A MICRON WHITE PAPER

Keep Your Data Secure: Fighting Back With Flash

Overview

Protecting data at rest is a critical concern for enterprises of any size. As more corporations have deployed mobile and portable computing (laptops, tablets, etc.), the definition of a data storage endpoint has long since gone beyond a traditional desktop. These new computing platforms — including cloud — provide tremendous flexibility and productivity for the modern knowledge worker, but put critical and sensitive data beyond the physical security measures that an IT department can implement. The advent of cloud computing alone has resulted in huge amounts of personal, private or company-confidential data being stored in data centers all over the world.

ENCRYPTION FOR DATA AT REST

- Encryption is critical to secure data from the notebook to the data center.
- The Trusted Computing Group (TCG) standards provide a reliable framework for security.
- Encryption and flash provide fast and economical methods to destroy data when devices are decommissioned.
- Hardware encryption with self-encrypting drives (SEDs) frees up IT resources.
- Micron provides verifiable security features, including FIPS 140-2 Validated SEDs.

The need for additional security measures for mobile devices is obvious, but security is becoming increasingly important for ALL sections of an enterprise, from mobile platforms to desktops and workstations — even to storage devices in the data center.

Traditionally, storage devices in the data center such as hard disk drives (HDDs) and solid state drives (SSDs) have not been considered to be removable. Indeed, data center managers typically implement physical security features and procedures to protect servers and storage arrays from intrusions that could compromise storage devices and the sensitive data stored on them. However, the technology advances that have enabled mobile computing with smaller devices have now come to the data center, presenting the IT manager with a multitude of small, removable devices that pose new security issues as drives can be removed from the data center undetected.

Increased drive portability means drives are moved in and out of facilities more frequently. In addition to the rare incident of a theft or loss, storage devices are legitimately removed from the security of the data center at a rate of tens of thousands every day during the normal process of system maintenance and device decommission. Sensitive stored data can be compromised at this point, too, so additional security measures are required.

Because of these security risks, corporations around the world are tightening policies regarding data security, and many sectors are facing increasing regulation and legal requirements to implement and maintain verifiable data-at-rest security measures. The most obvious ones are the finance and health care sectors, as well as retail sales. All of these industries collect, manage and protect data regarding their customers' identities and financial information. Governments around the world are requiring that companies provide verifiable data protection through encryption. Today's self-encrypting drives (SEDs) can provide that by following industry-accepted standards for encrypted storage.

Data Encryption: Ensuring Peace of Mind

Today's corporate workforce has transitioned from one stuck at the desktop to a highly flexible, mobile workforce, relying on computers and storage devices that are smaller and more portable, but also more vulnerable to loss or theft. This shift means that IT departments must broaden the defense of sensitive data well beyond the data center. Firewalls, virtual private networks, and virus and malware protection all remain key components of an overall security strategy, but SEDs can provide the last line of defense for sensitive data stored at the endpoints. Solid state SEDs can deliver this last layer of security with unprecedented performance.

One of the key features of SEDs is a hardware-based encryption engine, built into the drive's controller. Advanced Encryption Standard (AES) 256-bit encryption is the gold standard for keeping sensitive corporate data locked down and secure. With this feature, an SED can automatically encrypt and decrypt all user and operating system data immediately and seamlessly, at the full bandwidth allowed by the interface.

The next step in SED implementation is to combine this state-of-the-art encryption with strong authentication. The most familiar form of authentication is a password. However, any number of authentication methods are available, from smart cards to iris scanners and fingerprint readers. These methods ensure that only authorized personnel have access to sensitive data.

Although the encryption function can reside in hardware on the SED, this authentication process is managed by software on the host computer. A common way to do this is via a password set in the computer's BIOS (basic input/output system). This password then acts as the key that unlocks access to the data stored on the drive. This solution is perfectly adequate for a single system, or perhaps a small business that manages only a handful of computers.

However, more advanced solutions are necessary for enterprises. Fortunately, there are software solutions available that can manage authentication and access to SEDs. The SED and the associated software provide a function known as pre-boot authentication (PBA). A PBA system creates a boot record that is opened prior to starting the operating system. The authentication process can then run in an environment that assures no operating system application is running.

