A MICRON WHITE PAPER

Securing Your Data in an Increasingly Insecure World

Overview

Digital information has completely transformed the way we live and do business. While the Internet exemplifies this change, industries such as health care and finance have been irrevocably changed as well. With this change comes the need for strong data security measures to protect information that is vital to personal privacy, business trade secrets and national security.

In this paper, we cover important data security topics/considerations, including data breaches, regulations and standards, and drive decommissioning, as well as system requirements and setup options. We also introduce the Trusted Computing Group (TCG) Storage Security Subsystem Class: Enterprise Specification, which is an essential part of a comprehensive data security plan for enterprises. Micron has TCG Enterprise-enabled solid state drives (SSDs) to meet your most demanding security needs.

Impact of Data Breaches Over the Years

Data breaches are nothing new; they have been plaguing us since the early days of information technology. Throughout the 1980s and 1990s, the only thing more certain than the march of technology was the extremes that criminals would endure to exploit it. What has changed over the years is the size, frequency and severity of data breaches.

Breaches of tens of millions of records have become commonplace. According to the Gemalto 2014 Breach Level Index, in 2014, more than one billion records were either lost or stolen — a 78% increase over the previous year. Unfortunately, this trend is not slowing with the amount of data being stored and its intrinsic value.

In its 2014 Digital Universe Study, sponsored by EMC, International Data Corporation (IDC) found that between 2013 and 2020, the digital universe would expand from 4.4 to 44 zettabytes — which amounts to 44 trillion gigabytes. IDC estimates that 40% of that data will require some level of data protection, but currently, only 20% is actually protected.

Rules, Regulations and Standards

Nearly every business in the global economy is governed by rules, regulations and standards that dictate how businesses should act, report their finances, and protect their data.

The Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley (SOX) Act all specify that sensitive data requires appropriate protection. These acts cover health care information, private data in the financial industry, and financial reporting data for all publicly traded companies. While these laws do not mandate specific mechanisms to protect this data, encryption is a generally accepted data protection practice.

Failure to properly secure your sensitive data can result in numerous penalties, including fines and criminal charges. For example, HIPAA's Omnibus Rule outlines fines that are levied against violating businesses — a maximum of $50,000 per violation, with a $1.5 million annual maximum. (See the Federal Register, Vol. 78, No. 17 for more details.) In its Stolen Laptops Lead to Important HIPAA Settlements news release, the U.S. Department of Health & Human Services reported that Concentra Health Services, a national healthcare company, was fined $1,725,220 in 2014 when a single unencrypted laptop was stolen from its offices.

Costs of Data Breaches

While laws and regulations may impose fines for data breaches, the true costs of breaches are much higher. Annually, the Ponemon Institute releases its Cost of Data Breach Study, which aims to break down and quantify the costs of data breaches.

In 2014, the average total cost for a data breach was $5.9 million, with an average cost per stolen/lost record of $201. More highly regulated industries fared much worse, with the healthcare industry averaging $316 per lost or stolen record.

Nearly 57% of the total cost of a breach resulted from loss of business. It is estimated that after a large public breach, nearly 15% of all customer relationships are lost. This is a rising trend as customers are becoming more savvy and aware of data security.

Unfortunately, the rate that breaches are occurring is only increasing. The Ponemon Institute estimates that the likelihood of a company experiencing a breach greater than 10,000 records over the next 24 months is 19%.

Encryption and Safe Harbors

These days, encrypted data (without the encryption key) is generally accepted as secure data. While many laws and regulations impose requirements about sensitive data, they also offer safe harbor protections to companies that use encryption. Safe harbors are provisions that reduce or eliminate a party's liability under the law if the party performed its actions in good faith or compliance with defined standards. More than 45 states in the U.S. currently have privacy laws that include encryption safe harbor.

HIPAA defines secured protected health information (PHI) as unsecured health information that has been rendered "unusable, unreadable or indecipherable to unauthorized persons." As a part of HIPAA's Breach Notification Rule, if the breach is greater than 500 PHI records, companies have 60 days to notify affected persons and media. Records that are encrypted are completely exempt from this requirement because a breach, in the view of HIPAA, never occurred.

The Ponemon Institute estimates that for an average breach, it costs companies nearly $500,000 just to notify the affected persons.

Threat Models

In order to determine how we can protect sensitive data, we need to know how that data can be exploited. The following threat models help us understand how data is vulnerable:

- **Data in Use:** Data being acted upon by applications or the operating system, typically in system memory.
- **Data in Flight:** Data being sent across some type of fabric, such as Ethernet, when remote systems are communicating.
- **Data at Rest:** Inactive data stored on a storage medium, such as a solid state drive (SSD) or hard disk drive (HDD), that has been powered off.

