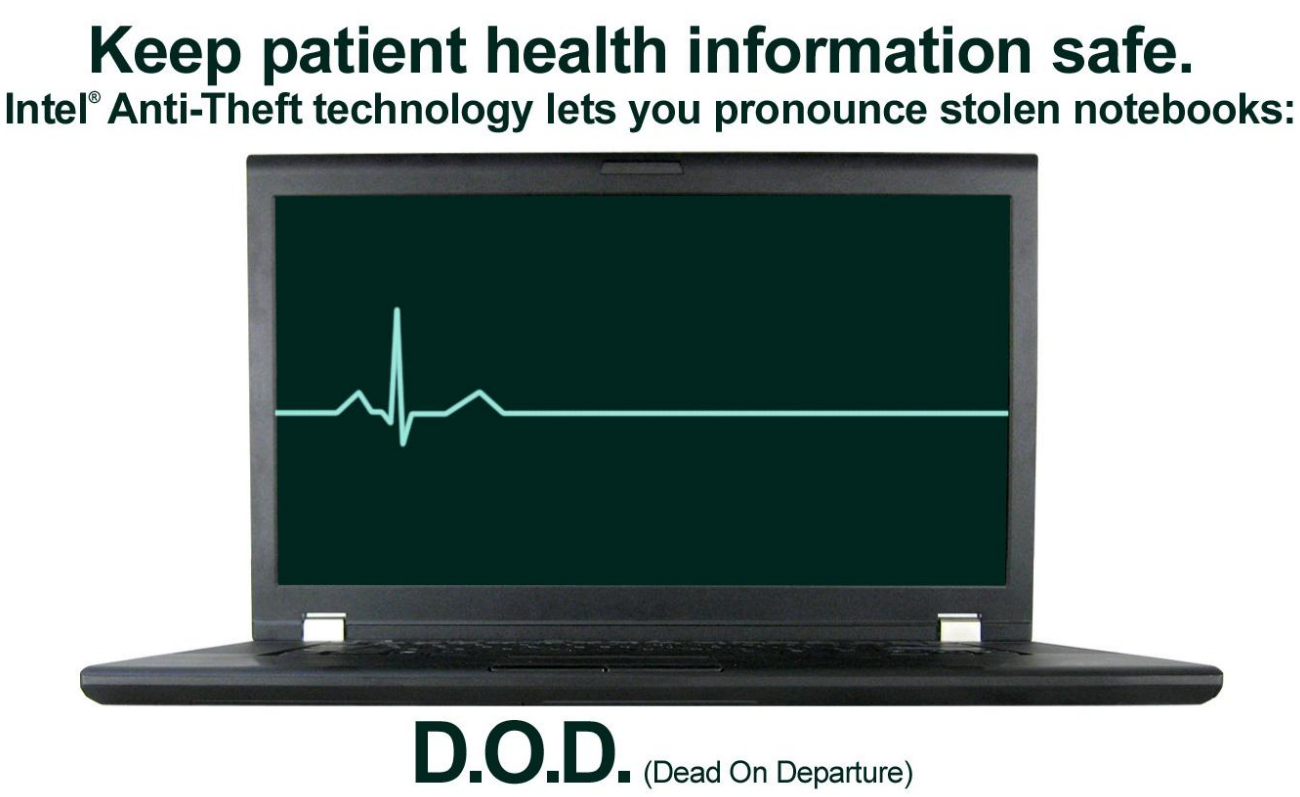
ADVANTAGES OF INTEL® vPRO™ TECHNOLOGIES FOR HEALTHCARE PROVIDERS IN NOTEBOOK THEFT SCENARIOS



OUR FINDINGS

When a healthcare worker's notebook PC containing electronic medical data is lost or stolen, the results can be catastrophic. Failure to protect sensitive patient data violates stringent health care regulations and can lead to notification penalties with high financial and reputation costs, and can erode patient trust in the healthcare provider. Using Intel® Anti-Theft Technology (Intel® AT), available on notebooks with Intel® Core™ vPro™ processors, mitigates these risks considerably by detecting loss or theft of a notebook and protecting its data. Intel AT adds value to full-disk encryption by protecting data even when encryption keys are weak or compromised. Principled Technologies tested the asset and data protection capabilities of Intel AT, as part of a Defense in Depth Strategy,[1] and found that it boosts healthcare organizations' ability to protect against data theft and loss to comply with healthcare security rules.

