



WINDOWS (SERVER) WITHOUT WINDOWS

EXPLORING THE POTENTIAL SECURITY BENEFIT OF SERVER CORE

By Jeffrey R. Jones
Security Guy
(and Microsoft Director)



Table of Contents

| | |
|---|----------|
| Executive Summary..... | 2 |
| About the Author..... | 3 |
| Overview | 4 |
| Windows Server 2008 Server Core..... | 4 |
| Reduced Footprint | 5 |
| Security Bulletin Analysis | 6 |
| Final Observations | 7 |

EXECUTIVE SUMMARY

With Windows Server 2008, the Microsoft Windows Server team introduced a new installation option – Server Core.

Server Core is a “minimal install” option of Windows Server that excludes much of the GUI and many applications – such as Internet Explorer and Windows Media Player – that would be present in a default installation.

In this report, I perform a brief analysis how much smaller the software footprint is for Windows Server 2008 Server Core and examine a theoretical Server Core version of Windows Server 2003 over the past two years to gauge how much Server Core might convey in terms of reducing security updates.

My analysis found that the footprint of Windows Server 2008 Server Core is over 74% smaller than a default full installation. Further, looking at the Windows Server Security Bulletins over the past two years, 40% of them would not have applied to a theoretical Server Core build. The results of the analysis are encouraging in terms of security progress.

ABOUT THE AUTHOR

Jeff Jones is a Security Strategy Director in Microsoft's Trustworthy Computing group. In this role, Jeff draws upon his 20 years of security experience to work with enterprise CSOs and Microsoft's internal security teams to drive practical and measurable security improvements into Microsoft process and products. Prior to his strategic position at Microsoft, Jeff was the vice president of product management for security products at Network Associates where his responsibilities included PGP, Gauntlet and Cybercop products, and several improvements in the McAfee product line. These latest positions cap a 20 year hands on career in security, performing risk assessments, building custom firewalls and being involved in DARPA security research projects while part of Trusted Information Systems. Jeff is a frequent global speaker and writer on security topics ranging from the very technical to more high level, CxO-focused topics such as Security TCO and metrics.

Jeff actively encourages readers to challenge his assumptions, analysis and conclusions and provide critical feedback – but asks for equal (or better) rigor in methodology and analysis to support the challenges, as opposed to enthusiastic espousal of unsupported evangelistic fervor.

OVERVIEW

One of the things that I frequently recall from the early part of my career in Security is when we would talk about what it took to design and implement code that had “better security”, we would always come back around to “good security = good engineering”. Use effective modularity. Do single functions in one place. Provide well-defined interfaces and use them. Avoid complexity. Grant only the least privilege necessary to a given task.

That carries over to design and deployment. In security consulting, would you advise an enterprise to have their firewall be a single purpose server or multi-purpose, where the firewall also is the mail gateway? Even if the mail gateway software was not sendmail of the 1990s, you would probably still advise the single purpose server implementation.

One of the efforts in Windows Server development that seems to me to personify these principles was the Windows team efforts to increase modularity and evolve Windows Server so that a much more minimal installation could be deployed for key Server Roles. In the shipping version of Windows Server 2008, that option has been realized in the form of the Server Core installation option.

WINDOWS SERVER 2008 SERVER CORE

What exactly is Server Core? From a security perspective, the key feature is probably just general “reduced attack surface area.” The amount of code installed that the IT manager has to worry about is simply less in terms of managing security risk. I’m not claiming this was a Microsoft innovation (other operating systems have ‘minimal build’ options), but it is chock full of security goodness, nonetheless.

Much of what normal users think of as “part of” Windows is not present in a Server Core deployment. All of these are absent:

- The Windows Graphical User Interface ... gone
 - Note that a low level set of graphics and dialog capability is present
- Internet Explorer ... gone
- Outlook Express ... gone
- File Explorer ... gone
- Media Player ... gone
- much, much more ... gone
- Sound device drivers ... no longer needed

In fact, [this link](#) describes the roles that are available in Server Core:



- Active Directory Domain Services
- Active Directory Lightweight Directory Services (AD LDS)
- Dynamic Host Configuration Protocol (DHCP) Server
- DNS Server
- File Services
- Print Server
- Streaming Media Services
- Web Services (IIS, but without ASP.NET)
- Hyper-V

Those are all on top of the core infrastructure capabilities as well. You do have IPv6, the Windows firewall and the set of architectural protective mechanisms such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) and the results of the Windows Services Hardening efforts (see [this detailed post](#) by the “Ask the Performance Team” blog).

REDUCED FOOTPRINT

How much surface area reduction has occurred with Server Core? To properly answer that, we would need to do a study of the potentially exposed network services, applications and other OS components. I am not going to tackle that interesting question here, but we can do some rough checks that may be indicative.

I performed two installations of Windows Server 2008¹ in Virtual PC 2007 to try and gauge how much reduction a Server Core installation represented over a standard default installation. Results are shown in the table below:

| Installation Option | Required Disk Space |
|--|---------------------|
| Default full installation of Windows Server 2008 ¹ | 6.52 GB |
| Server Core installation of Windows Server 2008 ¹ | 1.72 GB |

¹ The RTM (release to manufacturing) version of Windows Server 2008 Standard.



At a gross level, the Server Core installation represents a deployment reduction of 74% over the standard default installation, meaning a significant portion of the default Windows Server code is not present on the disk at all.