Another advantage of PBA is that, unlike in some BIOS solutions, all the system hardware is up and operating. The PBA can take advantage of Internet connectivity, doubly securing the computer. If a

system is known to be out of the owner's control, the IT manager can scan the Internet for the rogue computer, and upon first access, can lock down the computer permanently so that any unauthorized user cannot access sensitive data.

These software solutions are available through independent software vendors (ISV) who work very closely with drive manufacturers to ensure compatibility between the SED and the management software.

The SED manufacturers and the ISVs ensure compatibility by conforming to storage security standards created and managed by the Trusted Computing Group (TCG). The mission of the TCG is to enhance the security of the computing environment in disparate computer platforms. The concept of trusted systems has been around for years. In trusted systems, computers, software, and peripherals will behave in defined and expected ways. The behavior is enforced by protocol, controlled by an encryption key, and inaccessible to the host system or the user.

The TCG maintains protocols that cover encryption and data protection across the full spectrum of computing environments, from endpoint and data processing to data transmission. However, the pertinent protocols specifically for data storage are the following security subsystem classes (SSC):

- **TCG SSC Opal**: This standard applies to mobile computing platforms like laptops and tablets and increasingly to desktop computing. It effectively secures data at rest for powered-off, authentication-locked devices. The Opal protocol provides for pre-boot authentication, which enables authentication before the operating system boots, preventing any OS-level application from detecting or intercepting the authentication key or password. The Opal protocol provides for management of multiple users on an individual storage device, each with a unique encryption code and uniquely managed authentication codes, or passwords.

- **TCG SSC Enterprise**: This data security standard refers to storage devices used in servers, enterprise main storage and data centers, and other enterprise-class applications. It ensures that data at rest is protected through encryption, even in the event that physical security measures in the data center fail, and a storage device or system goes missing. As in the Opal SSC, the encryption key is generated by the SSD and can never leave the drive. This is especially important in enterprise-class computing, because the resource-intensive key-generation function is done automatically by the storage devices, alleviating a great burden from the IT team. The TCG Enterprise protocol enables enterprise-level security that is managed from a system console controlling a TCG enterprise-compliant RAID card or host bus adapter (HBA).

- **TCG SSC Opalite and Pyrite**: These are new subsystem classes to meet the requirements of diversifying computing environments. SSC Opalite provides a reduced feature version of Opal that includes full encryption and is intended for SMB and consumer environments that do not require support for many users and administrators. Pyrite provides password-locking features, but does not provide encryption.

Although the TCG Opal and Enterprise specifications were created in parallel over the last several years, TCG Enterprise has been more recent in implementation. TCG Opal has been considered more critical because of the immediate importance to protect mobile computers. Enterprise encryption, in general, has been widespread, but much of that encryption has been done by the host computing system. The more recent introduction of SEDs within the enterprise represents a powerful and significant new storage security innovation.

Enhanced Encryption and Device Decommission in the Enterprise

As more end users rely on mobile computing, and as storage devices grow ever smaller, the risk of physically losing control of important data is obvious. Less obvious is the growing risk of losing control of data when a storage device is decommissioned, especially when it is decommissioned from use in data center and enterprise computing environments.

It's unfortunately common for data on devices from high-profile companies and government agencies to be inadequately deleted before the devices are disposed of, redeployed, or even donated to charities, like the local grade school. This lack of effective media sanitization has led to sensitive data being inadvertently released into the public domain.

For traditional rotating media, such as hard disk drives, the accepted methods of data destruction can be both costly and slow. The process can even involve physically grinding or drilling holes through media, necessitating the purchase or lease of expensive equipment, or farming out hardware destruction to other firms. On the other hand, SSDs, and SEDs in particular, enable data to be purged in a much more efficient, fast, and inexpensive method.

Cryptographic erase of SSDs is a process that simply changes the encryption key on the drive. The system administrator, once authenticated, can issue a simple command to start a process where a random number generator onboard the SSD creates a new 256-bit encrypted key, and then securely erases the old key. Upon completion, literally in a matter of seconds, all the data on the drive is effectively unreadable.

SSDs also provide the uniquely fast and efficient ability to securely erase or sanitize the drive, even if encryption is not available. While physically overwriting the bits on a spinning hard drive can take many hours, for an SSD this process can be performed within minutes.

