ADVANTAGES OF DELL AND INTEL PERFORMANCE AND SECURITY FEATURES FOR HEALTHCARE PROVIDERS

Keep patient data secure with minimal performance cost.

Dell™ Latitude™ E6520 notebook, powered by 2nd generation Intel® Core™ i5 processor, kept work private.

Strict government regulations such as HIPAA and HITECH are boosting the penalties for confidential patient data breaches. As more doctors and nurses store the confidential patient data these regulations cover on portable devices such as notebooks, the risk of data loss and breach increases. While encrypting data is vital to keep data safe and comply with healthcare regulations, doing so has traditionally lowered performance drastically. Can providers comply with healthcare laws by encrypting patient data on notebooks and still enjoy excellent performance?

To answer this question, Principled Technologies tested an endpoint security solution on a Dell Latitude E6520 notebook with a 2nd generation Intel Core i5 processor, a solution that includes both hardware- and software-based performance and security features. Built into the processor's hardware are Intel Anti-Theft Technology (Intel AT), which can locate and lock down a missing system, and Intel AES-NI, which speeds up encryption/decryption. On the software side, Dell Data Protection|Encryption encrypts notebook data without the traditional performance hit, and Dell System Track (also available as Computrace® Complete) protects data even when encryption keys are weak or compromised and helps owners locate stolen notebooks and lock down or delete sensitive data remotely.

Using both software- and hardware-based security features creates a layered defense strategy that makes it tougher than ever for thieves to access confidential data.

MAY 2011
A PRINCIPLED TECHNOLOGIES TEST REPORT
Commissioned by Intel Corp.

HEALTHCARE DATA SECURITY: AN OVERVIEW

When a healthcare organization experiences device theft, and has failed to protect sensitive client data, the costs and consequences are serious; data breaches violate stringent health care security and privacy rules and regulations, and cause a patient to lose confidence in his or her healthcare provider.

The most significant regulations governing healthcare organizations are the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. HIPAA establishes a set of national standards for the privacy and security of certain health information. HITECH builds on these standards, and further enforces them with stringent penalties. To learn more about these regulations, see Appendix A. To read about industry research quantifying the cost of data breaches, see Appendix B.

Defense in Depth

The National Security Agency borrowed the concept of Defense in Depth from the US military. It employs a varied, layered defense strategy against electronic attacks, and follows the paradigm of Protect, Detect, and React. In addition to having protection techniques in place for when attacks hit, IT companies should detect attacks before they occur and recover from them after they have hit.

Eliminating vulnerabilities in people, technology, and operations is crucial to creating a balanced defense. Effective training of security personnel helps ensure that IT staff is able to handle threats. For technology, acquiring a variety of relevant defense applications (such as Intel AT, in the healthcare space) is vital. Finally, a successful operation effectively manages the sum of the organization's defense operations on a daily basis.

To learn more about Defense in Depth, visit http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

ENCRYPT YOUR DATA WITHOUT A PERFORMANCE HIT

The National Security Agency recommends a complete, layered strategy for protecting against electronic attacks (see sidebar). With such a strategy in mind, Dell and Intel provide layers of protection, both software and hardware based, that you can apply to your notebook. Dell Data Protection|Encryption (DDP|E) protects your data without slowing your system down, thanks to Intel processors featuring Intel Advanced Encryption Standard New Instructions (AES-NI), which accelerate the encryption and decryption process by using processor hardware to speed up portions of the AES algorithms. This means that encryption no longer causes an unacceptable performance drop.