Several well-known data breaches resulted from direct attacks on data in use and data in flight. Protecting this type of data requires securing the system at a software level (for example, the operating system and password manager).

Securing data at rest requires a completely different set of strategies because data at rest (as defined by TCG) is stored on a powered-off storage medium. Therefore, the primary threat, unlike data in flight and data in use, is physical access.

In client computing, theft of data at rest is incredibly common. The ever-increasing use of laptops and mobile devices — most without any type of security — makes the issue exponentially worse. This is partially due to the increased capabilities of these devices, which lead to large amounts of sensitive data being stored on them.

For enterprise computing customers, protection of data at rest may seem straightforward because we assume that the storage medium stays within a physically secured area, but in reality, many of the same issues exist.

A MICRON WHITE PAPER
Securing Your Data in an Increasingly Insecure World

There are two primary ways that data at rest is compromised in data centers. The first, which is by far the least common, is theft. Theft in data centers is usually attributed to malicious insiders, who are trusted employees or contractors who have physical access to the storage hardware.

The second and much more common way that data at rest is compromised in a data center is through accidental loss. Data centers can hold tens of thousands of drives. In a typical year, hundreds or thousands of storage drives will fail, be decommissioned or be lost. For all of these cases, the chain of custody for sensitive data can be lost, which constitutes a data breach.

At one point, IBM estimated that 90% of all drives returned for repair contained some amount of recoverable data. This specific example shows a failure to implement or execute a drive decommission plan, and the result can be costly. There are numerous examples of drives that contain privileged information making their way into public hands due to this failure.

Media Sanitization

All drives that at some point contained sensitive data will eventually be removed from service. Whether it be through warranty returns or planned obsolescence, drives will eventually leave the relative safety of the data center. When this happens, businesses must be able to ensure that all sensitive data is removed. This is one of the major areas of exposure for data at rest.

Fortunately, the National Institute for Standards and Technologies (NIST) gives specific guidelines for sanitizing media. In its Guidelines for Media Sanitization, NIST defines media sanitization as: "a process that renders access to target data on the media infeasible for a given level of effort."

NIST outlines three methods that can be used to sanitize media, which are described in the following sections.

Destroy

As defined by NIST, "Destroy renders target data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data … shred, disintegrate, pulverize or incinerate by burning the device in a licensed incinerator."

When SSDs first became commercially available, physical destruction was the only agreed-upon technique to ensure media sanitization. However, destruction is an incredibly costly endeavor, and physical destruction limits reuse of the device, which effectively increases the total cost of ownership (TCO).

Destruction of media on-site requires time, labor, capital equipment and environmental considerations that may be outside of a company's abilities. Off-site destruction requires use of a company that is certified by the National Association for Information Destruction that follows environmental standards such as R2 or e-Steward and is able to ensure chain of custody, among other things.

Both destroy methods are costly and environmentally unfriendly when compared to drive reuse.

Clear

As defined by NIST, "Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple, non-invasive data recovery techniques; typically applied through the standard READ and WRITE commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported)."

In order to clear a storage drive sufficiently, NIST recommends executing a single pass of writes with a fixed data value, such as all zeroes. While this sanitizes the vast majority of data, it does not destroy all data in a modern SSD.

Nearly every SSD ships with more raw NAND than is exposed to the user. This additional space is call overprovisioning, which increases performance and write endurance. With a single-pass overwrite, data in the overprovisioned area may still contain sensitive data that could be recovered with forensic methods and is, therefore, not a completely secure method for media sanitization.

Even with a modern 1TB SATA SSD, a single overwrite can take nearly 40 minutes. While this is significantly faster than the 200 minutes it would take to clear an HDD, imagine a data center that is decommissioning dozens or hundreds of drives at a time.

What makes the discussion even more unclear is that data destruction software and data destruction companies commonly recommend a three-pass overwrite for drives based on the outdated Department of Defense (DoD) 5220.22-M policy. The DoD removed all references to single versus multiple passes the same year that NIST released SP-800-88.

