PC-Disable Delivers Intelligent Client-Side Protection for Lost or Stolen Notebooks

Absolute Software*[1] and Intel deliver a new level of theft deterrence and data defense through integrated hard-ware and software technologies for notebook PCs. Computrace,* a leading IT asset-management and security solution from Absolute Software, is taking advantage of Intel® Anti-Theft Technology – PC Protection (Intel® AT-p),[2] which is designed into system hardware. Through Computrace, an authorized information technology (IT) administrator can remotely delete data on a notebook, or the notebook can now intelligently lock itself down and prevent an OS from booting. If the notebook is reported lost or stolen, the IT administrator simply flags it in the Computrace Web portal and sets up a "poison pill" so the next time the notebook "phones home," it will be disabled. In both cases, whether the notebook locks itself down or receives a poison pill, and even if the hard drive is reformatted or replaced, anti-theft security options remain in place. Getting the system operational again is easy – authorized users can quickly restore the system with a one-time reactivation token provided by the IT department. IT now has a more reliable, robust approach to protecting assets and minimizing financial and/or legal risk from lost or stolen notebooks.

Absolute® Software

intel®

Table of Contents

Executive Summary

Keeping data secure in a mobile environment is not just a daunting challenge, but a critical requirement. Loss and theft of notebooks computers leaves sensitive data vulnerable, while financial and legal exposure causes additional problems and disruptions to business. In addition, companies must comply with increasingly stringent regulations in data security and privacy.

Computrace,* a leading IT asset-management and security solution from Absolute® Software,[1] now takes advantage of Intel® Anti-Theft Technology – PC Protection (Intel® AT-p).[2] Intel AT-p enhances existing Absolute solutions by adding client-side intelligence, designed into notebook hardware, to detect potential theft and respond. Computrace has traditionally allowed IT administrators to remotely delete data on the system. Enabled by Intel AT-p, Computrace now also allows IT administrators to remotely (via client notification) or automatically (via client-side intelligence) lock down a system quickly in case of loss, theft, or suspicious circumstances. Reactivation after PC Disable is easy – a key advantage of the Computrace solution is that the lock down is not a data-destruct process. The user or IT administrator can easily restore a notebook to typical working condition by entering a one-time reactivation token (provided by IT).

IT now has a local, tamper-resistant defense that works even if the OS is reimaged, the hard drive is replaced, or the notebook is disconnected from the network (via timer expiry). Over time, the integration of this hardware-based technology with the robust Computrace solution could also help reduce the incidence of theft, since a notebook that disables itself also becomes less attractive to steal. The result can be better protection of assets and sensitive data on notebooks, rapid reactivation when systems are returned, and reduced business risk.

Intelligent client-side defense for lost or stolen notebooks

Absolute Software and Intel deliver a robust, integrated solution to protect notebook PCs from unauthorized access.

Traditional challenges in defending data on notebooks

IT administrators face significant hurdles in protecting assets and data on notebooks that are lost or stolen. Such notebooks are vulnerable to a variety of attacks designed to reconfigure the device for another use and/or gain access to sensitive data stored on the system.

Sensitive data is still highly vulnerable

To find out how effective typical anti-theft measures are, the Ponemon Institute conducted several studies, including surveys of over 2,600 IT and information security professionals in eight countries.[3,4] Results showed that:

- 72% of U.S. employees are allowed to store sensitive and confidential information on their notebooks.[3]
- 92% of IT security professionals reported notebook theft or loss in their organization.[4]
- Lost or stolen notebooks result in a data breach 71% of the time.[4]
- 89% of employees ask others to watch their notebook while traveling.[4]

Users and thieves circumvent software-based security measures

One of the problems with notebook security is that anti-theft software products can be installed and uninstalled relatively easily. Software-only approaches also require that the OS is loaded and working properly, which means they may fail if the OS is compromised or inoperable. With a software-only agent, a thief may be able to circumvent the agent by reformatting or replacing the hard drive to make the notebook usable again, or remove the hard drive to another system to access the data on the disk. Employee behavior makes it even easier for thieves. For example,

