AN INDIVIDUAL LAPTOP THEFT CAN BE MORE THAN A TERRIBLE INCONVENIENCE — it can damage an organization’s competitiveness and the trust of its customers. And that’s just one theft. At a macro level, PC theft statistics are even scarier.

A study by the Ponemon Institute showed that 71% of lost or stolen laptops result in a data breach. Laptop theft was attributed to 59% of computer attacks in government agencies, corporations, and universities during 2003, according to the Baseline 2004 study. And the Privacy Rights Clearinghouse states that since 2005, more than 150 million personal records have been exposed due to PC theft.

Fortunately, today’s PC and data thieves face decreasing demand for their wares. The reason: more and more stolen PCs lead authorities right to thieves’ doors, thanks to security innovations from Lenovo, Intel, and Absolute Software. These technology leaders have assembled a formidable array of anti-theft solutions that make it almost impossible to use or sell a Lenovo notebook if lost or stolen.

“Poison Pill,” PC Disable can deactivate a stolen or missing notebook remotely or via intelligence policies. Once deactivated, thieves can’t reactivate the PC even if the operating system is reinstalled or the hard disk replaced. If a Lenovo notebook is stolen, IT managers can also track, react to, or control the lost unit using Absolute Software’s Computrace®, a leading theft management solution which supports Intel Anti-Theft (AT) technology.

DEACTIVATION: AN EFFECTIVE DETERRENT

This versatile mix of anti-theft solutions begins with the Intel Centrino 2 processor with vPro technology and the PC Disable feature. Also known as the

JUST THE FACTS

The PC and data theft market has thrived in recent years. According to recent studies by the Ponemon Institute:

- 92% of IT security professionals reported laptop theft or loss in their organization.
- 42% of business managers don’t have encryption on their laptops.
- 56% of employees have disengaged company-provided encryption.
- 89% of employees ask others to watch their laptop while travelling.
- 55% of the time, IT is unable to prove a laptop was encrypted when stolen.

A survey of 163 Fortune 1,000 companies found that roughly 70% of all reported security breaches were due to insiders.

CUSTOM OPTIONS FOR ANTI-THEFT PROTECTION

Intel AT features several unique ways to detect potential loss/theft situations, activate “theft mode,” and respond according to a customized IT policy, including:

Excessive Login Attempts: The system is disabled after an IT-determined number of login failures.

“Phone Home” and Central Server Notifications: Notebooks flagged as lost or stolen by IT will phone home the next time the thief connects to the Internet. Intel AT then receives the stolen notebook server notification and disables the notebook.

The Computrace agent can also remotely delete data to shred sensitive files.

“Phone Home” Timers: Programmable timers perform regular check-ins with the theft-management server within IT-defined time periods. Anti-theft protective actions can then be taken if the regular check-ins do not occur successfully.
STOP THIEF!

**COMPUTRACE: ALWAYS ON THE CASE**

The Computrace solution, enhanced by Intel AT, operates unobtrusively and without employee knowledge or inconvenience. Without employee action, it conducts functions such as:

- **Emergency Remote Data Deletion**
  Deleting data at the file or whole disc level.

- **Lifecycle Data Delete**
  Wiping computers clean before retirement or reissue.

- **Forensics**
  Identifying accessed files after a PC is stolen or recovered.

When a Lenovo notebook is reported lost or stolen, Computrace and Intel tracking technology continue to play a key role. If desired, Absolute recovery services **law enforcement experts** will investigate a theft, recover the device(s), and collaborate with authorities to **bring the thieves to justice**.

The Intel/Computrace solution offers a range of anti-theft capabilities for each customer's unique needs. These anti-theft features can also be used to manage, record and analyze the movements, locations, network access history, and software on each computer. And anti-theft measures can be undone without harming a recovered PC.

To help prevent future problems, Computrace and Intel AT also **identify security “holes”** to be addressed through hardware, software, or personnel training.

**STOP NOTEBOOK THEFT IN ITS TRACKS**

With these options, customers may choose to track a stolen Lenovo notebook and attempt recovery, or use the Intel AT disable capability to deactivate a notebook immediately after it is stolen or goes beyond its reporting parameters.

Intel AT hardware-based detection mechanisms will even work without a network connection, and can also integrate with existing encryption solutions’ preboot authentication module.

**LENOVO: THE HEART OF THE ANTI-THEFT SOLUTION**

With embedded Computrace software, Lenovo has the only notebooks that can fully **activate the Intel AT system** against PC thieves and data snatchers. Call it an all-in-one crime fighter, and only Lenovo has it.


---

**Turn your notebook into a crime-fighter.**

Contact your local Lenovo or Intel solutions provider or call 877-852-7445 for information about Lenovo notebooks with Intel AT technology.