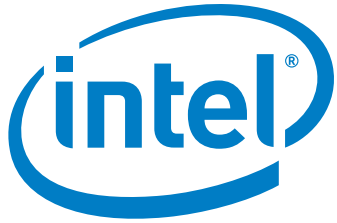


White Paper

Intel Information Technology

Client Platforms and

Solutions Notebook Security

Strengthening Enterprise Security through Notebook Encryption

IT@Intel shares its experience in planning a smooth and cost-effective implementation to protect sensitive and valuable information across all corporate notebooks.

Rex Rountree, Encryption Service Manager, Intel Information Technology

Carol Kasten, Data Protection Manager, Intel Information Technology

Michael Amirfathi, Engineering Information Protection and Encryption Services Manager, Intel Information Technology

December 2008

IT@Intel

Executive Summary

Lost and stolen notebook computers are a source of significant business risk for many companies. It is difficult, if not impossible, for IT organizations to control the information stored on hundreds or thousands of employee notebooks. Yet with the worldwide proliferation of privacy laws and regulations, protecting the kinds of sensitive and valuable data that are often found on notebooks has become a critical issue for corporate risk managers. There are many documented cases in which a lost or stolen notebook has exposed not only corporate secrets, but also the personal information of the company's employees, customers or business partners, resulting in significant legal liability, cleanup costs, and brand impact.

In assessing the risk to the business, Intel IT determined that a single major notebook-related data breach could cost USD 5 million or more in direct costs alone. Our solution was to encrypt all corporate notebooks, so even if a system is stolen, data cannot be accessed by malicious individuals. The total cost of implementing the encryption solution is significantly less than the potential cost of a single breach.

This white paper describes, in detail, Intel's business reasons for adopting notebook encryption, as well as the plan Intel IT developed to help ensure a smooth, secure, and cost-effective implementation.

Table of Contents

Notebook Theft and Enterprise Security

Beginning in 1995, Intel IT began an enterprise-wide shift toward mobile computing.

This move was based on an internal analysis that showed equipping an employee with a notebook and wireless networking capabilities would provide more than five percent time savings in a typical workweek. By replacing 6,400 desktops with notebook computers, we achieved productivity gains valued at USD 26 million.[1] We now deploy notebooks to about 80 percent of our workforce (Figure 1), and consider our broad use of mobile computing to be an important and strategic business advantage. We also continue to evaluate our usage models and make appropriate changes to further improve employee responsiveness, productivity, and satisfaction.

Along with its many benefits, employee mobility introduces new business risks that must be mitigated. Notebook users connect to the Internet and the Intel corporate network from home and Wi-Fi* hotspots, as well as from customer and vendor sites. Intel IT employs a multi-layered security approach to protect notebooks, data, and the network during these interactions. Protections include hardened and managed notebook configurations, virus protection, firewalls, intrusion detection applications, and virtual private networking (VPN) for secure communications.

This multi-layered approach has been effective in protecting Intel's networked assets, but there is another risk that has grown dramatically in recent years—the risk that sensitive information will fall into the wrong hands due to a lost or stolen notebook. Lost and stolen notebooks are among the most common security incidents businesses face today and a major cause of personal information loss. One measure of the risk can be found in a recent report by Dell and the Ponemon Institute, which reports that up to 12,000 notebooks are lost in U.S. airports every week, and 65 to 70 percent of these systems are never re-claimed.[2] The Privacy Rights Clearinghouse adds another reason for concern. According to that organization's statistics, notebooks have been involved in 37 percent of documented security incidents that have lead to the compromise of personal information.[3]

In assessing the potential risk to Intel, one metric we evaluated was the cost of providing credit monitoring for individuals whose records might be compromised in a notebook-related data breach. We felt this would provide a very conservative estimate of the costs we would be likely to incur. Our analysis showed that, in a major incident, these costs could easily top USD 5 million. A more general look at potential costs was provided by the Ponemon Institute in a 2006 survey that assessed the real-world costs incurred by companies who had actually experienced data breaches.[4] According to that report, the average cost per company per breach was USD 4.8 million, with amounts ranging from USD 226 thousand to USD 22 million.