Purge

As defined by NIST, "Purge applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques." NIST recommends more than one method to effectively purge an SSD:

- **Block Erase:** When a BLOCK ERASE command is sent to the SSD, all NAND devices are erased, including their overprovisioned areas. After the command is issued, it cannot be stopped. Unlike overwriting a drive — which can be stopped by power-cycling the system — the BLOCK ERASE command continues to execute, even after power is restored, until the command has completed. This process typically takes one minute.
- **Cryptographic Erase:** This method only applies to data that was written after encryption was enabled. A cryptographic erase deletes only the media encryption keys; it does not delete the encrypted data. Most modern SSDs use a 256-bit advanced encryption standard (AES), which is considered to be unbreakable with current and future technology. Therefore, deleting the encryption keys renders the data unreadable. Cryptographic erase takes less than one second to complete, which is orders of magnitude less than all other options. When applied to a large data center, cryptographic erase can save thousands of hours and millions of dollars in decommission costs.

Without encryption, the process to fully sanitize and decommission a drive can take time, be extremely complex and be very costly. As a result, many companies do not fully implement the process or the process can fail for individual drives.

TCG Enterprise Specification

TCG is a not-for-profit international industry standards group formed to develop, define and promote open, vendor-neutral industry standards for trusted computing platforms. In 2009, TCG developed the TCG Storage Security Subsystem Class: Enterprise Specification (TCG Enterprise), which created a framework that drive manufacturers can use to effectively secure their data in an enterprise environment.

As stated in the specification, TCG Enterprise's scope is fairly narrow: "This specification defines a limited set of TCG trusted storage functionality that, combined with full disk encryption (FDE), protects the confidentiality of user data at rest. Only a single threat scenario is addressed: removal of the storage device from its host system involving a power cycle of the storage device and subsequent unauthorized access to data stored on that device."

TCG also maintains the OPAL Storage Subsystem Class Specification, which has a similar scope for client drives as opposed to enterprise drives. Where these two specifications differ is that TCG Enterprise marries the drive to a specific RAID controller in the host. When TCG Enterprise is enabled, not only is hardware encryption enabled on the drive — it is forever paired with the connected RAID controller. If the drive is removed for any reason, the data is effectively secured until it is reattached to that RAID controller. Provisions are in place to migrate the drive to other systems, which is covered in the Configuration section of this paper.

A MICRON WHITE PAPER
Securing Your Data in an Increasingly Insecure World

Encryption

In its simplest form, encryption is a mechanism used to obscure data from any unintended audiences. Encryption can take many forms, from software encryption performed by the host to hardware encryption performed on the storage device.

As part of its enterprise specification, TCG requires the use of FDE using either AES 128 or AES 256. Although sometimes used interchangeably, FDE and self-encrypting drives (SEDs) do have some distinct differences.

While FDE is a more generic term used to describe the full encryption of a storage device by either software or hardware, self-encryption is a method of FDE that is always hardware-based. When used in the context of TCG Enterprise, FDE refers to drives that are self-encrypted (SEDs).

With hardware encryption, the encryption engine is integrated into the drive's controller, which offers numerous benefits over other encryption methods, including:

- **Security:** The decryption key is stored on the device so it is never accessible by the host system, which can leave the system vulnerable to attacks.
- **Ease of Deployment:** The drive is always encrypting data. There is no requirement to install and maintain key management systems.
- **Performance:** Because the encryption is performed at the device level, there is zero load on the host CPU to encrypt the data; an encrypted SSD performs identically to a non-encrypted SSD.

For more information about encryption on Micron's SSDs, see Micron's white paper, "Self-Encrypting Drives."

Addressing the Threat Models

To reiterate, TCG Enterprise does not protect systems that are powered up and online, even if encryption is enabled; it only protects data at rest, which helps to protect data against physical theft and accidental loss. If at any point a drive is removed from its host system, that drive is fully encrypted and its data is protected. This addresses any issues with a trusted insider removing a drive, or a careless worker not properly decommissioning a drive.

With TCG Enterprise, the decommission process is quick, easy and cost effective due to the ability to cryptographically erase the drive. This not only encourages companies to implement these processes, it also dramatically increases adherence to the processes. Adherence is a major factor because it only takes a single drive to fall out of the process for a data breach to occur.

TCG Enterprise Configuration Requirements

In order to set up and configure a TCG Enterprise system, you need two key components:

- **TCG Enterprise Drive:** Your drive(s) must be compatible with the TCG Enterprise Specification. Typically, this is an option you must select when purchasing a drive. Starting with the M500DC and M510DC SSDs, Micron plans to offer a TCG Enterprise option on all future data center and enterprise storage products.
- **TCG Enterprise RAID Controller:** Many modern RAID controllers support the TCG Enterprise option — either enabled by default or via an additional hardware key or software license. With a software key, you may also be able to enable TGC Enterprise on existing systems without having to replace deployed components. Due to the requirements of the TCG Enterprise system, host bus adaptors (HBAs) are not supported.

