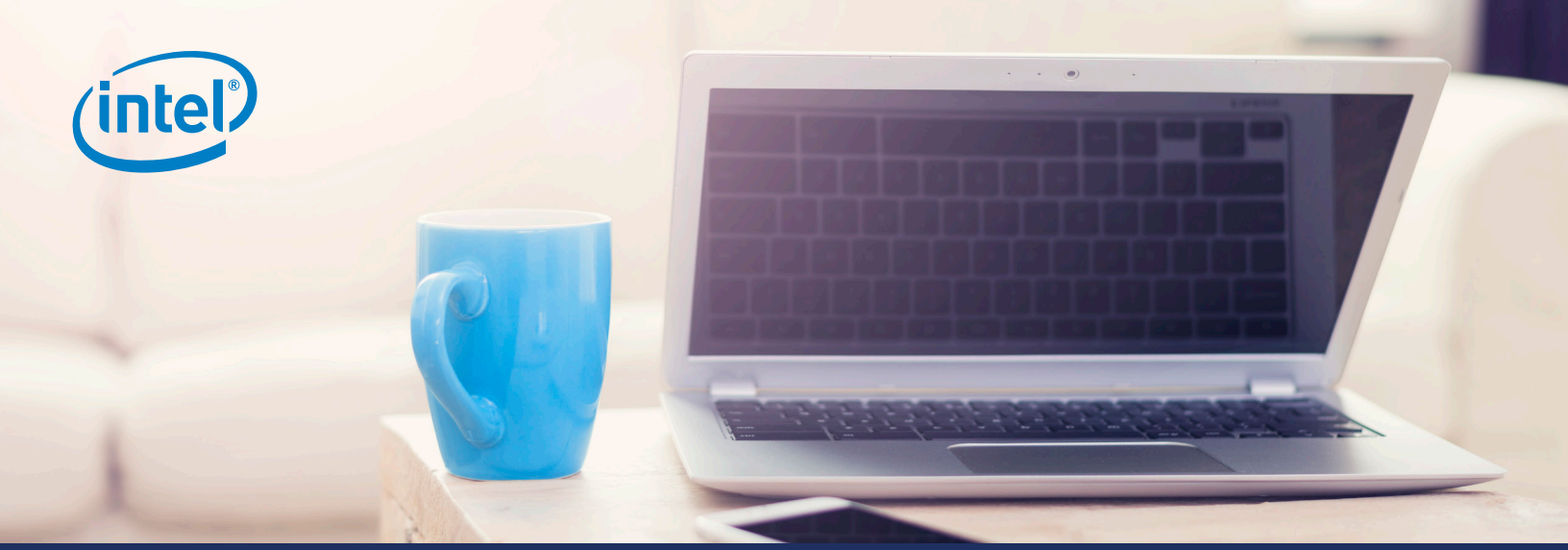

WinMagic® Protects Data Beyond the Digital Fence

SecureDoc™ Automates Safe Hibernation

Security planners at least have a fighting chance to secure data when laptops and mobile devices are onsite and within range of the WiFi network. But once those devices venture out, companies cannot rely on end users to always put their device in a state in which security-sensitive variables are cleared from memory.

Combining hardware and software security into one solution is a good answer for protecting data at rest and data in motion. A prime example is WinMagic® SecureDoc™, an industry-validated, encryption-and-key management solution that secures data at rest, regardless of where it is stored. SecureDoc is well-trusted and used by more than five million clients in over 84 countries. Headquartered in Mississauga, Canada (near Toronto), WinMagic was formed in 1998 and now has 150 employees, with offices in Japan, Germany, the United Kingdom, the United States of America, India, and Tokyo. Some of the largest healthcare, finance, education, retail, manufacturing, and government organizations worldwide rely on SecureDoc.

Using the Intel® Enterprise Digital Fence application, SecureDoc provides enhanced protection so that when a device travels beyond a defined safe area, the software wakes up and secures itself by entering a mode where the keys or credentials are not vulnerable to attack. This combination is a big step, according to Garry L. McCracken, vice president of technology for WinMagic Inc. With more than 30 years of experience in data communications and information security, McCracken has been responsible for the development of full-disk encryption solutions for desktops, laptops, and other mobile devices.

One challenge in providing a secure solution is to provide sufficient security to please IT managers while still allowing ease-of-use that doesn't frustrate users. "When you close the laptop lid and put your computer to sleep, it might take less than a minute to boot it back up when you need it again," McCracken said. "Coming quickly out of sleep mode is a feature that many enterprise and corporate users demand. However, a problem with the sleep feature is that credentials and other important information often remains in the device's memory. And if that device were to be lost or stolen while in sleep mode, it's more vulnerable than typical corporate security policies allow."

If the device is SecureDoc enabled and determines that it left sleep mode in a strange location, it can initiate defenses. With Intel® Smart Connect Technology[1], the device is periodically wakened from sleep to see if it is still connected to a safe network.

With the Intel Enterprise Digital Fence Technology Plugin, the concept of a trusted LAN is introduced, allowing the SSID of the LAN to be configured as "trustworthy." If the computer wakes up on a trusted LAN, it will update its apps with current data and then resume sleeping. But if the computer wakes up in a bicycle basket across town where no trusted LAN is available, hibernation is forced, and waking the computer requires a password.

To continually provide industry-leading security solutions, WinMagic stays directly tied into advances in industry standards, tracks roadmaps at leading technology companies such as Intel, and works with its PC OEM partners such as Lenovo and Hewlett-Packard. WinMagic worked with Intel well in advance of the first shipment of Intel® Core™ vPro™ processor-based devices to ensure the SecureDoc software worked well on those platforms, especially with the Intel® SSD Professional Family of Opal* solid state drives (SSDs).

Designed for remote manageability, Opal SSDs allow the IT administrator to initialize the drive for activation and to set passwords ensuring only authorized users have access. WinMagic was deeply involved with the development of Opal framework, the Trusted Computing Group's (TCG) industry standard, and is a contributor-level member of the TCG. An international industry-standards group, the TCG develops specifications for self-encrypting drives (SEDs).

There's always more work to do—McCracken points to future storage technology as a key focus. "Currently, the common way to connect SSDs to your laptop is via a SATA—serial ATA bus. That SATA connection is just not fast enough anymore and has become the bottleneck in the performance of your computer. The answer to that is NVMe (Non-Volatile Memory PCI Express), which is a different memory model that links directly to the CPU. NVMe is a newer and faster way to attach directly into the memory. And, although it's much faster, it will have security challenges. Our customers will want us to update for that new standard."

Contact WinMagic for more information about their SecureDoc solution at **winmagic.com/products**.

Additional Resources

Trusted Computing Group: **trustedcomputinggroup.org**

WinMagic* Sleep-and-pba: **winmagic.com/blog/2014/09/17/sleep-and-pba/**

Intel® SSD technology: **intel.com/content/www/us/en/solid-state-drives/professional-family.html**

WINMAGIC®
DATA SECURITY

[1] Intel® Smart Connect Technology requires a select Intel® processor, Intel® software and BIOS update, Intel® Wireless adapter, and Internet connectivity. Solid-state memory or drive equivalent may be required. Depending on system configuration, your results may vary. Contact your system manufacturer for more information.

 0915/RH+M3 333149-001US