**PRODUCT BRIEF**

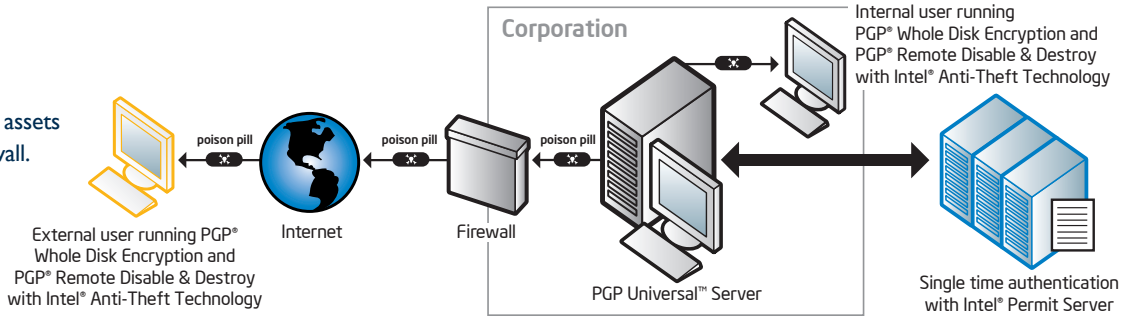
PGP® Whole Disk Encryption with support for Intel® Anti-Theft Technology
As implemented in the 2nd generation Intel® Core™ processor family

# Multi-Level Security Against Data Loss or Laptop Theft

## A solution from Symantec integrated with Intel® Anti-Theft Technology (Intel® AT) provides strong protection against data loss or laptop theft

When it comes to effective data security, one of the most effective solutions is to combine hardware and software to protect data confidentiality in case of theft or loss. In an effort to enhance conventional data protection techniques, Symantec integrated Intel® Anti-Theft Technology (Intel® AT) with its PGP® Whole Disk Encryption solution to provide strong security and peace of mind to laptop users. A component of this solution, PGP® Remote Disable & Destroy (RDD), can render a stolen laptop useless and unreadable by unauthorized individuals. Together, these innovative technologies, forged in silicon within the select computers featuring Intel® Core™ processors, deliver exceptional data security and superior asset protection.

This solution protects data from malicious individuals inside an enterprise and also guards laptop assets when outside the corporate firewall.




## Strengthening Security with a Silicon-Based Solution

At the heart of Symantec with the Intel AT solution is a protected area, physically embedded in each Intel Core processor equipped with Intel AT, where Symantec encryption algorithms can run securely, providing strong resistance against tampering. By embedding these security mechanisms within the hardware, data is protected even if a hacker attempts extreme measures, such as reimaging the OS, changing the boot order of devices, installing a new hard drive in the laptop, or breaking connections with the network. Though this degree of protection is extremely strong, a recovered laptop can quickly be restored to service using a previously established passcode or a token provided by IT.

"As security threats continue to evolve and confidential information proliferates to a wide array of endpoints, Symantec has innovated to address the new needs in the market," said Bryan Gillson, senior director of product management at Symantec. "Symantec's goal is to provide effective, easy-to-use information protection products with the management capabilities needed to address today's stringent privacy and compliance regulations." Beyond compliance, financial loss is also a factor. According to Ponemon Institute,[1] the value of one lost laptop and its data is USD 49,246.

At a recent forum, In Defense of Data,[2] Intel's Chief Information Security Officer Malcolm Harkins commented, "Data wants to be free and employees will find a way to help it, albeit normally for the right reasons. It's futile, actually counterproductive, to try to build a wall around the data. To be successful, you have to run at the risk. Embrace it. Give it a hug. Take advantage of both technology and employees' aspirations in creating the best solution." Harkins goes on to explain that personal responsibility and technology—encryption, backups, and new anti-theft technologies—are the most effective way to protect data.

## Features and Benefits

The following table highlights some of the features and benefits of PGP Whole Disk Encryption with support for Intel AT and PGP Remote Disable & Destroy.

| FEATURE | DESCRIPTION | BENEFIT |
|---|---|---|
| PC disable | Blocks the boot process using a local or remote poison pill, making the laptop unusable. | Reduces the risk of unauthorized access to data if a laptop is stolen. |
| Data access disable | Deletes cryptographic material to prevent access to encrypted data on the hard drive; the process can be performed using a local or remote poison pill. | Resists tampering or hacking by storing cryptographic material in the hardware, improving protection without increasing administrative complexity. |
| Simple reactivation process | Returns PC to full usability by means of a user-specific passphrase entered locally or a one-time recovery token supplied by IT. | Protects investments in PCs with a simple reactivation process that doesn't compromise overall security or data integrity. |
| Multiple ways to disable a PC | Provides a multi-level approach to disabling a laptop. Mechanisms include a network-based poison pill, locally generated disable timer, and local invalid login counter. | Strengthens security through multiple mechanisms so that organizations can optimize laptop protection to suit operational preferences. |
| Central management and administration | Provides a central management platform through PGP® Universal™ Server for activating, configuring, and monitoring anti-theft services for systems protected by PGP® Whole Disk Encryption with PGP® Remote Disable & Destroy. | Manages laptop security from a central point, and protects corporate assets stored on laptops—both inside and outside the company firewall. |
| Support for multiple protection groups | Lets IT groups define policies to match protection and recovery schemes to individual user and group profiles. | Provides a flexible means for organizations to implement their internal data security practices in a consistent manner. |

**Experience peace of mind and enhanced laptop protection through a multi-level security solution grounded in the industry-leading expertise of Symantec and Intel. Symantec, with the help of Intel® Anti-Theft Technology, advances the art and science of data security—to help ensure that your data assets are protected.**

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

[1] Source: "The Cost of a Lost Laptop," http://antitheft.intel.com/Libraries/Documents/Cost_of_a_Lost_Laptop_White_Paper_V_4.sflb.ashx.

[2] http://www.indefenseofdata.com/2011/01/clear-focus-on-risk-leads-to-laptop-security/

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.

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



0211/JKO/MESH/PDF 325052-001US