1. For more information, read the IT@Intel white paper, *Client PCs as Strategic Assets*, May 2007. http://www.intel.com/it/pdf/client-pcs-as-strategic-assets.pdf.
2. Source: *Airport Insecurity: The Case of Missing & Lost Laptops*, a study sponsored by Dell and independently conducted by Ponemon Institute, June 30, 2008. http://www.dell.com/downloads/global/services/dell_lost_notebook_study.pdf.
3. Altogether, these notebook incidents have compromised more than 30 million personal records. Source: Privacy Rights Clearinghouse Web site: http://www.privacyrights.org/ar/ChronDataBreaches.htm#2 and http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm.
4. Source: 2006 Annual Study: Cost of a Data Breach—Understanding Financial Impact, Customer Turnover, and Preventative Solutions, a summary of benchmark research conducted by the Ponemon Institute, LLC, October 2006. http://connect.educause.edu/Library/Abstract/2006AnnualStudyCostofaDat/44808?time=1221496162.

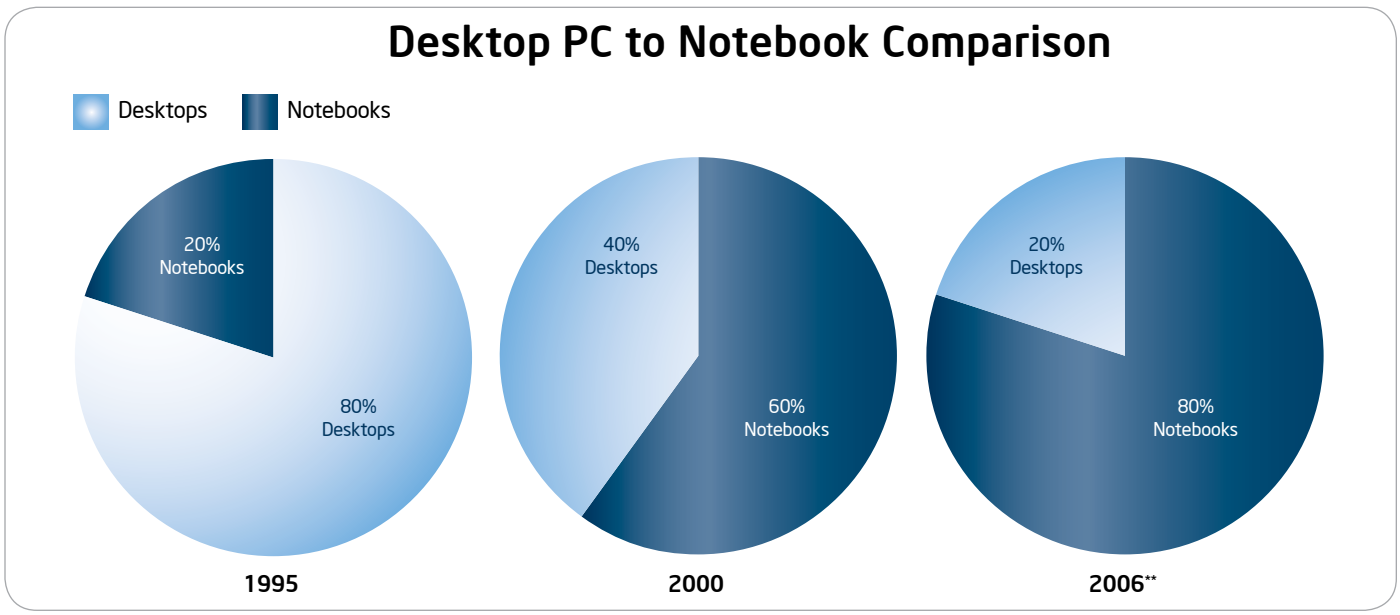


Figure 1. When Intel IT replaced 6,400 desktops with notebook computers, we realized productivity gains valued at USD 26 million (three year net present value). To extend these benefits, we increased notebook deployments across the company from 1996 through 2006, and now deploy notebooks to 80 percent of Intel employees. ***2006 Regional Breakdown of Laptops:* Europe 12.73%; Asia 20.41%; Americas 66.86%.