This element of speed represents a key advantage of SSDs compared to traditional rotating devices. Crypto-erase and the fast and easy sanitization process provide an enterprise with efficient and verifiable means to ensure that retired or redeployed devices don't take sensitive data with them.

Freeing Up IT Resources

SEDs, especially solid state SEDs, provide other advanced efficiencies for managing IT resources. On an SED, the encryption engine is always on, meaning that all the stored data is encrypted, regardless of whether authentication control has been enabled.

This means that when these security features are enabled, there is no requirement for a long encryption process for data that has already been stored on the device. As a result, an IT department can rapidly image many encrypted devices, and then move on to other important tasks. Traditional encryption systems require the use of servers specifically used for encryption key creation, management and backup. This function is not necessary for SEDs, because the drive itself controls the encryption key. The host system is then left with the task of managing authentication.

As mentioned previously, the TCG Opal standards, which allow remote access to lost computers through a console in the IT office, further alleviates the IT burden. For example, an IT manager can locate a notebook anywhere in the world, gain access, and wipe the drive to ensure data stays protected, or lock authentication to the device so that an intruder is effectively unable to access sensitive data.

The Micron Approach

Micron manufactures TCG SSC Opal- and TCG SSC Enterprise-compliant SEDs to meet the data-at-rest protection and security requirements of today's data-centric enterprise. Micron SEDs provide the hardware foundation enabling the protection of data in the event of the loss or theft of the storage device, so that when a business loses the physical control of the device, control of the data is never lost.

Micron's SEDs implement verifiable data protection methods, following standards that allow customers to know for certain that their data is protected, both at rest and after device decommissions.

Micron understands that sometimes these issues are so important that customers cannot rely merely on a company's assertion of effective data protection. For this reason, we have engaged third-party validation of our processes, ensuring that the supported Micron Sanitize, Sanitize Crypto Erase and Sanitize Block Erase commands function as advertised. Micron has worked with Kroll Ontrack to achieve these certifications, gaining independent recognition from a well-known industry leader for the effectiveness of Micron's encryption and sanitization methods.

Micron understands that the definition of a data storage endpoint goes well beyond a traditional computer or storage array. Micron is uniquely positioned to take advantage of the opportunity to offer comprehensive data-at-rest security with TCG encryption for client and enterprise SEDs.

FIPS 140-2 VALIDATED SEDs: The Next Step in Data-at-Rest Security

By following industry-accepted standards from the Trusted Computing Group, and by working with respected partners like Kroll Ontrack, Micron can provide verifiable security for data at rest. However, for many industries, especially government and government-related industries, even these industry-accepted measures are just the start.

Specifically, we refer to Federal Information Processing Standard (FIPS) 140-2 Validated SEDs. FIPS 140-2 is a specific standard for encrypted devices and includes many layers of protection schemes. By putting our drives into this rigorous validation process, and earning those validations in the end, we can offer the highest level of verifiable data security.

The main consumers of these FIPS 140-2 Validated SEDs are government agencies. But many industries, particularly banking and finance, can take advantage of this advanced, verifiable data protection when working with government regulators in the process of validating their data protection efforts.

Summary

Companies and their IT managers have long recognized inherent risks to stored data in mobile computing, and self-encrypting drives have long been seen as the leading solution to this risk. Proper deployment of SEDs provides verifiable protection of data on a mobile computing system, whether it's a laptop or a phone or a tablet.

But mobile computing is just part of the story. The shift to cloud computing has placed enormous volumes of sensitive data in data centers around the globe, focusing much more attention on enterprise encryption. The IT professionals who manage these data centers realize that SED adoption satisfies regulations and standards compliance, lowers total cost of ownership (TCO), increases IT efficiency, and most importantly, secures data by preventing data breach due to lost or stolen devices.

Micron is uniquely positioned to ease adoption with extensive expertise, advice and support. To continue the conversation, contact us at SED@Micron.com or follow us at Micron Storage (www.micron.com/storageblog) and @MicronStorage. For more information about Micron's FIPS 140-2 Validated SEDs, contact us by e-mail at federal@micron.com.