Choosing Secure Platforms in the Enterprise

Comparing Linux and Windows Security Head-to-Head

by Robert Frances Group, Inc.

March, 2004

ROBERT FRANCES GROUP
Business Advisors to IT Executives

Executive Summary

As Linux enters production use in enterprise environments, security is becoming an important comparison point against other platform choices for both desktop and server deployments. The greatest contention today is between Linux and Microsoft Corp.'s Windows. RFG compared the security levels of these products in the following areas:

1. **Core Platform** – The operating system and its core functionality.
2. **Deployment and Management** – Default security posture and management tools.
3. **Patch Management** – The processes involved in patch deployment.
4. **Network Layer** – Firewalling, security protocols, and integration.
5. **Application Stack** – Standard applications, such as e-mail clients.
6. **Standards Compliance** – Support for an adherence to industry standards.
7. **Certification** – Security certifications held by the product.
8. **Trusted Computing** – Support for integrity measurement and reporting for secured systems.

RFG found security levels in Linux generally exceeded those in Windows, providing a more secure and manageable environment out of the box with significantly more functionality in terms of security integration and management. Moreover, although software bugs are not unique to any one product, Linux systems are rarely the target of attacks, and those attacks tend to be limited in scope because user accounts and server applications do not (and should not) have access to the facilities viruses use to infect systems and destroy data.

Security Report Card

	Linux		Windows	
	Server	Desktop	Server	Desktop
Core Platform	A	A	B-	B-
Deploy/Managem.	A-	A-	C+	B+
Patch Managem.	A-	A	C+	C-
Network Layer	A	A	A-	A
Application Stack	A	A	A	A
Standards Compl.	A	A	B+	B+
Certification	B+	B+	A	A
Trusted Computing	C+	C+	C	C
Overall	A-	A-	B	B

There were a few exceptions, most notably Service Pack 2 for Windows XP, the current client version of Windows. This update brings Windows XP much closer to being a secure platform by default, especially at the network layer, so there is less disparity on the desktop. Microsoft also has a head start on certification efforts, although Linux is rapidly catching up and may equal Windows within the next 9 to 15 months.

On the other hand, RFG believes the new "server roles" facility in Windows Server 2003, while well-intentioned, may lull administrators into a false sense of security. Further, although Microsoft is working on the problem, the majority of Windows patches still commonly require a reboot during installation, causing system downtime and lost productivity.

Thus, RFG believes Linux is an ideal target platform from a security perspective for both desktop and server deployments, excelling in the most critical areas while promising to soon match or exceed Windows in the few areas where it is behind.

Introduction

As Linux has emerged as a mainstream operating system in the enterprise, questions have arisen regarding the security of the platform for production environments compared to other possible choices. In this paper, RFG presents a qualitative security comparison between the Linux and Microsoft Corp. Windows operating systems. In each case, RFG has presented an unbiased view and described both the strengths and weaknesses of each product.

This comparison will explore the following eight areas:

1. **Core Platform** – The operating system kernel itself, and core functionality such as user authentication, auditing, etc.
2. **Deployment and Management** – The security posture of each product in its default installation state, as well as tools and interfaces for administration tasks.
3. **Patch Management** – Responses to vulnerability announcements, and the processes involved in patch deployment.
4. **Network Layer** – Protocol support, communication controls, and integration facilities.
5. **Application Stack** – Applications often considered part of a platform, such as e-mail clients.
6. **Standards Compliance** – Support for and adherence to industry standards.
7. **Certification** – Security certifications held by the product.
8. **Trusted Computing** – Support for digital rights management and secured environments.

Microsoft produces two versions of Windows – Windows XP, which is intended for desktop deployments, and Windows Server. When these products are discussed, the specific versions examined will be Windows XP Service Pack 2, and Windows Server 2003. Microsoft has not yet released a service pack for Windows Server. When Linux is discussed, the specific distributions examined will be the appropriate desktop or server product from Red Hat, Inc. or Novell, Inc. (which recently acquired SuSE, Inc.).

Core Platform

Linux and Windows are built around fundamentally different architectures. Linux has a monolithic kernel architecture, in which device drivers, memory and process management, and networking functions are integrated in a single file. In contrast, Windows has a modular, micro-kernel architecture in which these functions are managed by separate modules. This makes it easy to adjust for hardware changes such as converting from uniprocessor to multiprocessor architectures, but security must be carefully managed in this architecture as driver installation is a potential attack vector. Linux does have a module loading facility for drivers but fundamental changes such as multiprocessing still require installing a new kernel. However, it is also possible to disable module loading entirely, which makes it much harder to penetrate the kernel itself.