To further understand the associated risks, Intel IT established a Personal Data Loss Reporting process, which is used to follow up on all lost or stolen notebooks. Formal interviews are conducted to determine where, when and how a system was lost and what data, if any, was compromised. The good news for Intel is that our notebook loss rates are below the industry average. We attribute this to the emphasis we place on employee training, security policies, and regular security reminders. Nevertheless, notebooks are lost, and these lost systems represent real and significant risk to the business. We felt it was imperative to understand the nature and magnitude of the risk and apply appropriate security measures.

Two Kinds of Information – Two Complementary Strategies

Security is rarely an all-or-nothing proposition, so Intel security teams work to ensure that security investments are closely aligned with the value they deliver to the business (see sidebar, How Intel Optimizes Security Investments).

This requires a clear understanding of the specific types of information that are at risk so that appropriate security can be applied (Figure 2). In general, there are two categories of information that must be secured on Intel notebooks: Intel intellectual property (IP) and personal information.

Intel Intellectual Property (IP)

Intel intellectual property includes a wide range of business information, such as business plans, corporate financial data, technical product information, and production schedules. Sensitivity varies greatly for these types of information. In general, sensitive IP is not widely disseminated among Intel employees, and employees who do have access to such information take an active role in securing it through file-level encryption.

When used appropriately, file-level encryption provides strong protection for data, both on the hard drive and in transit. If there is a weakness for this kind of protection, it is not the technology, but rather the active participation it requires from notebook users. The user has to identify and encrypt sensitive files and folders. As with any employee-driven security solution, there are bound to be occasional mistakes.

