DIGISTOR®

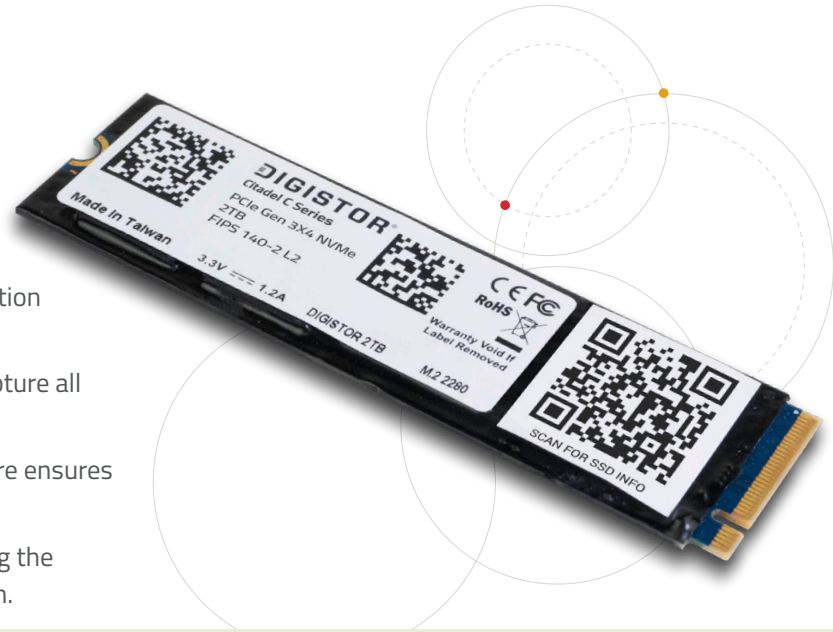
SECURE DATA STORAGE

DIGISTOR Citadel™ C Series

Secure data as only hardware can

- Hide data from cyber threat: unreadable storage partition protected by non-recoverable key
- Know who accessed data: secure data access logs capture all insider threat activity
- Retire or repurpose SSDs safely: verified device erasure ensures every data block has truly been wiped

DIGISTOR Citadel C Series SSDs, powered by Cigent®, bring the robustness to securing data at rest that only hardware can.



Pre-Boot Authentication

Additional Authentication for File Access

Non-Recoverable Key Protection

Unreadable Storage Partition Renders Data Invisible

Pre-Boot Authentication

Security made easy

Pre-boot authentication requires that a computer user provide trusted credentials to the drive before the laptop or desktop computer can detect and start up. This prevents unauthorized users from gaining access to the encrypted drive and its sensitive data.

Key Features

- Simple, easy-to-use protection from ransomware, physical, and other cyber attacks
- Worry-free deployment: Cigent software is tested and validated for use with DIGISTOR SSDs
- Address critical requirements for data governance and privacy programs such as CMMC, HIPAA, GDPR, GLBA, DSS, compliance requirements
- Multi-factor authentication (MFA) requires more than one authentication for access. Multiple authentication methods include password, CAC/PIV smartcard, and PIV-supported Yubikey
- Windows environment features
- FIPS 140-2 L2 NIST certificate #4294

Contact Us

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

Rev 2.0

Features and Capabilities

Now with Pre-Boot Authentication (PBA)

Feature	Citadel C Series
FIPS 140-2 L2 Certified	●
NIAP CC FDE AA	Pending
NIAP CC FDE EE	Drive Related
SATA Operation Support	AHCI
Pre-Boot Authentication (PBA)	●
PBA Authorization Factors	Password, CAC/PIV smartcard, PIV-enabled Yubikey
Post-boot Authentication	Facial recognition, fingerprint, PIN, Duo
Languages	English
Crypto Erase	●
Erase Disk	●
Change Authentication Keys	●
Activity Log	●
Mass Deployment Support	●
Failed Logins Before Lockout	●
Failed Logins Before Disk Erase	●
Password History	●
Database Backup	●
Install and Update Integrity Validation	●
Password Complexity Options	Always requires 4 character types
Two-Factor Authentication	●
Bulk User Import	
Unreadable Storage Partition Protected by Non-Recoverable Key	●
OS/Hypervisor Support	Windows, Linux
Verified Device Erasure	●

Compliance Regulations

DIGISTOR Citadel C Series SSDs help you meet these regulatory requirements

Regulation	Summary
FAR	Federal Acquisition Regulation
DFARS	Defense Federal Acquisition Regulation
TAA	Trade Agreements Act –Designates countries products can be bought from
SATA Operation Support	AHCI
FIPS 140-2 Level 2	Security requirements that must be met by cryptographic (encryption) modules
NIAP Common Criteria FDE_EE*	USG protection profile for Full Drive Encryption
CSfC DAR Capability Package 5.0	NSA Commercial Solutions for Classified (CSfC) policy for Data at Rest (DAR)
PM 9-12	Guidance for sanitization of storage devices for disposal or recycling
NIST 800-171	Protecting Controlled Unclassified Information (CUI) on Nonfederal Systems
CMMC (Levels 1-5)	Cybersecurity Maturity Model Certification
Executive Order (EO) 14028 May 12, 2021	Presidential order to all USG agencies for Improving the Nation's Cyber Security

Use C Series with Cigent Plus

One year or three year subscriptions available

Enterprise Management Console

- Multi-tenant, hosted or on-prem
- Policy setting
- Threat and event reporting
- Notifications

Enhanced Security Capabilities

- Enterprise auth factors
- Integration with NGAV and EDR
- RESTful APIs for SIEM integration

Contact Us

+1 (360) 816-1800, Opt 2 | **sales@digistor.com | digistor.com**

1000 SE Tech Center Dr., Suite 160, Vancouver, WA 98683

Rev 2.1