White Paper
Enterprise Security
January 2011

Safeguarding Critical Enterprise Assets and Data

Symantec PGP® Whole Disk Encryption and PGP® Remote Disable & Destroy with Intel® Anti-Theft Technology

Each year, an estimated two million laptops are stolen, and 97 percent of those are never recovered.[1] In addition, one in 10 people have lost a laptop, smartphone, or USB drive that contains corporate information.[2] In almost every case, these stolen hardware assets contain sensitive, valuable data that is proprietary or confidential. These statistics represent a serious financial risk to the enterprise in lost physical assets (hardware) and electronic assets (data and intellectual property). Enterprises need a reliable way to deter laptop theft, and if theft does occur, disable access to or destroy the previously encrypted stolen data even though the hardware is out of reach.

The Real Cost of Unprotected Assets

The average cost of a lost laptop is USD 49,246.[3] This amount includes the costs of hardware replacement and IT re-provisioning, the lost time and productivity of the employee during the replacement cycle, and lost business opportunities. For example, if the employee's laptop is stolen during a business trip, the presentations and demos stored on that laptop are no longer available to show to potential customers. The financial risks to the enterprise are further compounded by the loss of intellectual property, damage to the company's brand image, loss of public and investor confidence, costs to notify clients, and lost revenue.

If the data on a laptop is not protected and a breach occurs, the enterprise can suffer costly notification and reporting expenses and be at risk for litigation given the worldwide variety of privacy and data security regulations. In the United States, these include Sarbanes-Oxley (SOX), the Fair and Accurate Credit Transactions Act (FACTA), and the Health Insurance Portability and Accountability Act (HIPAA). The European Union has its own set of data security regulations.

Being able to remotely disable and destroy previously encrypted corporate data before the data is exposed to unauthorized use can reduce the financial ramifications of stolen assets. Since 2005, more than 355 million personal records have been exposed.[4] The Ponemon Institute calculates the cost of each lost personal record at USD 204 in the United States;[5] the average organizational cost of a data breach in the United States is USD 6.75 million.[6]

intel | Symantec™ | intel ANTI-THEFT TECHNOLOGY

The Ponemon Institute calculates that 12,000 laptops are stolen every week at airports.[7]

CONTENTS

Executive Summary 1
- The Real Cost of Unprotected Assets 1
- When Assets Are at Risk 2
- Solution 2

Taking the Risk out of Mobile Data 3
- Discourage Theft 3
- Protect the Platform and the Data 3
- Choose the Right Level of Protection 4
- Choose the Right Recovery Method 5
- Complement Your Enterprise's Overall Security Profile 5

Inside the Technology 5
- Symantec PGP® Whole Disk Encryption 6
- Symantec PGP® Remote Disable & Destroy with Intel Anti-Theft Technology 6
- Deploying Symantec PGP® Whole Disk Encryption and PGP Remote Disable & Destroy with Intel Anti-Theft Technology 7

Conclusion 8

When Assets Are at Risk

Simply put, if your enterprise's data isn't encrypted, that data is at risk. If your company's workforce is equipped with laptops that are not protected by remote disable capabilities, both the hardware and the data are at risk.

The Ponemon Institute calculates that 12,000 laptops are stolen every week at airports.[7] Other situations may also expose a laptop and its data to danger, such as shipping a laptop from one location to another, crossing international borders where customs officials require access to the laptop, or employees taking their laptops with them when exiting the company. In fact, employees and contracted third-parties are responsible for 64 percent of all reported security breaches.[8] When a laptop has reached the end of its useful life, recycling the hardware is relatively easy—but helping to ensure the data is also decommissioned is a must to minimize corporate risk.

Solution

Enterprises must take proactive steps to protect their critical assets. Deploying Symantec PGP® Whole Disk Encryption (WDE) along with PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft Technology (Intel® AT) provides IT administrators with intelligent protection of lost or stolen assets—both physical and electronic. This security solution enables the destruction of corporate data, even if the laptop is out of the enterprise's control.

