Protecting Sensitive Data on Laptops is More Important Now Than Ever

Businesses are facing regulations, fines, and consequences for breaches of sensitive data

Data breaches continue to increase in number and cost

Businesses have access to many robust security solutions. These include anti-virus applications, intrusion prevention systems (IPSs) and intrusion detection applications, as well as encryption, data loss prevention (DLP) solutions, and authentication applications (identity and access management solutions). Yet, with all the security applications and approaches available today, companies are still vulnerable to data loss and theft. In fact, according to a 2010 Ponemon Institute benchmark study, the average laptop has about a 7 percent chance of being lost or stolen.[1] Businesses are struggling not only to protect sensitive data, but also to prove compliance with increased security regulations in both Europe and North America.

Sensitive data is still increasingly vulnerable

Many factors contribute to the continued rise in data breaches, including:

- **More sophisticated equipment and software applications for hackers.** With less investment, it's easier to break through security and commit data breaches.
- **An increasingly mobile workforce.** As users become more mobile, laptops—and their data—are more exposed to loss and theft. For example, health-care workers are often mobile, not just within hospitals and health-care centers, but between campuses. Other vulnerable groups include consultants, financial advisors, sales and marketing users, construction engineers, and other workers who travel between job sites.
- **Laptops are often shared in environments such as data centers, schools, and customer service centers.** Sharing laptops among many users not only makes sensitive data more vulnerable to loss or theft, but it also puts data at greater risk of unauthorized access.
- **Bulk shipments of laptops.** The military, government agencies, and educational organizations are particularly vulnerable to laptop theft during transport.
- **Expensive assets.** Customized telecommunications laptops for field technicians, for example, are particularly tempting to thieves. As a result, their sensitive data are at greater risk of exposure.
- **Security applications installed at the OS or BIOS level.** These can be robust solutions, but are at risk of being circumvented or disabled.
- **Security credentials are often stored in software.** This makes them vulnerable to attacks aimed at gaining access to applications and data.

User behavior continues to increase risk

Users themselves can also cause security problems. They often keep passwords in places that a thief can access—such as on a sticky note kept with a laptop or in a wallet. In addition, assets aren't always returned at the end of a lease or when users move to new positions or new companies. While loss of assets is costly because of end-of-lease buyouts, costs can escalate because of exposure of sensitive data stored on those unreturned systems.

Data breach costs are still rising

Companies face both direct and indirect costs in the aftermath of a data breach:

- **Stiffer fines, more post-incident requirements, and higher post-incident costs.** For example, the average organizational cost of a data breach increased to USD 6.75M in 2009.[1]
- **Loss of intellectual property.** 71 percent of laptop thefts result in a data breach, exposing not only client and consumer data but proprietary data as well.[3]

NEW IN INTEL® ANTI-THEFT TECHNOLOGY (INTEL® AT): Protection for decrypted data after resume from S3 sleep state

One of the traditional vulnerabilities of encryption on laptops occurs when a laptop resumes from standby (S3) sleep state. Files that were decrypted before the system entered sleep state remain decrypted when the system wakes. The decrypted data can be easily accessed by thieves, and even by unauthorized users who simply lift the lid of the laptop to steal the data. Access is allowed because, upon resume from S3, a traditional laptop bypasses the pre-OS authentication screen for the encryption application.

Intel® Anti-Theft Technology (Intel® AT) closes that window of vulnerability and enforces pre-OS encryption by requiring that the user re-authenticate when the system resumes from S3. The user must enter his or her credentials within a predefined period of time before regaining access to the decrypted files. This feature is available on laptops with 2nd generation Intel® Core™ processors with vPro™ technology.

- **Legal costs of investigation, notification, and resolution of the incident.** Last year's average per-victim cost was USD 204, an increase of USD 2 per customer record compared to similar costs in 2008.[1]
- **Credit monitoring.** A company may need to provide costly credit monitoring for individuals who could be affected by the data breach.
- **Damage to the brand.** Loss of public and investor confidence, business opportunities, and revenue that result from a company's damaged reputation is responsible for USD 144 (70 percent) of the USD 204 average cost of a compromised record.[1]

Strict new regulations

To help protect clients and consumers, regulatory bodies are passing increasingly strict laws both in Europe and North America.

In the United States, most states now have a data-breach notification law or similar legislation that regulates data security and accountability. These state laws include requirements for public disclosure of breaches as well as potential fines or other sanctions.

Managing and mitigating risk: A robust, layered approach

In today's high-risk environment, the security of assets and sensitive data requires a layered approach (see Figure 1) that reaches beyond the OS and BIOS down into hardware. By implementing intelligent hardware-based technologies (such as tying encryption to a laptop's hardware), IT administrators can better protect sensitive data. This protection extends even after a laptop goes missing and even if a thief has access to security credentials.

