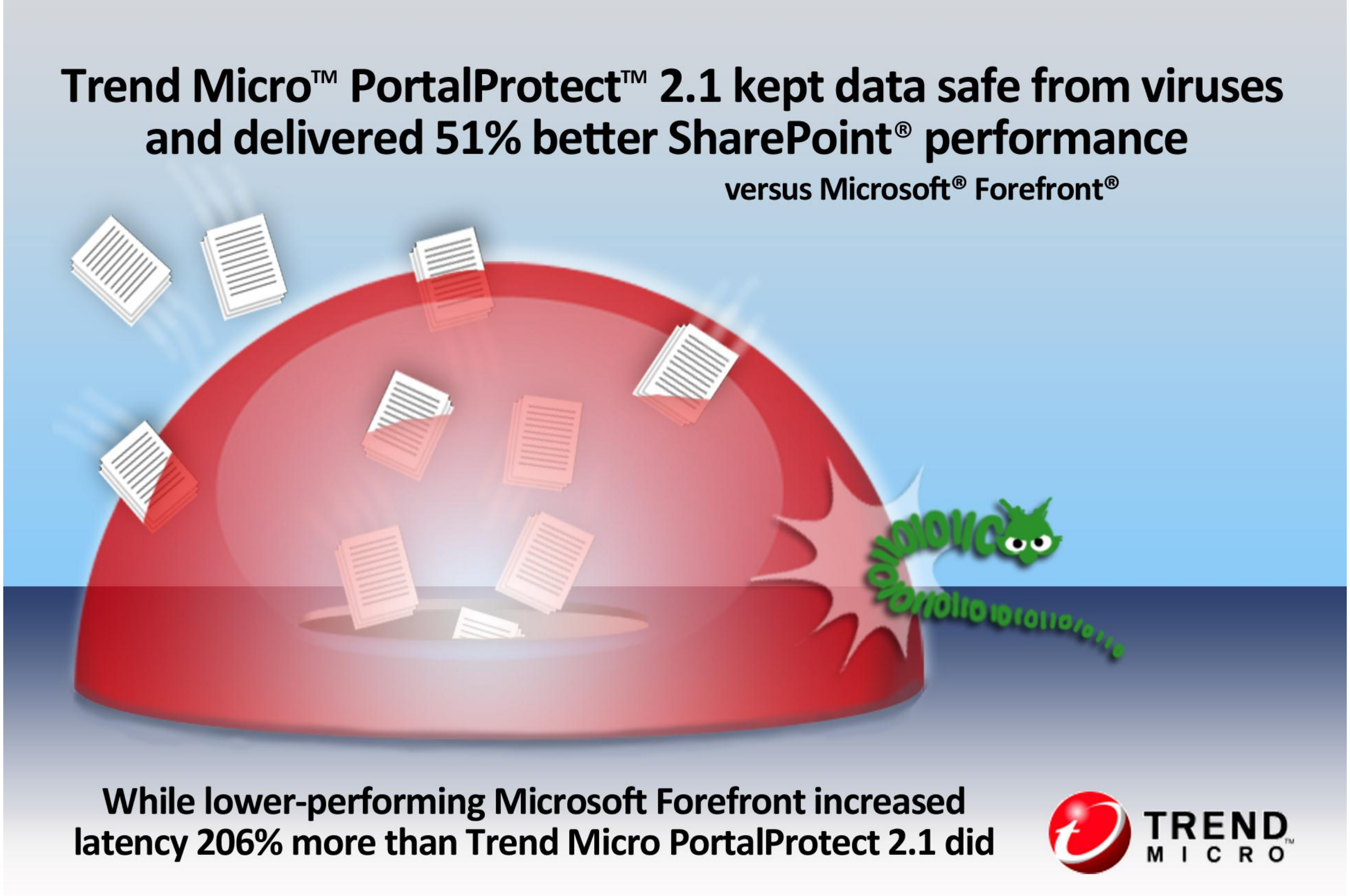
SHAREPOINT PERFORMANCE: TREND MICRO PORTALPROTECT VS. MICROSOFT FOREFRONT


Trend Micro™ PortalProtect™ 2.1 kept data safe from viruses and delivered 51% better SharePoint® performance
versus Microsoft® Forefront®
While lower-performing Microsoft Forefront increased latency 206% more than Trend Micro PortalProtect 2.1 did
TREND MICRO™

Busy organizations require two things from their IT infrastructure: great performance and reliable protection. Workers constantly access a company's SharePoint server, uploading and downloading documents through their portals. To keep the data safe, anti-malware software scans every document uploaded to the server, to ensure a safe collaborative experience. This safety, however, has the potential of reducing performance and increasing wait times (access latency) while accessing and completing SharePoint tasks. Organizations should ideally select a product that offers complete protection while causing the least amount of overhead on the server.