The security implications of source code availability have been hotly debated. Theoretically, this allows for far more extensive and public review, so vulnerabilities should theoretically be

identified more quickly than in a closed source product. Customers may also audit the code themselves, although few of RFG's clients report doing so.

In contrast, Microsoft has stated that Open Source products are inherently less secure for exactly the same reason, because individuals with malicious intent have the opportunity to look for vulnerabilities. RFG believes this claim does not hold up. In a recent review of Microsoft's patch release bulletins, RFG found that 80% of the vulnerabilities discovered in 2004 alone were reported by third parties with no access to the source code for the products affected, and the trend in 2003 is similar. This is despite several years of supposedly aggressive and thorough internal code reviews.

Microsoft's statements rely on a concept known as "security through obscurity," a concept that cryptographers and security professionals typically distrust because disclosures threaten the security of the system. This very issue recently caused Microsoft customers trouble -- in Feb. 2004, a portion of the Windows code base was leaked on the Internet, and an exploit for a vulnerability discovered in the code was released the next day, forcing administrators to scramble to deploy a patch to fix the problem.

Both platforms provide the key Authentication, Authorization, and Accounting (AAA) features required for business use. These include the Kerberos protocol for user authentication, access control lists (ACLs) to define rights to files and system functions, and user behavior auditing. Both platforms also provide public key infrastructure (PKI) facilities, cryptography application programming interfaces (APIs), and the ability to encrypt filesystems.

Windows has an advantage in the area of encrypted filesystems. Although there is only one choice available in Windows, Microsoft's Encrypted File System (EFS), it performs well under most circumstances and supports directory lookups to obtain X.509 public key certificates from a user's profile. There are several options available for Linux, the foremost of which are CryptFS and Transparent Cryptographic File System (TCFS). However, these can be more complex to set up and, unless properly configured, may not perform as well under high workloads. It is also more difficult to configure these facilities to use directory services for key lookups.

Finally, Linux has a big advantage over Windows because it includes a mechanism called Pluggable Authentication Modules (PAM). PAM is an extensible authentication layer that provides applications with the same authentication API regardless of the actual authentication mechanism used. PAM-aware applications can be connected to database or directory servers, traditional "flat files", Kerberos, and SecurID and biometrics facilities without requiring application-specific configurations. Linux also supports a kernel-oriented security module layer called Linux Security Modules (LSM). LSM is a counterpart to PAM; where PAM can authenticate a user, LSM can control that user's access to system resources, such as files, network facilities, and system devices.

Bottom Line for the Core Platform

Linux receives high marks because its code is subject to public scrutiny, its PAM and LSM facilities are extremely powerful, and it is possible to disable loadable modules entirely. Areas of improvement include development of more LSMs and enhancing encrypted filesystem support. Windows is ahead in the area of encrypted filesystems, but loses points because of the lack of extensibility in its security architecture and its troubling reliance on security through obscurity.

	Linux		Windows	
	Server	Desktop	Server	Desktop
Core Platform	A	A	B-	B-

Deployment and Management

There is significant variation in the packaging of each product. Windows is an integrated product produced by a single vendor, and ships with a number of core components such as Internet Explorer (IE). In contrast, Linux is typically obtained in the form of a "distribution," a package that includes the Linux kernel, tools from the GNU project, and products such as the Mozilla Web browser. These products are functionally separate components that may be removed or simply not installed without affecting the functionality of the system. Although the tight integration of products such as IE in Windows may enable certain features such as application embedding, from a security perspective this approach has distinct disadvantages. Extensive feature integration is often especially inappropriate in a server environment.

Microsoft made a big step forward in Windows Server 2003 with the introduction of a concept known as "roles." Until a role, such as "File Sharing" or "Web Serving," is added to the system configuration, it will not provide those services, and new server installations have all roles disabled by default. However, ten network ports still remain open for services such as Remote Procedure Call (RPC), the source of several critical vulnerabilities in the past year. It is extremely difficult to deploy a functioning Windows system with no ports open. This incomplete execution of the roles concept can leave administrators with a false sense of security.

In contrast, most Linux distributions can be deployed with absolutely no services enabled by default, and administrators may then deploy and protect only the specific application the server is intended to run. And, while there are checklists available for both operating systems that guide administrators in locking the systems down, there are also tools available for Linux that automate this process, such as Bastille, as well as distributions that are security-hardened by default, including Adamantix, OpenWall, EnGarde, SELinux.