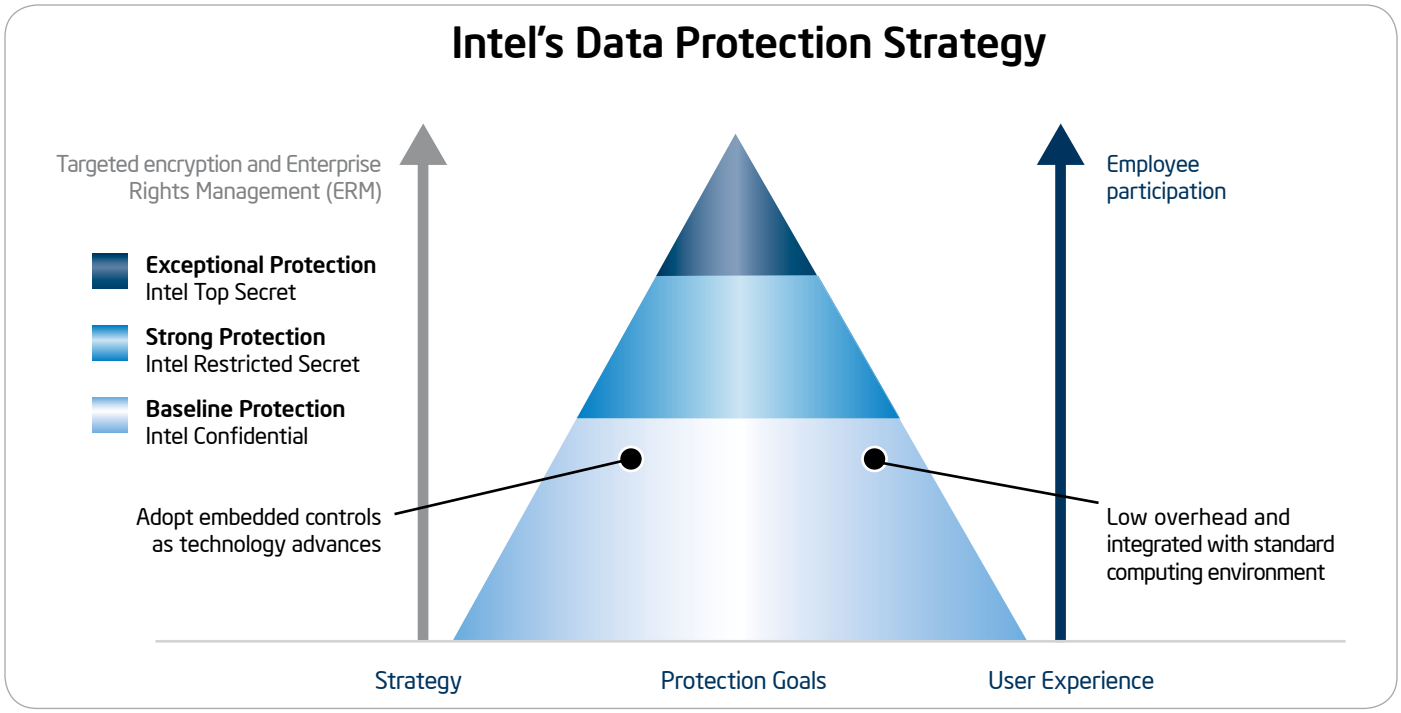


Figure 2. As a general rule, Intel security teams apply safeguards based on the sensitivity of the information at risk. Employee notebooks can potentially contain a wide range of sensitive information.

However, the number of notebook users that need this kind of protection is relatively small. With targeted training and reminders, we believe file-level encryption provides an essential layer of security.

The hard disk encryption solution discussed later in this paper also provides strong protection for Intel IP on employee notebooks. However, we will continue to use file-level encryption, because it provides important additional protection. With file-level encryption, even if a notebook is in active or standby mode when it is lost or stolen, the most sensitive information is still protected. File-level encryption is also portable, so files remain encrypted when they are transported electronically or stored in other locations, such as a USB device or a shared drive.

How Intel Optimizes Security Investments

Intel IT does not treat security as an all-or-nothing proposition. Instead, we see it as a continuous balancing act, in which we work to align our security investments with the business value they deliver (Figure 3).

These efforts include:

- Monitoring evolving threats, as well as the legal and regulatory environment, so we understand risks and requirements.
- Researching emerging security solutions to assess their effectiveness in mitigating risk, their compatibility and interoperability with our existing security solutions, and their total cost of ownership (TCO).
- Taking into account that strong security tends to constrain the use of data and systems, which can impact employee productivity and overall business efficiency.
- Balancing cost, risk, and business impact to deliver reasonable protection and the best overall value to the business.

Personal Information

Personal information comes in many forms and is virtually everywhere in today's digital world. Since Intel policy allows reasonable personal use of notebooks by employees, personal information on a lost or stolen notebook could include the employee's own financial information, personal contacts and communications, or even sensitive medical information. It might also include private information relating to family members, friends and business associates, as well as Intel customers or vendors.

Several factors contribute to the business risk associated with personal information.

- **Long-Lasting Sensitivity –** Many kinds of personal information, such as an individual's social security and driver's license numbers, remain valid for a lifetime. Such information can reside for years in forgotten files on a notebook, making it difficult, if not impossible, to know what sensitive information may be at risk when a notebook is lost or stolen.
- **A Strong and Growing Threat Matrix –** There has been an explosion in the number of criminals stealing and using personal information for identity theft and fraud. The Privacy Rights Clearinghouse has documented data breaches compromising more than 230 million records since January 2005.[5] Today's notebook thieves are sophisticated, organized, and focused on profit. Multi-phased attacks are not uncommon, and once information is compromised, the thieves can take advantage of an established black market infrastructure that includes Web sites designed specifically for buying and selling personal information.
- **Security Breach Laws –** The business risk of personal information loss is magnified by today's security breach laws. As of June 2008, 44 U.S. states have enacted data breach notification laws that require companies to report security incidents that expose unencrypted personal information.[6] Most of these laws are modeled on the first instance, which was the California Security Breach Information Act (SB1 386).[7] Many countries around the world also have laws and regulations that govern the protection of personal information. This legal and regulatory environment introduces a new level of liability and visibility for businesses. Many major corporations and government agencies have had to report data breaches due to lost or stolen notebooks.[8] The worst cases have potentially compromised personal information for millions of individuals, cost many millions of dollars in cleanup costs, and seriously damaged the responsible organization's credibility and brand.