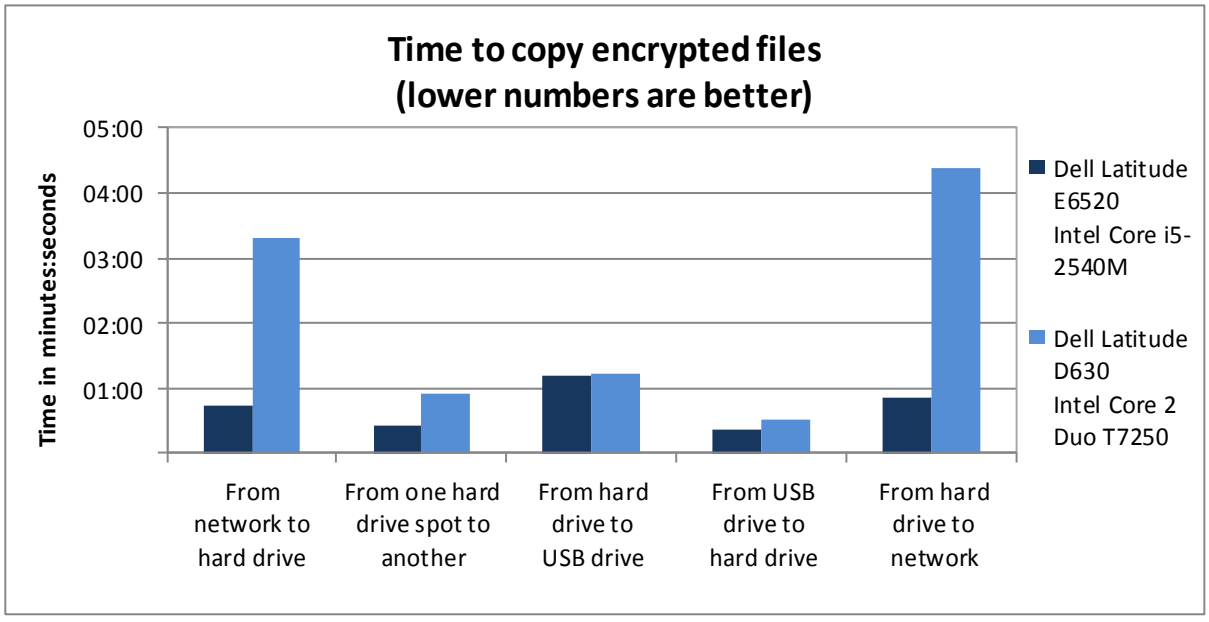

Figure 1: The Intel Core i5-2540M processor-based notebook performed encrypted file copies considerably faster than the older Intel Core 2 Duo-based notebook. (Lower numbers are better.)

We performed several encryption and decryption file-copy tests on a Dell Latitude E6520 with a 2nd generation Intel Core i5 processor and on an older Dell Latitude D630 with an Intel Core 2 Duo T7250 processor. (See Appendix C for detailed system configurations.) As Figure 1 shows, the newer notebook encrypted and decrypted as much as 80.2 percent faster.

While encryption and other tools help keep an organization HIPAA compliant, most users are concerned with the negative performance impact encryption has traditionally had on a notebook. To measure the performance impact of encryption, we performed the same file copy tasks on the Dell Latitude E6520 before we encrypted the hard drive. Figure 2 compares the time the Intel Core i5-2540M processor-based Dell Latitude E6520 took to perform the tasks on the unencrypted and encrypted drives. The tests took approximately the same time on the encrypted disk as they did on the unencrypted disk.

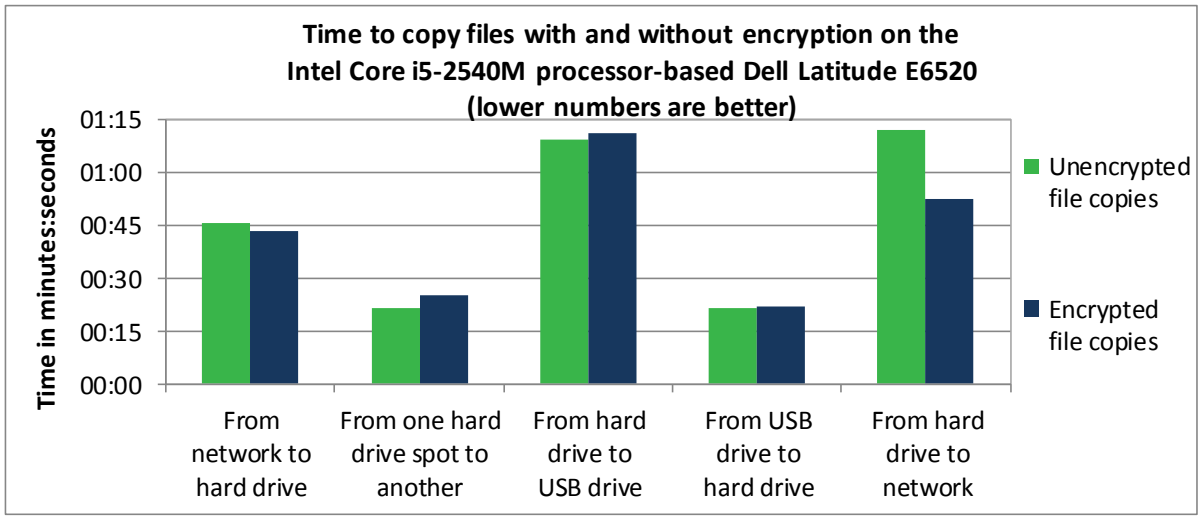

Figure 2: The Intel Core i5-2540M processor-based notebook performed encrypted file copies at rates comparable to unencrypted file copies, showing little to no performance hit. (Lower numbers are better.)

DELL SYSTEM TRACK—PROTECTING YOUR DATA AND ASSETS

Dell System Track Services, available for the new Intel Core i5 processor-based notebooks that allow you to enable the anti-theft feature, helps you locate lost or stolen systems and, most importantly, protect the sensitive patient records that reside on these machines. Through the online System Track Portal, your IT administrator can

- Monitor your connection status, locate systems, and track physical location using geolocation
- Protect data and provide system security using Remote Data Deletion and System Lock
- Locate and help retrieve missing systems

SOFTWARE-BASED PROTECTION

Dell Data Protection/Encryption

Encrypts data to keep it secure, without a performance penalty

Dell System Track

This software allows you to monitor and locate missing systems, and lets you lock down or delete data remotely

HARDWARE-BASED PROTECTION

Intel AES-NI

Accelerates encryption and decryption to protect your data without a performance hit

Intel AT

Built into the processor hardware so it cannot be erased, Intel AT locks a system down, making data inaccessible to anyone without the correct passcode

Arming your notebooks with Dell System Track and its data protection and retrieval features helps you adhere to privacy regulations; avoiding penalties for violating such regulations lowers the total cost of ownership for each notebook.

