DIGISTOR®
A CDSG COMPANY

Is Your Data at Rest (DAR) Truly Secure?

If there's anything we've learned over recent years, it's that our computer systems in general—and the precious data stored on them in particular—are susceptible to attack by hackers. These bad actors can range from independent entities to nation states. Anyone from individuals to institutions may be targeted, where the latter includes the military, federal agencies and organizations, critical infrastructure (such as power grids, oil pipelines, transportation systems), industrial and manufacturing concerns, banking and financial establishments, and medical facilities. While federal organizations in the USA have long been concerned by security, the necessity of fully securing their digital assets has been brought into sharper focus by recent cyber-attacks and data breaches, such as the 2020 SolarWinds assault.

In this case, hackers penetrated Texas-based SolarWind's systems and added malicious code into the company's Orion software system, which customers use to manage their IT resources. As reported by The Wall Street Journal, a number of federal agencies were compromised, including the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury. Also, private companies like Microsoft, Cisco, Intel, and Deloitte, were attacked, along with other organizations such as the California Department of State Hospitals and Kent State University. In May 2021, President Biden enacted his Executive Order on Improving the Nation's Cybersecurity. In part, this executive order directed all branches of the federal government to improve their efforts to identify, deter, protect against, detect, and respond to cybersecurity threats. (While

this executive order addresses the United States Federal Government, enterprises and businesses of all sizes should also take steps to secure and protect their data.)

The first step in securing digital data is understanding that, at different times, it may exist in one of three distinct states. These states are data in transit (which may also be referred to as data in motion or data in flight), data in use, and data at rest. Data in transit is information that is flowing through a network, including private corporate networks and public networks such as the internet. Data in use refers to active data that is being accessed and manipulated by a software program and is stored in a non-persistent digital state, typically in the computer's random-access memory (RAM) or in the caches and registers associated with the central processing unit (CPU). Data at rest (DAR) refers to data that is physically housed in a storage device.

When most people hear the term "computer security," they think in terms of threats like viruses, malware, and ransomware, along with solutions like firewalls and antivirus software. These solutions predominantly focus on external threats by protecting data in transit and data in use. However, many security breaches and data loss incidents may be traced to insider threats in the form of unauthorized access to sensitive information, or to computers and/or their drives being mislaid or stolen. Thus, protecting DAR is now understood to be a critical piece of a zero-trust solution. This paper introduces the concepts involved with regard to protecting DAR, it presents various scenarios that different organizations employ (not all of which are effective), and it details what is required to truly secure DAR to a level that is acceptable to the federal government.

Cherry-Picking Checkboxes Won't Suffice

Fully protecting DAR is a non-trivial matter. As we will see, this doesn't mean easy-to-use solutions are not available; what it does mean is that there are a lot of considerations that need to be addressed.

For the purposes of this paper, we will focus on Windows and Linux, which are the predominant operating systems used by military, federal government, critical infrastructure, and industrial applications. Also, we will focus on DAR that is housed on a solid-state drive (SSD) because this is the most common and problematic scenario.

Unfortunately, many organizations think that ticking selected checkboxes has them covered. For example, fully securing DAR in an efficient manner that doesn't slow the computer requires the use of a self-encrypting drive (SED).

Such a device contains a hardware encryption engine (EE) that automatically encrypts data as it is written to the drive and automatically decrypts the data as it is read from the drive. It's not unknown for an organization to replace the standard SSDs in its computers with their SED counterparts, tick the SED box on their checklist, and assume that their DAR is secure. In reality, unless the drive is also cryptographically locked, anyone can power-up the computer and access the data with impunity. Thus, a key feature of an effective DAR security solution is for the drive to be cyber-locked with a data encryption key (DEK), thereby protecting it from bad actors who gain access to the SSD, either on its own or while residing in a computer.

The main point here is that is not sufficient to cherry-pick a subset of checkboxes. As will be discussed, fully securing DAR requires ticks in all of the appropriate checkboxes.

