CIGENT®

AlwaysPROTECTED™

Securing Mission Data

May 2025

Cigent Overview

CIGENT®
AlwaysPROTECTED™

Protects mission data with integrated Secure Storage Solutions providing layered protection

- Founded by leading expert in data recovery and sanitization for and with top Federal agencies
- Cleared personnel (TS/SCI) with decades of DoD and IC mission and data protection experience
- Data-at-rest encryption with advanced threat protection, data access controls, and sanitization capabilities
- Extensive ecosystem of OEM device and FSI partnerships

Increasing Challenge of Securing Mission Data at the Edge

Proliferation of devices operating at the edge…

PCs, Workstations, Enterprise Storage

Manned and Unmanned Vehicles

IOT and ICS devices

…That are collecting, storing, and processing sensitive data…

Expanding Impact of AI

- Protection of Classified, CUI, and PII data
- Protection without compromising mission operations
- Protection across all stages of the data lifecycle

…Requiring protection for data-at-rest, in-use & at end of life

Advanced Data Recovery

Insider Threats

Data Sanitization

Compliance Requirements

CIGENT

Cigent Mission: Protect Sensitive Data at the Edge

Data-at-Rest Protection

CSfC for DAR Compliance

Inner & Outer Required Protection Layers

Data Access Control

Zero-trust Access Mitigates Risk

Data Segmentation, Control & Log Access

Verified Data Sanitization

Recycle, Repurpose, Emergency

Crypto & Block Erasure with Verification

Administration at Scale with Command Line Interface

Cigent Data Protection Portfolio

Cigent Secure Storage

Portfolio of SSDs delivering full drive hardware encryption protection

- Include **Cigent PBA**
- **Secure Firmware** addresses advanced data recovery and quantum threats
- PCs, Workstations, Servers coverage with multi-drive (RAID) support

Pre-boot Authentication

- Software enabling SSDs
- Secure authentication environment
- Required for CSfC for DAR outer-layer

Software Full Drive Encryption

- Pre-OS authorization and MFA capabilities
- Independent crypto-library from Cigent SSDs
- Required for CSfC for DAR inner-layer

All offerings include Command Line Interface

CIGENT

Cigent Protects Data on Extensive Range of Devices

Traditional Computing

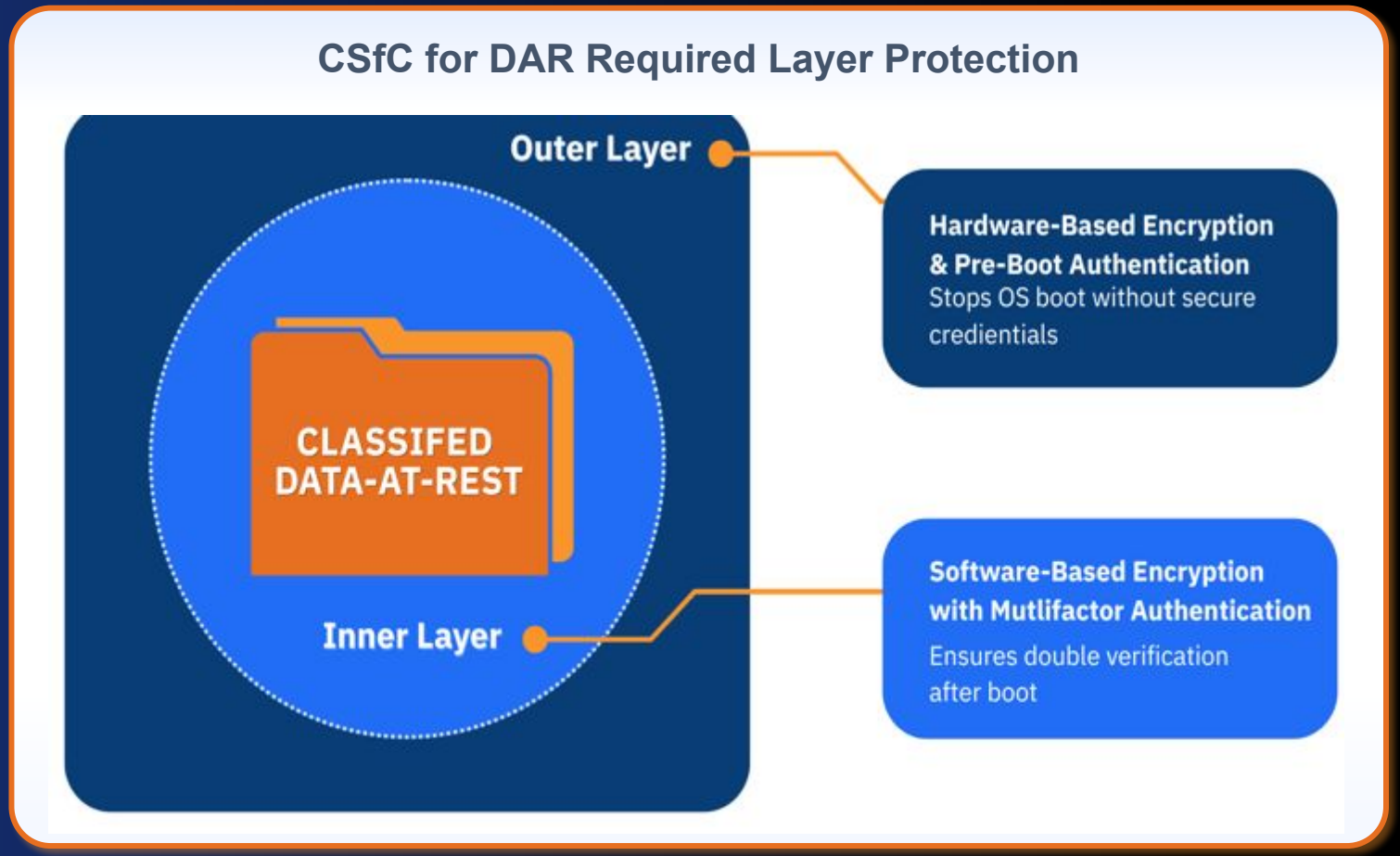
- Address CSfC for DAR compliance
- Multi-drive (RAID) support
- Simplify administration
- Streamline acquisition & deployment

