# **DIGISTOR**<sup>®</sup> secure data storage

# Use Citadel SSDs to Secure Your Data at Rest (DAR)

Protect against unauthorized access to laptops, desktops, and servers

- Easily Meet Federal Cybersecurity Requirements
- Commercial Pricing Enables Wide
   Deployment
- Operating System Agnostic

Citadel<sup>™</sup> FIPS certified self-encrypting SSDs are the only SSDs to integrate pre-tested multifactor authentication and pre-boot authentication (PBA) in low-cost, easily deployed, common form factors. Citadel offers a hardware-based Data at Rest (DAR) security solution that's easy to implement and affordable enough to deploy widely across commonly used laptops, desktops, workstations, and tactical servers.

Powered by CipherDrive<sup>™</sup>, the built-in PBA unlocks access to the encrypted operating system or virtual machine on the Citadel SSD along with the data stored there. This secured data is encrypted by NSAapproved Advanced Encryption Standard (AES) 256-bit encryption at the hardware level. Once booted, Citadel allows no-overhead access to encrypted data at the full performance of the system. **DIGISTOR**<sup>®</sup> SECURE DATA STORAGE

## Secure Your Data at Rest

In accordance with collaborative Protection Profiles (cPP), Citadel SSDs can be installed and will manage key exchange with the DIGISTOR Secure SED (cPP Encryption Engine). The DIGISTOR line of Citadel SSDs is a secure storage solution available to be integrated into a one or two-layer security solution today.

#### NIST Certification #3926

#### **NSA Standardized Security**

Citadel SSDs contain NSA-listed Authorization Acquistion (AA) capability that provides access to the FIPS-certified DIGISTOR Secure SED Encryption Engine (EE). This allows government customers to securely store sensitive Data at Rest in accordance with NSA standards.

**Remote Computers** - Secure your mobile workforce using Citadel's pre-boot authentication feature to unlock access to software. Citadel SSDs protect the entire contents of the drive, not just individual files or folders, mitigating field deployed laptop data security issues. They are easy to use and require minimal configuration.

**Loss and Theft** - While hard drives and SSDs can be removed from any system for attempts to retrieve data through sophisticated cyberattacks, Citadel SSDs protect sensitive information and intellectual property through locking the SSD and full-disk encryption.





# DIGISTOR®

## **Citadel SSD Security Features**

- Encryption AES-256, FIPS PUB 197 specification
- Authorization Acquisition (AA) under Common Criteria cPP
- Compliant under collaborative Protection Profiles (cPP)
- Pre-Boot Authentication (PBA) supports booting and chain loading VMs / SecureView and other hypervisors
- PBA Admin and Management capabilities
- 2-Factor / Multi-factor Authentication support
- Support for CAC/PIV/CIV and SIPRNET cards and tokens
- Cryptographic Erase (CE)
- User Management
- TPM 2.0 support
- Key Management Custom AK and DEK

#### Military Grade Encryption

Citadel SSDs use military grade encryption AES 256-bit algorithms and are FIPS 140-2 Level 2 certified with tamper evident coating.

#### Self Destruct / Crypto Erase

Citadel SSDs support an optional "self-destruct" feature with a configurable "dead man switch" that deletes the SSD's encryption keys. A Security Officer or Administrator can also issue a Crypto Erase command to cryptographically erase all the data on the drive.



## **Privacy Compliance**

#### **Comply with Data Protection Mandates**

Build Citadel into solutions to address Federal, state and local, as well as international privacy compliance rules and policies such as:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- The Payment Card Industry Data Security Standard (PCI-DSS)



Common Criteria

010101

-1010

 $1 \ 0$ 

 $\cap$ 

1 N

#### Hardware Technology

- On-device encryption
- FIPS 140-2 L2 (NIST Certification #3926)
- Tamper-evident coating
- TAA-compliant

#### **CipherDrive Pre-Boot Authentication Technology**

- FIPS 140-2
- Common Criteria NIAP Listed
- NSA Component Listed CSfC Hardware Disk Encryption Standard (PCI-DSS)

### Easy to Install and Easy to Manage Security

	05/14/2021 14:47:34	Product License Expiration Date: July 11 2021
	DIGISTOR CITADEL SSD	
	CipherDrive v1.2.2	
	Pre-Boot Authentication Login	
		ITCARD
DIGISTOR® SECURE DATA STORAGE		
	Password	۲
	Settings Console	
	Enroll Smart Card	
	Login	

DIGISTOR					Administrator Logout
Dashboard Jser	Add		System Users		Import
Settings V	Username	Role	Auth Type	Email	
faintenance V	Administrator	Admin		admin@testmail.com	UPDATE TO DELETE
ogs V Disk Information	scuser1@SmartCards.com	LoginUser	<b>— —</b>	Scuser@testmail.com	✓ update <sup>®</sup> delete
bout CipherDrive	Security	SecurityOfficer	<b></b>	security@testmail.com	& UPDATE B DELETE
	Login	LoginUser		login@testmail.com	🖉 UPDATE 🗒 DELETE
	Helpdesk	Helpdesk		helpdesk@testmail.com	UPDATE TO DELETE

#### **Pre-boot Lock**

A pre-boot authentication layer is built into Citadel SSDs to authenticate a user (using either a password or smart card) before the operating system boots. This pre-boot authentication, combined with full disk encryption, protects the entire DIGISTOR SSD and not just individual files.