On the desktop, Windows fares a bit better, provided customers are up to date. Windows XP Service Pack 2 includes a number of improvements, the most critical of which are restricting features such as Universal Plug-and-Play (UPnP) to the local network, making it more difficult to execute buffer overflow exploits, and making security a very visible issue through a new Security Center console. Microsoft also revised the RPC layer to improve its security, although RPC is still enabled by default.

Unfortunately, both Windows versions continue to hide their internal operations from administrators. The Microsoft Management Console (MMC) and binary registry database were designed with good intentions to simplify user interfaces and consolidate application and system configuration information in a single location. However, these design choices place layers of abstraction between the administrator and the operating system. Few Windows administrators truly understand the relevance of even a fraction of the keys in the registry, or even that layers such as the Portable Operating System Interface (POSIX) exist, a standard removal item on the Windows 2000 security hardening checklist. This makes it difficult for administrators to proactively develop their own security rules, forcing them to rely solely on Microsoft for advice regarding how to harden their systems.

On Linux, configuration information, driver files, network facilities, and process data is exposed to administrators through a direct command-line driven interface grounded in over 40 years of evolution. Although command-line interfaces are rarely described as beautiful or highly integrated, administrators can view and address security management issues directly. Security personnel with Unix skills do tend to command higher salaries, and this often worries IT executives.

However, in past studies in which RFG has examined this point, RFG found that these administrators are often much more productive, as their skill sets are harder won and thus tend to be more complete, and they can typically manage more systems in less time than their Windows counterparts. Further, security patching in Windows still generally requires a reboot. Although Microsoft is working on this problem, the disproportionately larger number of reboots for Windows compared to Linux patches drives up patch testing and deployment times and application downtime, and thus total cost of ownership (TCO), in Windows environments.

Linux also provides two security facilities not present in Windows, support for "jailed" services and User-Mode Linux. Both are designed to allow administrators to deploy applications such as a Domain Name Services (DNS) server or message transfer agent (MTA) in an isolated environment on the system. Even if an unpatched vulnerability is exploited, the intruder will have no access to the rest of the system, and will thus be unable to attack other services or gain elevated privileges.

Finally, third-party tools to provide antivirus, file integrity, vulnerability scanning, and other features are available on both platforms. The only difference is the cost associated with each product, as there are a number of Open Source security products available for Linux.

Bottom Line for Deployment and Management

Linux is an excellent choice in terms of deployment and security management, but the very number of choices in each area can be daunting, and this will hold it back to some degree until the best choices in each area become clearer through best practices. Windows Server 2003 is unfortunately still far behind the pack, and its primary redeeming feature, server roles, can give administrators a false sense of security. In contrast, Windows XP SP2 goes a long way to improving the security of the platform.

	Linux		Windows	
	Server	Desktop	Server	Desktop
Deploy/Managem.	A-	A-	C+	B+

Patch Management

Patch management is a special case of system administration and management and has important security implications. Unpatched systems are the most common vectors for intrusions and infections by Internet worms and Trojan horses. On the server, reboots and unexpected patch side effects can result in downtime and possibly lost revenue. On the desktop, users are rarely security-savvy and do not spend their time perusing software vendor security portals looking for patches to install. Despite this, administrators are often (rightly) reluctant to enable automatic update facilities because this prevents them from testing the patches, leaving the company exposed to faulty patches that may create new problems.

New products from Microsoft promise to improve the situation in Windows, especially Windows Update Services (WUS), which will allow administrators to test patches before deploying them to internal systems. Unfortunately, WUS will not be released until at least the end of 2004, and the current option, Software Update Services (SUS), falls short on management controls and scalability, and only addresses a limited set of products and patches. Also, although Microsoft is working to improve this situation, the majority of Windows patches still require system reboots, and Microsoft has only planned to reduce this number by 30% in 2004.

Linux patch management solutions vary by distribution vendor, but the two most common, from Novell and Red Hat, both provide automated distribution options that can be cached on local repositories, like WUS, allowing administrators to test patches before deployment. Moreover, only kernel patches require reboots during installation, and the majority of "Linux"

vulnerabilities have actually been in secondary products such as the Apache Web server or the Sendmail message transfer agent (MTA), not in Linux itself. Administrators can thus deploy patches without reboots in many cases by simply restarting the affected service, eliminating the typical 3-8 minute reboot cycle.