5. Source: The Privacy Right Clearinghouse. http://www.privacyrights.org/ar/ChronDataBreaches.htm and http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm.
6. Source: National Conference of State Legislatures. http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.
7. "The catalyst for reporting data breaches to the affected individuals has been the California law that requires notice of security breaches. It is the first of its kind in the nation, implemented July 2003." Source: Privacy Rights Clearinghouse Web site. http://www.privacyrights.org/ar/ChronDataBreaches.htm#7
8. "Lost or stolen laptops and other digital media storage accounted for 20 percent of [date] breaches [so far in 2008]. Source: "Report: Data breaches Expose About 30M Records in '08," by Brian Krebs, The Washington Post. http://voices.washingtonpost.com/securityfix/2008/10/516_data_breaches_in_2008_expo.html

Clearly these are major business risks. One way to mitigate them would be to monitor and control personal information on employee notebooks. However, there are simply too many pieces of potentially sensitive information and, in Intel's case, they are embedded in gigabytes of data per notebook on tens of thousands of systems. Tracking and securing this information would be complex and cost-prohibitive.

Another approach would be to let each employee secure sensitive information on his or her notebook using the same file-level encryption solution we use to protect Intel IP. That would require tens of thousands of employees to understand risk and security processes. Even with training and constant reminders, slip-ups can and would occur. We believe this strategy would put an excessive burden on end-users and would still leave Intel exposed to unacceptable risk.

Another approach was needed, and it was important that Intel IT get ahead of the curve on this issue. With such clear risks, business units and employees might be inclined to deploy their own solutions. This would provide only spotty and inconsistent protection against personal information breaches and would not provide the kind of central governance and oversight needed to effectively mitigate business risk. It might also disrupt notebook management and prevent the recovery of information for business and legal purposes.

Full Disk Encryption

To solve this challenge, Intel IT decided to encrypt all data on every employee notebook. When properly implemented, encryption provides a strong and automated security solution that does not depend on active employee participation. It is based on a mature technology, can be implemented across all notebooks and provides a foundational layer of security that can be integrated with other technologies.

Perhaps most importantly, it is the only legally recognized approach to data protection. In many jurisdictions, organizations are required to report personal information breaches only for unencrypted data, so encrypting all data on every notebook not only protects data, but also substantially mitigates liability, visibility, and potential cleanup costs.

In evaluating encryption strategies, Intel IT selected full disk encryption. With this approach, the entire hard disk is encrypted, including data, applications, the operating system, and free space. Our rationale was that anything less than full disk encryption increases the attack surface[9] of the system, which we believe adds to overall risk. The greater the attack surface, the more effort we would have to expend in identifying and resolving potential vulnerabilities. For example, some encryption solutions leave certain files unencrypted, so the system can boot up before the user is required to authenticate their identity. With this approach, we would have to expend additional effort to understand and mitigate potential vulnerabilities that might be introduced by these unencrypted files. With full disk encryption, this is not an issue.