Emerging Markets

- DAR protection for high-risk assets
- Automotive standards for extreme environments
- Data segmentation, access control & logs
- Emergency data sanitization

Data-at-Rest Protection for CSfC Compliance

- Multiple layers of quantum-resistant encryption validated by NSA, NIAP
- Cigent meets NSA “manufacturer diversity requirement” to provide single CSfC DAR solution
- Alternative option to utilize Cigent PBA and FDE with partner validated SSDs



Data Access Control

1. Drives can be partitioned with distinct access controls
2. Locked partitions cannot be cloned or wiped; are not even visible to adversary
3. Step-up authentication required to access partitions
4. File-level encryption maintains encryption when data is exfiltrated
5. Encrypted data access logs record all activity – can be exported for analysis, used for forensics

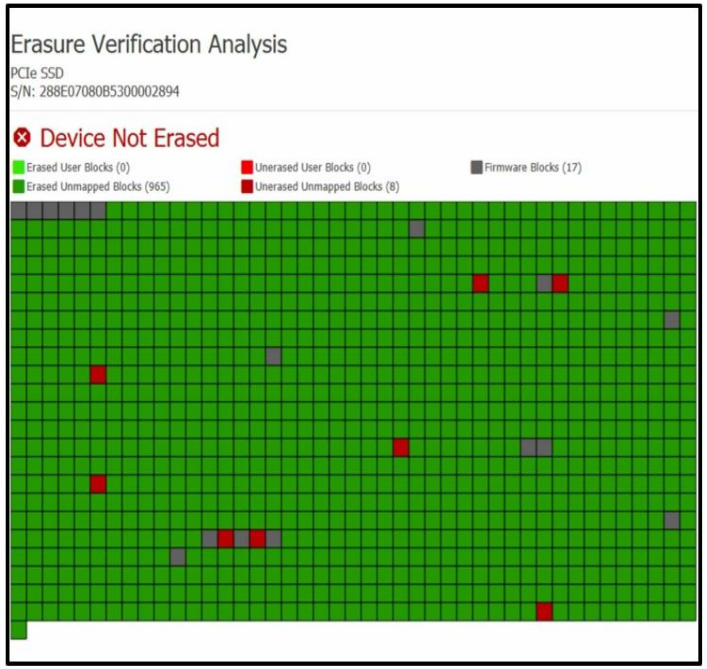
- Limit risk of malicious code insertion
- Prevent cloning and wiping attacks
- Mitigate risk of accidental or intentional data leakage
- Protect against insider threats