OUR PROCESS

We evaluated theft detection and response using three notebooks and one tablet, all with 2010 Intel Core vPro processors secured with Intel AT. Intel AT's hardware-based theft detection, response, and recovery mechanisms require activation with a service subscription from an Intel AT-enabled software and theft-management service provider. For our tests, we used Computrace® Complete security software by Absolute® Software. We conducted four test scenarios involving a range of ways that Intel AT can respond to theft and restore data access to the rightful owner of a notebook after its return.

[1] http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

JANUARY 2011
A PRINCIPLED TECHNOLOGIES TEST REPORT
Commissioned by Intel Corporation

PROJECT OVERVIEW

To test the key features of Intel AT with Computrace Complete, we evaluated three notebooks from three different vendors and one tablet from a fourth vendor, all with Intel AT technology, in four theft scenarios relating to the healthcare industry. Intel AT and Computrace Complete let an information technology (IT) department set up flexible policy-based responses to notebook theft or loss. A lost or stolen notebook can either disable itself by blocking the boot process or disable access to encrypted data by deleting essential cryptographic material stored on the chipset. These responses, which occur when the notebook detects suspicious activity, such as the failure of the user to connect to the Internet within a specified period, turn the notebook into a non-bootable "brick" that is useless to unauthorized users. Bricking does not destroy the patient data, but makes it inaccessible to anyone who steals or finds the system, thus preventing a potentially catastrophic data breach.

Test scenarios

We developed and tested four scenarios that simulate the theft or loss of a healthcare provider's notebook or tablet containing locally stored patient information. For all four scenarios, we evaluated how well Intel AT with Computrace Complete, and sometimes combined with encryption, protected the device from potential data breaches. For the three scenarios that let the rightful owner retrieve his or her data after the device is returned, we determined how quickly the owner could put the device back into use. Below, we summarize the four scenarios. More detailed descriptions appear in the What We Tested section.

- **Scenario 1: Protecting data by setting a rendezvous timer and restoring access with a password.** In this scenario, the user need not be aware of the theft; if the thief removes the device, and does not connect it to the Internet within a specified timeframe, the anti-theft solution activates a mechanism to prevent the thief from booting into the OS. In this scenario, the data is encrypted, so any attempts by the thief to remove the drive to get to the data, or to hack into the data another way, will fail. Upon return of the system, the rightful owner or IT administrator uses a password recovery token supplied by the IT administrator to restore complete access to all data.
- **Scenario 2: Protecting data by remotely disabling the system with a device freeze and restoring access with a recovery token.** In this scenario, the owner knows the device has been stolen. Upon discovering the theft, he or she contacts IT to request a device freeze, which preserves the data. As in the first scenario, the data can be encrypted, which protects it from any attempts by the thief to access the data. Upon return of the system, the rightful owner's IT administrator requests an authorization code using an endpoint security solution (in our case, Absolute Software) that restores complete access to all data.
- **Scenario 3: Using remote notification to delete data from the system.** In this scenario, the user discovers the theft immediately and notifies his or her IT administrator. However, the data on the device has not been encrypted. Because the highest priority is ensuring that the thief cannot access

the patient data, the IT person executes a permanent data delete. This extreme solution means that the rightful owner of the system loses access to the data even if the system is returned; therefore, this scenario has no data recovery component.

- **Scenario 4: Using geolocation to lock down a stolen device and restoring access with a recovery token.** In this scenario, the user is unaware of the theft. As part of their regular IT asset security protocol, they have already created geofences within the Customer Center to contain their devices. The next time the device contacts the Customer Center, location information will be collected. If the device is outside of the boundary, the customer will be alerted and can invoke an Intel AT lock to lock the system down. If the device does not have a GPS receiver, the device location can be determined using Wi-Fi technology. Windows Location & Sensor API compatible location sensors will also work (for Windows 7 clients only). Upon return of the system, the rightful owner or IT administrator can use a recovery token to restore access to the device.

Test hardware and software

We repeated each test scenario using notebooks from three major vendors, along with one tablet specially designed for use in healthcare facilities, and secured each system with data files we encrypted using DiskCryptor, a free encryption tool, and with Intel AT managed by Computrace Complete from Absolute Software. Detailed configuration information on the systems appears in Appendix A.

About Intel Anti-Theft (AT) Technology

The latest version of Intel AT is available on notebooks with Intel Core vPro 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. Once Intel AT locks down the device, the thief can no longer use it. Intel AT prevents the thief from re-installing the operating system (OS), even if the hard drive is replaced.