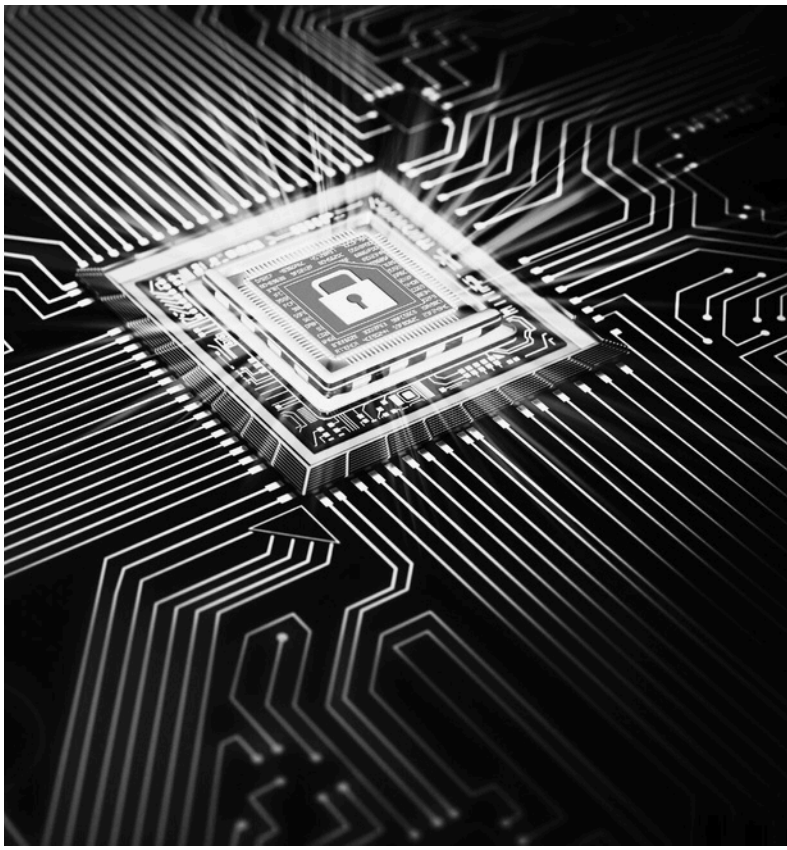
Is It Compliant? Is It Validated? Is It Certified?

There are a variety of DAR solutions available on the market. But how can a prospective user decide which solutions will perform as promised and which will fail miserably? The answer is to adopt only solutions that are compliant with any necessary regulations and that have been validated and certified by appropriate authorities.

To be acceptable for use by the federal government, for example, a DAR solution must be TAA compliant, NIST-validated, FIPS-validated, and CSfC-listed (these are some of the checkboxes alluded to in the previous section), but what does all of this actually mean?Let's start with the drive itself. The Trade Agreements Act (TAA) includes the requirement that the General Services Administration (GSA) must acquire only U.S.-made or TAA-compliant products. This means that the drive cannot originate in a non-TAA-compliant country.

Although this may appear to be a self-evident requirement when it comes to implementing a secure DAR solution, it can sometimes be difficult to determine a product's true origin. As was previously noted, a key feature of an effective DAR security solution is for the SSD to be cyber-locked with a DEK. One critical step in the process of legitimately accessing the data is authorization acquisition (AA), in which the user enters a password that releases the DEK to the SSD's EE. If AA occurs prior to booting the OS (this is the preferred scenario as discussed below), this is referred to as pre-boot authentication (PBA). A higher level of confidence regarding AA is provided by employing multi-factor authorization (MFA).

The Trusted Computing Group (TCG) is a consortium of technology companies whose goal is to promote and implement trusted



computing concepts. The TCG's Opal Storage Specification defines features of data storage devices (such as SSDs) that enhance their security. TCG Opal manages the encryption and decryption of information within the storage device itself, thereby enabling fast encryption/decryption and minimizing the risk of data leakage without undermining system performance. In the case of SEDs, the TCG Opal 2.0 standard includes the concept of a shadow Master Boot Record (MBR) that can support an AA function, which—on a boot device—would be a PBA. The Opal standard also defines a

locking mechanism that prevents the SSD from being replicated.

When it comes to encrypting the data, the SED must employ a suitably robust algorithm, such as AES-256, which is part of the Commercial National Security Algorithm suite of cryptographic algorithms that are approved by the National Security Agency (NSA) to protect our nation's most critical assets. federal Information Processing Standards (FIPS) are standards and guidelines for federal computer systems that are developed by the National Institute of Standards and Technology (NIST) in accordance with the federal Information Security Management Act (FISMA) and that are approved by the Secretary of

Commerce. A FIPS 197 certification guarantees that the AES cryptographic algorithm has been implemented correctly and has sufficient entropy. A FIPS 140-2 certification assures that the SED's EE has been properly designed and secured. Furthermore, a FIPS 140-2 L2 ("Level 2") certification—which is required for most DAR applications—ensures that there is visible evidence of any attempt to physically tamper with the drive.