Intel® AT: Intelligent, automated policy-based protection

Intel® Anti-Theft Technology (Intel® AT) adds a deep layer of protection for laptops.[4] An intelligent and automated technology, Intel AT is built directly into laptop hardware. Intel AT can detect theft conditions and respond locally and automatically based on IT policy, or respond to a remote poison pill sent by a central server. Remote poison pills (and reactivation messages) can be sent over an IP-based or 3G-based network.

IT administrators can now be more assured that a laptop is under control of the authorized user. If lost or stolen, the laptop can be rapidly and automatically locked

A layered approach to security, including hardware-based Intel® Anti -Theft Technolgy (Intel® AT)

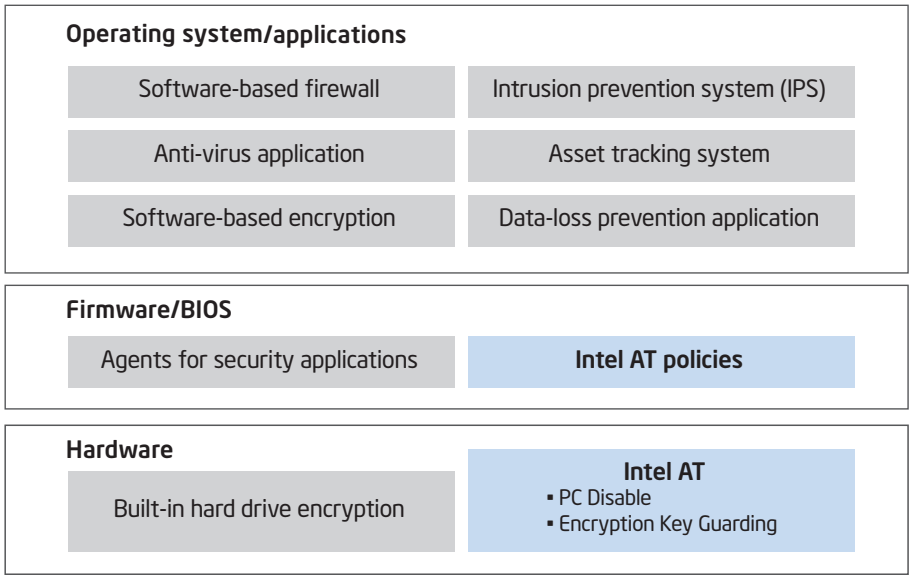

Figure 1. A layered approach to protect assets and sensitive data on laptops. Security is installed at the OS level, integrated in BIOS and firmware, and also designed into hardware. This layered approach helps businesses manage and mitigate risk and improve compliance with new regulations.

down based on IT policy, and its encryption information can be protected. This helps IT administrators improve compliance with strict regulations, minimize data breaches even after a laptop goes missing, and reduce post-incident costs.

Rapid local or remote policy-based detection and response

Security vendors are taking advantage of local and remote tamper-resistant triggers that can detect a suspicious condition:

- **Excessive login attempts (local).** Multiple failed login attempts in a pre-boot authentication (PBA) screen.
- **PBA login timer expires (local).** If the user does not log into the PBA screen successfully within the IT-specified time frame, the laptop enters theft mode.
- **Rendezvous timer expires (local).** A local, hardware-based timer expires if the laptop does not check in with the central server within an IT-specified interval of time. This feature is a local trigger implemented in hardware; it works regardless of network connectivity.
- **Notification from server (remote) via IP-based network.** A flag set in the central server triggers a poison pill, which is sent to the laptop via a wired or wireless LAN the next time the system checks in.
- **Notification from server (remote) via 3G-based network.** IT administrators can automatically or manually send a poison pill via an encrypted SMS text message over a 3G network.[5] This allows IT administrators to remotely and rapidly trigger a lock down even without LAN/WLAN-based connectivity.
- **PC tampering (local).** A lock down can be triggered when Intel AT detects changes in the firmware of the laptop or removal of the CMOS battery.

These flexible responses allow IT to specify the conditions that determine a lock down or trigger the disabling of encryption credentials. Laptops themselves can now respond automatically, intelligently, and rapidly to a variety of suspicious circumstances.

Protect the asset, protect the data

When a suspicious condition is encountered, Intel AT responds based on IT policy. For example, Intel AT can disable the laptop by blocking its boot process at the hardware level. This prevents the system from booting from any device, including from a hard drive, secondary drive, USB drive, CD, DVD, or other peripheral device. Even if a hard drive is reformatted or replaced, the system remains disabled. Unable to boot, the laptop is essentially a "brick" and is of little use or resale value to a thief.

Intel AT can also delete or disable (block) essential cryptographic information required for encryption/decryption. Even if a thief gains access to encryption credentials, the keys or other essential cryptographic information stored in the system have been erased or disabled and cannot be used to decrypt the data. Only after IT restores the keys and reactivates the system can the data be decrypted again.

With Intel AT, assets and data can remain protected, giving companies more time to resolve an incident before an actual data breach occurs and notification requirements take effect.

