



## PGP Corporation and Intel collaborate on laptop anti-theft technology

12 May 2009

Data security company **PGP Corporation** and Intel Corporation are partnering to provide Intel anti-theft technology (Intel AT-p) in PGP's whole-disk encryption systems. It will provide combined asset and data protection as well as help with notebook theft deterrence.

Intel anti-theft technology, which is available in many of the latest notebooks with Intel Centrino 2 with Intel vPro technology, is a hardware-based asset protection and theft deterrence system that protects notebooks through disable options via a 'poison pill' when theft or loss is determined by local detection mechanisms or remote server notification.

The combined solution will offer business customers options to block access to sensitive data that is secured by PGP data encryption solutions.

“Time after time, we’ve seen that data breaches due to lost or stolen notebooks can have a detrimental impact to a public or private organization — protecting data and personal information has never been more critical,” said Steven Schoenfeld, vice president Products and Strategy, PGP Corporation.

“The collaboration with PGP Corporation on asset and data protection solutions helps to define a new security paradigm for organizations of all sizes to help deter theft of costly hardware and protect the often more valuable data inside,” said George Thangadurai, director, Strategic Planning, and general manager, Anti-Theft Program, Intel Mobile Platforms Group.

According to the recently released 2008 Ponemon *Cost of a Data Breach Studies*, compromised customer records in the US costs a company \$202 per record, £60 in the UK and €12 in Germany. Without proper asset and data protection practices, these breaches can cause significant damage to a company’s brand and finances.

PGP Corporation will integrate with the local and remote theft detection mechanisms provided by anti-theft technology and provide recovery options. When a notebook is lost or stolen and the theft condition is asserted, the system will disable the notebook and block access to encrypted data even if the user’s credentials have been compromised.

Once the notebook has been recovered and the theft condition is cleared, the hardware can easily be re-activated locally using a pre-provisioned user pass-phrase or a remote server-assisted one-time use recovery token. Since the data on the recovered notebook is not deleted and the

protection is non-destructive, the data can be securely retrieved upon routine pre-boot authentication.