Intel Anti-Theft Technology is here!

What is Intel® Anti-Theft Technology?

The new generation of notebook PCs with Intel vPro technology include Intel Anti-Theft Technology. Intel Anti Theft offers you the option of activating hardware-based client-side intelligence to secure the PC and/or data if a notebook is lost or stolen. Because the technology is built into PC hardware, it provides local, tamper-resistant defense that works even if the OS is re-imaged, a new hard-drive is installed, or the notebook is not connected to the network.

Intel® AT Feature	**How It Works**	**Benefit**
Detection (Triggers)	· Excessive login attempts -- The system keeps track of an IT-determined number of login failures in a pre-boot authentication (PBA) module. · Timeframe login requirement – if the user	· Local detection mechanisms (login failures and work even if no network connection is available

	does not log in to central server by a specific time/ date (per IT policy), the PC can trigger a response · Notification to the central server – Upon notification from the end-user (loss/theft), IT flags the notebook in a central server database (hosted in the internet). The next time the "new owner" connects the system on the internet, the notebook calls home, synchronizes with the central server and receives the "poison pill" (PC Disable and/ or Data Disable) per IT policy	· Ability to integrate with existing encryption solutions' PBA · Flexible policy engine allows IT to determine which detection mechanism should used and what action to take
Data access disable	Local or remote poison pill deletes or blocks access to software-based encryption keys (or other critical cryptographic material) thereby disabling access to encrypted data stored on the hard drive. ,	· Fast, secure way to protect data from unauthorized access. · Minimizes potential of attack on keys stored on hard drive. · Tamper-resistant.
PC disable	Local or remote poison pill renders the PC inoperable by blocking the OS from booting .	· Minimizes the potential of a stolen notebook being used and sensitive data being accessed. · PC Disable can be triggered locally or remotely Tamper-resistant.

		· Over time, it becomes a theft deterrent.
Reactivation	Return notebook to full functionality via: · Local passphrase that was preprovisioned by user. · Recovery token (one-time use) provided by IT.	· Simple, inexpensive way to restore notebook to full functionality without compromising local security features for data access disable or PC disable.

Detection mechanisms

Intel Anti Theft includes three programmable, interdependent hardware-based timers to help identify unauthorized access to the system: a rendezvous timer, a disable timer, and an unlock timer. Using these programmable timers, Thanks to hardware-based PC intelligence, Intel AT can detect potential loss/theft situations, shift into "theft mode," and respond according to your IT policy. a

Local, hardware-based detection and trigger mechanisms include:

· Excessive login attempts -- The system is disabled after an IT-determined number of login failures in the pre-OS screen.

· Timeframe login requirement -- The system is disabled if the user does not log in to central server by a specific time/date.

Detection can also be done via a remote connection to the theft management serve over the internet.

· Notification to the central server -- If IT flags the notebook in the central server database, the next time a "user" logs into the network, the notebook calls home, synchronizes with the central server and, receiving the server's notification, disables the PC, according to IT policy. (Note: Encryption vendorshave the option to host this service on the Internet in order to allow communication with notebooks outside the corporate firewall.)

There are several automated poison-pill responses to theft mode. These can be activated locally and automatically (based on the detection mechanism), or remotely by IT. The responses are also flexible, and can be programmed to:

· Disable access to data, by deleting software-based encryption keys or other cryptographic credentials required to access encrypted data on the hard drive.

· Disable the PC, by blocking the boot process, even if the hard drive is replaced or reformatted.

· Disable both the PC and access to data. Erases encryption keys and disables the PC.

Excessive login attempts can trigger poison pill for PC disable

Disabling a PC after excessive login attempts can be an effective way to prevent loss of encrypted data. For example, an engineer's notebook and wallet might be stolen in an airport. The thief might try to log in using information from the engineer's wallet but -- based on IT policy -- after five login attempts, the Intel Anti-Theft trigger is tripped, and the system locks down . In this case, encryption keys for encrypted data are erased from the hard drive, and the PC is disabled. Even if the thief removes the hard drive and installs it in another device, the security credentials that provide access to encrypted data on the hard drive have been erased and cannot be stolen. Until reactivated by the authorized user or IT, the PC will not boot, and the encrypted data cannot be accessed.

Server login timeout can trigger poison pill for PC disable

In another example, a research scientist's notebook might contain highly sensitive data about a new invention. In this case, IT has defined the triggers on the scientist's notebook to require that the scientist log in daily. During a family event, the scientist takes time off and does not log in for two days. Based on locally stored policy for the login timeframe, the notebook enters "theft mode," disables itself, and erases the encryption keys for encrypted data on the hard drive. Even if the notebook is removed from the lab while the user is away, the notebook has secured itself until the scientist returns and reactivates the system.

Easy reactivation and full system recovery

To speed up recovery when a notebook is being returned to service, Intel AT also includes two rapid reactivation mechanisms:

· Local passphrase, which is a strong password preprovisioned in the notebook by the user. To reactivate the system, the user simply enters this passphrase in a special pre-OS login screen.

· Recovery token, which is generated by IT or by the user's service provider via the theft management console, upon request by the user. For reactivation, a one-time recovery token is provided to the user via phone or other means, and the user enters the token in a special pre-OS login screen.

Both passphrase and recovery token return the PC to full functionality. Both methods offer a simple, inexpensive way to recover the notebook without compromising sensitive data or the system's security features.

Intel Anti Theft: Built-in protection and recovery

With Intel AT, businesses now have built-in client-side intelligence to help secure sensitive data regardless of the state of the OS and network connectivity. This hardware-based technology provides compelling tamper-resistance and increased protection to extend your security capabilities anywhere, anytime, on or off the network, and minimize business risk.

Where Can I Get It?

Intel® AT-capable notebooks

- Lenovo ThinkPad* T400
- Lenovo ThinkPad T500
- Lenovo ThinkPad X301
- Lenovo ThinkPad X200
- Lenovo ThinkPad W500
- Lenovo ThinkPad R500

Fujitsu Lifebook* E8420

- Fujitsu Lifebook T5010

Absolute* Software

Look to Absolute* Software to enable their software for Intel® AT.

Resources to Learn More About Anti Theft

White Papers

Cost of a Lost Laptop: A Study Conducted by the Ponemon Institute

Computrace® LoJack® with Intel® Anti-Theft Technology Whitepaper

Blogs

Inside Dope for Notebook Thiefs

Will you tell your users when AT-p is deployed?

Laptop Security is a Three-Legged Stool

“Two days” in the life of an Intel® vPro Anti-Theft Technology for Asset Protection (AT-p) User

IT Striking Back at Laptop Thieves

Videos

Intel Anti-Theft at the Beach - Josh demos Intel Anti-Theft Technology

Videos showcasing how Intel® Anti-Theft Technology works