Better Encryption to
Better Protect Our Country

Fighting Data Breaches that Threaten National and Homeland Security

To succeed at their missions, federal military, intelligence and homeland security organizations and their allies and partners require real-time, actionable information in the field. Enterprise applications and mobile technologies, especially laptops, are essential tools for this task and help advance operational capabilities. Unfortunately, storing an ever-growing amount of sensitive national and homeland security data on mobile devices also increases the risk of accidental and intentional data loss.

The Advanced Persistent Threat (APT), cybercrime and even independent organizations are to blame for the many breach attempts against national and homeland security agencies. When breaches are successful — such as the April 2009 theft of terabytes of data on the Pentagon's $300-billion Joint Strike Fighter or WikiLeaks' multiple 2010 releases of classified U.S. military and diplomatic information — they can put mission success, or even lives, at risk.

Not surprisingly, national and homeland security organizations view protecting laptop data from unauthorized access as a critical responsibility. While encryption and encryption key management are used throughout government to protect critical data, they also pose challenges. How can national and homeland security organizations implement enterprise-wide encryption that is totally secure, easy-to-deploy, use and maintain and won't hinder field operations?

Four key related challenges are listed at the right:

Key Data Breach Mitigation Challenges

IT Security

The U.S. Departments of Defense (DoD) and Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) have mandated IT security regulations and standards for national and homeland security organizations and their partners. These organizations must implement policies and equipment that protect critical assets from cyber attacks launched by either outside or inside threats.

Information Sharing

U.S. government must securely share sensitive national and homeland security information with partners at the State and local levels. International operations require U.S. warfighters to securely share battlefield data with non-traditional and often-shifting allied, coalition and other partner operations. This broadening collaboration requires the means to ensure only authorized access to data and automatic enforcement of security policies.

Fast, Hassle-Free Use

Burdensome handling requirements for equipment handling classified information can impede needed real-time collaboration, while long certification times can keep improved products from reaching the field. The equipment must ensure that both front-line and support personnel can do their jobs without the technology, or rules for handling it, getting in the way.

Logistics

Laptops that carry classified information require COMSEC Controlled Items (CCI) handling procedures to prevent data from falling into the wrong hands. Unfortunately, the restrictive CCI rules can impede real-time collaboration that is essential for field operations. Additionally, national and homeland security organizations need enterprise-wide protection that is proven, meets government standards, works across platforms and has known acquisition and operational costs.

Self-Encrypting Drives and Wave's EMBASSY® Software Protect National and Homeland Security Data

Options abound for protecting sensitive data but many experts consider full-disk encryption (FDE) the best because it encrypts everything on a hard drive, eliminating many vulnerabilities that attackers can exploit to gain unauthorized access to data. Unfortunately, software-based FDE, the most common form of FDE, has exploitable weaknesses — which means it can't guarantee that lost data is unreadable. This fact leaves national and homeland security agencies at continued risk for catastrophic breaches.