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 Computrace Complete from Absolute Software

Computrace Complete technology allows organizations to centrally track and secure their IT assets within a single cloud-based console – the Customer Center. 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 Customer Center to activate Intel AT, set Intel AT policy, and monitor the notebooks.

HEALTHCARE DATA SECURITY: AN OVERVIEW

When a healthcare organization experiences the types of device theft that we simulate in our scenarios, and has failed to protect sensitive client data, the costs and consequences are serious; the 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 Health Insurance Portability and Accountability Act (HIPAA) of 1996 established a set of national standards for the privacy and security of certain health information. 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 Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 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.[2] 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

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

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.

Industry research quantifies the risk and cost of data breaches:

- Notebook theft is the primary cause of data breaches.[3]
- The cost per record violated was about $294 in the healthcare sector in 2009, before the additional penalties associated with HITECH.[4] 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.[5]
- 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.[6]
- 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.[7]
- 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.[8]
- More than 10 percent of all notebooks in health and pharmaceutical companies will be lost or stolen sometime during their useful life.[9]
- 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.[10]
- 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.[11] 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

[3] Source: http://www.healthcareitnews.com/news/laptop-thefts-top-cause-health-data-breaches
[4] Source: http://hipaasecurityassessment.com/blog/state-enforcement-of-breach-notification-rules-is-on-the-rise/
[5] 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
[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid.*
[9] Source: http://antitheft.intel.com/Libraries/Documents/Ponemon_Intel_Billion_Dollar_Lost_Laptop_Problem.sflb.ashx
[10] Source: http://gtra.org/attachments/292_complianceprotectionrecovery.pdf
[11] 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

performance of an implementation of AES by 3 to 10 times over a completely software implementation.

WHAT WE TESTED

This section provides an overview of the test system setup and the four test scenarios we conducted. The results of our testing appear in the What We Found section. Appendix B provides the detailed steps we followed in our testing.

Setting up the test systems

We purchased three notebooks capable of supporting Intel AT, and Intel provided us with one healthcare-specific tablet. Upon receipt of each system, we verified the BIOS of each device as the latest version available, and enabled Intel AT in the BIOS, if necessary. We registered with Absolute.com for a free 90-day trial.[12] After logging onto Absolute Software's Web site, we downloaded and installed the Agent package via the link on our Absolute administrator home page. Within an hour of installing this package, we had successfully enrolled our devices. We confirmed this by launching the Intel Management and Security Status control panel and selecting the Intel AT tab, and by running an Asset Report in the Absolute Customer Center.

In the Customer Center, we created a geofence (an enclosed area with defined boundaries) on an Internet map that included our building and parking lot area. Then we created a rule so Computrace would alert us if a device strayed outside of the geofence. The Computrace Agent in each device reports location information using GPS or Wi-Fi technology. For our test, we received an email alert to advise us that our device was located outside of the geofence we created.

We also created rules so the service would alert us to changes in location based on IP addresses, and detect and notify us whenever the last call time was greater or equal to 48 hours. The hardware-based Intel AT timer can be set within the Customer Center to immediately lock the device if contact does not occur within a pre-defined period of time.

For the purposes of our encryption testing, we encrypted the system volume with DiskCryptor. We placed an Excel® spreadsheet containing fictional patient records in the encrypted volume.

[12] See your notebook vendor for vendor-specific pricing on Computrace Complete.

Scenario 1: Protecting data by setting a rendezvous timer and restoring access with a password

We simulated what happens when a notebook is lost or stolen and fails to call in or rendezvous within the time we defined using the rule/alert in the Customer Center. We did this by turning the notebooks and tablet off, and then turning them on after the timer would have expired. As soon as the devices powered up, the following message appeared: "Intel Anti-Theft system lock due to: Disable Timer Expired."

To restore access to the system, we had to enter a password, either the user password created when we set up the Intel AT Defaults, or a Server Token password generated in the Customer Center. To generate the token, we logged into the Customer Center and entered the Platform Recovery ID displayed on the locked device. A password was sent to the security administrators, or signing officers of the company designated during the initial Computrace Complete setup. When we entered this Server Token password at the Intel AT lock screen of the locked device, we regained full access to the device.