This solution is available on laptops equipped with Intel® Core™ processors. Upgrading to this technology as part of the normal PC refresh process enables enterprises to take advantage of Intel AT protection without any additional hardware cost.

The benefits of deploying PGP WDE along with PGP RDD with Intel AT include the following:

- The presence of PGP WDE and PGP RDD with Intel AT can serve to deter theft, reducing financial and legal risks to the enterprise.
- PGP WDE provides data encryption to safeguard the data if a laptop is lost or stolen.
- PGP RDD with Intel AT adds tamper-resistant, hardware-based proactive protection that lets an IT administrator, with the click of a mouse, disable a lost laptop and access to the laptop's previously encrypted data—increasing confidence that corporate data is protected. Even if the login credentials are known, access to the encrypted data will be prevented.
- When IT administrators suspect credentials have been compromised, they can disable a laptop so that all valid credentials are locked and are no longer usable—only an administrator with a valid recovery token can access and unlock the data.
- PGP RDD with Intel AT provides secure decommission for reused, recycled, or replaced hardware—corporations no longer have to worry about weak user passwords or lingering sensitive data.
- A central management and reporting console enables IT administrators to set policies, demonstrate compliance, identify unencrypted laptops, and respond rapidly to loss or theft, even without a network connection.

Taking the Risk out of Mobile Data

To truly protect their assets, enterprises need to employ methods to deter theft as much as possible and provide security for both physical hardware and the data residing on that hardware. A viable security solution needs the following characteristics:

- Is independent of the OS or network functionality
- Addresses a range of security priorities and allows IT administrators to balance operational and security costs
- Provides a range of recovery and reactivation methods, including remote disable and destruction of data
- Complements the enterprise's overall security profile

The combination of PGP WDE and PGP RDD with Intel AT meets all these requirements.

Discourage Theft

Deploying PGP WDE and PGP RDD enabled with Intel AT can help prevent theft from happening, thereby providing significant cost saving to the enterprise. For example, a potential thief roving the airport looking for unguarded laptops may be more inclined to bypass those that display a visual deterrent mark, such as the Intel AT logo.

Similarly, employees exiting the corporation will not be tempted to "forget" to return their laptops if they know that the laptops will be inoperable and the data inaccessible.

Protect the Platform and the Data

As shown in Figure 1, four main components comprise the PGP WDE and PGP RDD with Intel AT security solution, which delivers robust encryption with local or remote system disable:

- **Prevention.** As discussed earlier, the very presence of these technologies can help discourage theft because potential thieves know that the laptop and data will have no value once they are stolen.
- **Detection.** Laptops protected by Intel AT have local theft and tamper detection mechanisms, and also support remote disable.

SOLUTION IN ACTION: USER-REPORTED THEFT PROMPTS POISON PILL

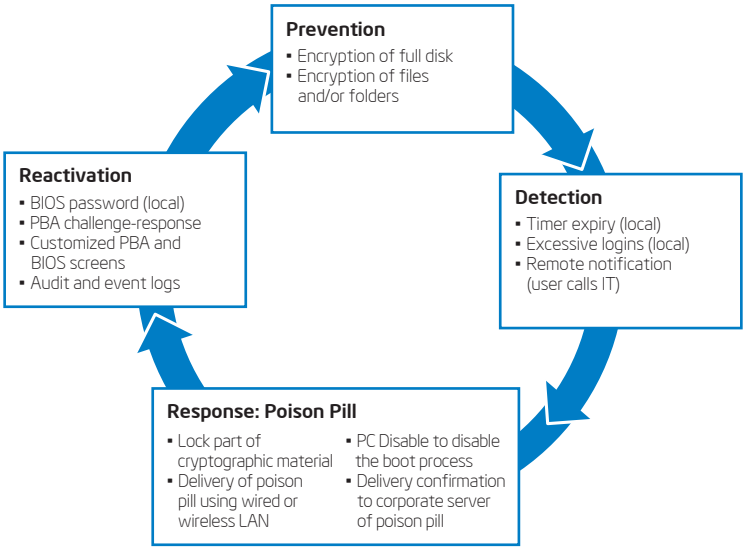
The following is just one example of how Symantec PGP® Whole Disk Encryption (WDE) and PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft Technology (Intel® AT) helps protect your enterprise's assets:

Julie, a financial services officer, manages accounts for several small banks. Her laptop contains sensitive information about each subsidiary bank, as well as thousands of client records from their databases. The folders containing these files are encrypted; however, while flying back to the home office, her laptop is stolen at the airport. Despite the encryption, Julie immediately calls IT, and the administrator flags the laptop on the PGP Universal™ Server as stolen.