Next, the National Information Assurance Partnership (NIAP) is responsible for the U.S.

implementation of the Common Criteria (CC), which is an international standard (ISO/IEC 15408) for IT product security certification. The CC is a framework that provides criteria for independent, scalable, and globally recognized security inspections for IT products, and it forms the basis for a government-driven certification scheme required by federal agencies and critical infrastructure. Adhering to the CC standard assures that the SED's AA and EE functions have been properly engineered and that any interfaces between the AA and EE are free from information leakage.

CSfC, which stands for "Commercial Solutions for Classified," refers to a program established by the National Security Agency (NSA) that enables commercial off-the-shelf technologies to be used in securing classified information. CSfC solutions are a set of standards and guidelines designed to ensure that these commercial products, when combined in specific configurations and implemented correctly, meet the stringent security requirements necessary for safeguarding classified data.

This approach allows government agencies and organizations to leverage the latest advancements in cybersecurity from the private sector, reducing costs and streamlining the process of obtaining secure communications and data protection capabilities while still maintaining the necessary levels of confidentiality, integrity, and availability demanded by classified environments.

Meeting all the required compliances and attaining the mandated validations and certifications is time-consuming and expensive.

FIPS certification alone can take 18 months or more plus additional time for the lengthy CSfC-listing validation—which is why so few

SED manufacturers manage to tick all of the checkboxes required to implement a federally approved DAR security solution.

When is DAR Most Secure?

Some people will say that DAR is at its most secure when it's stored on the SSD in an encrypted form and the SSD is powered all the way down. (In some high-security mission-critical environments, the SSD itself may be removable, which allows it to be easily detached from the main system for the purpose of being locked up in a safe or transported to another location.) As we've discussed, however, simply having the SSD encrypt the data and powering it down does not, in fact, guarantee that the data is truly secure. In reality, data is at its most secure when the SSD holding the data is an SED with a hardware EE, accessing the data requires AA, and the SSD's cryptographic methods (including its EE and AA) are validated by a third-party such as NIST.

Searching for a Solution

For the purpose of this portion of our discussions, let's assume that we are working with the most common usage scenario, which is that that the data and the OS (Windows or Linux) reside on the same drive, while noting that there are other deployment possibilities, including the use of Virtual Machines (VMs). With regard to providing a DAR security solution, it could be that the IT group in an organization has been tasked with adding these capabilities to legacy machines, or the group may be building a new batch of custom machines for use within that organization. Another possibility is a global OEM that is building computers for sale to a wide range of customers.

Consider someone working with a computer that currently has no DAR protection capabilities whatsoever. In this case, one option is to purchase off-the-shelf encryption software and load it onto the SSD containing the OS, data, and other application programs. When the encryption software is run, it will shut down the system and encrypt every part of the drive. If no cryptographic lock is placed on the contents, then when the system is powered

up, everything—starting with the operating system—will be decrypted automatically. This is akin to putting all of your valuables in your house but not having a lock on the front door. Furthermore, encryption and decryption are computationally expensive activities. Since everything in this scenario runs through the CPU, this will result in the system slowing down. So now you have a system that runs slowly because it's encrypting and decrypting everything while—at the same time—not actually protecting anything. Generally speaking, this would be classified as a less-than-optimal solution.

Another alternative is to purchase an SED, which automatically employs hardware-based encryption and decryption without impacting the host CPU. This relates back to our earlier checkbox discussions because somecompanies assume that simply having an SED in the system means their DAR is secure. However, if

the drive has not been cryptographically locked, then anyone can boot up the system and read the data. Alternatively, they can extract the drive, take it somewhere else, and boot it up in another system. Furthermore, this latter scenario allows for the drive to be cloned tens, hundreds, or thousands of times—it doesn't matter that the data is encrypted because it can still be duplicated—and concerted attacks can be mounted on the cloned drives.