SECURITY BULLETIN ANALYSIS

With the modularization and reduction of the Server Core installation, it seems safe to imagine that some of the future security updates might apply to a default or full installation but would not necessarily apply to a Server Core deployment.

While we have to wait for events to happen to get the full and accurate answer to that question, I believe there is an analysis we can do that may provide some insight into what the answer might be. We can:

- Using Windows Server 2008 as a model, define what a theoretical Server Core installation option of Windows Server 2003 would have consisted of
- Examine the Security Bulletin history of Windows Server 2003
- Determine what security updates would have applied to the theoretical Windows Server 2003 Server Core installation

CAVEAT: Obviously, there was no Server Core option for Windows Server 2003. This entire analysis represents a “what if?” scenario, examining the real set of Windows Server 2003 Security Bulletins and comparing against the executable and library code updated with each security update.

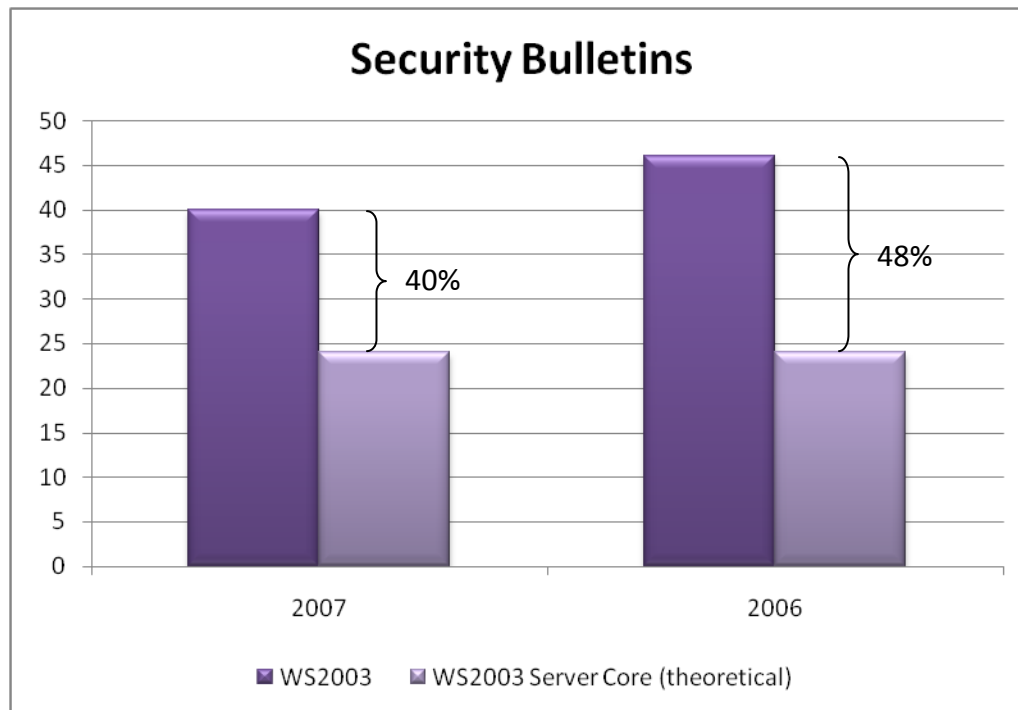
Initially, I did my own very rough analysis, simply looking at each Security Bulletin and comparing it against my high level knowledge of the applications excluded from a Server Core installation. For example, I excluded all updates for Internet Explorer. I sent it over to Andrew Mason, the program manager behind the Server Core project, to review. Andrew set me straight, in that it isn't quite that simple.

Luckily though, Andrew was willing to provide more detailed feedback and, using his knowledge of exactly which DLLs and executables were included in Server Core, examined each of the Security Bulletins affecting Windows Server 2003 during 2006 and 2007 and identified:

- **Did not apply.** Which security updates only modified components not present in Server Core
- **Fully applied.** Which security updates modified components were all components were present in Server Core

- **Partially applied.** Which security updates modified some components in Server Core and some components not in Server Core.

With this information, I was able to complete the analysis with much more confidence than I would have had in my own rough approximations. Of the 46 Security Bulletins affecting Windows Server 2003 during 2006, 22 of them did not apply to a (theoretical) Server Core build. Similarly, of the 40 Security Bulletins affecting Windows Server 2003 during 2007, 16 did not apply to a Server Core build. This is charted in the figure below.



These results look encouraging. Nearly half of the security updates released in 2006 for Windows Server would not have applied to a Server Core build and 40% of those in 2007 would not have applied either.

FINAL OBSERVATIONS

In the past, when I've produced server vulnerability scorecards, I've always compared "full Windows Server" with reduced Linux Server builds. Though Windows Server 2003 had options like Internet Explorer Enhanced Security Configuration and security professionals know to lock other components down, still the components were *there* and represent a risk that needed to be considered conservatively.

With the release of Windows Server 2008, there is now another option for administrators wanting to deploy several common roles. For those roles that can be



March 10, 2008

served with Server Core, there is a reduced footprint on the server and fewer components that need to be administered and maintained. If my analysis of a theoretical Server Core version of Windows Server 2003 for 2006 and 2007 are any indication, Server Core also represents a tool in helping manage server risk.

I am very happy that the Windows Server team made progress in making the Server product more modular and in providing a tested and supported "minimal installation" for Windows Server. With this option, combined with the security quality benefits of the applied SDL process, the defense-in-depth protective features, and other security improvements, the Server team has taken some solid steps in improving server security.