Because Julie's laptop is protected by PGP WDE and PGP RDD with Intel AT, it checks in with the PGP Universal Server as soon as the thief accesses the Internet. The laptop then receives the poison pill sent by IT and immediately enters theft mode. The laptop also sends an acknowledgment to the server that the poison pill was received. Next, the laptop locks critical elements of the decryption security credentials stored in the hardware and disables the system's boot process. This sequence of events is invisible to the thief until the system is rebooted, at which time unauthorized access will be prevented until the platform is recovered.

Meanwhile, the thief takes the laptop to a secure location and removes the hard drive, intending to place it in another reader to try to access the security credentials and sensitive data. However, because critical parts of the security credentials were stored in Intel AT hardware and are now locked, they are inaccessible. The drive remains encrypted and the client records protected.

The bank is also protected because it can prove that the data on the stolen laptop is encrypted, and with the encryption keys locked, the data is inaccessible (confirmed poison pill receipt) and not considered at risk. The bank may be exempt from the data-breach notification regulations that contain an encryption safe-harbor and therefore can minimize the costs of the stolen system.



LAN - local area network; PBA - pre-boot authentication

Figure 1. Symantec PGP® Whole Disk Encryption (WDE) and PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft Technology (Intel® AT) delivers a full-circle solution for protecting sensitive data on laptops. IT administrators can now encrypt data, protect cryptographic material in hardware, and lock down the laptop to disable the boot process, rendering it useless after being lost or stolen.