Reactivation is fast and easy

Intel AT does not destroy user data. The boot process is only disabled, and data is not erased. (Key elements of encryption keys can be disabled or erased.) When a laptop is recovered, the IT administrator or an authorized user can rapidly restore the system using one of several methods. These include entering a local passphrase, entering a one-time recovery token generated by IT (or the user's service provider), reactivation via a PBA module, or remote reactivation via an encrypted SMS message over a 3G network (requires a laptop with a 3G modem that supports Intel AT).

NEW IN INTEL® AT: Use a 3G network for PC lock down, reactivation, and location beaconing

With Intel® Anti-Theft Technology (Intel® AT), IT administrators can now use encrypted SMS messages over a 3G network to send a poison pill, remotely unlock a recovered laptop, or tell the system to send location information back to the central server.

- **Poison pill delivery via an encrypted SMS message over a 3G network.** Intel AT includes a direct hardware link between Intel AT and the 3G module. IT administrators can now take advantage of 3G connections to remotely and rapidly disable a laptop regardless of the state of the OS.
- **Remote reactivation via an encrypted SMS message over a 3G network.** IT administrators can now rapidly and easily reactivate a laptop within minutes after the system is recovered.
- **Automated or on-request location beaconing.** Intel AT version 3.0 can send location information back to the central server via an SMS message over a 3G network (the 3G card must support GPS and Intel AT 3.0).[5] Location information can be sent as latitude and longitude or as a relay of a MAC address. IT administrators can now request the system's location information to help with asset recovery. Beaconing can also be automated so that, after the laptop enters stolen mode, location information is sent back to the central server on a pre-determined schedule.Beaconing can be enabled only when the laptop is in stolen state, which protects the user's privacy while the system is in normal mode but allows tracking if the system is stolen. Some ISVs may allow users to choose whether to enable Intel AT-based GPS beaconing for stolen laptops to help with asset recovery.

IT administrators can now respond rapidly and remotely to suspicious circumstances by communicating with Intel AT over a 3G-based network, regardless of the state of the OS.

Enhance higher-level security solutions

Working together, OS-based applications, BIOS-level solutions, and intelligent hardware design can greatly increase the overall security of a mobile device. The combination can also create opportunities for creative data-protection solutions (Table 1).

Improve security and compliance, reduce corporate risk, and lower costs

Businesses are under increasing social and regulatory pressure to comply with data-security regulations. In today's economy, they are also under increasing financial pressure to centralize and automate security and minimize post-incident costs. To address typical vulnerabilities in security solutions, IT administrators must take a layered approach. This means integrating robust OS- and BIOS-based security solutions with automated, intelligent policy-based technologies built into the laptop's hardware. Such an approach provides IT with both high-level and low-level data protection, as well as local and remote protection of expensive assets and sensitive data. With greater overall protection, businesses can improve compliance, minimize the risk of a data breach, and lower post-incident costs.

Table 1. Intel® AT enhances security solutions

Area of improvement	With Intel® AT, security solutions can now . . .
Full-disk encryption	Store essential encryption information in the laptop's hardware (instead of software), and automatically and intelligently disable or delete encryption information when the laptop is lost or stolen.
Geofence capabilities	Support geofencing capabilities by using GPS and other location features to identify when a laptop leaves a particular campus, area, or state, or crosses an international border. Upon notification, an IT administrator can send a poison pill (via an IP-based or 3G-based network) to disable systems taken outside their designated boundaries.
Compliance	Receive confirmation of delivery of a poison pill to a lost or stolen laptop. This helps businesses prove compliance, by showing a regulatory body that the system remains disabled and/or its data remains inaccessible even after it goes missing.
Asset recovery	Specify a customized pre-boot lost-and-found message that tells authorities and Good Samaritans how to return the laptop to its rightful owner. For example, a message could say, *"This laptop belongs to ACME Industries and has been reported missing. To return the laptop, please call 1-123-456-7890."* After a lock down, trigger a location beacon to help with location and recovery.

To learn more about Intel AT, as well as the OEMs and ISVs who offer Intel AT features in their security solutions, please visit **anti-theft.intel.com**.

[1] Source: "The Billion Dollar Lost Laptop Study", Ponemon Institute, LLC, September 2010.

[2] Source: Worldwide PC 2010–2014 forecast, IDC, April 2010.

[3] Source: "The Cost of a Lost Laptop," Ponemon Institute, LLC, April 2009.

[4] Intel® Anti-Theft Technology (Intel® AT). No computer system can provide absolute security under all conditions. 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.

[5] This feature requires a laptop with Intel® Anti-Theft Technology (Intel® AT) 3.0, a 3G laptop modem that supports Intel AT 3.0 functionality (for example, the Ericsson F5521gw), and OEM-enabled communication between the 3G modem and laptop.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Copyright © 2011 Intel Corporation. All rights reserved.Intel, the Intel logo and Intel Anti-Theft technology logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others. Printed in USA 0211/JO/MESH/PDF Please Recycle 325053-001US