- Only 34% to 58% of notebooks are configured for encryption to protect sensitive data.[3,5]
- 56% of employees who have encryption on their notebooks disengage the encryption solution.[4]

Costs are high and regulations increasingly strict

The real cost of a lost or stolen notebook is significant. Ponemon Institute studies show that costs average $49,000 per notebook based on multiple factors such as intellectual property loss and data breach, especially when a business must notify clients or the public of the breach.[3] Although encryption can reduce that cost by almost $20,000, Ponemon Institute surveys revealed that, for 55% of lost or stolen notebooks, IT cannot prove a notebook was encrypted at the time of loss or theft.[3,4]

Keep sensitive data out of the wrong hands

Absolute and Intel have collaborated closely to deliver a new level of intelligent client-side protection for assets and sensitive data and intellectual property stored on notebooks. Computrace* has traditionally allowed IT administrators to remotely delete data. Enabled by Intel® Anti-Theft Technology – PC Protection (Intel® AT-p), Computrace now provides IT with new capabilities to rapidly lock-down a notebook if the system is lost or stolen. IT can then rapidly reactivate the system when it is recovered. This gives IT a powerful set of options to respond to loss, theft, or suspicious circumstances:

- **Flag systems** that are or might be lost or stolen.
- **Send a data-destruct command** to erase sensitive data, by file, file location, or file type, or by erasing the entire contents of the hard disk.
- **Recover stolen notebooks,** with help from the Absolute Theft Recovery Team.
- **Disable a notebook that doesn't check in** within an IT-defined period of time.
- **Send a poison pill** to lock down the notebook and prevent an OS from booting.
- **Unlock a notebook** once security is reestablished.

Complementing other security measures

Computrace with Intel AT-p complements encryption layers and other security measures by allowing security responses that range from rapid client-side lock-down to full data destruction and the physical recovery of stolen computers. The new security capabilities can also integrate with existing encryption solution pre-boot authentication modules.

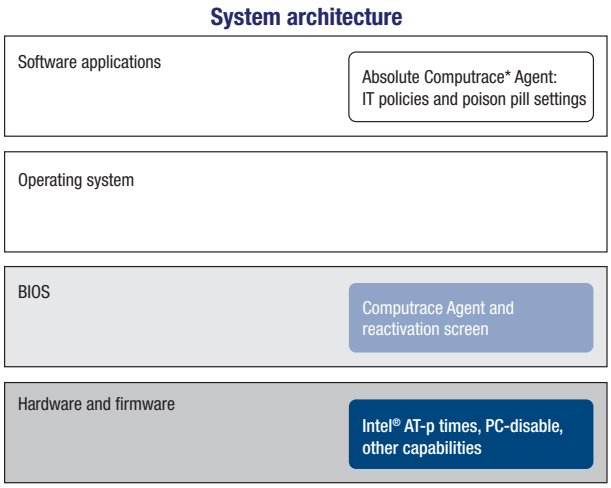

Figure 1. Architecture for Absolute's Computrace,* as enabled by Intel® Anti-Theft Technology – PC Protection

Traditional solutions	Computrace* with Intel® AT-p	Benefits of Computrace and Intel AT-p
Software-based	Hardware/BIOS/ software-based	• Tamper-resistant hardware-based capabilities • Allows a rapid response to loss or theft, even without a network connection • Addresses compliance via flexible policies • Reduces corporate risk
No PC disable	Local/remote PC disable	
Relies on network connectivity	Works with and without network connectivity	
Typically relies on OS and/or hard drive	PC Disable (via timer expiry) remains active even if OS is missing or reinstalled, hard drive is reimaged or replaced, or BIOS is reflashed	

Table 1. Advantages of client-side intelligence in theft management

Tamper-resistant technology

Because Intel AT-p is designed into the notebook's hardware, the new anti-theft capabilities are more protected from tampering (see Figure 1). The new capabilities do not depend on the OS. Also, timer expiry can work even if notebooks are not connected to the network, the OS or BIOS is reinstalled, or the hard drive is reformatted or replaced. The Intel AT-p feature called PC Disable, once activated, also works regardless of boot device: hard drive, USB key, CD, DVD, and so on.