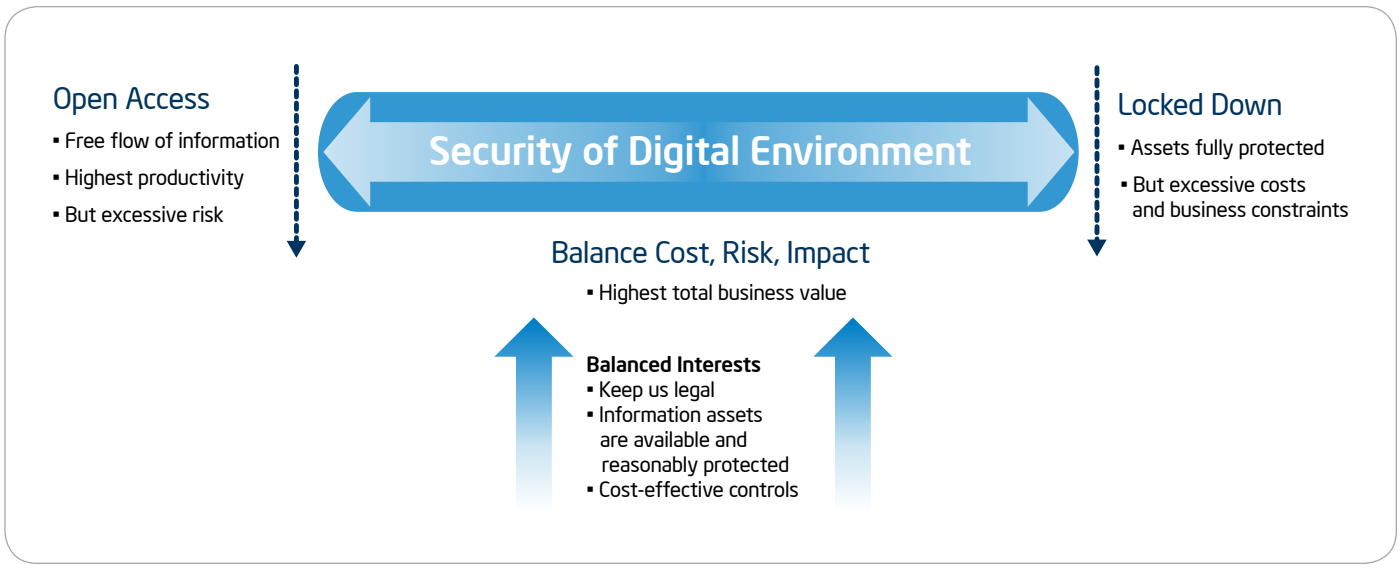


Figure 3. Intel's security posture: a balancing act.

9. According to Wikipedia, "the attack surface of a software environment is the scope of functionality that is available to any application user, particularly unauthenticated users." http://en.wikipedia.org/wiki/Attack_surface.

Requirements for Enterprise Deployment

An implementation of full disk encryption across all employee notebooks would entail considerable risk in its own right, since it impacts the great majority of Intel employees. To mitigate this risk, Intel IT established the following requirements for the solution.

- **High Security –** Encryption technology is basically the same across all products and implementations. However, tools, interfaces and the underlying architecture and infrastructure are not. Our solution had to be consistent and interoperable with Intel's existing notebook security solutions. It also needed to provide secure key storage on the notebook and support multi-factor authentication. Finally, to ensure the solution meets legal and regulatory requirements, the product had to have standard certifications, such as FIPS (Federal Information Processing Standard) and NIST (National Institute of Standards and Technology).

- **Enterprise Manageability –** To ensure effective management, the solution had to be consistent with Intel's existing management tools and processes. This required full interoperability with Intel® vPro™ technology, to ensure we could remotely power up, boot and access an encrypted notebook for monitoring, troubleshooting, and updates (see the sidebar, Intel® vPro™ Technology – Better Security Through Enhanced Client Management). Of course, this requirement was also essential for security, since an unmanaged computing environment is inherently insecure. Specific required features included:
  - Policy management, key management, and escrow capability;
  - Monitoring to ensure and enforce compliance;
  - Detailed reports for auditing and managing compliance; and
  - Tools and methods for enforcing full disk encryption on non-compliant systems and for recovering data from encrypted notebooks. This had to include e-discovery capabilities, which require the ability to collect information remotely.

- **Minimal Impact on Notebook Users –** The solution had to be simple for notebook users in order to minimize disruption, training, and help desk requirements. The impact on notebook performance also had to be minimal. We did not want to irritate users or decrease their productivity.

- **Smooth Deployment –** The solution had to support automated deployment using Intel IT's existing notebook management infrastructure. It also had to provide tools for detecting and fixing deployment issues to avoid costly manual assistance for failed installations.

- **OS Compatibility –** The solution had to be fully compatible with all of the operating systems and operating system versions in Intel's notebook environment.