As we indicate above, setting up the custom settings for Intel AT-capable devices was a simple process in which we set up the default timer period, timer action, lock request action, Intel AT message, and password. Even if a notebook has been locked down, it is easy for an authorized IT administrator to unlock it using the password. During the boot process, Intel AT presented us with the option to enter the User Password or Server Token Password. Entering the Server Token Password took us past the Intel AT message screen, and into the OS, presenting us with a notebook restored to its original state and again usable by its rightful user.

Scenario 2: Protecting data by remotely disabling the system with a device freeze and restoring access with a recovery token

Through the Absolute Customer Center, the signing officers or authorized IT administrator can remotely request a device freeze for a stolen notebook. Once a device freeze request has been made, the notebook or tablet locks itself down, preventing access to the operating system desktop. After simulating the theft of our mobile devices, we were easily able to set up a device freeze in the Absolute Customer Center so that the next time the devices called in, they would be disabled.

In that process, the IT administrator must first request an authorization code from Absolute Software. Once the administrator receives the device freeze authorization code via email (we received ours within 1 minute), the IT administrator simply selects the device from the list of Intel AT-based devices, and submits a device freeze request. The administrator must enter the Absolute Customer Center signing officer's password and the device freeze authorization code before the endpoint security solution will grant the device freeze

request. Computrace Complete had disabled the device by the next call, or "rendezvous" (we initiated a test call using the Absolute test call application installed with the Computrace package). On our devices, the screens went blank with a custom message we created for the device freeze policy. To unlock the system, the IT administrator can request a passcode through the Absolute Customer Center and then enter the passcode by pressing ESC on the locked system, keying in the passcode, and pressing Enter. The system then reboots, allowing full access to the operating system, with the data and platform in their original state.

Scenario 3: Using remote notification to delete data from the system

This scenario tests the Computrace Data Delete feature. We simulated what happens when a user immediately discovers and reports the theft of a notebook or tablet and the data on the system has not been encrypted. In this scenario, upon learning of the theft, Absolute Software immediately begins to collect information on the location of the device. However, if the user wants the notebook or tablet locked down more quickly, Computrace can set a theft flag in the Customer Center, which instructs the agent to lock down the stolen device the next time it calls in. If the user is less concerned about retrieving the device and more concerned about protecting the data, he or she can request a remote data delete, which we performed in our test scenario. By selecting Request Data Delete in the Data Delete section of the Customer Center, we selected the specific device from our inventory, and chose to delete all files, including the OS. Computrace performed seven data overwrites of the disk to ensure the thief could not ever gain access to the notebook.

Scenario 4: Triggering a geolocation alert or IP address change alert, and locking down a stolen device and restoring access with a recovery token

For this scenario, we simulated what happens when a device, purchased for use in a doctor's office or healthcare facility, is taken from the premises. This scenario tests the Computrace Complete geolocation feature, enabled through Intel AT. This feature is most effective with GPS or Wi-Fi-equipped devices. To test this scenario, we created a geofence around the perimeter of the Principled Technologies office building, and disabled all other alerts. We took the four test systems home, connected to the home WiFi network, and manually called into Absolute by running ctmweb.exe, because our test devices were not equipped with GPS. The Absolute servers generate a geofence breach alert by sending an email to the IT department or signing officer. Next, the security administrator in the Absolute Customer Center can choose to invoke a freeze, if the device is, in fact, stolen. As with other alerts, we unlocked the notebook with the User Password or Server Token Password.

For devices that are not equipped with GPS, setting an alert for a change in IP address, as we describe in the Creating an IP address change alert section, achieves the same goal. As in the geofence test, we disabled all other alerts to isolate the effect of the change in IP address. When a device is removed from a doctor's office or hospital, the next time it connects to the Internet, the device will be given a new IP address. An alert was generated to the signing officer in email, specifying a change in IP address, allowing the security office the opportunity to invoke a freeze.

WHAT WE FOUND

Using Intel AT with Computrace Complete allowed us to successfully disable the devices in all four of our theft scenarios, protecting private patient data in accordance with federal regulations. In scenarios where the devices were recovered, we were able to provide access to the data and the platform in their original state.

In terms of a stolen computer, the Absolute Theft Recovery team can perform forensic and investigative work to aid in the recovery of the device, including device location and the identity of the unauthorized user. The team provides this intelligence to local police who can use it to investigate the crime, arrest the offender, and recover the stolen computer. The Absolute Theft Recovery Team staff consists of former law enforcement officers, which gives them the advantage of knowing how to work with the law enforcement community.

Computrace Complete technology also allows the Absolute Theft Recovery team to provide insight to the extent of a data breach by determining any files that were accessed post-theft.