Faster lock-down and rapid recovery

Traditionally, Absolute has been able to recover 3 out of 4 stolen notebooks that call in to the Monitoring Center.[6] This high rate of recovery is one of the key advantages of Absolute security solutions. In addition, Computrace has traditionally provided IT with robust methods to erase sensitive data from notebooks that are lost or stolen.

Enabled by Intel AT-p, Computrace now adds a fast, intelligent client-side ability to lock down the notebook and prevent any OS from booting: hard drive, USB key, CD, DVD, or other boot devices. (see Table 1).

- Timer expiry works even if theft/loss is not reported, and even if the notebook cannot communicate with the central server. For example, timer expiry works even if central server communication is disabled via port blocking, or the agent is prevented from running.
- Poison pill delivers a rapid local PC disable.
- Reactivation is easy and fast.

When a notebook is reported lost or stolen, IT has several options. IT can recover the notebook for forensic capture (see what has been accessed), remotely delete the data on the machine, or send a poison pill to the notebook to disable the notebook and turn it into a "brick" – an unusable weight. Or, if the notebook has not checked in to the central server before its timer expires (an IT-programmable event) the system identifies a suspicious circumstance and locks itself down.

Timer expiry allows for intelligent local response

Computrace provides a local intelligent response to suspicious circumstances through the use of hardware-based Intel AT-p timers. These timers establish rendezvous requirements for notebooks. A rendezvous is an authorized check-in via the Internet, with the theft-management server. This check-in must occur within the IT-defined time period. For example, a financial advisor might be required to connect to the Internet daily, to ensure their notebook can check in and download its asset and location information. This check-in helps Computrace identify whether or not the notebook is "safe" and under control of the intended user. Computrace tracks this check-in activity and, based on IT policy, triggers a response if necessary, such as locking down the system based on local timer expiry.

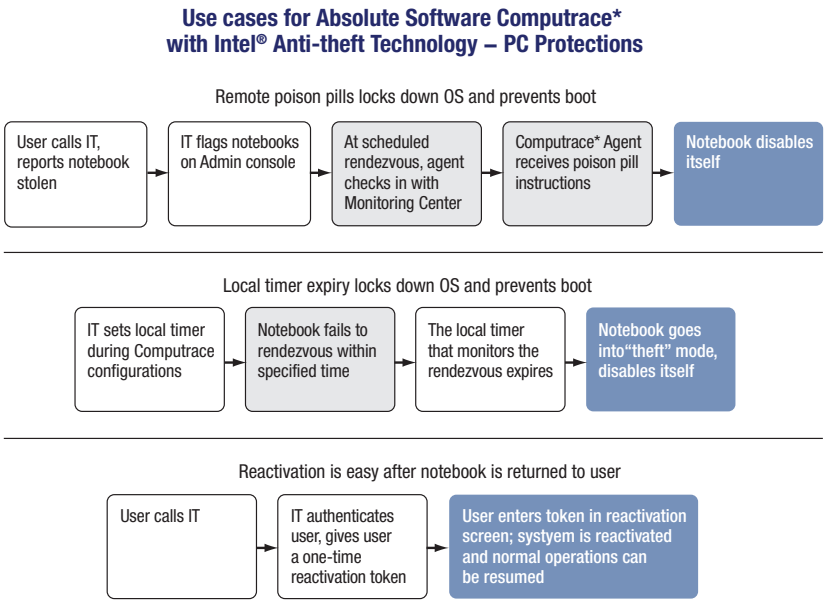

Figure 2. Use cases for poison pill, local timer expiry, and reactivation

Timer expiry works regardless of state of network, OS, BIOS, or hard drive

Because the timer resides within the notebook itself, it works even if the notebook does not connect to the network. Built into the notebook's hardware, the timer continues to work even if the OS is reinstalled or the BIOS is reflashed, other security solutions have been removed, or the hard drive has been reformatted or replaced. Once the notebook itself is disabled, replacing the hard drive does not circumvent the blocked boot.