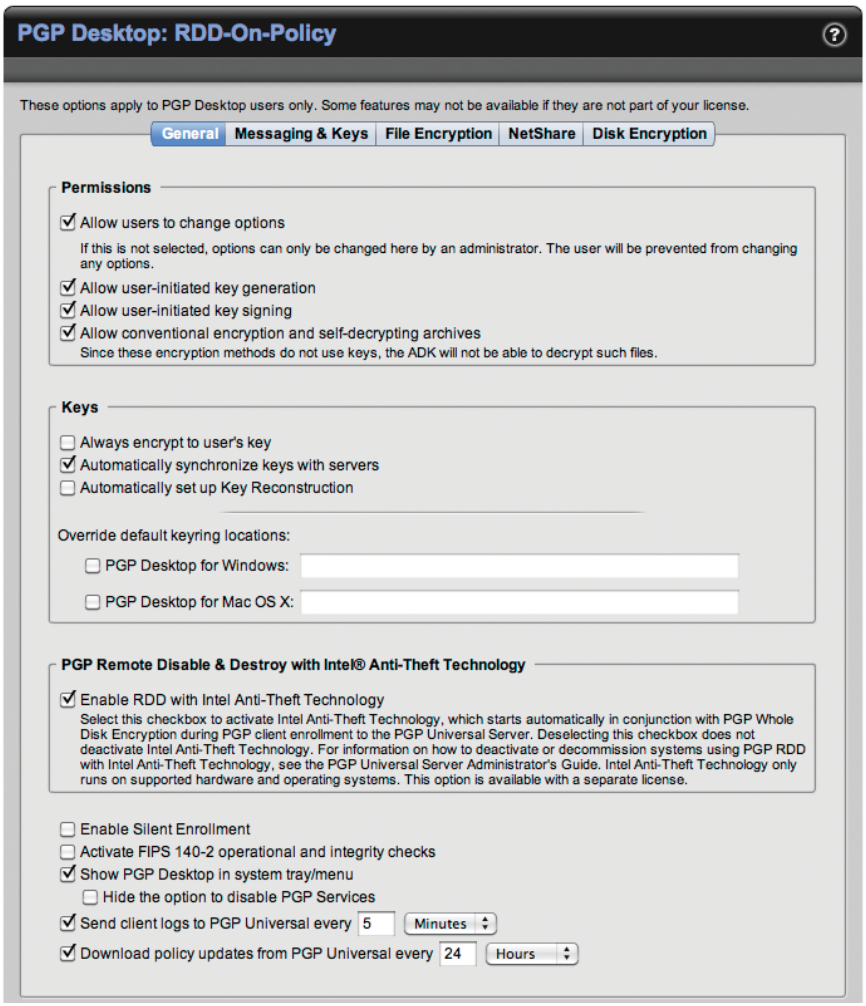


Figure 2. Symantec PGP® Whole Disk Encryption (WDE) and PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft Technology (Intel® AT) allow a range of options when setting IT policy.

SOLUTION IN ACTION: DATA IS PROTECTED EVEN WITHOUT AN INTERNET CONNECTION

The following example shows how Symantec PGP® Whole Disk Encryption (WDE) and PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft Technology (Intel® AT) help protect your data—even if the stolen laptop doesn't connect to the Internet:

Frank, a design engineer, is working on a sensitive new project. Early one week, he leaves for a training conference, and while he's gone his laptop is stolen from his office. Since Frank will not return for several more days, the theft is not immediately noticed.

However, because of the importance of Frank's project, IT policy requires the laptop to check in with the PGP Universal™ Server daily. When the laptop fails to connect with the server, the local rendezvous timer is triggered. The next time the laptop powers up, it enters theft mode and disables itself.

A few days later, the thief tries to power up the laptop, but the OS will not boot, so access to the system and use of the laptop is thwarted.

- **Response.** Once a laptop has been identified as lost or stolen, not only does encryption protect the data, but also the entire PC is completely disabled and cannot be reused.
- **Reactivation.** If a laptop is recovered, the PC can be reactivated either locally or remotely, and data access is also re-enabled.

Choose the Right Level of Protection

Every enterprise has a different, unique set of priorities. For some, limiting operational costs is important, with asset security less so. For others, hardware and data security far outweigh operational cost considerations. The combination of PGP WDE and PGP RDD with Intel AT lets IT administrators select from a range of centrally managed encryption solutions and build a comprehensive, flexible encryption strategy on a single platform.

In addition to the various levels of encryption that PGP WDE provides, PGP RDD with Intel AT offers customizable layers of protection for both the hardware and data, including the following capabilities:

- A stolen laptop can be disabled remotely over local area networks (LANs), wireless LANs, and 3G networks.
- Even if the laptop doesn't connect to the Internet, security-protected local timers can detect suspicious behavior, such as an excessive number of login attempts, an unusually long time before credentials are entered, or failure to check in with the central server.
- Whether triggered locally or remotely, the poison pill disables the laptop by blocking the boot process at the hardware level.
- IT policy determines the cases in which access to previously encrypted data should be temporarily or permanently prevented.
- Access to encrypted data is disabled by disabling the encryption credentials at the hardware level.

- The customizable "theft mode" message can contain instructions on how to return the laptop to its rightful owner when the platform is booted in the theft mode.
- Responses can be combined to provide different levels of lock down for different users.

The application's user interface shown in Figure 2 depicts some of the settings and options available with PGP WDE and PGP RDD with Intel AT.

PGP RDD with Intel AT also supports secure decommission, which can help lower the risk and cost of decommissioning a laptop at the end of its life. Secure decommission extends the anti-theft capability by removing or encrypting data from the hard drive while keeping the laptop operational for its re-use or resale. With secure decommission, laptops and hard drives can be reused or recycled without worrying about unauthorized users accessing sensitive data.

Choose the Right Recovery Method

Both PGP WDE and PGP RDD with Intel AT offer easy reactivation of disabled data or hardware. For example, PGP WDE includes support for both administrator-managed passphrase recovery using a Whole Disk Recovery Token (WDRT) and local self-recovery, where secure questions and responses allow users to recover their own passphrase without having to call the help desk. PGP WDE also includes support for Intel® Active Management Technology, enabling remote access to systems encrypted with PGP WDE.

