[STRATEGIC SECURITY]

Full Disk Encryption Evolves

Opal standard paves the way for self-encrypting hard drives

Earlier this month, the Naval Hospital in Pensacola, Fla., began notifying thousands of individuals that personally identifiable information about them had been lost when a laptop disappeared. In August, the National Guard announced that a laptop containing personal information on 131,000 members had been stolen. We could go on—rarely does a month go by without an organization revealing the loss or theft of a laptop brimming with sensitive data.

Full disk encryption, or FDE, is the preferred mechanism to address this threat because, as the name implies, the technology lets IT encrypt the entire hard drive so that sensitive data is protected, no matter where it resides. But unfortunately, FDE adoption comes at a price: complex and costly deployments, additional licensing fees, and one more application for IT to support.

HOW SOFTWARE AND HARDWARE APPROACHES COMPARE

	Pros	Cons
Software	> Widely deployed > Flexible encryption options > Strong management options	> May not support all systems > Costly > Potential performance impact > Susceptible to cold boot attack
Hardware (Opal)	> OS agnostic > Great performance > Inexpensive > Immune to cold boot attack	> Requires new laptop > Most only supports 128-bit AES > Limited management options

Now, adoption of a new standard for hardware-based FDE, called Opal, aims to alleviate some of that pain.

The Need For FDE

No organization can plead ignorance of encryption options. Microsoft Windows, Mac OS X, and Linux all have built-in support for file-system-level encryption.

But while encrypting a file system, or providing an encrypted folder on an employee's laptop, is better than nothing, it still leaves too much to chance. Did the employee put *all* sensitive data into that target folder? Was anything left in caches or temporary directories? And perhaps most critical, without FDE, if a device is stolen or lost, how do you definitively know that all of the sensitive information it contained was encrypted?

Short answer: You don't.

Vendors including Check Point Software (via its PointSec acquisition), Guardian Edge, McAfee (via its Safeboot acquisition), and PGP offer software-based FDE suites that can help you avoid all these problems. With software-based FDE products, the data on the drive can only be accessed when the operating system is booted and the encryption keys unlocked. But the technology isn't perfect—software-based FDE also has drawbacks. First, a number of software FDE products don't support Linux or Mac OS X. Second, depending on the age and processing power of the laptop, the encryption process can slow down a machine.

Finally, encryption keys are stored in the computer's memory, which makes them vulnerable to a class of so-called "cold boot" attacks, in which encryption keys are recovered in RAM.

Enter Opal

In January 2009, the Trusted Computing Group released the final specification of the Opal Security Subsystem Class, a standard for applying hardware-based encryption.

Moving hard-drive encryption into

At A Glance SELECTED FULL DISK ENCRYPTION PLAYERS

Opal hard-drive manufacturers: Fujitsu, Hitachi, Samsung, Seagate Technology

Opal management software vendor: Wave Technology

Laptop vendors shipping Opal drives: Dell, Lenovo

Software-based FDE vendors: Check Point Software, Guardian Edge, McAfee, Microsoft, PGP

hardware has a number of advantages. For starters, it works with any OS. It also moves the computational overhead of the encryption process to dedicated processors, alleviating any computing load on the system's CPU.

In addition, the encryption/decryption keys are stored in the hard-drive controller and never sit in the system's memory, making "cold boot" attacks ineffective.

Hardware-based FDE also simplifies the key escrow dilemma—that is, the need to manage encryption keys. Simply put, the keys used by the hard drive can be unlocked only by a passphrase entered during the pre-boot sequence. The passphrase is sent to the hard drive controller *before* the OS boots, so the keys never leave the hard drive's hardware. Also, multiple passphrases can be configured to unlock those keys.

Note that software-based FDE products do allow you to choose the encryption algorithm and variable key strengths, while most Opal drives are limited to AES-128. We see this as being an issue only for organizations that require specific algorithms or larger key sizes.

Management's A Must

Consider yourself warned: Without an integrated management infrastructure, enterprise deployment and support of Opal-compliant hard drives will be a nightmare. There are a few key features that are essential. For starters, organizations must manage boot passwords and password resets. If an employee leaves, becomes unavailable, or just forgets the password, IT needs a way to access the data on the drive. Conversely, if an IT administrator leaves, the organization must be able to change admin accounts.

Another necessary function is the ability to report on the state of a given laptop or asset. If a device goes missing, can you demonstrate beyond a reasonable doubt that the drive was indeed protected via encryption? This capability will have a major impact on compliance with state breach disclosure laws and limit the fallout from potential data loss.

These use cases require a centralized management platform that can communicate with endpoints. We're aware of only one vendor—Wave Technology—that's shipping a management platform to tie all of this together. Wave uses a "pre-boot" operating system to set up admin and user accounts for unlocking the hard drive's encryption keys before the OS boots, and also has a Windows agent that can sync these accounts with Active Directory.

So will software-based FDE products go the way of the dodo? Not likely—organizations with global software FDE deployments aren't about to rip them out. It also will take time for companies to swap in laptops with Opal-compatible drives. Software FDE vendors certainly don't project a sense of urgency, either. McAfee and Check Point say they see the need for managing hardware- and software-based FDE. But neither has announced timelines for Opal support.

In contrast, on the manufacturing side, vendor support for hardware-based FDEs is good. In the last six months, Fujitsu, Hitachi, and Samsung have debuted Opal-compliant drives, and system vendors Dell and Lenovo are shipping laptops with Opal-based drives. In fact, the hardware-based approach is going to come faster than some FDE vendors are envisioning. The technology will find a warm reception among organizations struggling with their FDE strategies, because the advantages are too compelling to ignore.

Greg Shipley (gshipley@neohapsis) is CTO of Neohapsis, an information security and risk management firm.