



Testing the Effect of Encryption on Disk Performance

Full-disk encryption testing shows no performance
difference from systems without encryption

Contents

Executive summary	3
PassMark performance test background	4
Performance theory	5
Performance testing methodology	8
Performance test results	10
Conclusion	11

Executive summary

This report presents the results of measuring the difference in disk performance between a disk encrypted with Check Point Endpoint Security Full Disk Encryption™ and an unencrypted disk. Testing included a laptop 750MHz PIII, and a desktop PC 3GHz P4. Both of these devices ran Windows 2000 Professional SP4.

The effect of using a disk encryption product is usually negligible for a business user. Efficient encryption algorithms such as the Advanced Encryption Standard (AES) and standard powerful CPU processors in typical PCs contributed to minimal impact by encryption on overall performance. Most users will not notice a performance difference even though a certain degree of performance degradation is present whenever encryption is used. Results reported in this white paper measure actual performance effect of encryption for the two mentioned configurations.

PassMark performance measuring software (see www.passmark.com/products/pt.htm) was used to measure disk performance. We used PassMark's comprehensive test suite to measure performance of a PC where disk performance is weighted by an importance factor of 20 percent of the total performance. When running the whole test suite, the desktop configuration with Check Point Full Disk Encryption installed showed only -2.9 percent performance drop from the unencrypted configuration (see Fig. 1).

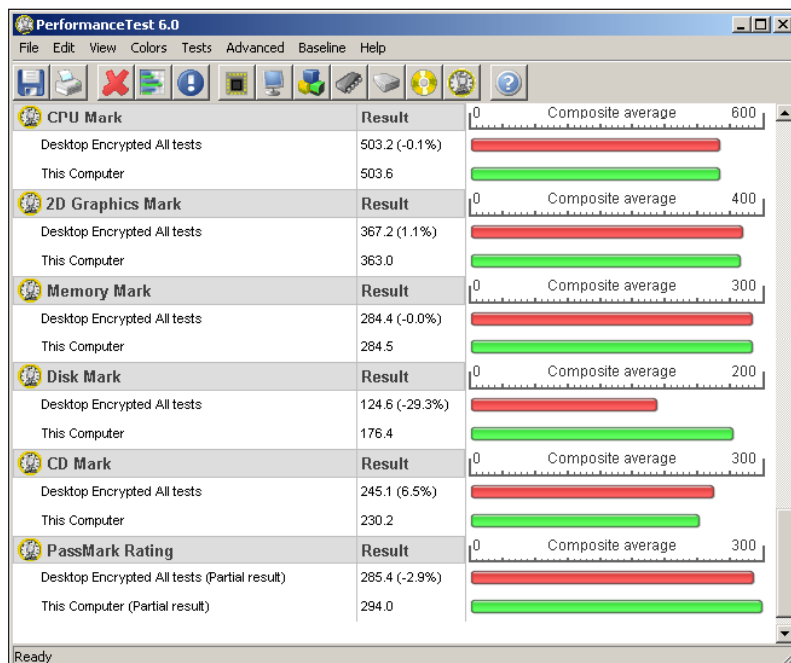


Fig. 1. PassMark rating for all tests (excluding 3D graphics)

Performance measured three types of disk operations: large file sequential read, large file sequential write and, the most important, the random seek combined with read and write operation.

The Random Seek + Read/Write test most accurately represents real-world use for a majority of users because files on disks fragment after a few weeks of use. Storage and retrieval of files on fragmented disks requires assembly from or writing data to many different places on the disk. Sequential reads usually only happen when the operating system is started fresh; sequential writes mostly happen when the disk is brand new. This is why the best real-world measurement of a data transfer rate is a random seek, which emulates moving the head to different tracks on the disk while reading/writing a file on a fragmented disk. It is the latter test that best describes the performance difference between a disk with disk encryption and an unencrypted disk.

