CIGENT®

AlwaysPROTECTED™

Securing Mission Data

April 2025

Cigent Overview

CIGENT®
AlwaysPROTECTED™

Protects mission data with integrated Secure Storage Solutions providing layered protection

- Capabilities developed for and with top Federal agencies
- Cleared personnel (TS/SCI) with decades of DoD and IC mission experience
- IQT & US DOD Phase I and Phase II SBIRs completed contracts (Phase III IDIQ $100M award in process)
- Prime or subcontractor on multiple contracts (including additional OTA and ATO for DAR solutions in process)
- Extensive ecosystem of integrations with leading suppliers

Cigent Customers

US Federal Government















Federal System Integrators



CIGENT

Recent Cigent Projects

DISA WINDAR with AT&T BPA

Many Deployed FIPS-secure PCs

MSTIC for OT ICS DAR Solutions

Manned & Unmanned Vehicle Project

Flyaway Kits and Edge Data Centers

Overseas Travelers Data Security

Increasing Challenge of Securing Mission Data at the Edge

Proliferation of devices operating at the edge…

PCs, Enterprise Storage, External Media

Manned and Unmanned Vehicles

OT and ICS devices

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

Expanding Impact of AI

- Protection of Classified, CUI, and Sensitive 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

Device Sanitization

Compliance Requirements

CIGENT

Cigent Device Coverage

Secure Mission Data across Edge Devices

PCs

Integrated Solution

Dual DAR CSfC: inner & outer layers

Enterprise Key Management

Servers

X2 Controller Speeds

RAID Dual DAR CSfC: inner/outer

Enterprise Key Management

External Media

Clone/Wipe/Hex Reader Prevention

Secure Key Storage

Multiple Hidden Partitions

Vehicles Manned & Unmanned

Hidden Data Partitions

Automated Erasure

Automotive Grade Temperature

Industrial Control Systems

Read-only Mode

Malware Prevention

Insider Threat Logs

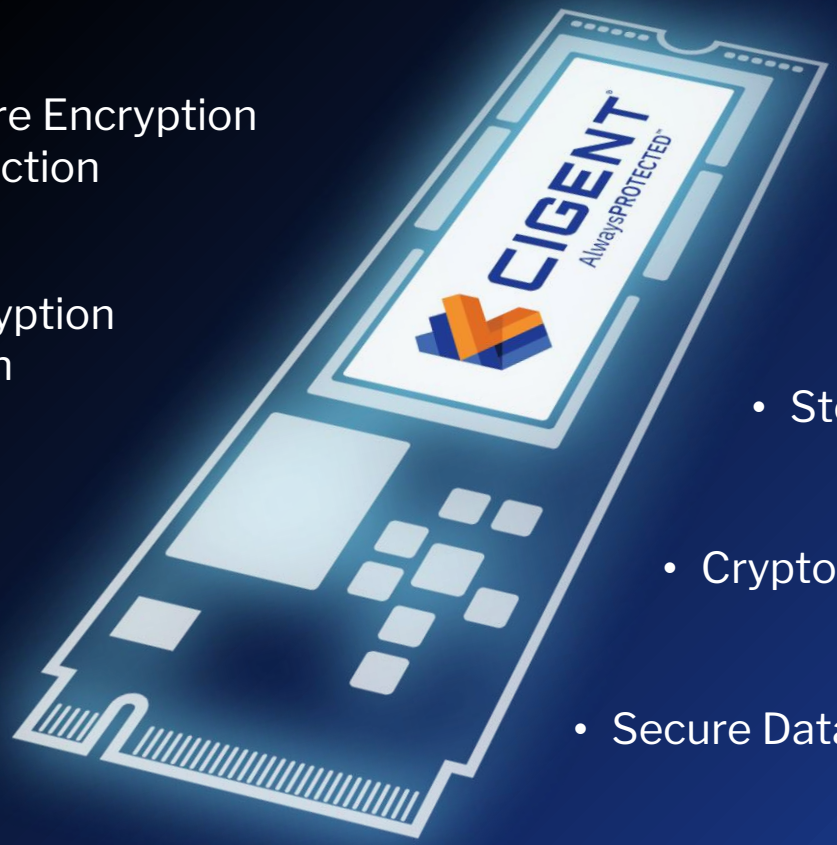
The Cigent Mission

Secure mission data on edge devices from all threats

- Classified, CUI, & Sensitive data protection
- Lifecycle data protection:
  - Encrypted data-at-rest (three layers)
  - Protects data when device is in use
  - Prevent and detect insider threats
  - Verified device sanitization for ops/repurpose
- Extensive breadth of coverage including traditional and emerging compute devices