Use case: Undetected theft, but missed check-in locks down notebook

In this case, a design engineer (Marsha) is working on a sensitive new project. Early one week, Marsha leaves for a training conference, and while she's gone, her notebook is stolen from her office. The thief does not immediately power up the notebook, but hides it in a safe, temporary place. Since Marsha will be gone for several more days, the theft is not immediately noticed.

However, because of the importance of the engineer's project, IT policy is that the notebook must check in with the Monitoring Center each day. After being stolen, the daily check-in was missed. As determined by locally stored policy (set by IT), the next time the notebook powers up, it enters "theft mode" (see Figure 2). The notebook then disables itself. Even if the thief tries to power up the system later, the OS will not boot, so access to the system and use of the notebook is thwarted.

Use case: End of life disable

Absolute's Computrace solution is also effective at the end of a notebook's life cycle. IT can simply use Computrace features to trigger a full system data-destruct, then send a poison pill to disable the notebook and prevent the system from rebooting. Only an authorized IT administrator can then unlock the system for reconfiguration or some other authorized use.

PC-disable is rapid and allows full reactivation

Computrace has traditionally provided IT with powerful mechanisms to remotely erase sensitive data if a notebook is lost or stolen. Although erasing a single file can be done quickly, erasing all files of a particular type or destructively overwriting the hard disk can take some time. The traditional issue has been that, the longer the system remains active, the more time an unauthorized user has to try to access sensitive data.

Enabled by Intel AT-p, Computrace allows a remote lock-down of a notebook as soon as the system connects to the Internet and checks in with the Absolute Monitoring Center. If the notebook's theft flag has been set in the server database, the poison pill is delivered when the notebook checks in. The notebook then disables itself and prevents the OS from rebooting. Even if the hard drive is replaced, the notebook will not boot. Only the reactivation screen is available.

With Computrace and Intel AT-p, IT can remotely turn a lost or stolen notebook into a "brick" that is useless to a thief.

PC disable works regardless of state of OS, BIOS, or hard drive

When triggered, the PC Disable capability can control the boot process. Because the capability is designed into the notebook's hardware, it remains in place even if the OS or BIOS is reinstalled, other security solutions have been removed, or the hard drive has been reformatted or replaced.

Use case: Stolen notebook

In this case, a financial advisor (Jeff) has been on the road to various clients in various cities. At the airport, Jeff sets his bag down to prepare to go through bag-check, and his notebook is stolen. Jeff immediately calls IT, and the administrator flags the notebook in the central database (see Figure 2 on page 5).

Typically, the thief does not wait long to power up the notebook and connect to the Internet to find out if the system is working and what kind of data is on it. However, protected by Computrace with Intel AT-p, the notebook begins its check-in with the Monitoring Center. As soon as the notebook checks in, it receives the poison pill set in the server by IT. The notebook then disables itself to prevent a reboot. The notebook is now a "brick."

To the thief, the rendezvous (check-in) process is invisible. All the thief sees is that the notebook has become inoperable and won't load the OS. Even if the thief tries to replace the hard drive, the poison pill remains in effect, blocking the boot process.

Use case: Lock down notebook before police report is completed

The Absolute Theft Recovery Team requires a police report before they begin work on tracking and recovering a stolen notebook. Sometimes users can get the police file number online, very quickly. Sometimes, especially overseas, the process can take half a day or more. Although many users typically want to retain contact with the notebook in the hopes of recovery, other users want to make sure the machine is not usable once it is out of their possession.