The result for Random Seek + Read/Write test revealed minor changes of 2.4 percent to 5.1 percent performance difference between an encrypted disk compared to the disk performance before encryption on the tested platforms (see Fig. 2). The difference for sequential reads and writes is significantly higher. A faster CPU improves performance for the sequential read/write but sequential read and write are much less of a concern in the common use of a computer. Even though encryption is CPU intensive, it is the seek time between tracks that really determines the practical rate at which a disk can assemble or write data, not the encryption application or CPU configuration.

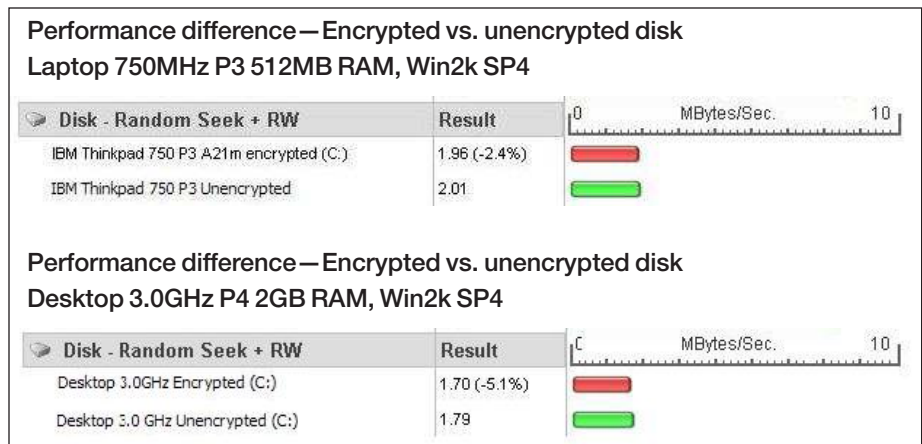


Fig. 2. Results for Random and Read/Write operations

PassMark performance test background

PassMark software includes different standard test suites. Each suite contains several tests to measure various aspects of computer system performance. The result of each test in a suite is combined into a section score (called a “Mark”), and presented using a particular unit of measurement in bar charts.

Following are standards test suites and tests in PassMark:

CPU test suite tests the performance of CPU operations.

- Integer (32-bit and 64-bit addition, subtraction, multiplication, and division)
- Floating Point (32-bit and 64-bit addition, subtraction, multiplication, and division)
- SSE (128-bit SSE operations such as addition, subtraction, and multiplication)
- Compression

- Encryption
- Image Rotation (rotate image coordinates in memory)
- Random String Sorting
- Find Prime Numbers

Graphics test suite tests standard two-dimensional graphical functions that exercise the standard Windows graphics functions, frequently used in a business computer setup.

- Quick Line Drawing: The color is changed every 500 lines to enable the lines to be seen in the test window
- Painting Bitmaps: A bitmap image is painted into a window as quickly as possible
- Outline Shapes: An ellipse and a square with rounded corners are drawn into a window
- Fonts and Text: Tests the performance of the graphics card with the typical rendering of fonts and text
- GUI: Tests the performance of the graphics card and windows display settings for interacting with the Graphical User Interface. The test includes the performance measurement of Common GUI controls: treeview, listview, sliders and edit boxes, as well as window movement and resizing

Hard Disk test suite measures performance when reading and writing files. We will explain further in a separate PassMark disk test section below.

CD/DVD test suite comprises one test that reads data from the CD drive.

3D Graphics test suite tests the DirectX 3D graphics system and is not part of most business configurations. Consequently, we did not run this test. This exclusion can be seen next to the PassMark result in the figure above indicated as “partial result.”

As noted in the PassMark Rating (Fig. 1) the overall performance is only very slightly affected by disk encryption, which is important taken in consideration of the different types of hard disk tests used in this analysis. Details for testing design, execution, and results are presented below.

