Maximize Security, Lock Down Hard Drive Firmware with Seagate Secure® Download & Diagnostics

Technology Paper

Visit with an elderly relative for any length of time and you'll eventually be treated to stories about how life was "in the old days." A recollection they might share would be how people always left their homes unlocked, or even left their car key in the ignition! Of course, times have changed and such lax attitudes toward security now seem quaint and utterly unthinkable in today's world.

The time is soon approaching when unsecured hard drives (HDD) will be similarly viewed with a similar mix of nostalgia and head-shaking disbelief. Every day seems to bring a new report of data security breaches in the corporate and government sectors, while individuals are frequently under siege by increasingly sophisticated (and persistent) viruses, malware and other security exploits. Simply put, the current threat environment holds an unprecedented quantity and variety of security risks. Yet the vast majority of hard drives (HDD) on the market seem mired in the past, offering very minimal, if any, security.

Recognizing this deficiency, Seagate is raising the bar for hardware-based drive security with Secure Download & Diagnostics (SD&D)—a standard feature on every HDD. SD&D prevents unauthorized access to a drive's firmware and blocks tampering with firmware executables and sensitive system-level data.

Why Firmware Security is Crucial

Given the enormous number of data security threats that now exist and the corresponding plethora of software solutions that seek to combat them, it is not surprising that an HDD's firmware—which is impossible for antivirus programs to scan—is often overlooked. But it is precisely because the HDD firmware is seemingly *under the radar* that makes it so attractive to cybercriminals.

In recent months, news reports have often featured alarming stories on malware that seeks to attack firmware in a wide variety of computer devices: hard drives, USB sticks, keyboards, web cameras, graphics and sound cards—essentially anything that contains firmware (even computer batteries). Because of the difficulty in detecting antivirus applications, rogue firmware has the potential to become a significant threat when used to execute malicious software in IT environments.

The consequences of infected, rogue firmware can be devastating. Costs associated with a data breach resulting from unauthorized access to user data might easily reach millions of dollars, along with the potential negative publicity and resulting damage to an organization's reputation and market share.

Maximize Security, Lock Down Hard Drive Firmware with Seagate Secure® Download & Diagnostics

How the Internet of Things Potentially Expands Threat

While the benefits of today's interconnected world are overwhelming, there are also significant downsides to having literally billions of devices—with susceptible firmware—linked together. The Internet of Things (IoT) magnifies the impact of security threats by potentially giving them the ability to rapidly spread from a single infected device to millions in a matter of hours. Clearly, the interconnectedness of the IoT is one of its greatest strengths but also a significant vulnerability.

The IoT makes it extremely difficult to avoid potential sources of infection by simply preventing contact with suspect devices. It is virtually impossible to know the history/audit trail of contacts for every device that an organization or individual encounters, and thus impossible to know how many degrees of separation might link a known and trusted device to an infected one.

The Seagate Solution

Building on a distinguished and successful history of innovation and product development, Seagate is a leader within the storage industry. Using a comprehensive approach to help ensure firmware security and integrity, Seagate has developed the following security technologies that protect the firmware in its drives whether they're installed in a host computer (*Secure Boot*) or removed from the system (*Locked Diagnostics Port*):

- Cryptographic firmware signing: Uses encrypted signature in firmware that is required for the host computer to launch (via Secure Boot) and to enable firmware downloads (via *Locked Diagnostics Port and Firmware Authenticity* and *Integrity Verification*).
- Secure Boot: Prevents host computer's OS from loading if the firmware's encrypted signature has been changed in any way; firmware signature is authenticated by the drive at host computer startup.
- Locked diagnostics port: Blocks unauthorized users from downloading firmware or accessing the drive's installed firmware; user authentication via Seagate® Secure Server required to unlock port. Prevents tampering with firmware executables and system-level data.
- Firmware authenticity and integrity verification: Checks for encrypted signature in firmware that is being attempted to be downloaded; firmware is rejected if not authenticated as an original Seagate firmware download.

Should malicious code be executed inside an authentic copy of an HDD's firmware, SD&D's tamper-evident binary feature enables any altered code to be identified and the firmware blocked from download. Furthermore, SD&D employs forensic logging to trace unauthorized attempts to load or manipulate firmware.

The net result is that SD&D prevents unauthorized access to the drive and thwarts attempts to tamper with the firmware, while still allowing authorized service personnel to access the firmware for diagnostic testing, perform field upgrades and conduct other service procedures.

Advanced Security, Data Protection Vital to Cloud

Security is perhaps the single greatest requirement of a cloud storage solution; users place enormous trust in the cloud provider to ensure their files are secure and any personally identifiable information (PII) in those files remains private. As such, advanced security and data protection capabilities are not merely desirable but absolutely compulsory in any cloud system or solution. SD&D provides an extremely effective tool to protect hard drive firmware from security threats, and does so at no additional cost to the cloud provider.

SD&D Leverages Legacy of Protection

Over ten years ago, Seagate pioneered development of Self-Encrypting Drive (SED) technology, the foundation upon which SD&D is built. SEDs provide instant secure erase functionality and enable always-on, data-at-rest security by encrypting all data and requiring password access after a drive has been powered off or removed from its host. An optional feature first available on laptop drives and later on desktop and enterprise models, SED technology represents a significant leap forward in data security.

Maximize Security, Lock Down Hard Drive Firmware with Seagate Secure® Download & Diagnostics

Conclusion

As the sheer number and types of threats in today's digital landscape continue to escalate, the need to secure all entry points from malicious attacks becomes increasingly clear. Hard drive firmware is a tempting target for attackers, offering them an often-overlooked way to breach a network's security barriers. Seagate is stepping up to this challenge by incorporating firmware protection elements from its industry-leading Seagate Secure SED technology into every drive it sells.

Offered as a standard, no-extra-cost feature on all hard drives in the Seagate portfolio, Seagate Secure Download & Diagnostics delivers a comprehensive, transparent means for organizations and individuals to protect their data from firmware-based security attacks.

seagate.com

AMERICAS Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, 408-658-1000
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00