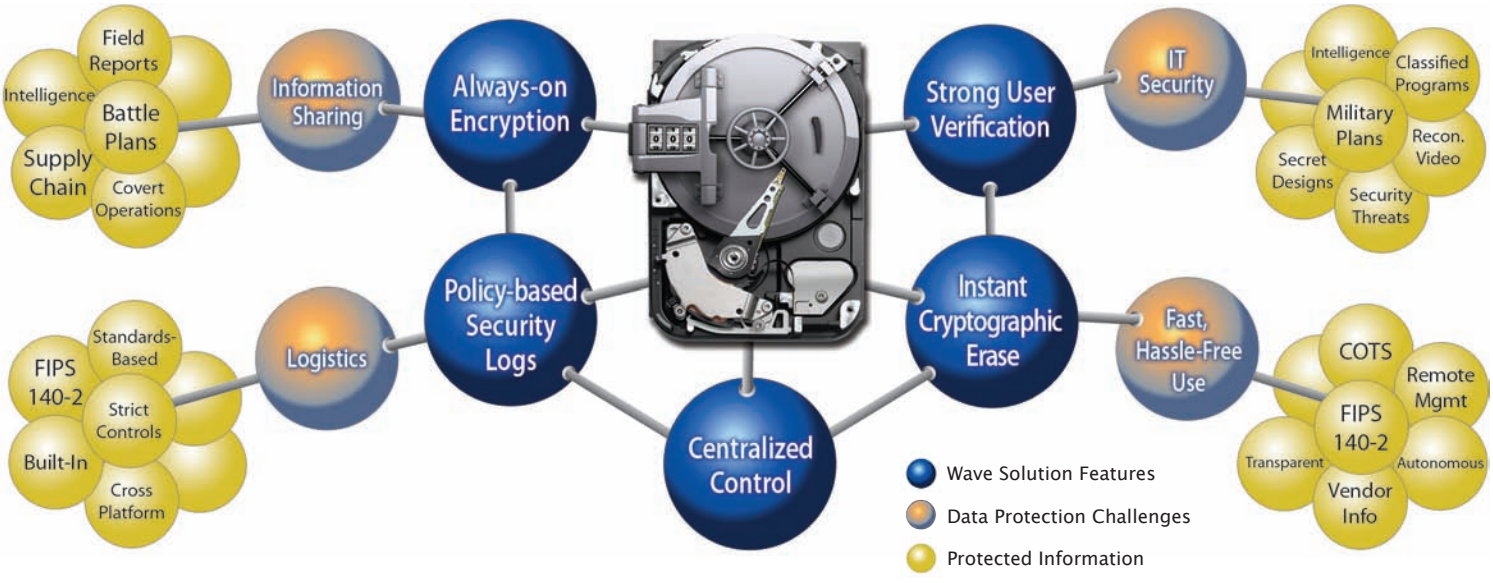
To overcome these hurdles and keep our nation's secrets safe, more organizations are turning to self-encrypting drives (SEDs). SEDs offer an alternative hardware-based FDE approach — making them more secure and less expensive to implement and maintain. SEDs house all encryption processes and keys in a protected hardware boundary impervious to software attacks. Further, they cost only marginally more than non-encrypted hard drives, require minimal IT overhead and are transparent to end users.

Wave Systems, a pioneer in hardware-based laptop security, has partnered with leading hard drive manufacturers Hitachi, Samsung and Seagate to provide enterprise security management for their SEDs. Wave's EMBASSY software transforms these self-encrypting drives into a complete managed enterprise encryption solution: one that centrally provisions security policies, limits access to only authorized users and — perhaps most importantly — provides foolproof assurance that sensitive information stored on an SED remains safe.

Through its partnerships with Seagate, NCI Information Systems, Inc. and other trusted government IT providers, Wave serves a growing number of customers in the U.S. Departments of Defense and Transportation and the General Services Administration. In fact, Wave's software has been installed on more than 70 million PCs worldwide.

Most importantly, Wave is the leading ISV for managing the security of Seagate Momentus Self-Encrypting Drives, the first SEDs to be certified under the NIST Federal Information Processing Standard 140-2 (FIPS 140-2). The certification means that these drives meet data protection standards that all U.S. and Canadian federal, state and local government agencies and regulated industries, such as defense, healthcare and finance must use to protect sensitive information on their computers and networks.

Because military, intelligence and homeland security organizations often have IT infrastructure that mixes new and existing technology, Wave understands the need to protect information on PCs that do not have self-encrypting hard drives. For those agencies that are adopting Windows 7, Wave software provides a comprehensive set of tools to automate and secure the configuration and administration of Microsoft BitLocker drive encryption. So whether you have decided to use the latest in hardware-based encryption, or the latest integrated OS FDE application, we've got you covered.



03-000286/ version 1.01

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com

wave®
Simplifying Encryption and Authentication