Microsoft's claim that the availability of the source code for Linux makes it more vulnerable is patently untrue. Microsoft has more enemies, and it is these individuals that produce the viruses that exploit vulnerabilities. There are currently thousands of Windows viruses, and as many as a dozen have caused significant grief for enterprise users in the past two years. In contrast, there are very few Linux viruses, and those that have been discovered have caused much less grief, even in enterprises with extensive Linux deployments.

It is also much more difficult to write viruses for Linux, as many of the more popular mechanisms for their actions, such as e-mail client scripting services, either do not exist or were designed to be inherently secure. There is no guarantee that Linux will remain below virus writers' radar screens, but there certainly is some return on investment in spite, if only through avoiding it. RFG also finds it disappointing that the majority of patches Microsoft has released in the past two years have credited third parties for the discovery of the vulnerabilities involved, despite Microsoft's supposedly extensive internal code audits and developer education. Clearly, closed source is no guarantee of increased security.

Bottom Line for Patch Management

Windows requires substantial improvements before it will be on a par with Linux, and desktops receive the lowest score because of the high cleanup costs many companies have experienced dealing with viruses. Linux lacks uniformity between distributions but otherwise does well, and fares slightly better on desktops because the ancillary services such as Web serving that are the primary targets for Linux attacks are generally deployed only on servers.

	Linux		Windows	
	Server	Desktop	Server	Desktop
Patch Managem.	A-	A	C+	C-

Network Layer

The core of any networking layer in a modern operating system is its ability to control and restrict network traffic flow, and in this Linux excels. Linux includes a filtering facility called "netfilter" that is both modular and extensible and includes over 50 core modules that handle

logging, network address translation, packet matching via a range of rules, and so on. In fact, this facility is more powerful than many commercial firewall and router products.

Windows does not provide nearly this level of functionality, but it does provide two redeeming features. First, virtual private networks (VPNs) based on the IP Security Protocol (IPSEC) are easier to configure in Windows, as this functionality is provided in Windows itself, not an add-on product as in Linux. On the other hand, the dominance of enhanced VPN clients in the enterprise, such as that from Cisco Systems, Inc., which are available for both Linux and Windows, makes this a minor issue. Second, some additional firewalling facilities are available in an add-on Microsoft product called Internet Security and Acceleration (ISA) Server, although this product's firewalling facilities are still not as powerful as netfilter.

In all other areas, Linux and Windows are comparable. Third-party tools to provide antivirus, file integrity, vulnerability scanning, and other features are available on both platforms, as are support for encrypted data streams via Secure Sockets Layer (SSL). Both platforms provide directory services functionality, Linux in the form of OpenLDAP and Windows in the form of Active Directory Services (ADS). Finally, both platforms provide remote administration interfaces. There may be differences in terms of the configuration interfaces and costs for each of these facilities, but from a purely security-oriented perspective, these are generally insignificant.

Bottom Line for the Network Layer

Both operating systems are comparable in this area. The firewalling facilities in Linux exceed those in Windows 2003 Server, but these are unlikely to be used as extensively in desktop systems. Also, it is somewhat easier to configure an IPSec VPN in Windows out of the box, but because of the dominance of specialized clients in the enterprise, and because they are available for Linux, this is not a significant difference.

	Linux		Windows	
	Server	Desktop	Server	Desktop
Network Layer	A	A	A-	A

Application Stack

As in the network layer, in these areas, Linux and Windows are generally comparable. Neither Linux distribution vendors nor Microsoft should be held accountable for security vulnerability in

products produced by other vendors simply because they are available for Linux or Windows. This comparison will thus focus on differences specific to Linux and Windows themselves.

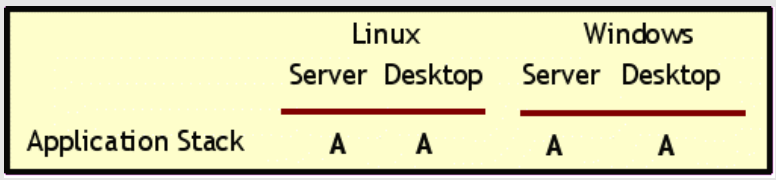
It is a common myth that Linux is invulnerable to viruses and worms, especially now that viruses are typically macros or scripts that propagate via vulnerabilities in script-enabled e-mail clients or Web browsers. However, many Linux applications do not yet support these interfaces, so for the time being it is true that it is more resistant to them, if only by virtue of not supporting the facilities that provide these attack vectors. Moreover, nothing prevents a Linux file server from being used as a storage point for a document-borne virus between two Windows clients. Antivirus best practices thus apply almost equally in both operating systems.