We compared the SharePoint performance impact of two solutions, Trend Micro PortalProtect for SharePoint 2.1 and Microsoft Forefront for SharePoint 2010. We found that SharePoint performance with PortalProtect 2.1 was **51 percent faster** than with Forefront. In addition to enabling better performance, Trend Micro PortalProtect offered a better overall SharePoint experience—running **Microsoft Forefront added 206 percent more response time** when accessing SharePoint Web data than running PortalProtect did.

JULY 2011
A PRINCIPLED TECHNOLOGIES TEST REPORT
Commissioned by Trend Micro Incorporated

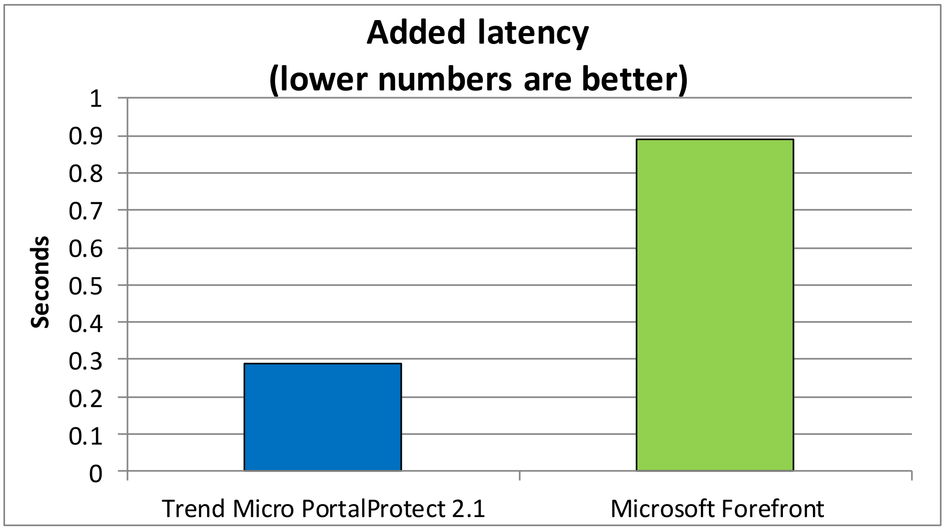
MINIMIZE RISKS

These days, access to information on a SharePoint server is not limited to an organization's employees. Increasingly, contractors, partners, and even some customers use SharePoint to enhance collaboration. While external attacks that seek to access your data are always a threat, users posting files or links on your SharePoint server can also unknowingly introduce malware to your system and could lead to data breach. Such breaches are costly for several reasons; including the severe hit consumer confidence takes when a company's data is compromised.

Big performance, little waiting

Scanning a SharePoint server for malware can often create latency, or waiting time, for users accessing their data. While we ran our performance tests, Microsoft Visual Studio® 2010 measured the latency a user would experience while accessing his or her SharePoint data. Figure 1 shows the average latency added over the baseline, in seconds, we recorded for the security solutions. As Figure 1 shows, the server running Microsoft Forefront added 206 percent more latency (waiting time) than Trend Micro PortalProtect, indicating that PortalProtect provided a better user experience. Lower numbers are better.

Figure 1: Latency added (waiting time) over the baseline using the SharePoint Web portal, in seconds, while the two security solutions scanned for viruses. Lower numbers are better.



Security, while important, should not come at the expense of performance. A security solution that keeps data safe without compromising performance is ideal for you and your users. We found SharePoint performance while running a virus scan with Trend Micro PortalProtect to be 51 percent faster than SharePoint performance while running Microsoft Forefront. (See Figure 2.)

