

Windows 7 Does it Change The Security Equation?

Microsoft Windows 7 delivers limited improvement towards addressing Enterprises issues regarding security deficiencies in Vista. Microsoft continues to rely on leading security vendors such as McAfee to secure its customers' investments in its infrastructure. Customers can fully secure their enterprises with the complete range of security products and services only available from leading vendors dedicated to security, such as McAfee.

SECURITY UPGRADES FROM VISTA TO WINDOWS 7

With Windows 7, Microsoft offers its customers an upgraded Vista operating system ("O/S"). Vista is widely viewed as having security deficiencies, and has been a key reason that Microsoft has consistently been the vendor with more public exploits than any other.¹ Windows 7 delivers improvements to the areas their customers regarded as the most serious of these deficiencies. In particular, with Windows 7 Microsoft has introduced:

- **Bitlocker 2.0 and Bitlocker-to-go** – Microsoft's users requested a way to keep sensitive data on all of their USB storage devices. In Windows 7, Microsoft extended BitLocker drive encryption support to removable storage devices, such as flash memory and portable hard drives. Microsoft calls this Bitlocker-to-go.
- **AppLocker** – Responding to strong user demand to address a key shortfall in Vista, Microsoft introduces its first set of white-listing capabilities. AppLocker provides some measure of control for IT administrators in helping them eliminate unknown and unwanted software in their environment.
- **Windows Filtering Platform (WFP)**. WFP allows Microsoft firewall to better co-exist with 3rd party firewalls by taking advantage of aspects of the Microsoft Windows Firewall in their own products. They can selectively turn parts of the Windows Firewall on or off, enabling the customer to choose which software firewall they want to use and have it coexist with Windows Firewall. This feature was actually already in Vista, but Microsoft didn't market it, apparently expecting that users would simply use the Microsoft firewall. However, they are now actively marketing this feature which tacitly acknowledges the strong preference on the part of Microsoft's users for using third-party firewalls.

Microsoft has also delivered a few other potential security efficiencies, including:

- Direct access, always on VPN access without having to retype credentials

¹ X-Force 2008 Trend Statistics, IBM

Windows 7 Security Features Assessment

Bitlocker 2.0

- No central management
- No content or context aware encryption
- No granular device and port control
- Active Directory ("AD") schema extension and domain membership is a must for backing up password to AD.

Bitlocker-to-go

- Provides read-only support for XP and Vista
- No bio-metric support
- Restrictions around certificate support for authentication
- No granular control

AppLocker

- Weak trusted update model
- Central management requires GPO management and WMI scripting expertise.
- No support for Java and Non-Windows Scripts (i.e. Perl)
- No granular control

Multi Active Firewall Policies

- No central policy management
- Relies on 3rd party Vendors adopting the Windows Filtering Platform which is highly unlikely.

- Biometrics – tied the biometric scanner into the O/S
- System restore – backup & recovery function, augmented by adding the ability to select applications within a time designated backup. I.e., much greater granularity on restore version

While Microsoft has delivered a solution which is effective for a SoHo (Small Office, Home Office) customer, the security enhancements to Windows 7 are less likely to meet the needs of larger companies, even Small and Medium Enterprises.

- Bitlocker 2.0 and Bitlocker-to-go offer limited authentication support, and there are certain restrictions around using certificates for smartcard authentication. The encryption speed is slow, and highly dependent on the type of USB stick, requiring up to two hours to encrypt a 50 gig removable drive. In this early implementation, key aspects of these features, such as set up, administration, and password recovery are cumbersome and have practical limitations.
- AppLocker has a weak trusted update model and the management of this feature can be taxing; particularly in contrast to mature security products such as ePolicy Orchestrator and McAfee Application Control.
- It is unlikely that customers would replace their current, proven 3rd party firewalls with Microsoft's since they offers no compelling reason to switch.

