PRODUCT BRIEF
Intel® Anti-Theft Technology

Help Protect Sensitive Data on Laptops with Intel® Anti-Theft Technology and WinMagic® SecureDoc™

It's not just a PC—it's your business. Lock it tight.

Keeping data and assets secure in a mobile environment is not only a daunting challenge, but it is also a critical requirement. The Health Information Technology for Economic and Clinical Health (HITECH) Act, Health Insurance Portability and Accountability Act (HIPAA), CS 1386, Gramm-Leach-Bliley Act (GLBA), data-breach notification rules, and other increasingly stringent regulations in data security and privacy have added complexity for companies with mobile users. The loss and theft of systems and data is not only costly to your company, but it can also result in financial or legal exposure and cause significant disruptions to business.

Laptops using Intel® Anti-Theft Technology (Intel® AT) powered by the 2nd generation Intel® Core™ vPro™ processor family provide IT administrators with intelligent protection of lost or stolen assets. Intel AT provides the ability to disable your laptop with a local or remote poison pill, if the system is lost or stolen. This technology allows for software-based disk encryption vendors to place a portion of the cryptographic material from the encryption key into the Intel® chipset to disable access to data stored on the encrypted hard drive, even if the end-user possesses the correct pre-boot authentication (PBA) credentials.[2] The poison pill can also block the laptop's boot process, rendering the system a "brick." Because the technology is built into laptop hardware, Intel AT provides local, tamper-resistant protection that works even if the OS is reimaged, the boot order is changed, a new hard drive is installed, or the laptop is disconnected from the network.

Intel® Anti-Theft Technology Feature[1]	HOW IT WORKS	BENEFITS
PC Platform Disable	Local or remote poison pill renders the laptop inoperable by locking down the system's platform. This method of PC disablement is nondestructive and can be easily and quickly reversed without harming the platform or affecting the data.	▪ Minimizes the potential of an unauthorized person using a stolen laptop and accessing sensitive data. ▪ PC disable can be triggered locally or remotely—an Internet or LAN connection is not necessary—under the following circumstances: - Excessive end-user attempts to log into the system. - The laptop misses its rendezvous time with the server (electronic check-in over the Internet), thereby issuing a local poison pill. ▪ The IT administrator can send a poison pill remotely to the stolen laptop across the Internet, intranet, or Short Messaging Service (SMS).
Data Access Disable	Local or remote poison pill facilitates WinMagic® SecureDoc™ in placing a portion of the cryptographic material into the Intel Chipset. Local or remote poison pill renders the encryption key broken, thereby disabling access to encrypted data stored on the hard drive.[2] The process is nondestructive and reversible. Entering a passcode restores access to the encrypted data and returns the laptop to its prior state for the authorized user.	▪ Helps protect encrypted data from access, even if the unauthorized user, such as a disgruntled employee, knows the passcodes or in situations when a password has been compromised. ▪ Allows encryption solutions to store and manage essential cryptographic material in hardware. ▪ Locking the laptop is a necessity in case the thief has possession of an unsecured passcode.
Recovery and Reactivation	Displays a custom recovery message when theft mode is triggered. Laptop functionality is restored using: ▪ Local passphrase that end-user pre-provisions. ▪ One-time use recovery token that IT provides.	▪ Recover lost laptops more easily. ▪ Simple, inexpensive way to restore laptop to full functionality without compromising local security features.

WinMagic® SecureDoc™: Enterprise-Ready Disk Encryption

Comprehensive Encryption for All of Your Data-At-Rest Security Needs

WinMagic SecureDoc is a scalable Full-Disk Encryption (FDE) software solution that ensures sensitive information stored on laptops across the enterprise is protected against theft and unauthorized access. SecureDoc PBA offers single- or multiple-factor PBA methodologies including password, smartcards, popular USB tokens, biometrics, Trusted Platform Module, and Public Key Infrastructure. SecureDoc Enterprise Server (SES) functions as a robust and reliable key management system for all your endpoints (running on Microsoft Windows*, Apple Mac OS*, and Linux*), providing a secure central repository for all encryption keys used to protect hard drives, laptops, removable media, and other encrypted endpoints.

SecureDoc's key features include:

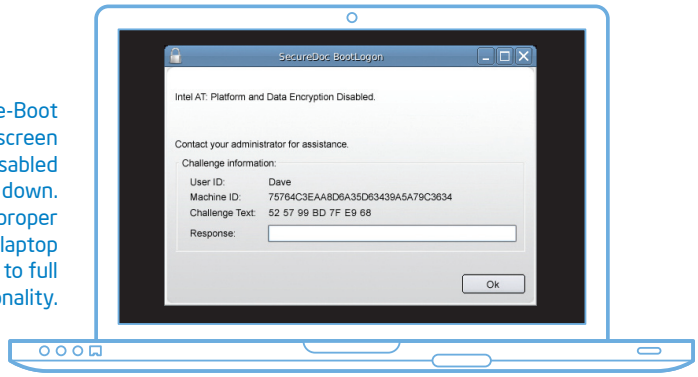
- Support for Windows, Mac OS, and Linux clients
- Encryption key management and escrow
- Dynamic key provisioning
- Synchronization with the active directory
- Password rules
- Password recovery tools (password hint, self-help, challenge response)
- Key labeling
- Auditing capabilities
- Policy-based encryption rules
- Easy deployment of client packages through LANDesk*, IBM Tivoli*, and Short Messaging Service (SMS)

Advantages of Opal-Compliant Self-Encrypting Drives

Opal self-encrypting drives (SEDs) are an easy and effective way to deliver a high level of security for digital information. The key advantages of SEDs include:

- **Quick and easy deployment.** SEDs utilize their own Advanced Encryption Standard (AES) encryption, therefore SecureDoc can instantly activate them, and they do not require the hard drive to become initially encrypted in software, which requires several hours to convert into an encrypted drive.
- **Zero performance degradation.** SEDs use their own hardware for encryption, so computing systems do not suffer performance issues (no system processor usage or time delay overheads).
- **Highest level of security.** The data encryption key does not leave the drive, hence preventing cooled-RAM attacks and simplifying key management.
- **Read-only PBA area.** Supports single or multi-factor authentication by ISVs using the drive's secure partition.
- **Crypto erase.** Enables instant secure disposal and repurposing of the self-encrypting drive, rendering all existing data unintelligible.
- **Transparency and flexibility.** The master boot record is not modified, therefore a kernel driver is unnecessary and no conflicts with other software occur.

The Pre-Boot Authentication screen when a laptop is disabled and locked down. With the proper credentials the laptop will be return to full functionality.



To learn more about Intel® Anti-Theft Technology, visit: **anti-theft.intel.com**

To learn more about WinMagic and its disk encryption product, SecureDoc™, visit: **www.winmagic.com/products/full-disk-encryption**

SOLUTION PROVIDED BY: WINMAGIC® DATA SECURITY Knowing You're Protected

WITH: intel ANTI-THEFT TECHNOLOGY

[1] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) 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. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel AT functionality has been activated and configured. Certain functionality may not be offered by some ISVs or service providers and 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.

[2] Intel® Anti-Theft Technology (Intel® AT) is available as an option on designated Intel® 2nd generation Core™ and vPro™ processor family. An Intel AT-enabled theft management or data encryption software subscription is required to activate Intel AT. See your sales consultant for more details.

0211/JKO/MESH/PDF 324777-001US

intel®