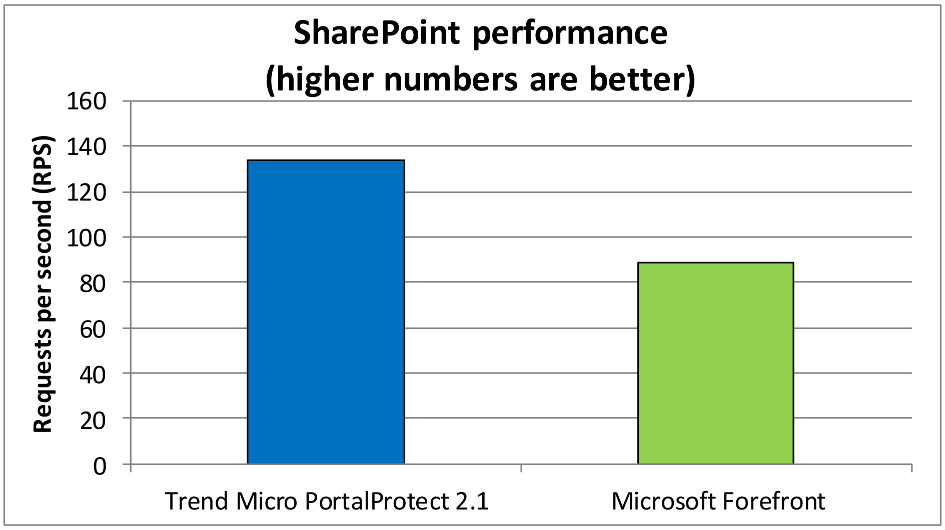


Figure 2: SharePoint performance, in requests per second, while the two security solutions scanned for viruses. Higher numbers are better.

WHAT WE FOUND

Figure 3 shows the latency results for the server, in seconds, while running no security, Trend Micro PortalProtect, and Microsoft Forefront. Lower numbers are better.

	Baseline (no security)	Trend Micro PortalProtect 2.1	Microsoft Forefront
Latency	0.25	0.54	1.14
Added latency (over baseline)	Baseline	0.29	0.89

Figure 3: Latency, in seconds, for the security solutions during our SharePoint performance tests. Lower numbers are better.

Figure 4 shows the throughput, in requests per second, we recorded for the server, while running no security, while running TrendMicro PortalProtect 2.1, and while running Microsoft Forefront in our SharePoint performance testing. Higher numbers are better, as they indicate that the server could handle more requests from users.

	Baseline (no security)	Trend Micro PortalProtect 2.1	Microsoft Forefront
Throughput (requests per second)	181.8	134.0	88.7

Figure 4: SharePoint performance, in throughput in requests per second, for the security solutions. Higher numbers are better.

Please note that when we tested Microsoft Forefront, we used the default scan setting of “Scan with the subset of engines that are available.”

WHAT WE TESTED

We used Microsoft Visual Studio 2010 to run a test that simulated 70 users simultaneously uploading documents to our SharePoint server. For these files, we generated a corpus consisting of about 7,000 files of varying types and sizes, and 43 files with various viruses. While the test was running, we recorded CPU utilization, and total requests per second on our SharePoint server using Windows Performance Monitor. We used Visual Studio's load test to record the latency. We first ran the tests with no security running to get a baseline performance score, and then tested with Trend Micro PortalProtect and Microsoft Forefront security solutions running to see the impact these anti-malware scans had on SharePoint performance.

For information about how we configured the servers for our tests, see Appendix A, and see Appendix B for detailed information about how we tested.

About Trend Micro PortalProtect for Microsoft SharePoint

Trend Micro PortalProtect secures your collaborations with a dedicated layer of protection that guards against malware, malicious links, and other threats that SharePoint administrators are often unaware of. Its Web reputation technology blocks malicious links from entering your Web portals, while its powerful content filtering and included DLP technology scan both files and Web components of SharePoint. For more information, visit http://us.trendmicro.com/us/products/enterprise/portalprotect/.

About Microsoft Forefront

Microsoft Forefront helps deliver end-to-end security and access to information through an integrated line of protection, access, and identity management products. For more information, visit http://www.microsoft.com/forefront/en/us/default.aspx.