If a lost laptop is recovered, PGP RDD with Intel AT lets IT administrators easily reactivate the laptop without any loss of data or damage. Intel AT supports sending a remote recovery token over the network, as well as a locally entered, one-time-use recovery passphrase for reactivating a disabled PC.

The following steps summarize the protection-and-recovery process that PGP RDD with Intel AT provides.

1. An IT administer enrolls the users and laptops (pre-boot authentication (PBA) using BIOS PBA or hard-disk drive PBA).

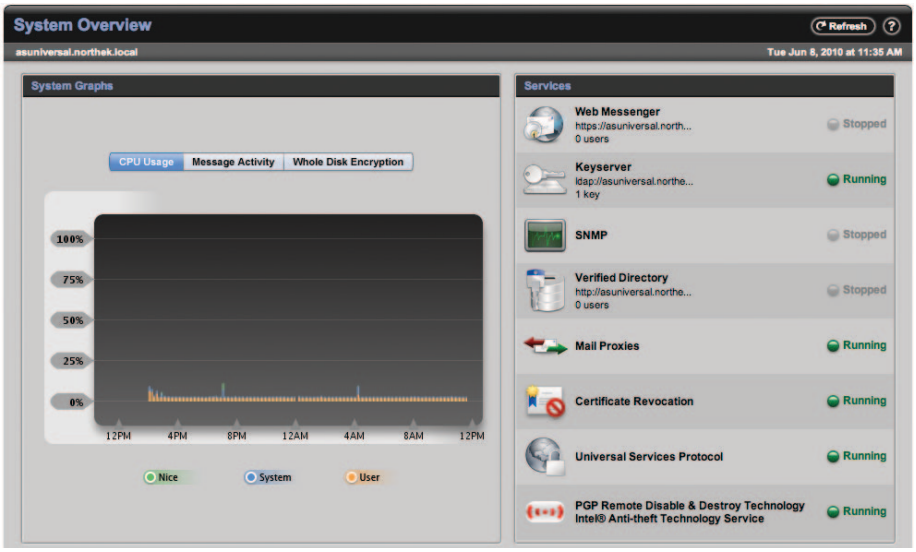


Figure 3. With Symantec PGP® Whole Disk Encryption (WDE) and PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft Technology (Intel® AT), stolen hardware and data are protected and easily reactivated if found.

2. If the laptop is reported lost or stolen, the administrator marks it as such (periodic contact with the PGP Universal™ Server to refresh theft status).
3. The laptop is marked for data access disable, system disable, or both.
4. If the laptop does not connect to the PGP Universal Server within a certain period of time, the timer on the chipset renders the system unusable and/or data inaccessible.
5. If and when the laptop is recovered, a simple reactivation process using a local passphrase or a one-time recovery token restores the laptop to full functionality.

Complement Your Enterprise's Overall Security Profile

PGP WDE supports a broad range of integrated applications to help secure e-mail, laptops, desktop PCs, instant messaging, personal digital assistants (PDAs), network storage, File Transfer Protocol (FTP) or bulk data transfers, and backups, in addition to managing third-party encryption applications. Plus, PGP RDD with Intel AT complements other security measures by allowing a wide range of security responses, from rapid cl ient-side lock down to full data disable.

PGP WDE and PGP RDD with Intel AT is designed to fit into an enterprise's holistic security profile, as the illustration of the application's user interface in Figure 3 shows.

Inside the Technology

PGP WDE and PGP RDD with Intel AT help businesses further minimize the risk of data breaches by giving IT the ability to trigger a full system lock down along with erasure of critical cryptographic materials. This fully integrated combination of encryption and lock-down capabilities offers a flexible, intelligent automated solution that works locally or remotely, on or off the network, to protect assets and their sensitive data.