Verified Data Sanitization

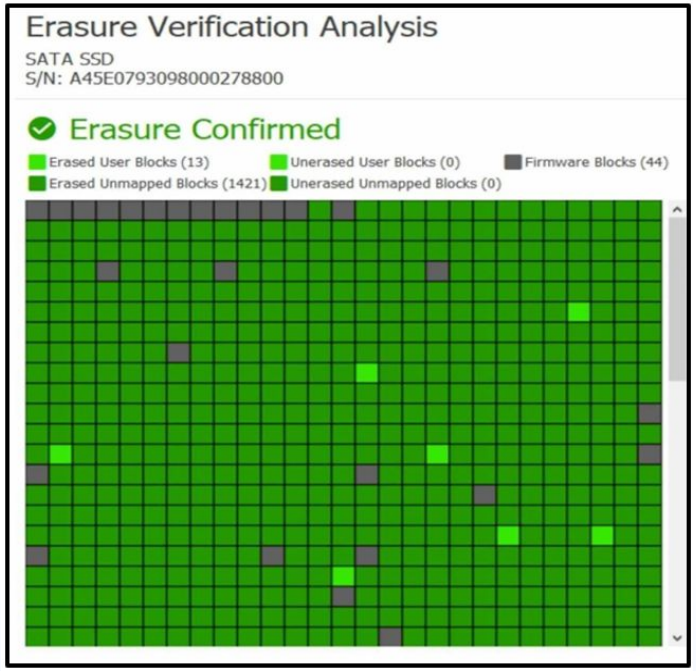
- Crypto erasure for instantaneous protection
- Block erasure for firmware data destruction
- Patented data verification to ensure all data erased
- Local, remote or rules-based execution
- Recycle or repurpose EOL drives | emergency sanitization

CSfC for DAR Required Layer Protection

Unsuccessful Data Erasure



Successful Data Erasure



Cigent Solutions Deployed Across US Defense Sector

US Federal Government













Federal System Integrators

CIGENT

Cigent Data Solutions for Data Protection

Single Solution

Cigent delivers hardware encryption, authentication, and encryption software to protect data at rest and meet CSfC compliance

Data Lifecycle Protection

Cigent solutions ensure DAR integrity with features to protect data when devices are in-use and at end-of-life

Streamline Procurement

Partnerships with leading device OEMs including Dell, HP, Getac, and Panasonic provides access to SSDs and software with PCs and Servers

Expertise & Experience

US-based and staffed organization with leading experts in data protection and cleared personnel to support US agency requirements

