Microsoft

Microsoft® Windows Server™ 2003 Service Pack 1

Top 10 Reasons to Install Windows Server 2003 Service Pack 1 (SP1)

1. **Reduce your servers' attack surface.**
   Security Configuration Wizard (SCW), one of the new features added to Windows Server 2003 in SP1, uses an intuitive, role-based process to guide administrators through attack surface reduction. You quickly and easily disable unused services, block unnecessary ports, modify registry values, and configure audit settings easily with SCW.

2. **Help protect newly installed servers.**
   Today's security environment is a continual search for new and potentially exploitable system vulnerabilities. Post-Setup Security Updates (PSSU), another new feature for new installs of Windows Server 2003 with SP1, blocks all incoming traffic to newly installed servers until the latest patches to Windows Server 2003 can be downloaded and applied. PSSU also guides configuration of Automatic Updates at the time of first log on.

3. **Get firewall protection from startup to shutdown.**
   Windows Firewall is built into Windows Server 2003 SP1. Windows Firewall is enabled only in new installation of Windows Server 2003 Service Pack 1 or when using Security Configuration Wizard. Windows Firewall in SP1 allows fine-grained control over server and client computers via Group Policy. Moreover, Windows Firewall provides boot-time protection for new installations of Windows Server 2003 SP1, lowering the risk of attack just after a server is started up and while it is shutting down.

4. **Bolster your defenses with "no execute" hardware support and software.**
   Data execution prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits. SP1 fully utilizes the DEP capabilities built into servers by many manufacturers, augmenting that with DEP software of its own.

5. **Help protect your system services with stronger defaults and privilege reductions.**
   Services such as RPC and DCOM are integral to Windows Server 2003 and thus make an alluring target for hackers. By requiring greater authentication for calls of these services, Service Pack 1 establishes a minimum threshold of security for all applications that use these services, even if they possess little or no security themselves.

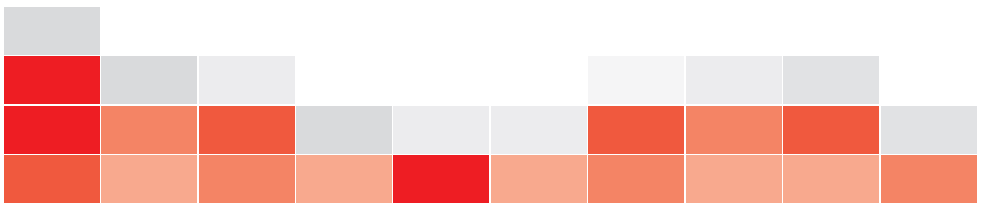
6. **Isolate out-of-date Virtual Private Network (VPN) assets.**
   VPN Quarantine automatically provides the means for limiting network access for machines on virtual private networks that are not current with regards to security updates. This prevents you from having to write your own ad hoc scripts to effect this facet of sound network security.

7. **Monitor and audit your IIS configuration settings.**
   The metabase is the XML-based, hierarchical store of configuration information for Internet Information Services (IIS) 6.0. The ability to audit this store allows network administrators to see which user accessed the metabase in case it becomes corrupted.

8. **Windows Firewall Policy Management**
   Windows Server 2003 SP1 includes new Group Policies that help IT Pros centralize client and server firewall management, including application rules, port rules, and firewall logging at the client and server to help improve security in the enterprise while maintaining centralized configuration and deployment.

9. **Secure Internet Explorer.**
   Internet Explorer now contains many enhancements to help secure Windows Server 2003. Among them, Internet Explorer more effectively stops downloads of spurious files and prevents web pages from accessing cached objects.

10. **Avoid potentially unsafe e-mail.**
    SP1 includes additional refinements to protect the network. Outlook Express now allows to you to open mail in plain-text mode, preventing HTML messages from running malicious code. Outlook Express prevents e-mail from downloading external content, thus stopping a means by which spam senders can validate your e-mail address. Outlook Express also checks e-mail attachments with Attachment Manager, eliminating the need for your own custom code to do so.



Microsoft Windows Server 2003