MICROSOFT WINDOWS 7 SECURITY FEATURES & FUNCTIONS VS. MCAFEE

Key Function	Microsoft	McAfee
Central management	Forefront/Stirling through <i>Microsoft System Center Operations Manager</i>	ePolicy Orchestrator ("ePO") – comprehensive, integrated security management platform
Central Compliance Reporting	Reporting limited to Microsoft Endpoint solutions	ePO provides integrated, centralized compliance reporting, dashboards and metrics
Central Deployment	SMS, Group Policy Objects, WMI scripting	ePO
Zero-day protection	Signature based anti-malware provides limited Zero-day defense Windows Firewall	Behavioral and signature based anti-malware Artemis near real-time protection HIPS providing behavioral protection, vulnerability shielding and buffer overflow protection Fully integrated host based firewall All combined in ePO with central deployment and reporting
Application Control	AppLocker support is limited to Executable, installer, script and DLL rules under Windows 7	McAfee Application Control (MAC) offers Change and Application Control, covers Microsoft as well as other scripting languages such as Java and Perl. It also provides memory protection, excellent manageability and Change Control support. MAC covers non Microsoft platforms.
File Integrity Monitoring & Change Control	None	McAfee Change Control
Granular Device Control	Only supports software based encrypted USB drives under Windows 7 Ultimate/ Enterprise.	McAfee offers Granular Device and port control based on Device ID, Serial ID, Device Type, etc. McAfee offers content and context aware encryption control.
Endpoint Encryption Solutions	<u>Bitlocker Drive Encryption</u> - Win 7 Ultimate/Enterprise, and Windows 2008 R2 <u>Bitlocker for Vista</u> Ultimate/Enterprise and 2003 Server <u>Bitlocker-To-Go</u> Windows 7 only	Complete Endpoint Encryption Solution for Managed and Unmanaged Systems, File and Folders, Removable Media, Mobile and Virtual Disks
Policy enforcement and Management	Only provides Software based Read/write encryption support on Windows 7 Ultimate and Enterprise. Inconsistent user experience under legacy OS for Bitlocker encrypted USB drives	Supports MXI and SanDisk Hardware encrypted USB Provides central management for Software Portable Endpoint Encryption on any USB device
End Point Protection	Ant-Malware, Firewall, Encryption for Microsoft infrastructure	Anti Malware, Firewall, Encryption, behavioral protection with HIPS(including buffer overflow protection), DLP

VISTA SECURITY DEFICIENCIES PERSIST WITH WINDOWS 7

Zero day vulnerabilities continue to appear with Windows 7 as they did with Vista. One [recent](#) vulnerability provided potential hackers with the ability to launch successful Denial Of Service attacks. These vulnerabilities require layered security approach and are best protected by technologies such as Host Intrusion Prevention Systems; a technology that is not part of Microsoft's offering.

The default User Account Control ("UAC") setting can allow applications to turn off the UAC functionality or make changes without notifying the user. With Multi-Active Firewall Policy Support, certain applications which are digitally signed are fast-tracked through UAC by default to reduce unnecessary user interaction. If the third-party application calls on malicious code "by proxy" through an existing Windows application which never invokes the UAC prompt — i.e., application piggybacking — then the malware can be automatically elevated to administrator user status which in turn allows it full, unrestricted access.

Microsoft Windows 7 provides limited progress in addressing their customers' issues regarding Vista security deficiencies and still leaves a number of security gaps.

Microsoft customers still need third-party security providers to secure their investments in Windows 7. Indeed, Microsoft's Windows 7 site explicitly recommends their customers use a 3rd party AV solution. See their recommendation at:

<http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx>

MICROSOFT IS NOT A SECURITY VENDOR

What Microsoft has not done is to broaden its presence in the larger security arena. When it comes to security, Microsoft believes that there is an overhead cost to being in the operating systems business, which requires them to invest in certain baseline security features within their operating systems, as the operating system provider. Security at Microsoft is a platform function — embedded in Operating System and from their perspective, "security" is what's in Windows.

Indeed, Microsoft has invested in standalone security products/services to protect and enhance its core franchise, and help their customers secure their investment in Microsoft infrastructure, not to help them secure their overall enterprises:

- Frontbridge — SaaS spam filtering business acquired to further enhance the leadership position of Exchange, already a \$1BB+ business;
- Internet Security and Acceleration ("ISA" - later integrated with Whale Intelligent Application Gateway) was a critical security product to enable remote access, clearly core to Microsoft's business;

- Server side (Sybari) and consumer (GeCAD Software Srl) anti-virus acquisitions were made to both backfill missing AV functionality into Microsoft's core products and to bring in needed engineering expertise. While these acquisitions did enhance the Windows platform they also extended support for third-party anti-virus vendors which Microsoft recognized were critical team members to orchestrating successful Microsoft deployments.

