Holding risk at bay

Hungarian system integrator WSH offers customers protection against laptop loss and theft with Symantec security software and Intel® Anti-Theft Technology

CHALLENGES

- **Insuring laptops.** System integrator WSH wanted to protect the security of its laptop fleet, which contains sensitive third-party data, against loss and theft
- **Introducing new services.** Based on its own experience of securing laptops, WSH also wanted to introduce a value-add client security service for its customers in order to increase revenue

SOLUTIONS

- **Safeguarding data.** Rolled out Symantec PGP* Whole Disk Encryption* (WDE*) and Remote Disable and Destroy* (RDD*) with Intel® Anti-Theft Technology[1] (Intel® AT) to its entire laptop fleet

IMPACT

- **Superior security.** WSH can now lock down lost or stolen laptops, disabling access to data even if the device is out of reach
- **Reaching customers.** Based on its own positive experience, WSH recommends laptops powered by 2nd generation Intel® Core™ processors with Intel AT, together with Symantec PGP WDE and RDD, to customers
- **Increasing revenue.** Ability to offer complementary 24/7 remote monitoring and management services to customers strengthens WSH's portfolio and increases revenue

"Symantec PGP WDE and RDD with Intel Anti-Theft Technology runs in the background, protecting the laptop without interfering with the user experience, offering both software and hardware security protection without noticeably slowing down the device."

Róbert Sali,
Head of System Integration, WSH

Rising security risks

Laptop loss and theft are on the rise. According to the Hungarian National Police Headquarters, 3,376 laptops were lost or stolen in Hungary in 2011[2]. The estimated value of these laptops was HUF 1.05 billion (GBP 2.9 million), while the associated security risks for corporations and mobile workers were immeasurable. More than ever before, enterprises need a reliable way to deter laptop theft and, if theft or loss does occur, the means to disable access to or destroy the stolen data even if the machine is out of reach.

As Symantec's largest solution supplier in Hungary, system integrator WSH Számítástechnikai, Oktató és Szolgáltató Kft. (WSH) was eager to protect the security of its own laptop fleet, especially against loss and theft. To this end, it was one of the first organizations in Hungary to use Intel and Symantec's jointly-developed security solution – PGP WDE and RDD with Intel AT – to secure laptops.

Based on its own positive experience using this solution, WSH decided to recommend laptops powered by 2nd generation Intel Core processors with Intel AT, together with Symantec PGP WDE and RDD, to customers. By doing so, it would be able to introduce a new revenue stream, helping it to improve competitiveness.

Laptop lockdown

Intel AT is available on select 2nd generation Intel Core and Core vPro™ processor family-based laptops when activated with a subscription from an Intel AT-enabled service such as Symantec PGP WDE and RDD.

Symantec PGP WDE and RDD with Intel AT helps businesses minimize the risk of data breaches by giving IT the ability to trigger a full system lockdown and seal critical cryptographic materials. At the simplest level, it deters would-be thieves by displaying the Intel AT and PGP WDE logo.

Full system lockdown helps businesses minimize risk of data breaches

At the heart of the solution is a protected area, physically embedded in each Intel Core processor equipped with Intel AT, where Symantec encryption algorithms can run securely, providing resistance against tampering. Since these security mechanisms are embedded in the hardware, data is protected even if the thief applies extreme measures such as reimaging the operating system, changing the boot order, installing a new hard drive, booting from an alternative device, or breaking connections with the network.

For example, if a thief removes the hard disk and tries to access it from another computer, the data is encrypted and the information is locked. The only way to access this information is to call the help desk and retrieve a one-time token.

In addition, 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 PGP Universal Server. The PGP Universal Server provides a central management platform for activating, configuring policies, and monitoring systems protected by PGP WDE with RDD.