The notebook syncs with, or calls into, Dell System Track regularly, providing system and location information each time it connects to the Internet. This enables IT administrators to delete sensitive data, lock the system down, and retrieve key files if they determine the notebook has been lost or stolen. If Intel Anti-Theft is enabled, the notebook will make that call even when the notebook is turned off. Because Intel Anti-Theft technology is a hardware-based solution on 2nd generation Intel Core processors, it cannot be deleted or removed as software-based solutions can. If the notebook remains offline longer than the interval set by IT administrators, Intel AT locks the notebook down, making data on the notebook inaccessible to anyone without the correct passcode. Together, Dell and Intel provide the multiple levels of security you need to protect sensitive data.

How we tested Dell System Track

To test the security features of Dell System track, we performed the following steps in the Dell Customer Center:

- Set up a rendezvous timer alert
- Created a geofence around our building, and then created a geofence breach alert
- Created an IP address change alert

We then disabled all but one of these policies, and broke the rule. After we broke the rule, we monitored our email for an alert that the policy had been broken, and checked the notebook to verify the behavior was as expected. For some of these tests, we forced a call from the notebook, rather than wait the normal 24-hour period that is the minimum for synchronizing with the servers.

When we took the notebook offline for more than 48 hours, we found that Intel Anti-theft technology had locked us out, and the only way to regain access was through a user password or security key. In our simulated geofence breach, we received an email telling us that the notebook had been taken outside our defined geofence. On the map, we were able to see, with almost pinpoint accuracy, the location to which the notebook had been taken.

Taking this test a step further, we invoked a device freeze, which forced the notebook to reboot. Only by keying in the passcode created for the device freeze could we regain access to the notebook resources.

In some cases, the system's owner may want specific data deleted from the system to prevent sensitive patient information from falling into the wrong hands. To see this in action, we placed the 425MB folder of files used in the file

copy tests in My Documents. After counting the number of Microsoft Excel files in the folder, we invoked a remote data delete from the Customer Center. We monitored the folder on the notebook, and within a short time, watched all of the Microsoft Excel files disappear.

As a last resort, the owner may decide to delete all files, including the operating system, to protect that sensitive patient information. This process is as simple as performing a targeted file delete, but it "bricks" the notebook, making it unusable.

For step-by-step details of the Dell System Track testing, see Appendix D.

ABOUT OUR TESTING

We wanted to determine whether providers complying with healthcare laws by encrypting patient data on notebooks and using other hardware and software-based security features could still enjoy excellent performance. To that end, we measured the time it took a current Dell Latitude E6520 with a 2nd generation Intel Core processor and a 3-year old Dell Latitude D630 with an Intel Core 2 Duo processor to encrypt and decrypt files. Once we learned that the Dell Latitude E6520 with an Intel Core i5 processor outperformed the older system significantly, we tested the time it took to copy files on an encrypted drive compared to an unencrypted drive, and found no performance penalty, or even improved performance, with encryption. For testing, we encrypted data using Dell Data Protection Encryption software (which takes advantage of Intel AES-NI), and secured the systems with Intel AT managed by Dell System Track software.

About Intel Anti-Theft (AT) Technology

The latest version of Intel AT is available on notebooks with 2nd generation Intel Core i5 processors. Intel AT is a hardware-based solution that third-party software can enable and manage. Intel AT allows users to disable a notebook at the hardware level in the event of loss or theft.

Intel AT provides local, tamper-resistant capabilities to disable a computer and access to any data it may contain.

Availability of Intel AT features and results depends upon the setup and configuration of the hardware, software, and IT environment. Our results are specific to our setup, hardware, and management software.

About Dell System Track Software

Dell has partnered with Absolute® Software to allow healthcare organizations to centrally track and secure their IT assets within a single cloud-based console – Computrace Complete for endpoint security accessed through the Dell System Track Customer Center portal or the Absolute Customer Center.

On Dell notebooks with the Computrace Complete agent built into the firmware, customers can identify computers that have gone missing, enforce policies, and remotely invoke pre-emptive or reactive security measures to safeguard each device and the data it contains. We used the Dell System Track Customer Center to interface and activate Intel AT, set Intel AT policy, and monitor the notebooks. Please note that Dell System Track and Computrace Complete provide the same important security features.