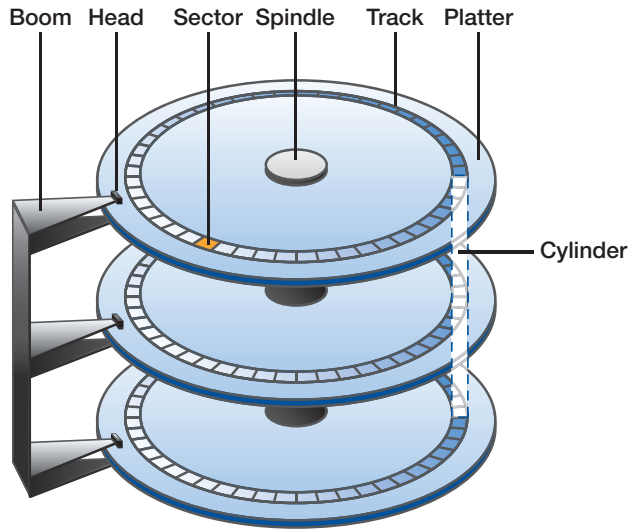
Performance theory

Understanding disk performance with encryption

Encryption is CPU intensive, even when using the Advanced Encryption Standard (AES). Efficient disk encryption programs are implemented using a low level filter driver, encrypting all data sent to the disk and decrypting data read from the disk. In general, the more efficient the encryption filter (i.e., the actual encryption algorithm and filter functionality), the less effect it will have on overall computer performance. A fast CPU will be able to crank data through the filter faster than a slow CPU. A slow disk will “load” the CPU less than a faster disk would since it would provide less data per time unit to be processed by the filter. Other issues with hard drives, such as average seek time, will have a greater effect on the result.

Hard disk architecture

A hard disk is a set of stacked platters, each with two surfaces and divided into concentric rings called tracks. Each track is divided into sectors—the smallest unit of information that can be read from or written to the disk. A sector is the smallest addressable portion of the disk.



To access a sector surface, the track and sector need to be specified for a particular operation. All tracks on one drive that can be accessed without the heads being moved constitute a cylinder. Each track has equal capacity, which means that inner tracks are more densely recorded. This allows the read/write head to have the same speed over each track. Sector sizes vary but are usually 512 bytes in size. There are normally thousands of tracks per disk surface. To improve I/O efficiency, transfers between memory and disk are performed in “block” units of one or more sectors.

The disk movement comprises three distinct physical operations that take time to carry out; seek time, rotational delay/latency time, and transfer time. To access a block on the disk, the system must perform a “seek” operation by moving the head to the appropriate track or cylinder. Time to complete this operation is called seek time. Seeking different tracks is likely to happen very frequently in a modern multi-threaded operating system environment, where several processes are contending for use of the disk at one time. Most hard disks available today have average seek times of less than 15 milliseconds (ms) and high performance disks have average seek times 7ms or less.

Once the head is at the right track, it must wait until the desired block rotates under the read/write head. This delay is the latency time. Average hard disks usually rotate at about 5,000 rotations per minute (rpm), which is one revolution per 12ms. The rotational delay is usually half a revolution, or about 6ms. As in the

case of seeking, these averages apply only when the read/write head moves from some random place on the disk surface to the target track. In many circumstances, rotational delay can be much less than the average. Once the data is under the read/write head, it can be transferred and the transfer time is given by the formula:

$$\text{Transfer time} = \frac{\text{Number of bytes transferred} \times \text{Rotation time}}{\text{Number of bytes on a track}}$$

Transfer time for one sector depends on the number of sectors on a track. For example, if there are 63 sectors per track, the time required to transfer one sector would be 1/63rd of a revolution. Total time to service a disk request is the sum of the seek time, latency time and transfer time. For most disks the seek time dominates, so reducing the mean seek time can improve the system performance substantially. The primary concern of disk performance is to minimize seek and latency times. This goal is often thwarted because disks are quickly fragmented in normal business use.

Normal fragmentation

Files in a file system are broken up into pieces called blocks. When a disk is new, there is space to store the blocks of a file all together in one place. This allows for faster sequential file reads and writes. As files are added, removed, and changed in size, the disk becomes fragmented, which leaves only small holes available for placement of new data. When a new file is written or when an existing file is extended, the new data blocks will be scattered across the disk. Scattered placement slows access due to seek time and rotational delay of the read/write head. Fig. 3 shows how fragmented a normal disk may be just one month after full defragmentation.