FINAL THOUGHTS

Securing your SharePoint server against internal and external threats is of the utmost importance. Using security software to scan files for malware is necessary, but can sometimes drive down performance, increasing user frustration and decreasing productivity. Not all security software is created equal, however— choosing a solution that protects your data without hurting performance or creating significant waiting times for users is key. In our tests, we found that using Trend Micro PortalProtect 2.1 delivered 51 percent faster throughput for SharePoint, with Microsoft Forefront having 206 percent more added latency than PortalProtect.

APPENDIX A – SERVER CONFIGURATION INFORMATION

Figure 5 provides detailed configuration information for the servers we used in our testing.

Servers	Dell™ PowerEdge™ R710 (SharePoint test server)	Dell PowerEdge R510 (SQL database server)	Dell PowerEdge T410 (Visual Studio test controller)
General processor setup			
Number of processor packages	2	2	2
Number of cores per processor package	4	4	6
Number of hardware threads per core	2	2	2
CPU			
Vendor	Intel®	Intel	Intel
Name	Xeon® E5520	Xeon X5570	Xeon X5660
Stepping	5	5	2
Socket type	1366 LGA	1366 LGA	1366 LGA
Core frequency (GHz)	2.26	2.93	2.80
Bus frequency (MHz)	1,333	1,333	1,333
L1 cache (KB)	4 x 32 KB	4 x 32 KB	6 x 32 KB
L2 cache (KB)	4 x 256 KB	4 x 256 KB	6 x 256 KB
L3 cache (MB)	8	8	12
Thermal design power (TDP, in watts)	80	95	95
Platform			
Vendor and model number	Dell PowerEdge R710	Dell PowerEdge R510	Dell PowerEdge T410
Motherboard model number	Dell 00W9X3	Dell 0W844P	Dell 0Y2G6P
Motherboard chipset	Intel 5520 Chipset	Intel 5500 Chipset	Intel 5500 Chipset
BIOS name and version	Dell 3.0.0 (1/31/2011)	Dell 1.5.3 (10/25/2010)	Dell 1.3.9 (04/07/2010)
BIOS settings	Default	Default	Default with Virtualization Enabled
Memory modules			
Vendor and model number	Crucial CT51272BB1339.36SFD1	Samsung M393B5170FHD-CH9	Crucial CT51272BB1339.36SFD1
Type	PC3-10600	PC3-10600	PC3-10600
Speed (MHz)	1,333	1,333	1,333
Speed in the system currently running @ (MHz)	1,067	1,333	1,333
Timing/Latency (tCL-tRCD-iRP-tRASmin)	8-8-8-20	9-9-9-24	9-9-9-24
Size (GB)	24	24	24
Number of RAM modules	6 x 4 GB	6 x 4 GB	6 x 4 GB
Chip organization	Double-sided	Double-sided	Double-sided

Servers	Dell™ PowerEdge™ R710 (SharePoint test server)	Dell PowerEdge R510 (SQL database server)	Dell PowerEdge T410 (Visual Studio test controller)
Hard disk			
HDD #1			
Vendor and model number	Seagate ST9146852SS	Dell MBA3147RC	Seagate ST373455SS
Number of disks in system	2	2	2
Size (GB)	146	146	73
Type	SAS	SAS	SAS
RPM	15,000	15,000	15,000
Controller	PERC 6/i	PERC 6/i	PERC H700
HDD #2			
Vendor and model number	N/A	Seagate ST3300657SS	Hitachi HUS154530VLS300
Number of disks in system	N/A	4	4
Size (GB)	N/A	300 GB	300 GB
Type	N/A	SAS	SAS
RPM	N/A	15,000	15,000
HDD #3			
Vendor and model number	N/A	Seagate ST3300656SS	N/A
Number of disks in system	N/A	2	N/A
Size (GB)	N/A	300 GB	N/A
Type	N/A	SAS	N/A
RPM	N/A	15,000	N/A
Operating system			
Name	Windows Server® 2008 R2 Enterprise SP1	Windows Server 2008 R2 Enterprise SP1	Windows Server 2008 R2 Enterprise SP1
Build number	7601	7601	7601
File system	NTFS	NTFS	NTFS
Language	English	English	English
Network card/subsystem			
Vendor and model number	Broadcom® BCM5709C NetXtreme® II	Broadcom BCM5716C NetXtreme II	Broadcom BCM5716C NetXtreme II
Type	Integrated	Integrated	Integrated
USB ports			
Number	4	4	6
Type	USB 2.0	USB 2.0	USB 2.0

Figure 5: System configuration information for the servers we used in our tests.