CIGENT

Back-up

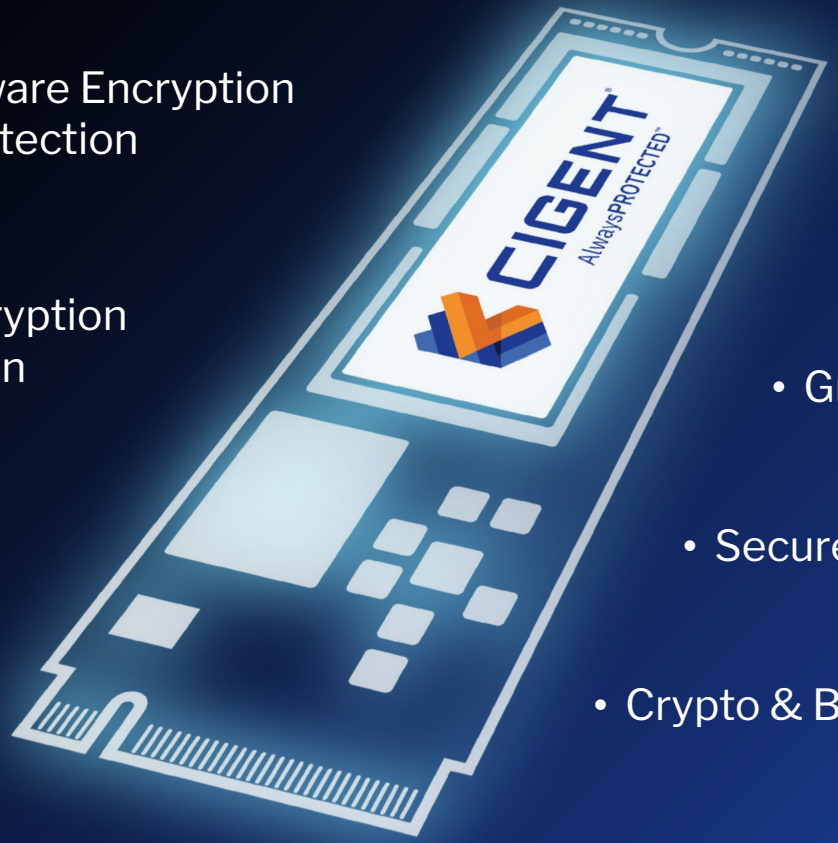
Cigent SSD Portfolio

	Capacity	CSfC Cert Status	Temp Ranges
M.2 2230	64 GB, 128 GB, 256GB, 512GB, 1TB	NIAP FDE_EE+AA Security Target 1.0 document (Oct 2024)	Automotive: -40°C to 105°C
M.2 2280	256GB, 512GB, 1TB, 2TB	NIAP FDE_EE+AA Security Target 1.0 document (Oct 2024)	Automotive: -40°C to 105°C
U.2, E3.S	1.92TB, 3.84TB, 7.68TB, 15.36TB	CSfC DAR Capability Package 5.0 for PBA Authorization Acquisition	Industrial: -20° C to 85°C

Cigent Data Protection Capabilities

CSfC for DAR Requirements

- Full Drive Hardware Encryption
  - outer layer protection
- Full Drive Software Encryption
  - inner layer of protection
- Pre-boot Authentication
- Multifactor Authentication