Our results show that Intel AT reliably protects assets and should minimize the financial and legal risks to a healthcare organization when a notebook is lost or stolen.

APPENDIX A - TEST SYSTEMS

Figure 1 provides configuration information for the systems we tested.

System	HP ProBook 6550b	Dell™ Latitude™ E6510	Lenovo® ThinkPad® T510	Motion® Computing C5
General				
Device type	Notebook	Notebook	Notebook	Tablet
Number of processor packages	1	1	1	1
Number of cores per processor	2	2	2	2
Number of hardware threads per core	2	2	2	2
System power management policy	HP Optimized	Dell	Balanced	Motion Optimized
Processor power-saving option	Enhanced Intel SpeedStep® Technology	Enhanced Intel SpeedStep Technology	Enhanced Intel SpeedStep Technology	Enhanced Intel SpeedStep Technology
System dimensions (length x width x height)	14-1/2" x 9-3/4" x 1-1/2"	14-3/4" x 10” x 1-1/4"	14-5/8” x 9-1/2" x 1-1/2"	10” x 10” x 1”
System weight	5 lbs. 12.5 oz.	5 lbs. 9 oz.	5 lbs. 10 oz.	3 lbs. 6 oz.
CPU				
Vendor	Intel	Intel	Intel	Intel
Name	Core	Core	Core	Core
Model number	i5-560M	i5-560M	i5-560M	i7-640UM
Stepping	K0	K0	K0	C2
Socket type and number of pins	Socket 1156 LGA	Socket 1156 LGA	Socket 1156 LGA	Socket 1156 LGA
Core frequency (GHz)	2.66	2.66	2.66	1.20
Bus frequency	2.5 GT/s	2.5 GT/s	2.5 GT/s	2.5 GT/s
L1 cache	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)	32 KB + 32 KB (per core)
L2 cache	512 MB (shared)	512 MB (shared)	512 MB (shared)	512 MB (shared)
L3 cache (MB)	3	3	3	4

System	HP ProBook 6550b	Dell™ Latitude™ E6510	Lenovo® ThinkPad® T510	Motion® Computing C5
Platform				
Vendor	HP	Dell	Lenovo	Pegatron Corp
Motherboard model number	146E	02K3Y4	4314CTO	Barton 1.8
Motherboard chipset	Intel QM57	Intel QM57	Intel QM57	Intel QM57
BIOS name and version	HP 68CDF Ver. F.04 (10/27/2010)	Dell A05 (08/10/2010)	Lenovo 6MET75WW 1.35 (09/29/2010)	Motion Computing A03 (12/09/2010)
Memory module(s)				
Vendor and model number	Samsung M471B5773CHS-CH9	Hyundai HMT325S6BFR8C-H9	Elpida EBJ21UE8BDS0-AE-F	Hyundai HTM125S6BFR8C-H9
Type	PC3-10600	PC3-10600	PC3-8500	PC3-10600
Speed (MHz)	1,333	1,333	1,066	1,333
Speed running in the system (MHz)	1,066	1,066	1,066	800
Timing/Latency (tCL-tRCD-tRP-tRASmin)	7-7-7-20	7-7-7-20	7-7-7-20	6-6-6-15
Size (MB)	2,048	2,048	2,048	2,048
Number of memory module(s)	2	2	2	2
Chip organization (single-sided/double-sided)	Double-sided	Double-sided	Double-sided	Double-sided
Channel (single/dual)	Dual	Dual	Dual	Dual
Hard disk				
Vendor and model number	Western Digital WD3200BEKT	Seagate ST9320423AS	Hitachi HTS725032A9A364	Samsung MMCRE64G8MXP-0VB
Number of disks in system	1	1	1	1
Size (GB)	320	320	320	64
Buffer size (MB)	16	16	16	N/A
RPM	7,200	7,200	7,200	N/A
Type	SATA 3.0 Gb/s	SATA 3.0 Gb/s	SATA 3.0 Gb/s	SATA 3.0 Gb/s