APPENDIX B - HOW WE TESTED

Our test bed consisted of four servers—a dedicated SharePoint server, a dedicated SQL server, an Active Directory® server, and a Microsoft Visual Studio server—and an isolated network. The Active Directory server is a basic active directory domain controller set up with defaults. We gave all servers and VMs appropriate IPs and logged them in on the domain. We installed Hyper-V on the Visual Studio and ran two identical VMs with 4GB RAM, 40 GB VHD, and two virtual processors. Each VM had Visual Studio Ultimate 2010 installed, and ran the test scripts against the SharePoint server.

We used Visual Studio 2010 to run a load test that simulated 70 users, evenly distributed between two virtual machines, simultaneously uploading documents to our SharePoint server. The load test was 25 minutes long, consisting of a 5-minute warm-up time, and a 20-minute run time. We set the load test so that all users simulated utilizing LAN connections, Internet Explorer® 7, and 1-second think times. The load test ran one Web test, which simulated a user on the SharePoint default Web site uploading a single file to the shared documents library. Each iteration of the Web test used a different user pulled from a pool of 100 users we created in Active Directory, and uploaded a different document from our corpus. The Web test consisted of about 7,000 files of varying types and sizes including DOC, DOCX, GIF, HTM, HTML, JPG, ONE, PDF, PPT, PPTX, TXT, XLS, XLSX, and XML files and, additionally, 43 files with various viruses.

While the test was running, we recorded CPU utilization and total requests per second on our SharePoint server using Windows Performance Monitor. We also recorded latency using the Web Page Response Time counter in Visual Studio load test parameters. After each run, we restored the database to its original state and rebooted the SharePoint server. We conducted three runs of each configuration: no security running, Trend Micro PortalProtect security scan running, and Microsoft Forefront security scan running. We determined the median run based on the requests-per-second score from each run.

Installing Windows Server 2008 R2 with SP1

We installed Windows Server 2008 R2 with SP1 on all of our test servers using the following steps:

1. Insert the installation DVD for Windows Server 2008 R2 with SP1 into the DVD drive.
2. Choose the language, time and currency, and keyboard input. Click Next.
3. Click Install Now.
4. Choose Windows Server 2008 R2 Enterprise (Full Installation). Click Next.
5. Accept the license terms, and click Next.
6. Click Custom.
7. Click the Disk, and click Drive options (advanced).
8. Click New→Apply→Format, and click Next.
9. After the installation completes, click OK to set the Administrator password.
10. Enter the administrator password twice, and click OK.
11. Click Start, type `change power-saving settings` and press Enter.
12. Click Change plan settings.
13. Change the Turn off the display drop-down menu to Never.
14. Click Save changes, and close the Power Options, Screen Saver Settings, and Personalization windows.
15. Run Windows Update to install the latest updates.

Setting up and configuring Microsoft SQL Server® 2008 R2

After installing Windows Server 2008 R2 SP1, we used the following steps to install and configure SQL Server 2008 R2 on one of our test servers:

Installing Microsoft SQL Server 2008 R2

1. Insert the installation DVD for SQL Server 2008 R2 into the DVD drive.
2. Click Run SETUP.EXE. If Autoplay does not begin the installation, navigate to the SQL Server 2008 R2 DVD, and double-click.
3. If the installer prompts you with a .NET installation prompt, click Yes to enable the .NET Framework Core role.
4. In the left pane, click Installation.
5. Click New installation or add features to an existing installation.
6. At the Setup Support Rules screen, wait for the check to complete. If there are no failures or relevant warnings, click OK.
7. Select the Enter the product key radio button, and enter the product key. Click Next.
8. Click the checkbox to accept the license terms, and click Next.
9. Click Install to install the setup support files.
10. If there are no failures displayed, click Next. You may see a Computer domain controller warning and a Windows Firewall warning. For now, ignore these.
11. At the Setup Role screen, choose SQL Server Feature Installation.
12. At the Feature Selection screen, select Database Engine Services, Full-Text Search, Client Tools Connectivity, Client Tools Backwards Compatibility, Management Tools –Basic, and Management Tools – Complete. Click Next.
13. At the Installation Rules screen, click Next when the check completes.
14. At the Instance configuration screen, leave the default selection of default instance, and click Next.
15. At the Disk space requirements screen, click Next.
16. At the Server configuration screen, choose NT AUTHORITY\SYSTEM for SQL Server Agent, and choose NT AUTHORITY\SYSTEM for SQL Server Database Engine. Click Next.
17. At the Database Engine Configuration screen, select Mixed Mode.
18. Enter and confirm a password for the system administrator account.
19. Click Add Current user. This may take several seconds.
20. Click Next.
21. At the Error and usage reporting screen, click Next.
22. At the Installation Configuration rules screen, check that there are no failures or relevant warnings, and click Next.
23. At the Ready to Install screen, click Install.
24. After installation completes, click Next.
25. Click Close.