On the other hand, as previously mentioned, patch deployment is a much more straightforward task in Linux than in Windows. Not only can this task be completely automated, it can also typically be performed without a system reboot, reducing system downtime and administrator involvement.

Finally, there are several additional layers that are more sophisticated than their commercial counterparts. These primarily revolve around intrusion detection systems (IDS), in which the Open Source Snort IDS has long been a yardstick by which commercial products are measured, and mail transport, in which the Postfix, Qmail, and Sendmail MTAs provide either more secure or functional (or both) facilities than Microsoft's version of this service. It should be said that these applications can be equally deployed on Windows, so overall, both platforms are relatively comparable in this area.

Bottom Line for the Application Stack

Both platforms are relatively comparable in this area, and security best practices are similar no matter which operating system is selected. Linux has a slight edge only in its resistance to more traditional boot-sector and other viruses that attack system-level devices, and the availability of Snort, Postfix, Qmail, and Sendmail, and since these may be deployed on Windows as well, this is only an advantage if administrators do not choose to use them.



Standards Compliance

There are a variety of standards to which an operating system might comply. Both Linux and Windows have an extensive list of these, and a number of key Linux and Microsoft developers have also participated in the creation of these standards. Moreover, some of these standards are not relevant in a head-to-head comparison because Windows is not a Unix-like operating system, and discussions of filesystem layout or the names of management tools are not relevant in this environment. However, two differences do leap out when the products are placed side-by-side.

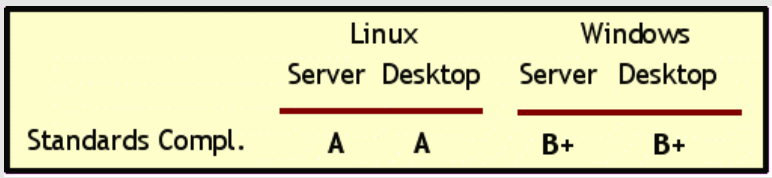
The first is Microsoft's "Embrace and Extend" philosophy, which has been endemic to its development efforts since the company's inception. Microsoft consistently develops products that comply with standards but provide additional functionality, and has been accused of doing so in its support of Java, Lightweight Directory Access Protocol (LDAP), HyperText Markup Language (HTML), and many other standards. Microsoft's stated reason for doing so has always been to provide additional functionality for administrators and developers. However, by creating supersets of existing standards Microsoft has set traps for developers that use these "features," preventing them from easily migrating their applications to other platforms.

The second issue is Microsoft's Shared Source model. This was initially created in response to criticism that inability to review the source code for the vendor's products to verify application compatibility with certain less than adequately documented APIs. Microsoft often compares Shared Source to Open Source, trying to highlight its benefits over the completely open model. However, no matter what it does, Microsoft will not accept code changes from external sources. Once a product reaches the end of its support life, it is completely dead to new development. Customers that may still be using these products could be left unable to respond to security vulnerabilities or driver support issues. They are also left to the whims of Microsoft's upgrade cycles; Microsoft has in the past been criticized for placing products on end-of-life status to force customers to upgrade more quickly than they might otherwise have done.

Finally, it must be said that Microsoft's continued and dogged dedication to a Windows-only strategy is making less sense every year. Operating systems are rapidly becoming a commodity in enterprise environments, as cash-strapped IT departments renew their focus on an application-oriented, services-delivery model. The lock-in produced by this philosophy is one of the top 3 factors listed by RFG clients considering Windows-to-Linux migrations, as it prevents IT departments from being elastic and flexible in responding to evolving business application requirements and even more rapidly growing security concerns, especially in e-commerce environments.

Bottom Line for Standards Compliance

Linux receives an top marks because standards compliance is its primary development model; new features and fundamental changes are often made solely to support new standards. Windows receives a B+ because it does indeed support a wide range of standards, but Microsoft has historically and continues to use its Embrace and Extend strategy to increase customer lock-in on its platform.



	Linux		Windows	
	Server	Desktop	Server	Desktop
Standards Compl.	A	A	B+	B+

Certification

Ironically, security certifications is one area where Linux still lags Windows. The reader should note that this does not necessarily mean Linux does not comply with the standards. Because Linux is neither developed nor backed by any one company or organization, it is often difficult for the community to raise the funds to submit the platform to often-expensive testing services.