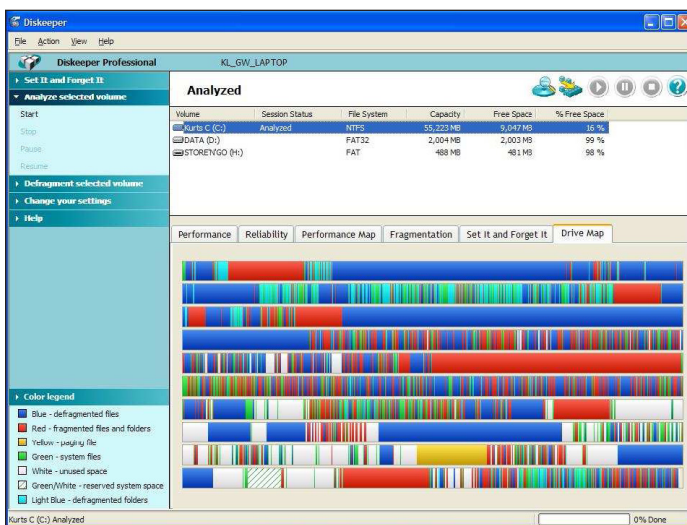


Fig. 3. Normal fragmentation pattern after four weeks of use

Performance testing methodology

Testing suite for measuring disk performance

PassMark performance measuring software was used to measure the actual disk performance. In order to find the answer to the true disk performance, we concentrated on using the standard disk performance tests, measuring only disk performance using three types of disk operations, large file (200MB) sequential read, large file sequential write, and most importantly the random seek combined with read and write operation.

There are a few factors which have a bearing on transfer speed, most importantly the manufactured access/seek time of a drive. Faster drives tested under the same conditions will simply record higher data transfer speeds.

A system cache also affects the read and write speed of a drive. The cache is a high speed area of memory which a Microsoft Windows operating system uses to store recently accessed data. If an application makes repeated requests for the same data, it can be taken directly from the cache very quickly without having to be decrypted again, and the cache reduces the necessity to read from the disk drive each time.

Caching is used by default by most applications, but an application may request uncached read and write operations. PassMark's basic test uses uncached operations to ease comparing results and make the result predictable. In the real world, data is cached and performance is considerably higher than when using uncached reads and writes.

PassMark's advanced test options allow for the ability to experiment with settings for higher performance. To enable easy comparisons between system results, we used the standard disk test settings.

As discussed above, the Random Seek + Read/Write operation is the test that accurately mirrors real-world use since it resembles operations on a typical fragmented disk. Results from this test are best used to judge the performance difference between a system with disk encryption and an unencrypted disk.

Test configurations

Two PC configurations were used for the tests. One was a laptop with a 750MHz P3 processor, 512MB of memory, and a 60GB hard drive with 5,400rpm 12ms average seek time. The other was a desktop PC with a 3GHz P4 processor, 2GB RAM, and a 10GB hard drive with 5,400rpm 9.4ms average seek time. Both ran Microsoft Windows 2000 Professional SP4.

Pretest preparations

We followed these precautions for effective and accurate measurement:

- Stop all other applications before running the performance test. This includes Internet connections, active live updates, taskbar programs, etc.
- Turn off virus checkers when running the disk tests because these applications usually degrade performance far more than disk encryption
- Once a test has been started, leave the test to run without starting or interacting with other applications (i.e., don't move the mouse or Alt+tab to other applications, etc.)