System	HP ProBook 6550b	Dell™ Latitude™ E6510	Lenovo® ThinkPad® T510	Motion® Computing C5
Controller	Intel PCHM SATA AHCI Controller	Intel ICH8M-E/ICH9M-E/5 Series SATA RAID Controller	Intel 5 Series/3400 Series SATA AHCI Controller	Intel 5 Series SATA AHCI Controller
Driver	Intel 8.9.6.1002 (01/08/2010)	Intel 9.6.0.1014 (03/03/2010)	Intel 7.0.0.1013 (06/04/2009)	Intel 9.6.0.1014 (03/03/2010)
Operating system				
Name	Windows® 7 Professional	Windows 7 Professional	Windows 7 Professional	Windows 7 Professional
Build number	7600	7600	7600	7600
Service Pack	N/A	N/A	N/A	N/A
File system	NTFS	NTFS	NTFS	NTFS
Kernel	ACPI x64-based PC	ACPI x64-based PC	ACPI x64-based PC	ACPI x64-based PC
Language	English	English	English	English
Microsoft DirectX version	11	11	11	11
Graphics				
Vendor and model number	Intel HD Graphics (Core i5)	Intel HD Graphics (Core i5)	Intel HD Graphics (Core i5)	Intel HD Graphics (Core i7)
Type	Integrated	Integrated	Integrated	Integrated
Chipset	Intel HD Graphics (Core i5)	Intel HD Graphics (Core i5)	Intel HD Graphics (Core i5)	Intel HD Graphics (Core i7)
BIOS version	2009.0	1994.24	1998.1	2026.0
Total available graphics memory (MB)	1,696	1,696	1,696	1,435
Dedicated video memory (MB)	64	64	64	64
System video memory (MB)	0	0	0	0
Shared system memory (MB)	1,632	1,632	1,632	1,371
Resolution	1,366 x 768 x 32-bit	1,366 x 768 x 32-bit	1,366 x 768 x 32-bit	1,024 x 768 x 32-bit
Driver	Intel 8.15.10.2119 (04/21/2010)	Intel 8.15.10.2182 (07/19/2010)	Intel 8.15.10.2253 (11/28/2010)	Intel 8.15.10.2219 (10/01/2010)
Sound card/subsystem				
Vendor and model number	Intel Display Audio	Intel Display Audio	Intel Display Audio	IDT High Definition Audio CODEC
Driver	Intel 6.12.0.3047 (02/03/2010)	Intel 6.12.0.3065 (06/21/2010)	Intel 6.14.0.3074 (10/15/2010)	IDT 6.10.6276.0 (03/23/2010)

System	HP ProBook 6550b	Dell™ Latitude™ E6510	Lenovo® ThinkPad® T510	Motion® Computing C5
Ethernet				
Vendor and model number	Intel 82577LM Gigabit Network	Intel 82577LM Gigabit Network	Intel 82577LM Gigabit Network	Intel 82577LM Gigabit Network
Driver	Intel 11.5.10.1011 (01/07/2010)	Intel 11.6.92.0 (04/12/2010)	Intel 11.5.10.1030 (07/22/2010)	Intel 11.6.92.0 (04/12/2010)
Wireless				
Vendor and model number	Intel Centrino® Advanced-N 6200 AGN	Intel Centrino Advanced-N 6200 AGN	Intel Centrino Advanced-N 6200 AGN	Sierra Wireless Gobi 2000 Mobile Broadband
Driver	Intel 13.1.1.1 (01/13/2010)	Intel 13.3.0.24 (07/14/2010)	Intel 13.4.0.9 (10/18/2010)	Qualcomm Inc. 3.0.2.3 (06/03/2010)
Optical drive(s)				
Vendor and model number	HP AD-7586H	HL-DT-ST DU30N	Optiarc AD-7700H	N/A
Type	DVD-RW	DVD-ROM	DVD-RW	N/A
USB ports				
Number	3	3	3	4
Type	2.0	2.0	2.0	2.0
Other	eSATA, Display Port, 5-in-1 Media Card	eSATA, Display Port, Media Card Reader	eSATA, Display Port, 5-in-1 Media Card	N/A
IEEE 1394 ports				
Number	1	1	1	0
Monitor				
LCD type	LED-backlit HD anti-glare	HD Anti-Glare LED	HD Anti-glare, LED Backlight	XGA TFT AFFS+ LED Blacklight
Screen size (inches)	15.6	15.6	15.6	10.4
Refresh rate (Hz)	60	60	60	60
Battery				
Type	HP TD06 Li-ion	Dell W1193 Li-ion	Lenovo 55+ Li-ion	Motion MC5450BP Li-ion
Size (length x width x height)	8” x 2” x 7/8”	8” x 1-7/8” x 3/4"	8-1/8” x 2” x 3/4"	4-7/16” x 4-1/2"
Rated capacity	5,000mAh / 10.6V (55Wh)	5,400mAh / 11.1V (60Wh)	7,800mAh / 10.8V (57Wh)	4,000mAh / 11.1V (42Wh)
Weight (oz.)	10.9	11.5	11.1	10.5

Figure 1: Configuration information for the four systems we tested.