Computrace allows authorized IT administrators to remotely delete data on a notebook. Enabled by Intel AT-p, Computrace now allows IT to immediately set a theft flag in the Monitoring Center database. This allows the Computrace Agent to lock down a stolen notebook the next time the notebook checks in with the Monitoring Center. The automated lock-down can help prevent a thief from accessing the system even before the police can complete and file a police report and the Absolute Theft Recovery Team can get involved.

Improving compliance with regulations

Hearing of recent highly publicized data breaches and, in some cases, with internal breaches of their own, businesses are aware of the financial, legal, and public relations costs of data losses. However, IT still faces significant challenges in meeting compliance laws designed to protect sensitive data.

Computrace* by Absolute Software is taking advantage of Intel® Anti-Theft Technology – PC Protection (Intel® AT-p) to improve theft management. Computrace with Intel AT-p addresses compliance throughout the theft-management cycle, from prevention to detection, response, reactivation, and recovery. This makes it easier to comply with increasingly stringent laws and regulations on privacy and security:

- Sarbanes-Oxley
- State data-breach laws
- Fair and Accurate Credit Transactions Act (FACTA) and the Red Flag Rule
- FACTA Disposal Rule
- Gramm-Leach-Bliley
- HIPAA

Data-erase or "bricking" – either way, the notebook is secured

Enhanced by Intel AT-p, Computrace offers a two-tier approach to theft management by allowing IT to remotely erase data on a notebook or fully disable a system that has been lost or stolen. Notebooks with the Computrace Agent either call in to the Monitoring Center and receive a destructive data erase and/or a poison pill, or the timer expires and the notebook locks down. Either way, the system is secured.

Easy reactivation and full system restore

Computrace with Intel AT-p makes it easy to reactivate a notebook. The user or IT administrator simply enters a strong one-time token in the reactivation screen – the only screen available after a lock-down. This resets the timer and allows the system to boot to its normal working state. With Computrace with Intel AT-p, IT has a simple, inexpensive way to restore a notebook without compromising sensitive data or the system's other security features.

Intel® Anti-Theft Technology

Independent of TPM and Intel® Active Management Technology (Intel® AMT)

- Intel AT-p works independently of a Trusted Platform Module (TPM). You do not need TPM in order to take advantage of the Intel AT-p capabilities in Absolute's Computrace.*
- Intel AT-p works independently of Intel AMT. Enabled by Intel AT-p, Computrace delivers hardware-based data security without sacrificing manageability.

Rapid reactivation when "missing" notebooks are located

In some cases, a "missing" notebook might actually be with a coworker. Or, a CEO might have forgotten to notify IT that he or she was going on vacation. In the past, a potentially missing notebook that contained sensitive data might have been instructed to perform a destructive data erase the next time it checked in with the Absolute Monitoring Center. Such a response might be a false positive – not fully warranted. Worse, such a response could require a lot of time for restore tasks – rebuilding the OS, restoring user files (if there were back-ups available), restoring user settings, and so on.

Enabled by Intel AT-p, Computrace now allows IT to lock down a potentially missing system without a destructive data wipe. When a notebook is "located," the user or IT administrator simply enters a one-time token to reactivate the system. This lets IT rapidly secure notebooks that might be missing, yet still reactivate and recover quickly and fully when the system is located.

Easy deployment

Computrace with Intel AT-p can be deployed like a typical patch or other software update, via IT's existing deployment application.

Select models of notebooks will ship preconfigured, or "ready," for Intel AT-p. IT administrators simply install and activate the Computrace Agent to manage the notebooks as usual, before deploying them to users.

Capgemini

Capgemini is a recognized global leader in IT consulting, technology, and outsourcing.[7] Within the company's Benelux region, all 7,000 consultants use a notebook.[8] Due to the global client base, consultants often travel long distances, including across several countries. Therefore, notebook loss or theft has been a traditional challenge for the Benelux IT department.

Recently, Capgemini Benelux conducted a pilot of Absolute Software Computrace* with Intel® Anti-Theft Technology – PC Protection (Intel® AT-p). Having seen the technology in action, Capgemini is impressed with how effectively they can now secure notebooks that might have been stolen from a car, left at a client site, or otherwise lost.

