

# Protecting Sensitive Data on Laptops is More Important Now Than Ever

Businesses are facing strict new regulations, higher fines, and more consequences for breaches of sensitive data

## White Paper

Intel® Anti-Theft Technology



### Why are data breaches still increasing in number and cost?

Businesses have access to many robust security solutions. These include anti-virus applications, intrusion prevention systems (IPS) 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 2009 Ponemon Institute benchmark study, data breaches from malicious attacks and botnets actually doubled from 2008 to 2009.<sup>1</sup> Businesses are struggling not only to protect sensitive data, but also to prove compliance with strict security regulations recently passed both in Europe and North America.

### Sensitive data is still increasingly vulnerable

There are many factors contributing to the continued rise in data breaches. These include the following:

- **Hackers have access to more sophisticated equipment and applications.** For less investment, it's easier to break through security and commit data breaches.
- **An increasingly mobile workforce.** Today's businesses are buying more laptops than desktops? As users become more mobile, laptops – and their data – are more exposed to loss and theft. For example, health-care workers are often extremely 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 among many users** in environments such as data centers and customer service centers. Not only does this make sensitive data more vulnerable to loss or theft, it puts data at greater risk of unauthorized access.
- **Bulk shipments of laptops** for the military, government agencies, and educational organizations are particularly vulnerable to theft during transport.
- **Expensive assets**, such as customized telecommunications laptops for field technicians, 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** can be robust solutions, but are at risk of being circumvented or disabled.
- **Security credentials are often stored in software**, which makes them vulnerable to circumventing authentication and encryption applications.

## User behavior continues to increase risk

Users themselves can also cause security problems. Also, users often keep passwords in places that a thief can access—such as sticky notes kept with a laptop or in a wallet. This removes the ‘security’ notion from security solutions. Such places include sticky notes kept with a laptop or written down in a wallet. In addition, assets aren’t always returned at end of lease or when users move on to new positions or new companies. While loss of assets is costly to business because of end-of-lease buy-outs, costs can escalate because of exposure of sensitive data stored on those unreturned systems.

## The costs of a data breach 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 \$6.75M in 2009.<sup>1</sup>
- **Loss of intellectual property.** 71% of laptop thefts result in a data breach, exposing not only client and consumer data but proprietary data as well.<sup>3</sup>
- **Legal costs of investigation, notification, and resolution of the incident.** Last year’s average per victim cost was \$202 with an average indirect cost of \$152 per breach victim. This year’s direct cost rose to \$60 from \$50 in 2008.<sup>1</sup>
- **Credit monitoring** may need to be provided for individuals who could be affected by the data breach. Because of this, in 2009, the per-victim cost for a data breach involving a lost or stolen laptop rose to \$225.<sup>1</sup>
- **Damage to the brand.** Loss of public and investor confidence, business opportunities, and revenue that results from a company’s damaged reputation is responsible for \$144 (70%) of the \$204 average cost of a compromised record.<sup>1</sup>

## Strict new regulations

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

### Recent changes in U.S. laws and regulations

Almost all U.S. states now have a data-breach notification law or similar legislation that regulates data security and/or accountability. With the recent passing of three new national acts, businesses must comply with an increasing number of data-protection regulations, manage third-party data security practices, and face stiffer fines for infractions. This makes it even more important for businesses to improve protection of sensitive data.

### Recent changes in European laws and regulations

The first data-regulation law of its kind was passed recently in Europe to help protect consumers’ personal data. Other laws, with higher ceilings for fines, have recently gone into effect in both the U.K. and Germany.

- European Union Telecoms Reform Package, 2009, including mandatory notification of breaches of consumers’ personal data.
- German Federal Data Protection Act (BDSG), July 2009, which requires notification of data breaches and increased fines for failing to protect personal data.
- In April 2010, the United Kingdom (U.K.) passed a law allowing the Information Commissioner’s Office to fine organizations up to £500,000 for severe data breaches that expose clients’ personal data.

These and other regulations, as well as social and economic pressures are prompting businesses to work harder to close vulnerabilities in their approaches to data protection.

## Strict new regulations increase fines and penalties for noncompliance

The number of regulations and laws going into effect is increasing, as are the fines and penalties for noncompliance. Some of the more notable acts that have recently gone into effect include:

- Personal Data Privacy and Security Act (PDPSA)
- Data Breach Notification Act
- Data Accountability and Trust Act (DATA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Health Information Patient Privacy Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- CS Senate Bill 1386
- Gramm-Leach-Bliley Act (GLBA)
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- European Union Privacy Directive

## Managing and mitigating risk: A robust, layered approach

In today's high-risk environment, 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, even if a thief has access to security credentials (such as by getting them from a sticky note in a user's wallet).