Configuring the databases

We stored the SharePoint databases and logs on a RAID 10 consisting of six 300GB hard drives. To maximize performance, we created the initial database files large enough that there was no dynamic growth during a test run. Each database file was set to 10 GB with the exception of the WSS Content database, which we set to 100 GB. We then created backup files for all the databases and logs to use as restore points to reset the databases and logs to their original states after each run.

Installing and configuring the Microsoft SharePoint Server 2010

After installing Windows Server 2008 R2 SP1, we used the following steps to install and configure SharePoint Server 2010 on a second test server:

Installing Microsoft SharePoint Server 2010

1. Insert the installation DVD.
2. Launch setup.exe, and click Install software prerequisites.
3. Review the list of software, and click Next.
4. Accept the EULA, and click Next.
5. When the prerequisites finish installing, click Finish.
6. On the main SharePoint installation menu, click Install SharePoint Server.
7. Enter your product license key, and click Continue.
8. Accept the EULA, and click Continue.
9. Choose the Complete server type, and click Install.
10. When the installation finishes, check the box for Run the SharePoint Products Configuration Wizard now, and click Close.
11. On the Welcome to SharePoint Products screen, click Next.
12. On the pop-up warning about services that will need to be restarted during the configuration, click Yes.
13. Choose Create a new server farm, and click Next.
14. Enter the name of your existing database server and database name.
15. Specify a username and password to connect to your database server, and click Next.
16. Enter a passphrase into the Passphrase and Confirm Passphrase fields, and click Next.
17. Leave the default settings on the Configure SharePoint Central Administration Web Application screen, and click Next.
18. Verify your settings, and click Next.
19. When the wizard has completed the configuration, click Finish.
20. Choose Run the farm configuration wizard on the Central Administration site.
21. Choose the services you wish to include in your server farm, and click Next.
22. Enter the specifications for the new site, and click OK.
23. Click Finish.

Installing and configuring the anti-virus software

Installing Trend Micro PortalProtect for Microsoft SharePoint 2.1

1. Navigate to the PP 2.1 folder, and double-click Setup.exe.
2. On the Welcome screen, click Next.
3. Accept the EULA, and click Next.
4. Choose Install PortalProtect for SharePoint server farm environment, and click Next.
5. Choose Fresh install PortalProtect 2.1.
6. Enter the Activation Code, and click Next.
7. Choose Install to local server, and click Next.
8. Leave defaults on the Configure Share/Target Directory screen, and click Next.
9. Leave defaults on the Web Server Information screen, and click Next.
10. Choose SharePoint SQL Server from the drop-down menu, enter the username and Password, and click Next.
11. Verify the SharePoint Database Access Account information, and click Next.
12. Wait for the check to Pass for new installation, and click Next.
13. Choose Use Local Server Administrator Group, and click Next.
14. Leave default settings on the Connection Settings page, and click Next.

15. Choose No, I don’t want to participate, and click Next.
16. Leave default settings on the Control Manager Server Settings page, and click Next.
17. Leave Email notification settings off, and click Next.
18. Click Install.
19. When installation completes, click Next.
20. Click Finish.
21. Open PortalProtect, and log in.
22. Click Security Risk Scan→Action, and change all the options from Notify to Do Not Notify.
23. Click Save.
24. Click Administration→Trend Support/Debugger, and uncheck all the options.
25. Click Save.
26. Check to see that all virus definition engines have updated. If not, manually update the engines.