Cigent Secure Storage Solutions

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



- Hidden Partitions
- Wipe & Clone Prevention
- Storage Embedded AI Data Monitoring
- Crypto & Block Erase | Verified Drive Sanitization
- Secure Data Access Logs

10 Patents Awarded, 5 Patents Pending

ONLY SOLUTION WITH INTEGRATED HARDWARE & SOFTWARE CAPABILITIES

CIGENT

Encryption Protection for Data-at-Rest

Meet compliance requirements | Protects data when device is compromised

Capabilities

- Three-layers of encryption: hardware FDE, software FDE, file
- Provides CSfC DAR inner & outer layer protection
- Crypto methodology validated by NSA, NIAP
- Pre-boot authentication and multifactor authentication

Benefits

- Secure Classified, CUI, & PII data against unauthorized access
- Layered security prevents even advanced adversary attacks
- NSA component list for CSfC for DAR, NIAP, FIPS 140-2
- Quantum resiliency and attack avoidance

Hidden Partitions Secure Essential Data

Drives and data undiscoverable | Protection when device is in use

Capabilities

- Hidden partitions that are unreadable at sector level
- Drives ranges are locked preventing Hex reader access & cloning
- Ranges remain locked while device is in-use with access authorized via step-up authentication
- Up to eight ranges on SSDs

Benefits

- Adversary unaware sector (and data) even exists
- Additional protection vs advanced data recovery techniques
- Create read-only environments for O/S, application code, system files
- Prevents cloning and wiping and other data attacks

CIGENT

Verified Data Erasure for Device Sanitization

Emergency data destruction | Drive reuse, repurpose, recycle

Capabilities

- Crypto wipe and full block-level erasure
- Patented, firmware verification that data has been permanently deleted with block-by-block scan
- Verified erasure documentation
- Can be securely executed remotely or on device pre or post boot

Benefits

- Efficient emergency data destruction capability with verification
- Allows drives to be safely repurposed or recycled
- Eliminates risk from future quantum computing capabilities
- Past performance by DoD for data destruction in TS environment

CIGENT

Data Logs for Insider Threat Protection

Prevents malicious actors from covering their tracks

Capabilities

- All data access recorded in encrypted, inaccessible logs
- Data access is logged even if adversary boots from external drive
- Logs can be exported to SIEM for ongoing analysis

Benefits

- Provides uncorruptible documentation of all data access
- Log data can identify anomalous activity, providing proactive prevention
- Invaluable post-breach forensics data for incident response, non-repudiation, and litigation

