explosion in malware variants and miss targeted attacks. Whitelisting and application control technologies offer hope (see "Application Control Market Update"), but it is hard to make them work for all desktops and all users. In some cases, the whitelists are too restrictive; in others, the whitelists struggle to keep up with changing end-user workstations. In contrast to vendors that have focused on a whitelisting approach, Symantec's "Quorum" technology focuses on filling the many shades of gray between whitelisting and blacklisting by using the characteristics of executable code and the user's Web hygiene across its installed base to make inferences about a particular code's "reputation."

The idea of using community intelligence for malware decision-making is not new. Prevx has been using community ("herd") intelligence for years (see "Cool Vendors in Security and Privacy, 2006"). McAfee's Artemis and Trend Micro's Smart Protection Network also leverage cloud-based services to track executables. Eventually, all endpoint protection vendors must offer a strategy for assessing pieces of code that are not explicitly whitelisted or blacklisted.

False positives are a significant concern with this approach. If Symantec's technology offers a workable alternative to a whitelisting approach, it will put pressure on vendors trying to build proprietary global whitelists (such as Bit9 and Signacert). Nonetheless, a global whitelist built and shared by the entire security industry would be in every independent software vendor's interest. All security measures should include explicit whitelists, such as a categorized database of known good applications, identified by hash codes, digital signature or the source of the code. However, there will always be some applications that don't appear on the whitelist. The Quorum database could be used to fill this gap. We believe organizations should favor endpoint vendors that used a combination of whitelisting, blacklisting and "graylisting" techniques.

RECOMMENDATIONS

All enterprises:

- Evaluate your endpoint protection vendor's strategy regarding the use of mechanisms other than signature-based detection for the identification of malware (including whitelisting and graylisting). Exceptions are inevitable. Focus on the vendor's mechanisms for exception management and handling the gray space of unknown executable code.

Symantec customers:

- Ask for access to the Quorum database for visibility into suspected malware your enterprise might encounter (such as research, forensics and code lookup).

- Pressure Symantec to incorporate the technology into Symantec Endpoint Protection 12, or in the first maintenance release, by mid-2010.

RECOMMENDED READING

- "Application Control Market Update" — Larger endpoint protection and management providers have been entering the market for application control solutions in response to user demand for augmentation of signature-based antivirus protection. **By Neil MacDonald and Michael Silver**
- "Magic Quadrant for Endpoint Protection Platforms" — Vendors in the endpoint protection platform market are competing on the strength of non-signature-based defenses, proactive management capabilities and data protection. **By Peter Firstbrook, Arabella Hallawell, John Girard and Neil MacDonald**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

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