FINAL THOUGHTS

The Dell Latitude E6520 powered by a 2nd generation Intel Core i5 processor offers medical organizations all the protection they need. Dell Data Protection| Encryption uses Intel AES-NI to encrypt data without a traditional performance hit, and Dell System Track uses Intel AT to protect your data and assets should they fall into the wrong hands. If your notebook is lost or stolen, you can track it down, lock it down, and, as a last resort, remotely delete all its data.

Even though it has all the layers of security you need to keep patient data safe and comply with healthcare regulations, the Dell Latitude E6520 powered by a 2nd generation Intel Core i5 processor also provides excellent performance—as much up to 80.2 percent better performance with encrypted drives than an older system.

APPENDIX A – HIPAA AND HITECH ACTS

The HIPAA Privacy and Security Rules defined by the US Department of Health and Human Services protect the privacy of individually identifiable health information and specify administrative, physical, and technical safeguards for healthcare providers to use to assure the confidentiality, integrity, and availability of electronic protected health information.

The HITECH act builds on HIPAA and sets enforcement, accountability, penalty, and prosecution-related guidelines for those involved in sharing or accessing health information. This act establishes incentive funds to help pay for the adoption of electronic health records at hospitals and physician group practices. HITECH accountability provisions help ensure that, as more information is digitized, it will remain secure.

Enforcement is perhaps the most significant security provision of HITECH. The HITECH act stipulates a notification penalty for thefts of medical information of 500 or more patients. The rules require that, unless the provider has adequately protected the data, the provider must submit information about the breach, which is then posted on a US Department of Health Human Services Web page that identifies the provider and describes the breach.[1] The provider must also notify all affected patients, a costly process that can cause patients to drop the provider and seek care elsewhere. Additionally, some states levy additional penalties and fines on the provider for a data breach.

A provider need not report data losses if standard-validated encryption has rendered the data unreadable and if the provider keeps encryption keys on a separate device from the data that they encrypt or decrypt. When the provider has met those conditions, the U.S. government does not consider the loss a privacy breach, and notification need not occur. Rules also require that the key or confidential process needed to access the data also not be breached. Intel AT helps here with its ability to disable access to encrypted data by deleting a critical encryption key stored on the chipset. Bricking the notebook helps with compliance and helps health care providers prevent data breaches with breach notification.

[1] Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

APPENDIX B – INDUSTRY RESEARCH ON RISK AND COST OF DATA BREACHES

Below, we present highlights from industry research on the risk and cost of data breaches.

- Notebook theft is the primary cause of data breaches.[2]
- The cost per record violated was about $294 in the healthcare sector in 2009, before the additional penalties associated with HITECH.[3] The cost of breaches is rising.
- The average value of a lost notebook is $67,873. This value includes replacement cost; detection; forensics; data breach; lost intellectual property; lost productivity; and legal, consulting, and regulatory expenses.[4]
- What makes a lost notebook costly to a healthcare provider is the potential for a data breach. The occurrence of a data breach represents 80 percent of the cost.[5]
- The more quickly a healthcare provider learns that a notebook is lost, the lower the average cost of the incident. The average cost for same-day discovery is $8,950. When discovery occurs after 1 week, the cost rises to approximately $115,849.[6]
- Encryption makes a difference. The HITECH act recognizes encryption as a control to render data unusable as long as the encryption key is not with the stolen or lost device. To take full advantage of encryption, all essential cryptographic material should be stored away from the device in a secure network location or USB thumb drive. A lost notebook that has encryption costs almost $20,000 less than one without encryption.[7]
- More than 10 percent of all notebooks in health and pharmaceutical companies will be lost or stolen sometime during their useful life.[8]
- The theft of notebooks is influencing the security of health information. Thirty-nine percent of providers and 33 percent of payers reported having experienced security incidents in the last 6 months.[9]
- The majority of end-users and companies with significant amounts of confidential data on their notebooks do not take advantage of even basic security practices such as encryption, backup, and anti-theft technologies.[10] One reason end-users choose not to encrypt their data is due to a perceived negative effect on performance. The new 2010 Intel Core vPro processor family includes a set of new instructions, Intel Advanced Encryption Standard (AES) New Instructions (AES-NI), which Intel designed to implement some of the complex and performance-intensive steps of the AES algorithm using hardware to accelerate the execution of the AES algorithms. AES-NI can be used to accelerate the performance of an implementation of AES by 3 to 10 times over a completely software-based implementation.

[2] Source: http://www.healthcareitnews.com/news/laptop-thefts-top-cause-health-data-breaches
[3] Source: http://hipaasecurityassessment.com/blog/state-enforcement-of-breach-notification-rules-is-on-the-rise/
[4] Source: The Cost of a Lost Laptop, Ponemon Institute LLC, April 22, 2009, a study sponsored by Intel Corporation, ftp://download.intel.com/technology/product/cost_of_a_lost_laptop.pdf
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*
[8] Source: http://antitheft.intel.com/Libraries/Documents/Ponemon_Intel_Billion_Dollar_Lost_Laptop_Problem.sflb.ashx
[9] Source: http://gtra.org/attachments/292_complianceprotectionrecovery.pdf
[10] Source: http://newsroom.intel.com/community/intel_newsroom/blog/2010/12/02/missing-a-laptop-join-the-billion-dollar-club?cid=rss-258152-c1-262509

APPENDIX C - TEST SYSTEM CONFIGURATION

Figure 3 provides configuration information for the systems we tested.