Windows holds a number of security certifications, including the Common Criteria (C2) Common Access Protection Profile (CAPP) Evaluation Assurance Level (EAL) 4, both Common Criteria (C2) and the U.S. Department of Energy (DOE) Common Operating Environment (COE). CAPP and COE are the most critical for operating systems as they are often used as criteria for acceptance of a product in many government bodies and some large enterprises.

A number of commercial vendors as well as the U.S. National Security Agency (NSA) have recognized and worked to address this issue. Due to recent efforts by IBM Corp. and Novell, Linux has obtained CAPP EAL3+ and COE certifications, and efforts continue to help it attain CAPP EAL4.

The only other difference is that as a single vendor, Microsoft receives all vulnerability reports for its products, and it has worked diligently with security research firms to limit vulnerability disclosure until it has remedied the problems in question. In Linux, vulnerabilities are instead reported publicly to the developers, typically on security-focused mailing lists. Although these vulnerabilities are invariably fixed almost immediately after they are announced, there is still the chance that this public disclosure could lead to an exploit being released before a patch can be deployed.

Bottom Line for Certification

Linux still lags Windows in this area. However, it has come a long way in the last two years, and several companies have thrown their resources behind these efforts. Linux should be on a par with Windows within the next 9 to 15 months.

	Linux		Windows	
	Server	Desktop	Server	Desktop
Certification	B+	B+	A	A

Trusted Computing

Trusted Computing is a new concept wherein system hardware and the operating system collaborate to prevent unauthorized applications from executing, and in some cases to provide additional security mechanisms for data as well.

At this time, there is no clear standard for trusted computing. The Trusted Computing Platform Alliance (TCPA), whose founding members were Compaq (which has since merged with HP), Hewlett-Packard Corp., IBM, Intel Corp., and Microsoft, has been developing standards such as the TCPA Software Stack (TSS) and Trusted Platform Module (TPM). Microsoft's plans are also wrapped in an overarching strategy called Palladium, which it recently renamed Next-Generation Secure Computing Base for Windows.

Some vendors such as IBM have ambitiously begun releasing products such as encryption devices that comply with these standards. However, because all of these standards are still very early in their lifecycle, it is too early to tell which way the industry will go as trusted computing initiatives pick up speed. RFG believes IT executives should revisit this issue every 6 months to monitor the evolution of these standards and determine the appropriate time to make technology or vendor selections.

Bottom Line for Trusted Computing

Neither platform provides usable Trusted Computing functionality today, so both receive low marks, although these grades reflect more the state of the industry than any lack of interest or effort by developers on either side. Linux receives a slight edge over Windows because it is less likely to take an Embrace and Extend approach, and will most likely contain only standards-compliant functionality.

	Linux		Windows	
	Server	Desktop	Server	Desktop
Trusted Computing	C+	C+	C	C

Conclusion

Maintaining system security levels has become a time-consuming and expensive task in the enterprise, and any comparison of security features between products inevitably produces heated arguments among proponents of the products in question. Overall, both Linux and Windows show clear signs of improvement over the past two years, especially with the release of and Windows XP SP2. However, Linux still receives higher marks overall, especially in areas critical in enterprise use. The Report Card uses an unweighted average for each overall grade. Weighting the grades toward deployment and patch management, the two areas that encompass the greatest cost in the enterprise, would give Linux even higher marks overall.

Security Report Card

	Linux		Windows	
	Server	Desktop	Server	Desktop
Core Platform	A	A	B-	B-
Deploy/Managem.	A-	A-	C+	B+
Patch Managem.	A-	A	C+	C-
Network Layer	A	A	A-	A
Application Stack	A	A	A	A
Standards Compl.	A	A	B+	B+
Certification	B+	B+	A	A
Trusted Computing	C+	C+	C	C
Overall	A-	A-	B	B

Ultimately, most of Windows' low marks result from security issues related to Microsoft's strategies of Windows as the only acceptable operating system, and tight integration between subcomponents. IT executives must determine whether the perceived benefits of these views of computing requirements are sufficient to offset their security implications. RFG believes Linux is generally the better choice when security plays a significant factor in the selection process.

This report was developed by Robert Frances Group, Inc. with IBM assistance and funding. This report may utilize information, including publicly available data, provided by various companies and sources, including IBM. The opinions in this documents are those of RFG, and do not necessarily represent IBM's position.