Evaluating Products and Vendors

Because notebook encryption would impact so many employees, Intel IT performed an extensive evaluation of possible solutions. The evaluation included:

- **Research –** The team began by reviewing analyst reports and third-party product reviews, as well as vendor information, such as Web sites, brochures, datasheets, and white papers. We explored approximately ten vendors, and narrowed the list to about five prospects based on product capabilities, as well as each vendor's experience and reputation.

- **Lab Tests –** We brought each of the top prospects into the lab for further evaluation. At this stage, we tested the applications with respect to the requirements we had already established, such as deployment, manageability, and ease-of-use. We performed interoperability tests with our employee productivity suites. We also performed performance benchmarking, which included measuring the impact on system boot, system shutdown, and transitions to and from hibernation. We evaluated vendor support during this phase. Were they helpful? Proactive? Did they communicate well?

  A key component of our laboratory evaluations involved extensive penetration testing by Intel security experts. Encrypted notebooks were aggressively attacked to find vulnerabilities. These efforts also included research to learn if any vulnerabilities, tools or attack strategies had been reported online.

- **Customer Interviews –** In any large-scale deployment, issues tend to arise that were not evident during lab tests, so we interviewed a number of large enterprise customers for each of the vendors we were evaluating. One goal was to get their perspectives on our short-list of products and vendors. Another was to learn about real-world pitfalls and best known methods (BKMs) for deployment. Most of these companies had automated their installations, though a few had taken a blended approach and allowed certain business groups to do manual pulls. We found that:
  - No data losses had occurred, though, in some cases, notebook data had to be recovered using vendor tools.
  - Organizations found it useful to run disk error scanning and defragmentation utilities on notebooks prior to deployment. Those who did not experienced a one to two percent failure rate. In the past, hitting a bad sector on a hard drive would crash the system. However, today's leading solutions automatically halt the install when bad sectors are found. Disk error scanning and defragmentation can then be performed on these systems before retrying the install.
  - Deployment timelines varied greatly, from as few as 6,000 notebooks in 18 months to as many as 15,000 notebooks in three months. However, this seemed to depend more on the company and internal IT issues than on the selected encryption product.
  - All organizations experienced an increase in help desk calls during initial deployment, but call volumes returned to normal within a few weeks.
  - No problems were reported with recovery and e-discovery tools and processes.

Laying the Foundation

To ensure a smooth deployment, training, resources and management infrastructure had to be in place before installation. This included tools and training for:

- **Operations –** Operations teams had to be prepared for the initial deployment, and also for updates, notebook recovery, e-discovery, monitoring, and auditing. Recovery and e-discovery are particularly sensitive processes. Since they may at times involve accessing encrypted notebooks without employee cooperation, checks and balances are needed to meet legal and corporate requirements while still protecting end user privacy. Intel already had a comprehensive authorization framework in place, and that framework was extended to cover notebook encryption issues. (As an example, authorization from appropriate legal, business, and technical managers are required for a notebook to be accessed without the end user's consent.)
- **Help Desk –** Dedicated support staff had to be available during the deployment phase to help employees download, install, and provision the software as needed, and to help with follow-up issues. Based on our research, help would be required primarily for creating and resetting passwords.
- **End Users –** Communications were sent to all notebook users prior to deployment. These communications explained the need for encryption and set expectations for deployment and use. In particular, users needed to understand new password requirements and be prepared for some performance slowdown during first-time disk encryption. Performance after that would be normal, except for relatively small increases in the time required for boot-up, shut-down, and transitions to and from hibernation. In addition to the communications, a Web site was provided on the Intel employee Intranet for general information.

Intel® vPro™ Technology

Better Security Through Enhanced Management

Securing employee notebooks requires more than data encryption. It also requires effective client management to maintain security-hardened configurations. To help us manage employee notebooks (and desktops) more effectively, and at significantly lower cost, Intel IT is currently in the middle of a multi-year process that will upgrade our client systems and support infrastructure to take advantage of Intel® vPro™ technology.

Client systems that support Intel vPro technology include built-in, hardware-based capabilities that help to improve security, maintenance and asset tracking. These PCs can be accessed over wired and wireless networks by authorized management applications and support staff, even when the system is off, the OS is unresponsive, software agents are disabled, or the hard drive has failed.