System	Dell Latitude D630	Dell Latitude E6520
General		
Number of processor packages	1	1
Number of cores per processor	2	2
Number of hardware threads per core	1	2
System power management policy	Portable/Laptop	Dell
Processor power-saving option	Enhanced Intel SpeedStep® Technology	Enhanced Intel SpeedStep Technology
System dimensions (length x width x height)	13-1/4” x 9-1/2” x 1-3/8”	15-1/8” x 10-1/4” x 1-1/4”
System weight	5 lbs. 5 oz.	6 lbs. 1 oz.
CPU		
Vendor	Intel	Intel
Name	Core 2 Duo mobile	Core i5
Model number	T7250	2540M
Stepping	M0	D2
Socket type and number of pins	Socket P (478)	Socket 988B rPGA
Core frequency (GHz)	2.00	2.60
Bus frequency	800 MHz	DMI 2.0
L1 cache	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)
L2 cache	2 MB (shared)	512 KB (256 KB per core)
L3 cache	N/A	3 MB
Platform		
Vendor	Dell	Dell
Motherboard model number	0KU184	0NVF5K
Motherboard chipset	Intel GM965	Intel QM67
BIOS name and version	Dell A17 (01/04/2010)	Dell A01 (03/02/2011)
Memory module(s)		
Vendor and model number	Samsung M470T6554EZ3-CE6	Micron 8JSF25664HZ-1G4D1
Type	PC2-5300	PC3-10600
Speed (MHz)	667	1,333
Speed running in the system (MHz)	667	1,333
Timing/Latency (tCL-tRCD-tRP-tRASmin)	5-5-5-15	9-9-9-24
Size (MB)	512	2,048
Number of memory module(s)	2	1
Amount of RAM in system (GB)	1	2
Chip organization (single-sided/double-sided)	Double-sided	Double-sided
Channel (single/dual)	Dual	Single
Hard disk		
Vendor and model number	Toshiba MK8046GSX	Seagate ST9320423AS

System	Dell Latitude D630	Dell Latitude E6520
Number of disks in system	1	1
Size (GB)	80	320
Buffer size (MB)	8	16
RPM	5,400	7,200
Type	SATA 3.0 Gb/s	SATA 3.0 Gb/s
Controller	Intel 82801HBM (ICH8-ME)	Intel Mobile Express SATA RAID Controller
Driver	Intel 7.0.0.1020 (02/12/2007)	Intel 10.1.0.1008 (11/06/2010)
Operating system		
Name	Windows XP Professional	Windows 7 Professional
Build number	2600	7600
Service Pack	3	N/A
File system	NTFS	NTFS
Kernel	ACPI Multiprocessor PC	ACPI x64-based PC
Language	English	English
Microsoft DirectX version	9.0c	11
Graphics		
Vendor and model number	Intel GMA X3100	Intel HD Graphics 3000
Type	Integrated	Integrated
Chipset	Mobile Intel 965 Express Chipset	Intel HD Graphics
BIOS version	1466	2089.11
Total available graphics memory (MB)	256	775
Dedicated video memory (MB)	N/A	64
System video memory (MB)	N/A	0
Shared system memory (MB)	N/A	711
Resolution	1,280 x 800	1,366 x 768
Driver	Intel 6.14.10.5076 (06/12/2009)	Intel 8.15.10.2266 (12/16/2010)
Sound card/subsystem		
Vendor and model number	Sigma Tel High Definition Audio	IDT High Definition Audio
Driver	Sigma Tel 5.10.0.5515 (05/10/2007)	IDT 6.10.0.6316 (12/07/2010)
Ethernet		
Vendor and model number	Broadcom® NetXtreme® 57xx Gigabit Controller	Intel 82579LM Gigabit Controller
Driver	Broadcom 10.26.0.0 (03/06/2007)	Intel 11.8.81.0 (10/28/2010)
Wireless		
Vendor and model number	Dell Wireless 1395 WLAN Mini-Card	Intel Centrino Advanced-N 6205
Driver	Broadcom 5.60.18.9 (08/25/2009)	Intel 14.0.1.2 (12/21/2010)
Modem		
Vendor and model number	Conexant HDA D330 MDC V.92	N/A
Driver	Conexant 7.68.0.0 (09/06/2007)	N/A
Optical drive(s)		
Vendor and model number	TSSTcorp GSA-T21N	TSSTcorp TS-U333B
Type	DVD-RW	DVD-RW

System	Dell Latitude D630	Dell Latitude E6520
USB ports		
Number	2	3
Type	2.0	2.0
Other	NA	Media card reader
IEEE 1394 ports		
Number	1	1
Monitor		
LCD type	WXGA	WXGA LED
Screen size (inches)	14.1	15.6
Refresh rate (Hz)	60	60
Battery		
Type	Dell PC764 Lithium-Ion	Dell T54FJ Lithium-Ion
Size (length x width x height)	7-3/8” x 2-5/8” x 7/8”	8-1/4” x 2” x 3/4”
Rated capacity	5000mAh / 11.1V (56Wh)	5300mAh / 11.1V (60Wh)
Weight (oz.)	12	12

Figure 3: Test system configuration details.