TCG Enterprise Configuration

Configuring a TCG Enterprise system is simple and straightforward. When deploying drives on a RAID controller, the steps required to assign physical drives to the RAID array vary based on the RAID vendor, but they follow a similar process.

In order to configure a TCG Enterprise system prior to creating an array, you need to enable the feature. As with any drive joining an array, all data on the system will be lost.

Though it may vary per RAID vendor, you should be prompted for additional information, such as a security key identifier and a security key. This information is used to identify and lock the TCG Enterprise system.

It is important to store these keys in a secured area so that you can recover your data if you need to migrate the array to another controller. These keys are only used by the user and host software during a migration; they do not need to be stored anywhere on the host system. You may also see an option to supply an additional password during the boot process, but this optional.

TCG Enterprise Communication

After the system is configured, interacting with the drive is completely transparent to the user. What separates a TCG Enterprise device from a non-TCG Enterprise device is how the drive interacts with the host on power-up.

TCG Enterprise drives send and respond to special commands defined by TCG that are unique to the drive interface. These commands include:

T13 (SATA)	T10 (SAS)
TRUSTED NON-DATA (5Bh)	
TRUSTED RECEIVE (5Ch)	SECURITY PROTOCOL IN (A2h)
TRUSTED RECEIVE DMA (5Dh)	
TRUSTED SEND (5Eh)	SECURITY PROCOL OUT (B5h)
TRUSTED SEND DMA (5Fh)	

Table 2: Commands for TCG Enterprise Drives

When a drive powers on prior to any normal SATA/SAS commands being sent, the drive determines whether encryption was previously enabled. When encryption is enabled, the drive goes into a locked state until the secure commands are used to unlock it. These commands are issued between the SSD and the TCG Enterprise RAID controller, not by the host software.

Once the drive is unlocked, it responds to all normal SATA/SAS commands. At this point, all data communicated across the bus is unencrypted. Unlocking the drive essentially turns your data at rest to data in use or data in flight, which is an important distinction because TCG Enterprise's scope does not cover data in use or data in flight.

Drive Migration

If you need to migrate the array to another RAID controller (for example, in the event of controller failure), there are options available to migrate your data.

Once again, this may vary based on the RAID controller vendor, but when the array is migrated to the new system, the user is prompted for the security key created during the configuration step. After the key is entered, the configuration process is identical to that of unsecured drives.

Summary

The amount of data that we generate and store is growing exponentially. While we may joke about the number of silly, inconsequential photos and videos being uploaded daily, the reality is much more sobering.

As part of a connected society, nearly every piece of sensitive information about us is stored on a server, laptop or mobile device somewhere in the world. One effective way of protecting this valuable asset is through encryption.

Current encryption standards are not only considered unbreakable now, they are deemed strong enough that they will never be broken by any known means in the future. The idea of encryption is so pervasive that numerous rules, regulations and standards identify encryption as an effective way to secure data. In fact, as the Ponemon Institute points out, 50% of data breach victims expanded the use of encryption post-breach.

Still, when cybersecurity firm Kaspersky Lab surveyed companies in 2013, 65% of them did not use encryption of any type on their data. The remaining 35% used some level of encryption — but not necessarily an adequate level.

So if we know that information is valuable and that encryption helps protect that information, why is encryption still not broadly implemented? Kaspersky noted that lack of executive-level support, lack of resources and lack of knowledge were the top factors that prevented business from implementing encryption.

Learn More About TCG Enterprise SSDs

Contact ssd@micron.com or visit micron.com to learn more about Micron's TCG Enterprise-enabled SSDs.

TCG Enterprise Advantage:

With TCG Enterprise, you get all of the benefits of data encryption without having to deal with the perceived negatives.

Gain Executive-Level Support by Lowering TCO:

- **Easy-to-Deploy Solutions:** Eliminates the need for large, complex systems.
- **Complete Data Security:** Protects data at rest without costly software management systems.
- **Reduced Decommission Costs:** Reduces decommission costs with cryptographic erase.

Overcome Lack of Resources:

- **Reduced Administrative Tasks:** Once configured, eliminates additional configuration tasks, reducing maintenance.
- **Eliminates Key Management Systems:** Removes the need for software management systems with self-managed keys.
- **Hardware-Based:** Makes encryption is transparent to the host, so there is no penalty on system performance.

Overcome Lack of Knowledge:

- **Easy to Use:** Requires only a few additional setup steps, and no in-depth training or certification.
- **Always-Encrypting:** Because it is always encrypting, eliminates the need for additional knowledge to determine when the data is encrypting.

micron.com/storage