APPENDIX B - TEST PROCESS

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 www.absolute.com.
3. In the upper-right corner of the Absolute homepage, click Login, and select Absolute Customer Center.
4. Enter the user name and login for the administrator account.
5. At the Absolute administrator home page, scroll down to the bottom of the page, and click Download Packages.
6. Select Windows to begin downloading the ZIP file package.
7. Browse to the saved ZIP file, and extract its contents to the C:\ drive.
8. Once all the files are extracted, browse to the MSI_Deployment folder.
9. Double-click Computrace.msi to launch the Computrace agent installation package.
10. When the Confirm installation screen appears, click Next to begin the installation.
11. 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 www.absolute.com, if not already logged in.
2. In the upper-right corner of the Absolute homepage, click Login, and select Absolute Customer Center.
3. Enter the user name and login for the administrator account.
4. On the left side of the Absolute administrator homepage, click Data and Device Security.
5. Select Intel Anti-Theft Technology from the Data and Device Security sub-categories.
6. 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.

Creating a geofence and a geofence breach alert

1. Open Internet Explorer on any computer, and navigate to www.absolute.com, if not already logged in.
2. In the upper-right corner of the Absolute homepage, click Login, and select Absolute Customer Center.

3. Enter the user name and login for the administrator account.
4. On the left side of the Absolute administrator homepage, click Administration.
5. Click Geofences→Create and Edit Geofences.
6. Enter a name in the Geofence Name field.
7. Enter a description in the Geofence Description field.
8. Leave remaining defaults selected.
9. Zoom in until you are at street-level view, and the distance scale represents 150 yards.
10. Click Create Boundaries, and create a polygon of coverage on the map, line by line, with a series of clicks on the map.
11. On the left side, navigate to Alerts→Create and Edit Alerts.
12. Enter a name for the new alert (e.g., Geofence breach).
13. Enter a description for the alert.
14. Set the Suspicion level to 5.
15. Under Conditions, select Geofence Location from the Field drop-down menu.
16. Select Is Outside from the Rule drop-down menu.
17. Set the rule to the proper geofence, and set the time period to at least 1 hour.
18. Click Add Condition.
19. Under Scope, ensure that all enrolled devices are selected.
20. Leave the defaults for Alert Type and Alert Options.
21. Under Action, select Log event and notify.
22. Enter the appropriate email addresses to receive the alert.
23. Click Save.
24. On the left side, click View and Manage Alerts.
25. Ensure that the Geofence breach alert has a status of Active.

Creating an IP address change alert

1. Open Internet Explorer on any computer, and navigate to www.absolute.com, if not already logged in.
2. In the upper-right corner of the Absolute homepage, click Login, and select Absolute Customer Center.
3. Enter the user name and login for the administrator account.
4. On the left side of the Absolute administrator homepage, navigate to Administration→Alerts→Create and Edit Alerts.
5. Enter a name for the new alert (e.g., IP Address).
6. Enter a description for the alert.
7. Set the Suspicion level to 5.
8. Under Conditions, select IP Address (Local) from the Field drop-down menu.
9. Select Changed from the Rule drop-down menu.
10. Click Add Condition.
11. Under Scope, ensure that all enrolled 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.

Setting up a rendezvous timer alert

1. Open Internet Explorer on any computer, and navigate to www.absolute.com, if not already logged in.
2. In the upper-right corner of the Absolute homepage, click Login, and select Absolute Customer Center.
3. Enter the user name and login for the administrator account.
4. On the left side of the Absolute administrator homepage, navigate to Administration→Alerts→Create and Edit Alerts.
5. Enter a name for the new alert (e.g., Last call time greater than 2 hours).
6. Enter a description for the alert.
7. Set the Suspicion level to 4.
8. Under Conditions, select Last Call Time from the Field drop-down menu.
9. Select Greater or Equal To from the Rule drop-down menu.
10. Set the Criteria to 2 days (48 hours).
11. Click Add Condition.
12. Under Scope, ensure that all target devices are selected.
13. Leave the defaults for Alert Type and Alert Options.
14. Under Action, select Log event and notify.
15. Enter the appropriate email addresses to receive the alert.
16. Click Save.
17. On the left side, click View and Manage Alerts.
18. Ensure that the IP Address alert has a status of Active.