Alternatively, if a user calls IT to report a stolen laptop, an administrator can flag the laptop on the PGP Universal Server as stolen. The laptop then receives a poison pill sent by IT and immediately goes into a special "stolen" mode. The laptop also sends an acknowledgment to the server that the poison pill was received. This is important for organizations exempt from data-breach notification regulations that contain an encryption safe harbor.

If and when a laptop is recovered, reactivation is straightforward: PGP WDE includes support for IT-managed pass-phrase recovery (using a recovery token). PGP WDE also includes support for Intel® Active Management Technology (Intel® AMT)[3], which enables remote access to systems encrypted with PGP WDE.

Like an anti-virus application, Symantec PGP WDE and RDD with Intel AT runs in the background, protecting the laptop without interfering with the user experience, offering both software and hardware security protection without noticeably slowing down the device. In addition to 2nd generation Intel Core and Core vPro processor family-based laptops, Intel AT will also be available on all of Intel's 2nd generation Ultrabook™ devices.

Why WSH?

WSH offers customers planning and 24/7 remote monitoring and management services which complement Symantec PGP WDE and RDD with Intel AT. Its long-standing relationship with Intel means that it has the know-how to advise customers on best practices in deploying and managing Intel AT.

"We offer a lot of training sessions for IT managers at our education centers. Here, using our demonstration suite, we show them what Symantec PGP WDE and RDD with Intel AT is capable of," said Róbert Sali, head of system integration at WSH. "IT managers are able to try out the technology first hand, remotely locking down and reactivating devices in real-life scenarios.

"If they like what they see," Sali continued, "then we can sell them a new laptop fleet powered by 2nd generation Intel Core vPro processors with Intel AT, together with Symantec WDE and RDD. Alternatively, if they already have laptops powered by Intel Core vPro processors with Intel AT we are able to help activate the anti-theft component for them. Whatever the customer's need, we'll find a solution.

"Protecting data is significant for small businesses and sole traders as well as large corporations," Sali said. "Physicians and lawyers, for example, use laptops on a daily basis. If they were to lose their laptops or if they were to get stolen, sensitive data may get into the wrong hands, causing them huge problems. Many of these businesses do not have their own dedicated IT departments to offer them assistance, and this is where we can really add value by offering them a round-the-clock managed service for a fixed monthly or annual fee."

WSH is able to manage all client devices from the central management console, regardless of whether they are connected to the corporate network or not. It can monitor the location of the equipment with the help of Web-based mapping services using GPS or Wi-Fi. Any confidential data can be remotely deleted and an audit log file created to comply with government and corporate requirements relating to data protection.

Finally, WSH customers can also take advantage of the wider remote management capabilities of Intel® vPro™ technology[4], either managed in-house by their own IT department or as part of a managed service offered by WSH. In many cases, the IT manager is able to remotely diagnose and resolve IT problems, eliminating the need for costly and time-consuming desk-side visits.

Spotlight on WSH

WSH Számítástechnikai, Oktató és Szolgáltató Kft. has had a presence in the Hungarian IT market segment since 1995. Wholly Hungarian owned, its primary business lies in organizing professional IT training, providing IT consultancy and support and advice around IT security, as well as systems integration. For further information, visit: www.wsh.hu

Visit Intel's Technology Provider website at **www.inteltechnologyprovider.com**

Find the solution that's right for your organization. Contact your Intel representative, visit Intel's Business Success Stories for IT Managers (**www.intel.co.uk/Itcasestudies**) or explore the Intel.com IT Center (**www.intel.com/itcenter**).

[1] **Intel® Anti-Theft Technology** No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware, and software, and a subscription with a capable service provider. Consult your system manufacturer and service provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft.

[2] Source: http://www.lopottlaptop.hu/index.php

[3] **Intel® Active Management Technology** Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit http://www.intel.com/technology/platform-technology/intel-amt.

[4] **Intel® vPro™ technology** Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit http://www.intel.com/technology/vpro.

0412/JNW/RLC/XX/PDF 327292-001EN