"This poison-pill technology is going to be of immense value in keeping our notebooks safe," says Don van Gelder, Infrastructure Architect at Capgemini Nederland BV. "Not just for our own consultants, but for a large percentage of our global client base. It's going to let us secure assets in circumstances that simply couldn't be addressed before – for systems that were out of our reach. Now we have a secure, policy-driven process to quickly lock down a system until it is recovered, improving both security and compliance."

BMW

Securing assets is a priority for the BMW Group.[9] Intrigued by the potential of the new Intel AT-P technology, BMW recently conducted a pilot of the Absolute solution with Intel AT-p in their production environment. BMW was very interested in seeing how the theft-management technology would improve end-of-lease processes by allowing IT to lock down a system at the end of its lease if the system was not returned. The company has been looking for tamper-resistant ways to secure assets and encourage a nearly complete rate of return.

"We are extremely pleased with this lock-down technology," says Thomas Schmidt, IT solutions, the BMW Group. "It could complement our existing client-management processes and would help us further improve asset management and reduce costs."

In the future...

Absolute primarily sells today's solutions as managed services, in which IT remotely accesses notebooks through a Web console. The company expects to release an enterprise-level stand-alone monitoring center for in-house deployments within the year.

Protect assets and data more effectively and lower corporate risk

Utilizing Computrace with Intel AT-p, IT administrators can manage assets, remotely delete data, recover stolen notebooks, and "brick" computers that are on or off the Internet and company networks. IT now has tamper-resistant options for securing data, fully deactivating a missing notebook to make it worthless to a thief. IT also has a fast, inexpensive way to reactivate a "bricked" notebook and return it to its normal operating state. Over time, as thieves learn that notebooks become useless very quickly, companies could see a reduction in traditional notebook theft.

The combination of the Computrace security solution with hardware-based Intel AT-p delivers a new level of client-side defense against notebook loss or theft. IT administrators can now secure an asset even if the theft or loss is not realized immediately, whether or not the system is connected to the Internet or network – and this protection works, regardless of the state of the hard drive, BIOS, or OS. This enhanced protection extends IT's security capabilities on and off the network to protect assets and sensitive data and minimize business risk.

To learn more about Intel Anti-Theft technology, visit **www.intel.com/technology/anti-theft**

For more information about Absolute Software products that support Intel AT-p and lists of notebooks that are ready for Computrace and Intel AT-p, visit **www.absolute.com/intel**

Absolute® Software

intel®

[1] All information about Absolute Software was provided by Absolute Software.

[2] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) for PC protection (also referred to as the 'poison pill' in some documents) requires the computer system to have an Intel AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. Intel AT-p (PC Protection) performs the encrypted data access disable by preventing access to or deleting cryptographic material (e.g., encryption keys) required to access previously encrypted data. ISV-provided Intel-AT-capable encryption software may store this cryptographic material in the PC's chipset. In order to restore access to data when the system is recovered, this cryptographic material must be escrowed/backed up in advance in a separate device or server provided by the security ISV/service provider. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel AT-p functionality has been activated and configured. The activation process requires an enrollment procedure in order to obtain a license from an authorized security vendor/service provider for each PC or batch of PCs. Activation also requires setup and configuration by the purchaser or service provider and may require scripting with the console. Certain functionality may not be offered by some ISVs or service providers. Certain functionality may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[3] Source: The Cost of a Lost Laptop, The Ponemon Institute, LLC. April 2009.

[4] Source: The Human Factor in Laptop Encryption, The Ponemon Institute, LLC. December 2008.

[5] Source: IT Facts, March 21, 2008.

[6] Source: the Absolute Software knowledge base.

[7] All information about Capgemini was provided by Capgemini.

[8] Source: Capgemini knowledge base.

[9] All information about the BMW Group was provided by the BMW Group.

0409/WW/OCG/XX/PDF

♻ Please Recycle

Order Number: 321847-001US