Protecting Sensitive Federal Data at the Edge

Executive Order 14028, “Improving the Nation’s Cybersecurity,” issued May 12, 2021 sets expectations for storage for sensitive, unclassified data. For all endpoints Federal organizations are to mitigate risk of data loss or compromise by adopting cybersecurity capabilities including full drive hardware encryption, pre-boot authentication (PBA, and multifactor authentication (MFA). These layered capabilities meet FIPS certification and EO 14028 requirements.

AES-256 Full Drive Hardware Encryption

FIPS 140-2 certified full drive hardware encryption is the foundation for protecting data on endpoints. Cigent encryptions uses proven methodology and technology ensures keys are inaccessible to advanced threat actors. Cigent encryption solution have been validated by leading Federal agencies including NSA, NIAP, and NIST.

PBA with MFA

PBA is a critical security capability that prevents adversaries from circumventing full-drive encryption. It provides a separate, secure authentication prior to initiating boot. PBA is completed with optional Multifactor Authentication (MFA), requiring the use of both a U/N Password and a smart card (CAC). Like encryption methodology and technology, PBA has been validated by Federal agencies.

To ensure the integrity of sensitive data Cigent complement hardware encryption with unique, patented data protection capabilities.

Enterprise Administration

Cigent provides an enterprise management console that can be deployed in the cloud or on premises and a Command Line Interface (CLI) supporting key management, compliance reporting, policy setting, and deployment automation.

Cloning and Wiping Prevention

Regardless of device state, data is unreadable, preventing data from being cloned or wiped. Hidden partitions uniquely protect sensitive data even when the device is in use.

Data Erasure

Data can be erased through a local or remote command utilizing crypto and full block erase. Provides emergency data erasure and can enable drive reuse.

Secure Command Logs

All data activity is recorded in secure, tamper-proof logs. Prevents malicious actors from “covering their tracks” with irrefutable documentation of activities.

WHY CIGENT?

Cigent provides unparalleled technology, ecosystem, and expertise to ensure your sensitive data is protected no matter what your mission. The Cigent solution was developed for and with US Federal agencies by leading experts in data recovery and sanitization. Cigent is a trusted partner in addressing your data protection at the edge requirements. We will work with you to understand your mission requirements and ensure you have data protection that will enable your success.

Book a demo today!