Scenario 1: Protecting data by setting a rendezvous timer and restoring access with a password

1. Shut down the target system, and wait 48 hours.
2. Power on the target system.
3. Verify that the system is locked.
4. Verify that the administrator received an email alert.
5. Enter the User Password created as part of the Intel AT Defaults in the Absolute Customer Center.

Scenario 2: Protecting data by remotely disabling the system with a device freeze and restoring access with a recovery token

1. Open Internet Explorer on any computer, and navigate to www.absolute.com, if not already logged in.
2. In the upper-right corner of the Absolute homepage, click Login, and select Absolute Customer Center.
3. Enter the user name and login for the administrator account setup with Absolute.
4. On the left side of the Absolute administrator homepage, navigate to Data and Device Security→Security Authorization→Request Authorization Code.

5. Click Request Code.
6. Check the administrator account's email, and write down the authorization code provided in the authorization code email from Absolute.
7. On the left side of the Absolute administrator homepage, navigate to Data and Device Security→Data Freeze→Request Data Freeze.
8. Click Choose, and select the target device.
9. If there are any custom messages set up, select the desired message.
10. If not, leave Select a message blank, and click Submit.
11. Under Provide Authentication, enter the administrator Customer Center password and the Authorization Code provided in the email from earlier steps.
12. Click OK.
13. Locate the green box with a pass code at the top of the screen, and write down the passcode for use when unlocking the target system.
14. On the left side, click Device Freeze Summary Report.
15. The next time the target device calls in, the new device freeze request status will change from Freeze Requested to Frozen.
16. Log into the target system.
17. After logging in, the screen should be completely white, displaying any messages that were selected in the device freeze request process. This behavior shows that the system successfully received a device freeze command from the Computrace.
18. To unfreeze the device, press the Esc key.
19. Though no window appears, type in the pass code that you recorded in Step 13.
20. Press Enter. The system will restart.
21. Once the Windows login screen appears, log in. Verify that the system should now behave normally by opening the health information test file in Excel.
22. On the administrator computer, log into the Absolute administrator homepage again.
23. 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.

Scenario 3: Using remote notification to delete data from the system

1. Open Internet Explorer on any computer, and navigate to www.absolute.com, if not already logged in.
2. In the upper-right corner of the Absolute homepage, click Login, and select Absolute Customer Center.
3. Enter the user name and login for the administrator account.
4. On the left side of the Absolute administrator homepage, navigate to Data and Device Security→Security Authorization→Request Authorization Code.
5. Click Request Code.
6. Check the administrator account's email, and write down the authorization code provided in the authorization code email from Absolute.
7. On the Absolute administrator homepage, navigate to Data and Device Security→Data Delete→Request Data Delete.
8. Under Identifier, click Choose, and select the target device for the data delete.

9. Under Reason, select Other.
10. Under Data Delete Policy, select All Files Including OS.
11. Leave the default settings for Data Delete Options.
12. Under Data Delete Validation, check the box beside I accept the agreement.
13. Click Set Data Delete.
14. On the next page, ensure that all the information provided in the window is correct, and click Submit Data Delete Request.
15. Under Provide Authentication, enter the administrator Customer Center password and the Authorization Code provided in the email from earlier steps.
16. Click OK.
17. On the left side, click Data Delete Summary Report.
18. The new Data Delete request should be listed.
19. Once the process has begun, the status will be listed as Launched.
20. Log out.
21. To ensure a successful Data Delete, try to log into the target computer. If successful, you will no longer be able to log in.

Scenario 4: Triggering a geolocation alert or an IP address change alert, and locking down a stolen device and restoring access with a recovery token

1. Create a geofence and a geofence alert, as we describe above, and disable all other alerts.
2. Remove the enrolled devices from the premises.
3. Connect to the Internet on the enrolled devices not equipped with GPS or WiFi.
4. Manually initiate a call into the Absolute servers.
5. Reboot.
6. Check the administrator account's email, and verify receipt of a geofence breach alert from Absolute.
7. Repeat this by removing the geofence alert and creating an IP address change alert, as we describe above.
8. Connect to the Internet on the enrolled devices.
9. Manually initiate a call into the Absolute servers.
10. Reboot.
11. Check the administrator account's email, and verify receipt of an IP address change alert from Absolute.

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.