These investments have now been wrapped into Forefront (and the impending Stirling release which provides better integration and a central management server) but are designed as means of securing Enterprise-class customers' investments in Microsoft infrastructure – i.e., client, server (Exchange, Sharepoint, and Office Communication Server) and network edge — not to secure the overall Enterprise.

Even Microsoft Security Essentials (MSE) which replaces its traditional subscription-based AV offering (Windows Live OneCare), and which will be offered free of charge, is much narrower in scope than the consumer offerings of leading AV vendors such as McAfee. MSE will offer just anti-malware, while McAfee includes: parental controls, photo backup, firewall, anti-adware, etc. Not surprisingly, Amy Barzdukas, Microsoft's Senior Director of Product Management, said MSE is specifically aimed at the desktops with no purchased AV. Presumably Microsoft's motivation is to improve the user experience of Windows customers who will not, or cannot, purchase AV.

For Microsoft, security is not a logical extension of their primary business. They are in the operating system, desktop suite, and tools businesses (to allow for development in and around their operating systems). Their core business has very deliberately expanded into Web, Exchange, collaboration (Sharepoint, Live Meeting), and DataBase Management Systems. Security is very much an afterthought.

Microsoft also recognizes that their business model is incompatible with building a comprehensive security business. They would need to build a real time threat awareness capability on a global basis. They would need to proactively integrate their products and services with those of the other leading security vendors. They would need a separate, comprehensive security infrastructure to manage the businesses' overall security across the network, endpoints, data, and compliance in a single console.

Microsoft is not in the business of security. It does not aspire to be in the business of, nor realistically can become a leading security vendor.

Microsoft seeks to secure its customers' investment in Microsoft infrastructure

Dedicated security vendors such as McAfee provide the comprehensive set of security products & services required to secure the total enterprise

- ✓ Firewall
- ✓ Endpoint Protection
- ✓ Intrusion Prevention Systems
- ✓ eMail Security
- ✓ Data Security
- ✓ Web Security
- ✓ Vulnerability management
- ✓ Encryption
- ✓ Network Access Control (NAC)
- ✓ Policy & remediation

And make significant and ongoing investments in:

- ✓ Global threat intelligence
- ✓ Leading edge security threat identification and counter-measure technology

EFFECTIVE SECURITY IS MORE THAN ANTI MALWARE AND ENCRYPTION

Securing the total enterprise requires a breadth of coverage and depth of capability in the security arena that Microsoft simply does not have. Specifically:

- 24x7 global threat intelligence – a dedicated team of expert researchers that correlate events from around the world and track attacks in real-time
- Comprehensive set of security components and services, which are tightly integrated and interlocked within and across the set of components
- The ability to correlate events from each security component –e.g., endpoint, network, etc
- A layered security architecture to assure that breaches on one level are ultimately thwarted at another level
- Central management console and reporting, such as provided by McAfee’s ePolicy Orchestrator
- State-of-the-art technology embedded in the key features and functions such as: content and context aware encryption, central enforcement of granular device and port control, zero day protection, and data loss prevention

Microsoft lacks nearly all of these capabilities. As a result, Microsoft is continuing its strong support of, and in-depth working relationships with, leading security industry vendors.

PARTNERSHIP BETWEEN MCAFEE AND MICROSOFT SECURES THE ENTERPRISE

Today, the dynamics of the security industry degrade the usefulness of customers’ investment in Microsoft infrastructure.

- There are a 100+ security vendors across 11 major categories of security products. This proliferation of most point solution vendors makes it extremely difficult to create an integrated, interlocked security infrastructure.
- Industry fragmentation creates seams in what needs to be an otherwise impenetrable [security] fortress around the enterprise.
- There are almost no security management platforms which can integrate and effectively manage a patchwork of solutions from multiple vendors.
- Too often designing, building, and managing a security infrastructure becomes a drain on the enterprise, taking disproportionate amount of IT resources while hampering the ability of the business to invest in IT as a strategic weapon for success.