Studies have shown these and other Intel vPro capabilities can significantly reduce management costs in a typical IT environment. They can also help IT organizations:

- Automatically enforce approved configurations
- Automatically isolate client systems that are under attack by hackers or malware.
- Speed patch saturation across the client infrastructure.

For more information, visit the Intel vPro Technology Web page at: www.intel.com/technology/vpro/index.htm

Phased Deployment

Once the encryption product was selected, we began developing automated client installation packages to make the process as simple as possible.

We also created a download site, so notebook users would be able to download, install, and provision the software at their convenience. After a pre-defined window for employee-initiated downloads, we would enforce compliance by "pushing" the encryption software to any remaining unprotected notebooks.

Since we already had targeted encryption in place to protect the most critical data on employee notebooks, we decided to take plenty of time to thoroughly test our solution and processes through a series of small deployments. In each case, we documented technical and operational issues and developed appropriate fixes. We also coordinated these deployments with our planning process to optimize our infrastructure and training programs based on real-world results.

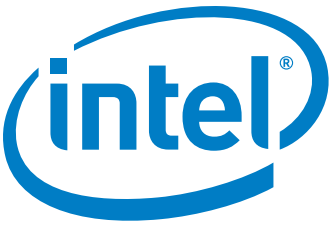
We defined the following phases of deployment:

- A Small Evaluation – Deployment to about 20 end users, all peers and colleagues of the encryption team.
- A Proof of Concept – Deployment to a larger test group of 100 ogy engineering and customer support groups. These individuals tend to be more computer-savvy than the average end user, and are generally more understanding and helpful in resolving issues.
- A Full Production Pilot – Deployment to 1,000 employees across a broad range of roles to simulate a full deployment, but with a smaller group of end users. The smaller group helps to ensure we can support all participants effectively, yet still uncover the kinds of issues that are likely to arise in an enterprise-wide rollout.
- The General Rollout – Implementation of encryption across all remaining employee notebooks.

The full production pilot is currently underway and running smoothly. Our early trial deployments confirmed that the main help desk issue involves providing notebook users with guidance for creating new passwords. Intel employees previously had two passwords for using their personal computers. One was a hard drive authentication password required to boot the system[10] and the other was an OS login password. We are retiring the hard drive passwords and replacing them with the notebook encryption passwords, so employees will continue to have two passwords.

However, in deploying the new encryption solution, we felt it was important to increase our password length and strength requirements. Though employees could continue to use their existing OS login passwords, many had to create a new password for the encryption solution to meet the new requirements. We therefore provided guidance via e-mail and the dedicated employee Web site, and prepared help desk personnel to assist with this issue. We also trained help desk personnel to use the vendor tools provided for remotely resetting encryption passwords.

10. At one time, hard drive passwords were considered a good addition to overall notebook security, but there are now several cracking tools available.



www.intel.com/IT

Moving Beyond the Current Solution

Encrypting notebooks is an important step forward in Intel's overall security solution.

We are also evaluating extending the use of disk- and device-level encryption across other computing and communications platforms. As more companies encrypt their notebooks, criminals can be expected to switch their focus to easier targets.

Attacks on smaller devices, such as cell phones and personal digital assistants (PDAs), are already increasing, and constant risk and technology assessment will be required to track value versus cost for extending full encryption across these other devices.

Conclusion

With new privacy laws and today's thriving black market for personal information, Intel IT determined that selective encryption of sensitive files was no longer sufficient to protect data on employee notebooks.

To mitigate the risks of personal information loss, we decided to implement full disk encryption as an additional layer of security on all notebooks. We believe the software-based solution we have chosen provides strong, comprehensive and cost-effective protection and complements our pre-existing security and management strategies.

Authors

Rex Rountree, Encryption Service Manager, Intel Information Technology

Carol Kasten, Data Protection Manager, Intel Information Technology

Michael Amirfathi, Engineering Information Protection and Encryption Services Manager, Intel Information Technology

Printed in USA
1208/REM/HBD/PDF

Please Recycle
320532-001US