This solution is available on laptops equipped with Intel Core processors. Upgrading to this technology as part of the normal PC refresh process enables enterprises to take advantage of Intel AT protection without any additional hardware cost. Enterprises with significant data security concerns may want to upgrade certain segments of their PC fleet earlier than normal to add Intel AT protection to their security repertoire—the cost of acquiring new hardware is minimal when compared to the potential cost of even a single data breach.

Symantec PGP® Whole Disk Encryption

PGP WDE provides end-to-end encryption support, based on the PGP software development kit, a mature cryptographic module validated by Federal Information Processing Standard (FIPS) publication 140-2. Table 1 (top) summarizes some of the main features of PGP WDE.

PGP Universal Server provides a Web-based administrative interface to establish and control automated user and key management, provisioning, policy enforcement, and logging. PGP Universal Server clients access key management, policy, and logging services through Simple Object Access Protocol (Secure) (SOAPS), a standard Web-enabled protocol. PGP Universal Server runs on a security-hardened Linux* derivative on customer-preferred compatible server hardware or in a VMware ESX* environment.

Symantec PGP® Remote Disable & Destroy with Intel Anti-Theft Technology

PGP RDD with Intel AT, available with Intel Core processor family laptops, provides hardware-based security building blocks to protect your laptop if it is lost or stolen. Intel AT's capabilities, including lock downs based on local timers and excessive login attempts, are designed into the system hardware. Because they are built into the laptop itself, these capabilities work

Table 1. Features of Symantec PGP® Whole Disk Encryption (WDE) and Intel® Anti-Theft Technology (Intel® AT)

PGP WDE

- Centrally managed and controlled; policy driven
- Rapidly deployed and maintained; completely transparent to the user
- Equipped with an extensible key and policy management system; can manage third-party and enterprise-developed applications
- Supports strong, multifactor authentication methods
- Supports removable media, including options for device control management
- Easily supported by help desk or IT personnel
- Expandable; new managed encryption applications can be added, as needed
- Includes encryption and key management support for other portable devices, including smartphones
- Extensible; organizations can add managed encryption to existing enterprise applications

Intel AT

- Transparently deployed with Symantec PGP® Whole Disk Encryption
- Pre-boot authentication (PBA) login timer
  - Triggers a response when failed login attempts exceed a policy-based threshold
  - Includes additional security to prevent automated attacks
  - Works both online and offline
- Rendezvous timer
  - Triggers a policy-based response if the laptop fails to check in with the central server
  - Works both online and offline
- PC tamper monitoring
  - Triggers a response if any of the key components of the laptop have been tampered with
- Laptop disable
  - Once disabled, the laptop cannot be rebooted, even if the hard drive is reimaged or replaced, and remains inoperable
- Data access disable
  - IT technician can send a remote poison pill in the form of an encrypted Short Message Service text message, which can be delivered over a local area network (LAN), wireless LAN, or 3G network
  - Encryption key material is stored in the chipset, and to protect the data the poison pill deletes some of the encryption components
- Reactivation
  - Reactivation screen of the disabled laptop can feature a customized message; for example, Please call John Smith at 800-555-1212 for a reward
  - Convenient local reactivation using a previously defined passphrase.
  - Easy remote reactivation using an IT-generated, one-time-use-only recovery token provided to the user
- Secure decommission removes or encrypts hard drive data while keeping the laptop operational for its re-use or resale

regardless of whether the system is connected to a network. Table 1 (bottom) summarizes some of the main features of Intel AT.

Deploying Symantec PGP® Whole Disk Encryption and PGP Remote Disable & Destroy with Intel Anti-Theft Technology

Deploying PGP WDE and PGP RDD with Intel AT is similar to deploying other enterprise solutions. The PGP Universal Server provides organizations with a single console to manage multiple encryption applications from the PGP® Platform. IT organizations can manage users, automate administrative activities, and establish policies to defend sensitive data. The back-end Intel permit server, hosted by Intel, allows the enrolling and un-enrolling of laptops with Intel AT. This deployment model offers the full range of encryption options and protects the laptop both inside and outside the enterprise.

Figure 4 illustrates how the Intel permit server and the PGP Universal Server work together to protect your enterprise's physical and electronic assets.