- Normalize amount of content on the disk. Capacity utilization and cluster size can affect the read/write performance of a disk. Position of the test file on the disk (inner cylinder or outer cylinder) can also affect the performance. The only way to avoid this problem is to only test newly formatted disks that have the same cluster size. For example, the performance can be degraded by more than 50 percent if the disk is almost full, compared to if the disk is newly formatted and almost empty
- A fragmented disk can adversely affect performance. Therefore, we ran the Windows utility for defragmenting a disk before testing. We did not defragment between encryption/decryption since this may move the place to which the test files are written and thereby change the result significantly. Therefore load Check Point Full Disk Encryption into a folder in “My Documents” before performing any test
- Windows can sometimes fire a process that can interfere with the accuracy of a test. A test may need to be run a couple of times or over a longer period of time to get an accurate result
- Adequate RAM is required to get a real indication of system performance. Results will be dramatically lower and inaccurate if Windows needs to swap processing out to disk during testing

Doing tests with PassMark

The disk standard test suite contains a number of tests that “exercise” the hard disk of the computer. For each test, a file is created in the root directory of the selected disk. The file size needs to be large in order to get an accurate measurement. The test file size is 200MB and the read and write block sizes used are 16KB. Under Windows 2000 and XP, each test uses noncached asynchronous file operations.

Disk Sequential Read. A large test file (200MB) is created on the disk under test. The file is then read sequentially from start to end.

Disk Sequential Write. A large file (200MB) is written to the disk under test. The file is written sequentially from start to end.

Disk Random Seek Read/Write. A large test file is created on the disk under test. The file is read randomly; a seek is performed to move the file pointer to a random position in the file, a 16KB block is read or written then another seek is performed. The amount of data actually transferred is as close to real-world use and is highly dependent on the disk seek time.

After taking the steps discussed in “Pretest preparations,” start the PassMark Performance Test 6.0 (or later) program. By default drive C: is used but this can be changed from the Preferences Dialog. Start with an unencrypted disk. Press the disk symbol on the line of icons or select from the menu Tests > Disk > All.

The test will start immediately (Fig. 4) and the results (Fig. 5) should be available in only a few minutes.

Save the results of the test as a new baseline under File > Save as baseline. Name the filename something easy to remember such as <Desktop 3.0GHz P4 Unencrypted>.bt. Then encrypt the drive and run the test again. Click on the bar

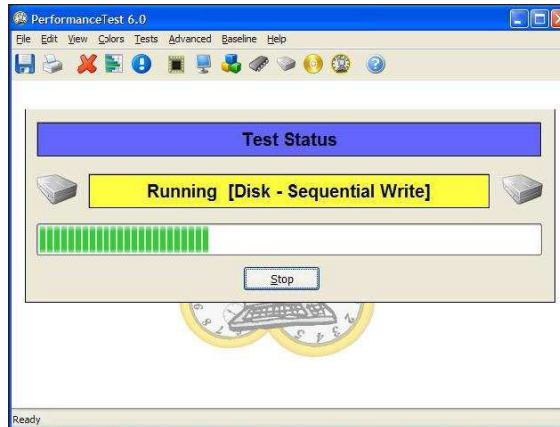


Fig. 4. PassMark disk performance test— Step 1, test in progress

Disk - Sequential Read	Result	0 MBytes/Sec. 30
This Computer (C:)	20.9	
Disk - Sequential Write	Result	0 MBytes/Sec. 30
This Computer (C:)	23.9	
Disk - Random Seek + RW	Result	0 MBytes/Sec. 10
This Computer (C:)	1.79	
Disk Mark	Result	0 Composite average 200
This Computer	168.7	
PassMark Rating	Result	0 Composite average 40
This Computer (Partial result)	33.7	

Fig. 5. PassMark disk performance test— Step 2, results shown

graph icon. Select the previous baseline created and click “add” and then OK. Now compare the actual results as shown below.

Note: To get the exact graphs shown below the PassMark result for the encrypted disk will have to be saved as a new baseline (similar to what is described for the unencrypted disk above), decrypt the PC, and run the test again.

Performance test results

Test results for the desktop and laptop platforms are shown in Figures 6 and 7.

The results show that in daily use (the test case of random seek + read/write), there is only a 2.5 to 5 percent performance difference for an encrypted disk compared to the disk performance before encryption on the tested platforms. The difference is hardly measurable. The difference in results between multiple test runs varies between 2 percent to 6 percent.

