DIGISTOR®
SECURE DATA STORAGE

Citadel™ C Series

Lock down access to critical data

DIGISTOR Citadel C Series SSDs, powered by Cigent®, prevent unauthorized access to sensitive data and applications.

SECURITY MADE EASY

With Citadel pre-boot authentication (PBA) a user must provide trusted credentials to the SSD itself before the computer can detect the presence of the SSD, let alone boot up. This prevents unauthorized users from gaining access to the encrypted drive and its data–even if the SSD is removed.

- **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

KEY FEATURES

- Simple, easy-to-use protection from ransomware, physical, and other cyber attacks
- Multi-factor authentication (MFA) requires more than one authentication for access. Multiple authentication methods include password, CAC/PIV smartcard, and PIV-supported Yubikey
- Worry-free deployment: NIAP- and CSfC-listed DIGISTOR SSDs are thoroughly tested easily integrated into off-the-shelf laptops and desktops
- Address critical requirements for data governance and privacy programs like CMMC, HIPAA, GDPR, GLBA, and DSS
- TAA compliant
- DIGISTOR FIPS 140-2 L2 SSDs are CSfC- and NIAP-listed and Common Criteria-certified via NIST (Certificate #4294)

Built-In Pre-Boot Authentication

Additional Authentication for File Access

Unreadable Storage Partition Renders Data Invisible

Non-Recoverable Key Protection

CONTACT US

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

FEATURES AND CAPABILITIES

Secure Data at Rest (DAR)

Feature	Citadel C Series
Pre-Boot Authentication (PBA)	✓
PBA Authorization Factors	Password, CAC/PIV smartcard, PIV-enabled Yubikey
NSA CSfC-listed	✓
NIAP CC FDE AA	✓
NIAP CC FDE EE	Drive Related
FIPS 140-2 L2 Certified	✓
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	✓
Unreadable Storage Partition Protected by Non-Recoverable Key	✓
OS/Hypervisor Support	Windows, Linux
Verified Device Erasure	✓
SATA Operation Support	AHCI

COMPLIANCE REGULATIONS

Citadel C Series SSDs help meet regulatory requirements

Regulation	Summary
FAR	Federal Acquisition Regulation
DFARS	Defense Federal Acquisition Regulation
TAA	Trade Agreements Act – Designates countries products can be bought from
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

TAA COMPLIANT

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

DIGISTOR®
SECURE DATA STORAGE