SOLUTION IN ACTION: PROACTIVE DATA PROTECTION, EASY REACTIVATION

The following example shows how Symantec PGP® Whole Disk Encryption (WDE) and PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft Technology (Intel® AT) combine the ability to disable access to data when necessary with the ability to easily reactivate that access:

Scenario 1. Tarun, an employee for a large health insurance company, has just returned from a two-week vacation. When he left, IT electronically "locked" his laptop, per company policy, thereby disabling access to the critical data he has stored on his system, should his laptop be stolen while he is away. Now that Tarun has returned to the office, he simply contacts IT support, which remotely unlocks his laptop in mere seconds, and he again has access to his laptop and the data it contains.

Scenario 2. Cecelia is traveling with her laptop to a remote research lab in Eastern Europe and has to cross several international borders—not all of which can necessarily be trusted to keep sensitive data safe. If a customs agent instructs Cecelia to enter her login credentials to access her encrypted hard drive, she must legally comply with the request. However, this puts her data at risk. To prevent potential data loss, IT marks the laptop as stolen—before Cecelia leaves the home office—thereby disabling access to data by locking critical cryptographic material at the hardware level. Cecelia can truthfully say that she cannot access the data, without breaking the law. But, when she arrives at the remote office, she simply contacts IT support and they remotely and quickly unlock the laptop.

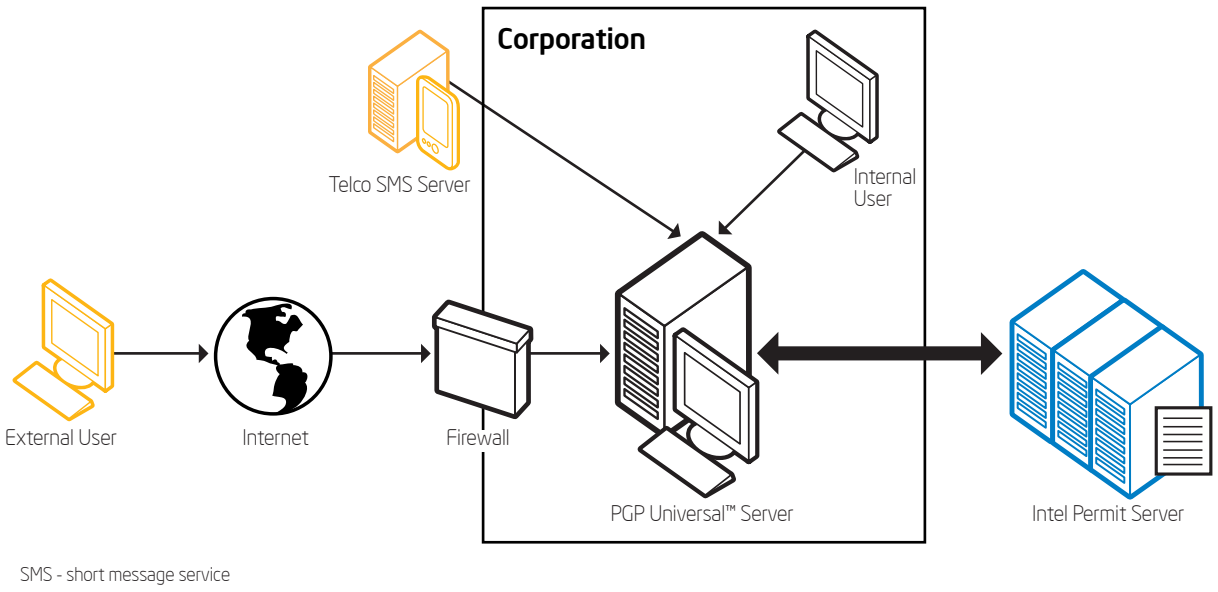


Figure 4. Deployment of Symantec PGP® Whole Disk Encryption (WDE) and PGP® Remote Disable & Destroy (RDD) with Intel® Anti-Theft (Intel® AT) Technology.