- Lock Feature
- H/W AES-256 Crypto
- Pre-Boot Authntication (PBA)
  - Built-In Multifactor Authentication
  - Least privilege role enforcement
  - Erase on repeated AA failure
  - Configuration management
- Third-Party Certifications
  - TAA
  - FIPS 197
  - FIPS-Validated
  - Common Criteria validated
  - NIAP Listed
  - CSfC Listed
- Current Technology Support
  - 2.5-inch (7mm) and M.2
  - SATA III & NVMe
  - Up to 2 TB
  - Up to 3.4 GB/s

This is probably an appropriate point to note that many people mistakenly believe that their operating system (OS) password provides sufficient DAR protection. When your system is being attacked by professional hackers, however, relying on the OS password is like not having a password at all. Thus, another critical aspect of a DAR security solution is that the process of unlocking the SED must take place prior to the OS being booted. Once you have a system equipped with an SED,
if you know how to use TCG Opal commands, you can write your own application that runs on the host computer, locks the drive down with a password, and forces the use of PBA, which means that AA is performed before the OS is booted. One problem here is this type of solution is tied to the OS. That is, if you create a solution for use with Windows, that solution won't work with Linux, and vice versa.

More importantly, your solution has not been validated or certified by the appropriate bodies, and so it cannot be used for federal and military applications. You may opt to purchase a third- party Opal-based solution, in which case the software will still be tied to a particular OS, and you must ensure that both the drive and the software have the appropriate certifications.

It should be noted that full military-grade, NSA-approved solutions that carry all necessary certifications are available but—in addition to being extremely expensive, thereby making them impractical beyond a very narrow set of highly specialized applications—these devices have largely failed to keep up with commercial densities, interfaces, and formats. There is a more affordable path ensuring that the solution is both commercial-of-the-self (COTS) and security-validated by the NSA. It is CSfC, an NSA strategy to provide cybersecurity solutions by taking advantage of commercially available and validated industry solutions.

Citadel SSDs are the Solution

The CRU Data Security Group (CDSG) has been honing the art of protecting data for over 30 years. DIGISTOR is the CDSG brand of fixed and removable rugged storage drives that are crucial to physically securing sensitive data for government agencies and other security- conscious organizations. Citadel FIPS-validated SEDs are the only SSDs to offer pre-tested and pre-integrated multi-factor authentication and pre-boot authentication (PBA). And the SSDs meet budget needs, while NSA security validation is thoroughly tested and represents a full CSfC layer of protection. One very important point that is applicable to OEMs and in-house IT departments is that Citadel drives are shipped deactivated and can be used "out of the box." That is, although these

Learn about the importance of CSfC in this blog: https://digistor.com/innovation-integrity-affordability-why-csfc-matters/

SSDs always automatically perform hardware encryption and decryption, this is invisible to the user and no AA is required at this stage. This means that the user can freely work with the drive prior to activating the PBA. In turn, this allows the user to test the drive out, load different operating systems, wipe the drive (this doesn't affect its security capabilities) , and start all over again.

Most importantly, the security software, which is pre-installed on the drive, supports multiple OS's—it doesn't care whether the user wishes to load Windows or Linux or use a VM. In the case of OEMs, this doesn't require any change to the build process apart from using the Citadel SSD as opposed to any other form of SSD.When the user is ready, it's a simple matter for the organization's cryptographic officer/administrator to access the console and activate the PBA, including granting or revoking access to multiple users, each with their own password, and activating MFA if required.

The administrator can also establish various policies, such as cryptographically wiping the drive following a specified number of failed AA attempts.

Conclusion

There are companies that make SEDs and that provide a mechanism to load the software required to secure DAR, but that don't actually provide the software itself. Conversely, there are companies who create the software required to secure DAR, but that are not associated with any particular drive manufacturer and whose software depends on the OS being used. All of this results in uncertified solutions.
Citadel SSDs—which can be embedded in the computer or presented as part of a removable drive assembly—offer a single deliverable in the form of an SED with integrated OS agnostic
software providing PBA and MFA for securing DAR, with both the hardware and software being fully validated and certified.
Citadel SSDs are unique in providing commercial
off-the-shelf (COTS) solution that are CSfC-listed and meet the CC standard, bringing military-grade security to federal agencies and critical infrastructure, as well as industrial, banking, and medical markets.
In addition to being fast and easy to commission and deploy, Citadel SSDs help users
tick all of the checkboxes required by federal and military agencies to meet President Biden's Executive Order on Improving the Nation's Cybersecurity at the highest level as well as other security mandates such as CNSSP #11.

CNSSP #11 is a critical part of the United States Federal Government's Cyber Security strategy. Learn about this policy component here: https://www.niap-ccevs.org/Ref/ FAQ.cfm#cat32

Contact Us
+1 (360) 816-1800, Opt 2 | **sales@digistor.com** 1000
SE Tech Center Dr., Suite 160, Vancouver, WA 98683

digistor.com