CIGENT

Enterprise Management

Multiple management approaches to align with your mission

Capabilities

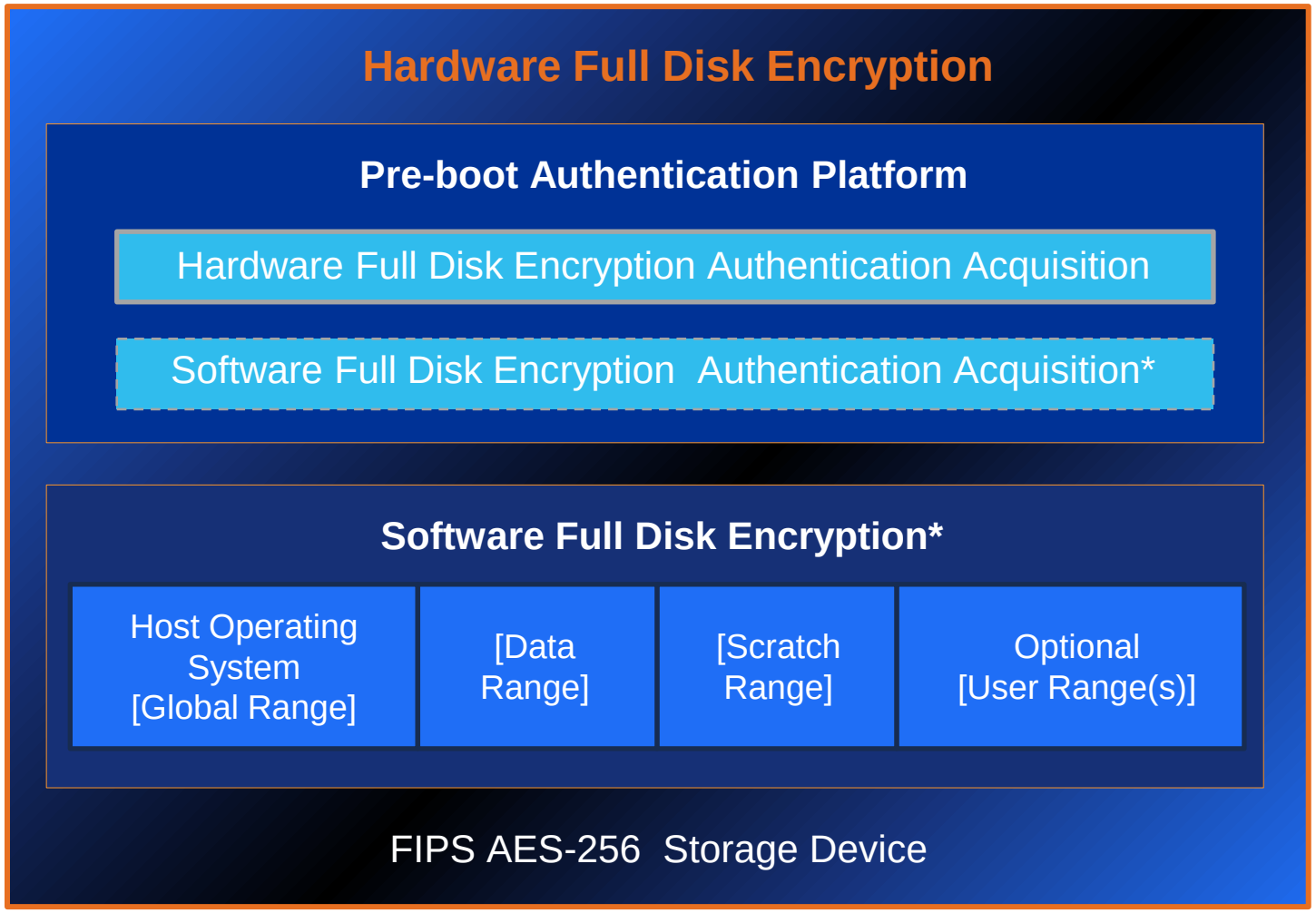
- Enterprise management console: on-prem or in cloud
- Remote key management and recovery, policy setting, PBA administration, compliance reporting
- Command line interface (CLI) for device administration and command automation

Benefits

- At-scale or device specific management options
- Securely and efficiently administer all elements of data protection
- Supports portfolio of Cigent and partner drives – PCs, Servers, Removable Media, Embedded

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

THANK YOU!

mission@cigent.com

(669) 400-8127

www.cigent.com

Cigent Capabilities

Mission–centric Organization

- Vertical integration with single hardware & software solution for data protection
- Keeps data protected with three-layers of encryption with PBA and MFA
- Enterprise management for efficient administration at scale
- Ecosystem of SI and device OEM partners for efficient procurement and support
- Team of US-based data protection experts with security clearance

Securing Mission Data

Protect data at rest, in use and end of life

Integrated , Layered Protection

- Three layers of encryption, PBA, and MFA
- Keeps data secret with hardware-based, hidden partitions
- Insider threat detection, tracking, & prevention utilizing secured data logs
- Device sanitization with automated emergency data erasure and verification

Mission-Centric Organization

- Operational experienced data experts with clearance
- US-based, “made in America” software development
- Simple procurement with ecosystem of FSI and OEM device partners including Dell and HP
- Mission-specific custom software and firmware capabilities

CIGENT

Expertise and Support

Support and guidance | Custom solutions

EXPERIENCE	CLEARANCE	MISSION	ECOSYSTEM
Decades of US Federal operational experience	All US-based organization with TS/SCI cleared personnel	Mission-centric organization with custom-solution experience	Extensive partner ecosystem including Dell and CSfC partner devices