Installing and configuring Microsoft Forefront Protection for SharePoint

1. Double-click the exe.
2. On the welcome screen, click Next.
3. Accept the License agreement, and click Next.
4. Choose the option for SharePoint stand-alone server, and click Next.
5. Choose Install to local server, and click Next.
6. Keep the default install path, and click Next.
7. Keep the default port number, and click Next.
8. Enter the user name and password for your SQL Server database, and click Next.
9. When the install is finished checking for requirements and gives a pass message, click Next.
10. Enter your domain information and Domain Admins group on the Management Group Selection, and click Next.
11. Leave default connection settings, and click Next.
12. Choose No, I don’t want to participate on the World Virus Tracking Program window, and click Next.
13. Leave defaults on the Control Manager Server Settings window, and click Next.
14. Leave defaults on the Email Notification settings window, and click Next.
15. Click Install.
16. Click Next.
17. Click Finish.
18. Open Forefront.
19. Click Policy Management→Advanced Options→Logging Options, and uncheck Enable Realtime Incident Logging, Enable Event Logging, and Enable Performance Counters. Click OK.
20. Click Monitoring→Configuration→Notifications, and disable all notifications.
21. Check to see that all virus definition engines have updated. If not, manually update the engines.

Installing and configuring the Microsoft Visual Studio 2010 server

Adding the Hyper-V role

1. Open Server Manager, and click Roles.
2. Click Add Roles.
3. On the Before You Begin page, check the Skip this page by default box, and click Next.
4. Select Hyper-V, and click Next.
5. On the Hyper-V Introduction page, click Next.
6. On the Create Virtual Networks page, click Next.
7. Confirm installation selections, and click Install.
8. Once the installation is complete, click Close.
9. When the system prompts a restart, click Yes.

10. Allow the system to fully reboot, and log in using the administrator credentials.
11. Once the desktop loads, the Hyper-V Installation Results window will finish the installation.
12. Click Close. The Hyper-V role will now be available in Server Manager under Roles.

Configuring the virtual network

1. Right-click the server name in the list on the left side of Hyper-V, and choose Virtual Network Manager…
2. Choose External, and click Add.
3. Name the Virtual Network, and choose the appropriate NIC for your test bed network from the drop-down menu.
4. Click OK.

Creating the VMs

1. Click Action→New→Virtual Machine.
2. On the Before You Begin window, click Next.
3. Enter the name of the VM, and click Next.
4. Assign 4GB of memory, and click Next.
5. Choose the virtual network you created from the drop-down menu, and click Next.
6. Create a 40GB virtual hard disk with a name and location, and click Next.
7. Choose Install an operation System later, and click Next.
8. Click Finish.
9. Install Windows Server 2008 R2 on your VM.

Installing Microsoft Visual Studio 2010

1. Add the .NET Framework feature via the server manager.
2. Double-click setup.exe.
3. Click Install Visual Studio 2010.
4. Click Next.
5. Accept the license terms, and click Next.
6. Choose the Full installation, and click Install.
7. Click Finish.
8. Copy the test files to the root of C.

Creating a second VM

1. With your original VM turned off, navigate to the VHD storage drive.
2. Create a copy of the VHD, and rename it.
3. Using the steps above, create a new VM with one exception.
4. Instead of creating a new VHD, choose Use an existing virtual hard disk and navigate to the VHD you copied and renamed. Continue the VM creation as normal.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.

Disclaimer of Warranties; Limitation of Liability:
PRINCIPLED TECHNOLOGIES, INC. HAS MADE REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF ITS TESTING, HOWEVER, PRINCIPLED TECHNOLOGIES, INC. SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE TEST RESULTS AND ANALYSIS, THEIR ACCURACY, COMPLETENESS OR QUALITY, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. ALL PERSONS OR ENTITIES RELYING ON THE RESULTS OF ANY TESTING DO SO AT THEIR OWN RISK, AND AGREE THAT PRINCIPLED TECHNOLOGIES, INC., ITS EMPLOYEES AND ITS SUBCONTRACTORS SHALL HAVE NO LIABILITY WHATSOEVER FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN ANY TESTING PROCEDURE OR RESULT.

IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC. BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH ITS TESTING, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC.'S LIABILITY, INCLUDING FOR DIRECT DAMAGES, EXCEED THE AMOUNTS PAID IN CONNECTION WITH PRINCIPLED TECHNOLOGIES, INC.'S TESTING. CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES ARE AS SET FORTH HEREIN.