Intel® Anti-Theft Technology reduces risk for lost or stolen laptops

The growing challenge of loss or theft of laptops and data
A world gone mobile takes its laptops along for the ride. For business, more mobile users means greater productivity—but also significantly greater risk. Even an employee in a non-sensitive corporate area can have sensitive data on their laptop. From client information to company emails, product specs to manufacturing details, financial data to corporate roadmaps to patent information—data of all kinds can be at risk when a laptop is lost or stolen. And a single data breach can damage a company for years.

In addition, the costs of a data breach are escalating to hundreds of thousands, even millions of dollars per breach. In fact, the average economic impact of lost laptops is estimated at USD 6.4 million per organization per year,

The growing challenge of loss or theft of laptops and data

For example:

- Users typically put their laptops in a standby state (S3 sleep state) after working for a while.
- In standby state, a laptop's memory is still active, and the OS, applications, and data—including the encryption keys—are still loaded in that memory.
- Users are not required to re-authenticate with encryption credentials when resuming from standby.

If a laptop is stolen while in the standby state, a sophisticated thief can access a system's data in spite of an encryption solution.

Businesses have an urgent need for a comprehensive anti-theft solution that works with existing security measures—such as encryption—to make security stronger and close vulnerabilities by protecting the laptop in any state.

Encryption—A partial solution
Businesses are taking aggressive measures to protect sensitive data and the assets—laptops, tablets, Ultrabook™ devices—on which they are stored. One such measure is encryption, which is now almost impossible to breach. However, even encryption, robust as it is, still has some vulnerability, and is still only a partial solution.

Enterprise solution enabled with Intel® Anti-Theft Technology (Intel® AT)
A comprehensive asset and data security solution is now available for enterprise. The Softex SecureDisable™ solution, enabled with Intel® Anti-Theft Technology (Intel® AT), protects laptops even in the S3 standby state, both inside or outside the corporate firewall.
Intel® Anti-Theft Technology

Intel AT is hardware-based technology built into all Ultrabook devices and built into many laptops equipped with 3rd generation Intel® Core™ processors and 3rd generation Intel® Core™ vPro™ processors. The hardware-based functionality of Intel AT includes detection and trigger mechanisms that let an IT administrator remotely or locally lock and disable access to a laptop and its data. With Intel AT, IT administrators can be more assured that unauthorized users cannot exploit vulnerabilities and circumvent existing security solutions.

IT administrators can remotely configure and implement all Intel AT detection and trigger mechanisms. These tamper-resistant mechanisms include:

- Excessive login attempts
- Excessive time spent in the pre-boot authentication (PBA) screen
- Missed check-ins with the central server
- Notification through a message sent over an IP-based wired or wireless local area network (LAN)

Access can be locked and/or the asset disabled remotely, over a wired or wireless LAN through policy-based settings or by the individual laptop. Access can also be locked and/or the asset disabled locally by policy based mechanisms.

Closing vulnerabilities in applications and encryption

Intel AT is built directly into the hardware. This means that Intel AT can be effective regardless of the state of the OS, security applications, and/or encryption solutions. IT now has a robust solution for protecting sensitive data even if a laptop’s OS is reimaged or its software-based security measures are disabled or defeated.

Intel AT is also independent of the hard drive, and can work locally, without a network connection. This means that IT can now take advantage of tamper-resistant, policy-based protection that works even if a laptop’s boot order is changed, a new hard drive is installed, or the laptop is disconnected from the network.

Intel AT also closes the traditional data encryption vulnerability of the S3 standby state. With Intel AT, an IT administrator can define an allowed time for login to the system after the system resumes from standby. If the login is not completed within that timeframe, the user must re-enter the encryption credentials before being allowed access to the laptop’s data. This feature is only available on laptops equipped with Intel Core vPro processor.

Simple, rapid reactivation

When a laptop is recovered by its authorized user, the laptop can be easily reactivated to full functionality. The user simply enters a local passphrase or a one-time reactivation code generated by IT.