APPENDIX D – DETAILED TESTING PROCEDURE

File copy testing

We used a 425MB folder containing a set of Word, Excel®, PowerPoint®, PDF, and image files for the file copy tests.

From network to hard drive

1. Place three copies of the folder into a network share.
2. Browse to the network share.
3. Copy folder 1.
4. Paste the folder into My Documents, and hand-time the process.
5. Repeat steps 3 and 4 with folders 2 and 3.
6. Take the median of the three file-copy tests.

From one hard drive spot to another

1. Place three copies of the folder into My Documents.
2. Browse to My Documents.
3. Copy folder 1.
4. Paste the folder onto the desktop, and hand-time the process.
5. Repeat steps 3 and 4 with folders 2 and 3.
6. Take the median of the three file-copy tests.

From hard drive to USB drive

1. Place three copies of the folder into My Documents.
2. Browse to My Documents.
3. Copy folder 1.
4. Paste the folder into the USB flash drive, and hand-time the process.
5. Repeat steps 3 and 4 with folders 2 and 3.
6. Take the median of the three file-copy tests.

From USB drive to hard drive

1. Place three copies of the folder onto a USB flash drive.
2. Browse to the USB flash drive.
3. Copy folder 1.
4. Paste the folder into My Documents, and hand-time the process.
5. Repeat steps 3 and 4 with folders 2 and 3.
6. Take the median of the three file-copy tests.

From hard drive to network

1. Place three copies of the folder into My Documents.
2. Browse to My Documents.
3. Copy folder 1.
4. Browse to a network share, paste the folder into the share, and hand-time the process.
5. Repeat steps 3 and 4 with folders 2 and 3.
6. Take the median of the three file-copy tests.

Dell System Track testing

Setting up policy-based protection in Dell System Track

Installing the Computrace agent on target systems

1. On the target system, log into Windows and set up an Internet connection.
2. Open Internet Explorer®, and navigate to https://CC.absolute.com/.
3. Enter the user name and login for the administrator account.
4. At the Dell System Track Customer Center home page, scroll down to the bottom of the page, and click Download Packages.
5. Select Windows to begin downloading the ZIP file package.
6. Browse to the saved ZIP file, and extract its contents to the C:\ drive.
7. Once all the files are extracted, browse to the MSI_Deployment folder.
8. Double-click Computrace.msi to launch the Computrace agent installation package.
9. When the Confirm installation screen appears, click Next to begin the installation.
10. When the installation is complete, click Close.

Manually initiating a call to the Absolute servers

1. Browse to the folder created in Step 8 of Installing the Computrace agent, above.
2. Double-click ctmweb.exe.
3. Enter the password for the Computrace agent to log in.
4. Click Test Call, and click Start to begin a test call to the Absolute servers.
5. It may take up to an hour before the system is enrolled as a device on the Absolute administrator Web site.

Creating the User Password in the Absolute Customer Center

1. Open Internet Explorer on any computer, and navigate to https://CC.absolute.com/, if not already logged in.
2. Enter the user name and login for the administrator account.
3. On the left side of the Dell System Track Customer Center homepage, click Data and Device Security.
4. Select Intel Anti-Theft Technology from the Data and Device Security sub-categories.
5. Select Set Intel Anti-Theft Technology Defaults, and set the following:
   a. Default Timer Period: 2 Days (the minimum period).
   b. Default Timer Action: Immediate system lock.
   c. Default Lock Request Action: Immediate system lock.
   d. Default Passcode for New Activations.

Setting up a rendezvous timer alert

1. Open Internet Explorer on any computer, and navigate to https://CC.absolute.com/, if not already logged in.
2. Enter the user name and login for the administrator account.
3. On the left side of the Dell System Track Customer Center homepage, navigate to Administration→Alerts→Create and Edit Alerts.
4. Enter a name for the new alert (e.g., Last call time greater than 2 days).
5. Enter a description for the alert.
6. Set the Suspicion level to 5.
7. Under Conditions, select Last Call Time from the Field drop-down menu.
8. Select Greater or Equal To from the Rule drop-down menu.
9. Set the Criteria to 2 days.
10. Click Add Condition.
11. Under Scope, ensure that all target devices are selected.
12. Leave the defaults for Alert Type and Alert Options.
13. Under Action, select Log event and notify.
14. Enter the appropriate email addresses to receive the alert.
15. Click Save.

16. On the left side, click View and Manage Alerts.
17. Ensure that the IP Address alert has a status of Active.
18. Select the newly-created alert using the check box, and click the Suspend button.