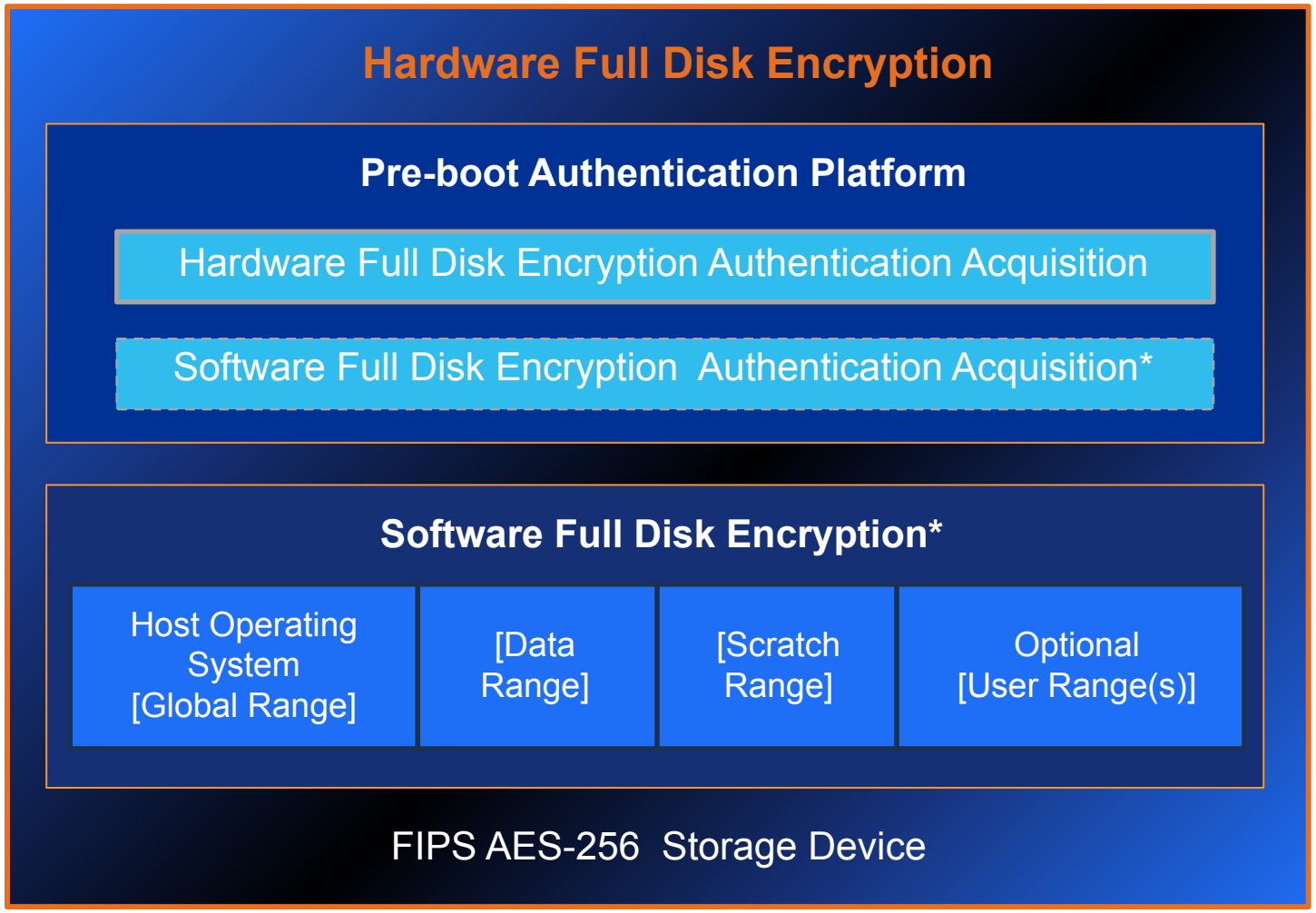
Advanced Data Protection

- File level Encryption
- Hidden Drive Partitions
- Granular Access Controls
- Secure Data Access Logs
- Crypto & Block Erase | Verified Sanitization

10 Patents Awarded, 5 Pending

CIGENT

Cigent Secure Storage Solution Architecture



*Software Full Disk Encryption Under Development (target Q1 GA)

- All primary storage ranges locked
- Shadow partition running Linux + Cigent PBA software
- All data encrypted on drive (protects against direct physical attacks)
- Range 0 locks all drive including “sub-ranges”
- Range 1, 2… (up to 8 unique and individual)
- Admin User and End User auths
- SSD firmware improvements to meet FIPS, NIAP CC FDE_EE, CSfC are activated by Cigent software

CIGENT

Cigent Software Data Protection for Data at the Edge

Protects sensitive data and meet CSfC for DAR compliance requirements

Pre-boot Authentication

With Cigent SSD provides outer-layer of CSfC DAR protection

Separate, secure environment for drive authentication

Prevents adversary from compromising OS boot

Software Full Drive Encryption

Provides inner of CSfC DAR protection

Deploy independently or complements SSD

Multifactor authentication: U/N Password and smart card (CAC) or security key

Advanced Threat Protection*

Prevent clone & wipe: create unreadable hidden partitions

Insider Threat: encrypted log files recording data transactions

Data sanitization: patented verification of data erasure by block

Windows & Linux • RAID Server Coverage • On prem enterprise mgmt. • Command Line Interface

*Available with optional software when using Cigent Secure Storage or Digistor Citadel Drives

CIGENT

Cigent Defense Market Messaging

Portfolio – what we offer

Cigent Secure Storage

Portfolio of SSDs providing full drive hardware encryption protection with multiple NSA NIAP validated drives.

- All Cigent SSDs include **Secure Firmware** addressing advanced data recovery and quantum threats
- All SSDs include Cigent PBA

Cigent PBA

Pre-boot authentication provides secure environment to authenticate SSD providing outer protection layer. PBA validated by NSA and NIAP.

Software FDE

Cigent Software full drive encryption provides separate inner-layer of protection with multi-factor authentication. FDE is being validated by NSA and NIAP.

Value Drivers – customer benefits

Secure Data at Rest

Layered protection of software and hardware encryption and authentication.

Provides single solution for CSfC for DAR outer and inner layer protection

Data Access Control

Zero-trust access mitigates risk of data loss with data segmentation, access control and secured data logs

Verified Data Sanitization

Address compliance mandates and emerging quantum threat with only firmware verification that all data has been eradicated

Administration at Scale

Command Line Interface (CLI) seamless integrates within existing management providing efficient administration at scale

Differentiation – our unique capabilities

Single Solution

Cigent provides SSDs, authentication, and encryption software to protect data at rest and meet CSfC compliance

Data Lifecycle Protection

Cigent solutions ensure DAR integrity with features to protect data when devices are in-use and at end-of-life.

Streamline Procurement

Partnerships with leading device OEMs including Dell, HP, Getac, and Panasonic provides access to SSDs and software with PCs and Servers

Expertise

US-based and staffed organization with leading experts in data protection and cleared personnel to support US agency requirements