SYMANTEC PGP® WHOLE DISK ENCRYPTION PERFORMANCE AND MANAGEABILITY FEATURES

Symantec PGP® Whole Disk Encryption offers numerous performance and manageability features, including the following:

- Supports Advanced Encryption Standard (AES) New Instructions for increased speed on the latest Intel® processors
- Supports Intel® Active Management Technology for increased recoverability and manageability in enterprise systems
- Built with high-performance PGP® Hybrid Cryptographic Optimizer (HCO) technology
- AES 128-bit and 256-bit encryption
- Supports .MSI and .PKG formats
- Supports Microsoft Windows* (including Windows Server*), Mac OS X*, Ubuntu*, and Red Hat* clients
- Supports Windows Preinstallation Environment and Bart's Preinstalled Environment for diagnostics and repair
- Additional Decryption Key (ADK) enforces cryptographic controls on administrative access to data. (For example, several vice presidents must enter their credentials to allow a process to complete.)

Conclusion

Laptop thefts are frequent and costly. PGP WDE and PGP RDD with Intel AT help deter PC theft and protect data, thereby reducing corporate risk. In combination, these two technologies offer tangible benefits to the enterprise, including the following:

- Encryption provides strong data protection.
- Local and remote intelligent theft and tamper detection enable quick response to theft.
- Disabled laptop becomes inoperable.
- Data can be remotely disabled or destroyed.
- Encrypted data is protected even if the user's credentials are compromised.
- Data cannot be recovered by moving the hard drive to another PC.
- Easy reactivation if the laptop is recovered.

Deploying PGP WDE and PGP RDD with Intel AT helps ensure that security defenses remain in place even after a laptop is missing or stolen. In turn, this helps businesses minimize risk and loss even while complying with the most stringent data security regulations.

To learn more about Intel and Symantec anti-theft solutions, visit: **http://www.antitheft.intel.com/Symantec**.

To learn more about Intel AT, visit **http://antitheft.intel.com**.

Find an Intel AT-enabled laptop at **http://antitheft.intel.com/find-a-laptop.aspx**.

To learn more about PGP encryption technology, visit **http://www.pgp.com/products/wholediskencryption/index.html**.

For more information, visit **http://www.pgp.com/products/index.html**.

Solution provided by: intel | Symantec

[1] "Getting over laptop loss," by Joris Evers, CNET News, June 30, 2006. http://news.cnet.com/Getting-over-laptop-loss/2100-1044_3-6089921.html

[2] Symantec Global Internet Security Threat Report, Trends for 2008. http://www.symantec.com/connect/downloads/symantec-global-internet-security-threat-report-trends-2008

[3] "The Cost of a Lost Laptop," a study sponsored by Intel Corporation and independently conducted by Ponemon Institute, LLC; May 2009. http://www.ponemon.org/data-security

[4] Chronology of Data Breaches, Privacy Rights Clearinghouse, March 2010. http://www.privacyrights.org/ar/ChronDataBreaches.htm

[5,6,8] "Fourth Annual Cost of a Data Breach," Ponemon Institute, LLC; February 2009. http://www.ponemon.org/data-security

[7] "Airport Insecurity: The Case of Missing & Lost Laptops," Ponemon Institute, LLC; July 2008. http://www.ponemon.org/data-security

No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT), also referred to as the 'poison pill' in some documents, 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. Intel AT performs the encrypted data access disable by preventing access to or deleting cryptographic material (e.g. encryption keys) required to access previously encrypted data. ISV-provided Intel AT-capable encryption software may store this cryptographic material in the PC's chipset. In order to restore access to data when the system is recovered, this cryptographic material must be escrowed/ backed up in advance in a separate device or server provided by the security ISV/service provider. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel AT functionality has been activated and configured. The activation process requires an enrollment procedure in order to obtain a license from an authorized security vendor/service provider for each PC or batch of PCs. Activation also requires setup and configuration by the purchaser or service provider and may require scripting with the console. Certain functionality may not be offered by some ISVs or service providers. Certain functionality 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.

Printed in USA ♻ Please Recycle 0111/RKM/KC/PDF 323009-002US