Creating a geofence and a geofence breach alert

1. Open Internet Explorer on any computer, and navigate to https://CC.absolute.com/, if not already logged in.
2. Enter the user name and login for the administrator account.
3. On the left side of the Dell System Track Customer Center homepage, click Administration.
4. Click Geofences→Create and Edit Geofences.
5. Enter a name in the Geofence Name field.
6. Enter a description in the Geofence Description field.
7. Remove the check in the box for Only test locations with high Confidence Levels against Geofench boundaries.
8. Remove the check in the box for GPS and Other Location Sampling technologies.
9. Zoom in until you are at street-level view, and the distance scale represents 150 yards.
10. Change the view to Aerial.
11. Click Create Boundaries, and create a polygon of coverage on the map, line by line, with a series of clicks on the map.
12. Click Save.
13. On the left side, navigate to Alerts→Create and Edit Alerts.
14. Enter a name for the new alert (e.g., Geofence breach).
15. Enter a description for the alert.
16. Set the Suspicion level to 5.
17. Under Conditions, select Geofence Location from the Field drop-down menu.
18. Select Is Outside from the Rule drop-down menu.
19. Set the rule to the proper geofence, and set the time period to at least 1 day.
20. Click Add Condition.
21. Under Scope, ensure that all enrolled devices are selected.
22. Leave the defaults for Alert Type and Alert Options.
23. Under Action, select Log event and notify.
24. Enter the appropriate email addresses to receive the alert.
25. Click Save.
26. On the left side, click View and Manage Alerts.
27. Ensure that the Geofence breach alert has a status of Active.
28. Select the newly-created alert using the check box, and click the Suspend button.

Creating an IP address change alert

1. Open Internet Explorer on any computer, and navigate to https://CC.absolute.com/, if not already logged in.
2. Enter the user name and login for the administrator account.
3. On the left side of the Dell System Track Customer Center homepage, navigate to Administration→Alerts→Create and Edit Alerts.
4. Enter a name for the new alert (e.g., IP Address).
5. Enter a description for the alert.
6. Set the Suspicion level to 5.
7. Under Conditions, select IP Address (Local) from the Field drop-down menu.
8. Select Changed from the Rule drop-down menu.
9. Click Add Condition.
10. Under Scope, ensure that all enrolled devices are selected.
11. Leave the defaults for Alert Type and Alert Options.
12. Under Action, select Log event and notify.
13. Enter the appropriate email addresses to receive the alert.

14. Click Save.
15. On the left side, click View and Manage Alerts.
16. Ensure that the IP Address alert has a status of Active.
17. Select the newly-created alert using the check box, and click the Suspend button.

Testing the features of Dell System Track

Protecting data by setting a rendezvous timer and restoring access with a password

1. Shut down the target system, and wait 50 hours.
2. Power on the target system.
3. Verify that the system is locked, and that you are presented with an Intel AT screen.
4. Verify that the administrator received an email alert.
5. Enter the User Password created as part of the Intel AT Defaults in the Dell System Track Customer Center.

Using a geofence or an IP address change to lock down the system and restoring access with a recovery token

1. Create a geofence and a geofence alert, as we describe above, and change the status of the alert to Active.
2. Remove the enrolled devices from the premises.
3. Connect to the Internet on the enrolled devices not equipped with GPS when you arrive at the offsite destination.
4. Manually initiate a call into the Absolute servers.
5. Reboot.
6. Verify that a geofence breach alert has been generated in the Dell System Track Customer Center, and that an email has been sent to the Administrators designated in the Users page of the Dell System Track Customer Center
7. After receipt of the email alert, you may perform a Device Freeze if the asset has been determined as stolen or missing.
8. Repeat this process by suspending the geofence alert and activating the IP address change alert, created above.
9. Connect to the Internet on the enrolled devices.
10. Manually initiate a call into the Absolute servers.
11. Reboot.
12. Verify that an IP address change alert has been generated in the Dell System Track Customer Center, and that an email has been sent to the Administrators designated in the Users page of the Dell System Track Customer Center.

Protecting data by remotely disabling the system with a device freeze and restoring access with a passcode

1. Open Internet Explorer on any computer, and navigate to https://CC.absolute.com/, if not already logged in.
2. Enter the user name and login for the administrator account setup with Absolute.
3. On the left side of the Dell System Track Customer Center homepage, navigate to Data and Device Security→Security Authorization→Request Authorization Code.
4. Click Request Code.
5. Check the administrator account's email, and write down the authorization code provided in the authorization code email from Absolute.
6. On the left side of the Absolute administrator homepage, navigate to Data and Device Security→Data Freeze→Request Data Freeze.
7. Click Select Devices, and select the target device(s).
8. Select All Devices from the Where Group is drop-down, and click Filter.
9. Select the check box for the target computer(s) and click Select Devices.
10. Fill in the Request Name.
11. Select a message to appear during the device freeze.
12. Select Specify a specific 8-digit numeric passcode for each device, and enter an 8-digit passcode.
13. Select the Force Reboot check box, and click Submit.