### Intel® AT: Intelligent, automated, policy-based protection

Intel® Anti-Theft Technology (Intel® AT) adds the third, deep layer of protection for laptops.<sup>4</sup> 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. 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 down based on IT policy and/or its encryption information can be protected. This helps IT administrators improve compliance with strict regulations, minimize data breaches, and reduce post-incident costs.

#### Rapid local or remote policy-based detection and response

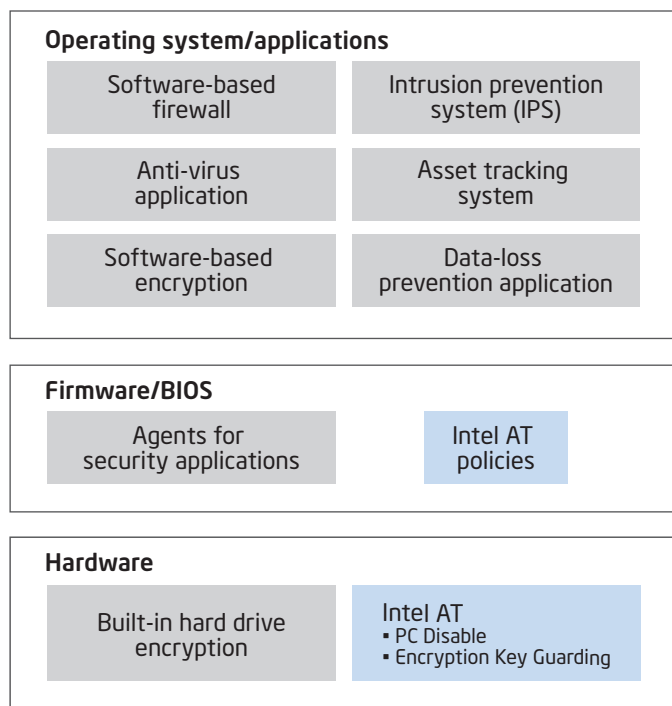
Security vendors are implementing both local and remote features of Intel AT. For example, security vendors are taking advantage of three types of flexible, tamper-resistant triggers that can detect a suspicious condition:

- **Failure of Login Attempts (Local):** Multiple failed login attempts in a preboot screen. Login can be authenticated via a required password, biometric data, or other methods.
- **Expiration of Rendezvous Timer (Local):** A hardware-based timer expires if the laptop does not check in with the central server within a specified length of time.
- **Notification from Server (Remote):** A flag set in a central server triggers a poison pill, which is sent to the laptop the next time the system checks in with the central server. A poison pill can also be sent via an encrypted SMS text message from the central server.

#### 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 PC 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 of little use or resale value to a thief.

## A layered approach to security, including hardware-based Intel® Anti-Theft Technology (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 and improve compliance with new regulations.

Intel AT can also delete or hide cryptographic keys or other essential 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 is not destructive technology. The boot process is only disabled, and data is not erased; only encryption information is guarded. When a laptop is recovered, an authorized user can rapidly restore the system by entering a one-time reactivation passphrase (provided by IT) in a preboot screen.

**Table 1. Intel® AT enhances security solutions**

Area of improvement	With Intel® AT, security solutions can now...
Enhance full-disk encryption	Store essential encryption information in the laptop's hardware, and automatically and intelligently hide or delete encryption information when the laptop is lost or stolen.
Geofence laptops	Use global positioning system (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 manager can send a poison pill that disables the laptop's boot process and/or disables essential cryptographic information to block access to encrypted data.
Prove compliance	Receive confirmation of delivery of a poison pill to a lost or stolen laptop. This helps business prove to a regulatory body that the PC is disabled and/or its data is inaccessible while the laptop is missing.
Improve asset recovery	Specify a customized preboot 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 1-800-ACME-123."

## 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. They can also create opportunities for creative data-protection solutions (see 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 weak 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, policy-based intelligent 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.

To learn more about Intel Anti-Theft Technology, as well as the OEMs and independent software vendors (ISVs) who offer Intel AT features in their security solutions, please visit [anti-theft.intel.com](http://anti-theft.intel.com).

<sup>1</sup> Source: 2009 Annual Study: Cost of a Data Breach, Ponemon Institute, LLC, January 2010.

<sup>2</sup> Source: Worldwide PC 2010-2014 forecast, IDC, April 2010.

<sup>3</sup> Source: The Cost of a Lost Laptop, The Ponemon Institute, LLC, April, 2009.

<sup>4</sup> 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 therefrom.

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 by visiting Intel's Web site at [www.intel.com](http://www.intel.com).

Copyright © 2010 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel Anti-Theft Technology mark are trademarks of Intel Corporation in the U.S. and other countries.

\*Other names and brands may be claimed as the property of others.