The difference in the test cases for sequential reads and writes is significantly higher but of less importance relative to the real-world use of a computer as we have examined in the previous sections. This explains why during startup, an encrypted disk is sometimes perceived to take a little longer time to start fresh than it did before encryption. There is no perceived difference in performance once the computer is running or when standby is used.

Although encryption is CPU intensive, system performance is all about seek time between tracks, not the encryption process or CPU configuration. In older

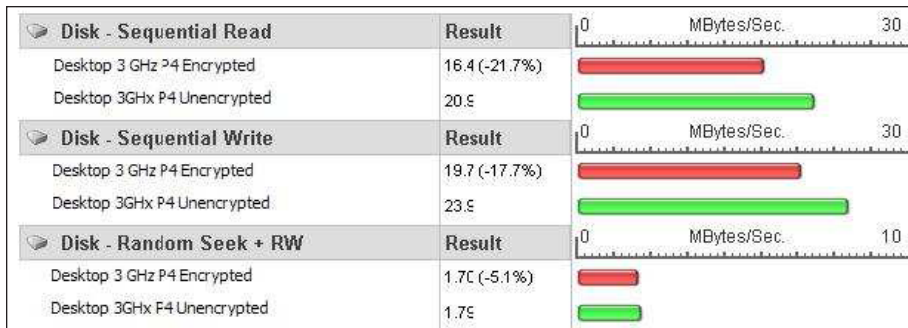


Fig. 6. Performance test—Encrypted vs. unencrypted disk
Desktop 3.0GHz P4 2GB RAM, Win2k SP4

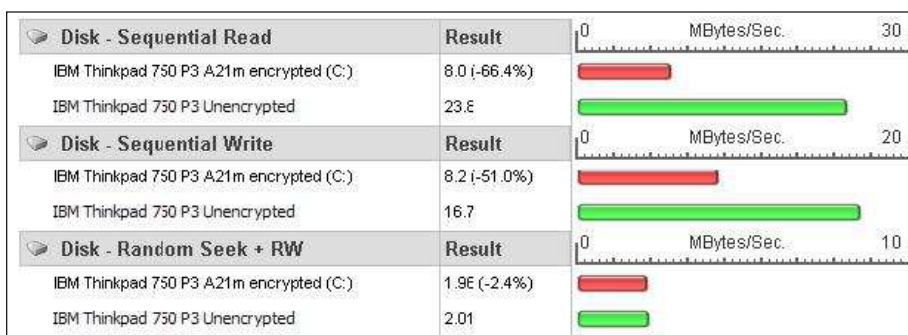


Fig. 7. Performance test—Encrypted vs. unencrypted disk
Laptop 750MHz P3 512MB RAM, Win2k SP4

systems where the hard drive has longer seek time or the CPU is slower, the effect of encryption is even less pronounced because the bottleneck is actually access to the data on the disk.

Conclusion

In practical business use, the performance effect of most disk encryption products is negligible. Efficient encryption algorithms such as AES, combined with the faster performance of modern laptops and desktops, make the case for disk encryption ever more appealing. A staggering performance increase in CPUs relative to the stagnating performance of data transfer rates of hard drives makes full-disk encryption the obvious choice over selective encryption products, which often leave sensitive data unencrypted.

When running the PassMark performance test program's standard test suite, a common PC configuration with Check Point Full Disk Encryption showed just a -2.9 percent overall performance difference compared to an unencrypted configuration.

When measuring actual disk performance, the Standard Disk test in the PassMark suite shows that in the test case mirroring daily business use of a hard disk, there is only a 2.5 to 5 percent performance difference between an encrypted and unencrypted disk. Furthermore, the nominal performance degradation of 2 to 5 percent will be further reduced by the use of caching.

In conclusion, for the average business user, testing clearly shows that protection of data using full-disk encryption includes no practical penalty in performance of the PC.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Check Point Endpoint Security product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Soleim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.