AVAILABLE ON ULTRABOOK™ DEVICES AND LAPTOPS

Intel® Anti-Theft Technology (Intel® AT) is available on all Ultrabook™ devices and many laptops equipped with 3rd generation Intel® Core™ processors and 3rd generation Intel® Core™ vPro™ processors. Intel AT is also available on select laptops equipped with previous generation Intel Core and Intel Core vPro processors. For a list of laptops enabled with Intel AT, click here.

Figure 1. Comprehensive protection. Intel® Anti-Theft Technology (Intel® AT) protects assets and sensitive data both inside and outside the corporate firewall using remote and local detection and trigger mechanisms.
Softex SecureDisable* enabled with Intel AT

Softex SecureDisable supports all features of Intel AT, and includes unique features that make it a compelling solution for businesses. SecureDisable has three key components:

- **Client.** The SecureDisable Client (installed on the laptop) communicates with the SecureDisable Server* to remotely manage Intel AT features.
- **Server.** The SecureDisable Server manages provisioning, policy configuration, and deployment of Intel AT through an existing management interface.
- **Plug-ins for popular management consoles.** Management console plug-ins allow administrators to remotely deploy, activate, and manage Intel AT-based laptops from an existing management console.

Works with existing encryption solutions

SecureDisable works with existing data encryption solutions, including full data encryption (FDE) and self-encrypting drives (SED). SecureDisable also includes a free, optional file and folder encryption (FFE) feature.

Asset and data protection

SecureDisable provides a mechanism for IT to remotely disable the laptop and receive confirmation that access to the laptop has been locked. SecureDisable also includes the SecureResume feature, which is enabled by the Intel AT-based S3 timer.

Built into the laptop hardware, the S3 timer is used to trigger the transition from standby to hibernation or shutdown after a specific period of time that an IT administrator can configure. The feature ensures that encryption keys are deleted from the laptop’s memory. The feature also requires users to re-authenticate before once again accessing the laptop and its sensitive data. With SecureDisable enabled with Intel AT, a serious vulnerability is closed for laptops that are lost or stolen in the standby state.

Easier to manage and deploy

SecureDisable includes plug-ins that make it easy for IT asset, help-desk, and security management personnel to manage Intel AT through an existing management console such as Microsoft System Center Configuration Manager*, the most widely deployed console, and BMC Remedy*. Softex SecureDisable now also includes a plug-in for McAfee ePolicy Orchestrator security console. In addition, IT administrators can use Windows* PowerShell scripts to automate the deployment and management tasks, or use a command line interface to manage laptops.

Flexible service delivery model

SecureDisable supports three service delivery models so IT administrators do not have to change their existing framework.

- **Enterprise hosts the solution.** Softex licenses the anti-theft solution to the enterprise. The enterprise hosts the server from within the corporate intranet.
- **Service provider hosts the solution.** Service providers (ITOs/MSPs) can license the anti-theft solution from Softex. The service provider can then offer the solution to customers as a standalone anti-theft service or as part of a portfolio of client security and management services.
- **Softex hosts the solution.** Softex hosts the server and offers the anti-theft service to medium and small businesses. Business IT personnel can then log into the hosted management console and manage their own Intel AT-enabled laptops.

Simple licensing model

Softex SecureDisable licensing is per laptop; a license is valid for the life of the laptop.

SUPPORT FOR MCAFEE EPOLICY ORCHESTRATOR*

Softex SecureDisable* enabled with Intel® Anti-Theft Technology can now be deployed and managed through McAfee ePolicy Orchestrator* (McAfee ePO*). McAfee ePO is a centralized platform that manages diverse security solutions from McAfee and third parties. The integration of SecureDisable and McAfee ePO lets enterprise spend less time on management and more time delivering enhanced protection for assets and data.

Figure 2. Management environment for Softex SecureDisable* enabled with Intel® Anti-Theft Technology (Intel® AT)
Intel® Anti-Theft Technology:
Intelligent protection and simple, rapid reactivation

Intel AT reduces risks associated with lost or stolen laptops. The Softex SecureDisable solution, enabled with Intel AT, is affordable, effective, and flexible, and works within existing management and security processes.

When taking advantage of Softex SecureDisable enabled with Intel AT, IT administrators can be assured that assets and sensitive data will be locked and secured both locally and remotely.

1 The Billion Dollar Lost Laptop Problem, Ponemon Institute, 2010.