McAfee works with Microsoft to secure their customers’ total business

McAfee

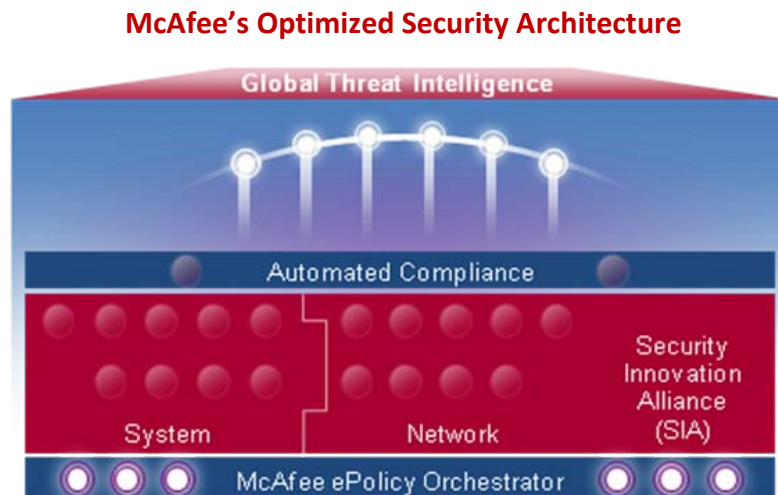
- ✓ **Comprehensive suite of security products.**
- ✓ **Optimized multi-layered architecture.**
- ✓ **Integrated compliance.**
- ✓ **ePolicy Orchestrator centralizes open security platform.**
- ✓ **Security Innovation Alliance of vendors using ePO as an integration point.**
- ✓ **Working with Microsoft to secure Microsoft infrastructure and the total enterprise**

These industry dynamics are deeply troubling to most enterprises seeking effective answers to a dizzying array of evolving security threats.

- The volume and velocity of external, and increasingly internal, threats is rising.
- The complexity and level of sophistication of the threat is also rapidly increasing.

The potential economic harm has escalated from troublesome spammers or modestly competent “script kiddies”, to highly skilled cyber criminals and cyber terrorists bent on financial gain or worse: economic destruction. McAfee delivers the security answers to the Enterprise with a complete suite of security products, a management platform which provides common integration for both McAfee and its ecosystem of Security Innovation Alliance partners with integrated compliance and Global Threat Intelligence -- McAfee’s Optimized Security Architecture.

McAfee’s Optimized Security Architecture delivers a total security infrastructure, in a seamlessly efficient way. This allows enterprises the freedom to innovate by enabling them to invest in IT as a competitive weapon, fully leveraging their investment in Microsoft infrastructure and as well as other vendors’ products and services.



Starting with a comprehensive System and Network suite of security solutions, and complementing it with the Security Innovation Alliance partners, McAfee creates a multi-layered architecture for the defense of your business.

By using Global Threat Intelligence (GTI) McAfee allows its customers to be predictive with real-time threat intelligence. Through GTI McAfee monitors the threat landscape so customers don’t have to. By doing so, McAfee helps organizations move to a proactive security posture.

Compliance is integrated into the security process. Whether driven by internal audits or external regulations, IT organizations spend an inordinate amount of

time collecting data and building reports to prove they have the right security measures in place. These tedious collection and reporting processes are often manual and are outside the normal IT workflow.

McAfee's ePolicy Orchestrator is the only comprehensive centralized security management platform. Siloed security products with separate management consoles create hundreds of manual hand-offs each day that tie up resources and introduce unnecessary levels of risk. To efficiently manage these security processes, the IT organization needs business-wide visibility across systems and networks, regardless of where those systems and networks are located.

The McAfee® ePolicy Orchestrator is an open security management platform, which is the integration point for McAfee system and network products, along with products developed by McAfee Security Innovation Alliance partners. With the global view that ePO offers, IT teams can simplify management and communication across security processes. Deployment and administration of these products, along with training, is greatly simplified, and the operational costs of managing security are greatly reduced. This visibility ensures that they can make decisions quickly and confidently.

McAfee' Optimized Security Architecture solves the security challenges confronting the Enterprise with a complete suite of security products, integrated into a multi-layered architecture, managed by ePO platform, with integrated compliance and Global Threat Intelligence to put the Enterprise ahead of the threat.

Microsoft continues to make progress in helping its customers secure their investments in Microsoft infrastructure.

Microsoft continues to look to, and recommends that their customers work with, leading third-party vendors such as McAfee to secure their investments in Microsoft infrastructure.

Dedicated security vendors such as McAfee are the only vendors with the comprehensive products and services to not only secure Microsoft infrastructure, but more importantly secure the total enterprise.

McAfee's comprehensive interlocked suite of security products, efficiently managed with the McAfee ePO security management platform, delivers security solutions that enable business to fearlessly invest in IT to drive success.