14. Under Provide Authentication, enter the administrator Customer Center password and the Authorization Code provided in the email from earlier steps.
15. Click OK.
16. On the left side, click Device Freeze Summary Report.
17. Force a call on the target computer(s).
18. When the call has completed, the new device freeze request status will change from Freeze Requested to Frozen in the Device Freeze Summary Report, and the target computer(s) will automatically reboot.
19. Log into the target system.
20. After logging in, the screen will be completely white, displaying the messages that were selected in the device freeze request process. This behavior shows that the system successfully received a device freeze from the Computrace.
21. Type in the passcode that you specified in Step 12.
22. The system will automatically restart.
23. Once the Windows login screen appears, log in. Verify that the system now behaves normally by opening the health information test file in Excel.
24. On the administrator computer, log into the Absolute administrator homepage again.
25. On the left side, navigate to Data and Device Security→Device Freeze→Device Freeze Summary Report. Once the system calls in, the device freeze status will change from Frozen to Unfrozen With Passcode.

Using remote notification to permanently remove specific data from the system

1. Copy a folder containing a mix of Microsoft Office documents, PDF files, and image files to the target system.
2. Open that folder, and sort the contents by type.
3. Scroll down so that the Microsoft Excel documents are visible in Windows Explorer.
4. Count the number of Microsoft Excel documents in the folder.
5. Open Internet Explorer on any computer, and navigate to https://CC.absolute.com/, if not already logged in.
6. Enter the user name and login for the administrator account.
7. On the left side of the Dell System Track Customer Center homepage, navigate to Data and Device Security→Security Authorization→Request Authorization Code.
8. Click Request Code.
9. Check the administrator account's email, and write down the authorization code provided in the authorization code email from Absolute.
10. On the Absolute administrator homepage, navigate to Data and Device Security→Data Delete→Request Data Delete.
11. Under Identifier, click Choose, and select the target device for the data delete.
12. Under Reason, select Missing, and enter today's date.
13. Under Data Delete Policy, select Custom Policy, and click the link to Create a Policy.
14. The Create and Edit Data Delete Policies page will load.
15. Enter Excel into the Policy Name field.
16. Enter a brief description in the Description field.
17. Select All MS Excel documents and click the Add>> button.
18. Click Save.
19. The Request Data Delete page will load.
20. Leave the default settings for Data Delete Options.
21. Under Data Delete Validation, check the box beside I accept the agreement.
22. Click Set Data Delete.
23. On the next page, ensure that all the information provided in the window is correct, and click Submit Data Delete Request.
24. Under Provide Authentication, enter the administrator Customer Center password and the Authorization Code provided in the email from earlier steps.

25. Click OK.
26. On the left side, click Data Delete Summary Report.
27. The new Data Delete request should be listed.
28. Once the process has begun, the status will be listed as Launched.
29. Monitor the folder on the target computer to verify that all Microsoft Excel documents disappear from the folder.

APPENDIX E – DETAILED TEST RESULTS

We ran each test three times on each notebook. We performed all tests on the drive after we encrypted both notebooks using DDP|E.

As Figure 4 shows, performing file copies to and from the Intel Core i5-2540M processor-based Dell Latitude E6520 hard disk is as much as 80.2 percent faster than on the older system.

Encrypted file copies	Dell Latitude E6520 (Intel Core i5-2540M)	Dell Latitude D630 (Intel Core 2 Duo T7250)	Time saved (minutes: seconds)	Time saved (percentage)
From network to hard drive	00:43.30	03:18.94	02:35.6	78.2%
From one hard drive spot to another	00:25.13	00:54.99	00:29.9	54.3%
From hard drive to USB drive	01:10.96	01:13.18	00:02.2	3.0%
From USB drive to hard drive	00:21.96	00:30.50	00:08.5	28.0%
From hard drive to network	00:52.28	04:23.53	03:31.2	80.2%

Figure 4: Time savings, in minutes:seconds, when performing encrypted file copies on the two systems.

In addition, we found that there is little to no adverse effect on performance on the new notebook after the hard drive has been encrypted using DDP|E (see Figure 5).

Dell Latitude E6520 Intel Core i5-2540M	Unencrypted file copies	Encrypted file copies	Time difference (minutes:seconds)	Time difference (percentage)
From network to hard drive	00:45.5	00:43.3	00:02.2	(4.8%)
From one hard drive spot to another	00:21.6	00:25.1	00:03.5	13.9%
From hard drive to USB drive	01:09.3	01:11.0	00:01.7	2.4%
From USB drive to hard drive	00:21.7	00:22.0	00:00.3	1.4%
From hard drive to network	01:12.0	00:52.3	00:19.7	(27.7%)

Figure 5: Time difference, in minutes:seconds, when performing unencrypted and encrypted file copies on the Intel Core i5-2540M processor-based Dell Latitude E6520.

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.