#### **Multiple User Support**

Citadel SSDs can be configured to allow different users to unlock the computer to allow the drive to boot the operating system.

ashboard				_	Fated Successful		
asnboard eer gs ✓	$\otimes$	0 Failed Attempts Since Last Successful Login	10 9 0 7 8				
gs sk Information bout CipherDrive	$\bigotimes$	Latest Successful Login 05/14/2021 14:55:21	5				
	$\triangle$	0 Disk SMART Errors					
	Login Sumr	nary	95-08-2823	05/19/2021 05/19/2021	05/11/2021 05	12/2021 05/13/2021	05/14/2021
	Successfu	l Login		Unsuccessful Lo	gin		
		Login	st Login: 021 14:55:21				

DIGISTOR			Administrator Logout
Dashboard			Search Trilter
User		Activity Log	
Settings V	Date	By User	Action
Configuration	05/14/2021 14:52:30	Administrator	Export configuration successful
Maintenance Y			-
Backup Database	05/14/2021 14:50:32	Administrator	Backup Database successful
Erase Disk	05/14/2021 14:49:16	Administrator	User login successful
Change DEK	05/14/2021 14:47:46	Administrator	User login successful
Change AK	05/14/2021 14:46:19	Administrator	User logout successful
License Upgrade	05/14/2021 14:45:54	Administrator	Updated User scuser1@SmartCards.com
PBA Upgrade	05/14/2021 14:44:57	Administrator	Added User Helpdesk
Deactivate/Uninstall PBA	05/14/2021 14:44:18	Administrator	Added User Login
Export Configuration	05/14/2021 14:43:43	Administrator	Added User Security
Update Disclaimer	05/14/2021 14:42:49	Administrator	User login successful
Logs	05/14/2021 14:39:50	scuser1@SmartCards.com	User login successful
Activity Log	05/14/2021 14:37:52	scuser2@SmartCards.com	User login failed
Login Log	05/14/2021 14:36:56	Administrator	User logout successful
Exception Log	05/14/2021 14:28:50	Administrator	User login successful
Admin Log	05/14/2021 14:21:56	Administrator	User logout successful
Latest Log			

#### Dashboard

The built-in dashboard gives a quick and detailed overview of the security profile of the computer.

#### Audit and Logging

Five detailed logging types are available. Administrators can review the security profile of the computer and mitigate unauthorized access. These reports can be used to meet privacy compliance laws.

## **Operating System Agnostic**



## **DIGISTOR Citadel Secure Storage SSDs**

#### **Technical Specifications**

Form Factors & Interfaces	<ul> <li>M.2 2280 PCle Gen 3x4 NVMe 1.3</li> <li>M.2 2280 SATA 6 Gb/s 2.5-inch 7mm SATA 6 Gb/s</li> </ul>	Advanced Flash Management	Static & Dynamic Wear Leveling Bad Block Management TRIM S.M.A.R.T.	Authentication Methods	CAC, USB, or YubiKey
Flash Type	BiCS4	MTBF	More than 1,600,000 hours	Confidentiality (Encryption)	AES-256 / FIPS PUB 197
Performance	SATA: Read: up to 550MB/s Write: up to 530MB/s NVMe: Read: up to 3,400MB/s Write: up to 3,100MB/s	Encryption	TCG Opal SSC hardware level AES 256-bit encryption	Authentication (Digital Signature)	Elliptic Curve Digital Signature Algorithm (ECDSA) over the curve P-384 with SHA-384 / FIPS PUB 186-4 RSA 2048-PSS with SHA-256 method / FIPS PUB 186-4
Power Consumption	Active mode: ≤2,300mW Idle mode: ≤110mW	Compliance	RoHS Compliant TAA Compliant	Integrity (Hashing)	SHA-384 / FIPS PUB 180-4
Temperature Range	Operation: 0°C ~ 70°C Storage: -40°C ~ 85°C				

Citadel SSDs are self-encrypting drives which secure all critical data using strong AES 256-bit encryption, with the encryption/decryption performed on the SSD hardware itself, independent from the host, which maintains the highest host performance by not impacting CPU load. Locked BOMs available.

#### All Available Configurations are TAA-Compliant and FIPS 140-2 L2 Certified

#### M.2 2880 SSD SATA

	Single Drive	Multi-Drive		Single Drive	Multi-Drive
512GB	DIG-M2S45126	DIG-M2S25126	512GB	DIG-SSD2S45126	DIG-SSD2S25126
1TB	DIG-M2S410006	DIG-M2S210006	1TB	DIG-SSD2S410006	DIG-SSD2S210006
2TB	DIG-M2S420006	DIG-M2S220006	2TB	DIG-SSD2S420006	DIG-SSD2S220006

2.5-inch SATA 6 Gbps SSD

#### M.2 2280 PCIe (3x4) NVMe SSD

	Single Drive	Multi-Drive
512GB	DIG-M2N2S45126	DIG-M2N2S25126
1TB	DIG-M2N2S410006	DIG-M2N2S210006
2TB	DIG-M2N2S420006	DIG-M2N2S220006

#### CipherDrive Technology is FIPS and Common Criteria Certified

## **Contact Us**

+1 (256) 933-0589 info@avant-inc.com