SECURING UXV DATA:

Comprehensive Protection for Critical Missions

UxVs store and collect critical, often classified data during missions.

Due to their mission parameters, this data is highly susceptible to recovery by adversaries. Unauthorized access can lead to significant consequences, including the compromise of algorithms and exposure of sensitive mission information—such as location, tactics, targets, and capabilities.

Many manufacturers lack the expertise to secure UxV data, with many relying on vulnerable mobile device platforms. Protecting UxV data is essential, but it must not disrupt operations and must extend across the entire UxV ecosystem of devices.

Why Cigent?

Cigent portfolio includes drives that meet automotive temperature standards, including M.2 2230 SSDs, SSD BGA, SD and Micro SDs.

Cigent solutions are validated and used by leading organizations, including the NSA, NIAP, and DISA. The Cigent team has decades of DoD and IC mission experience. Cleared personnel (TS/SCI) and a US-based software team can support mission-specific custom projects.

Cigent provides a layered approach inclusive of secure storage, firmware-rooted capabilities, and data access control software that secure UxV data.

Protect Data at Rest	Protect Data at Rest UxV data is secured with three layers of encryption including both hardware and software encryption. The solution meets NIST, FIPS, and CSfC DAR compliance requirements.
Ensuring Critical Data is Protected from Data Attacks	Cigent protection includes zero-trust access controls and isolated storage partitions. Capabilities ensure constant, secure availability of critical data only by trusted users and applications.
Insider Threat Mitigation	Cigent reduces the risk of insider threat by controlling access with segmented data access controls. Additionally, data access logs provide an uncompromised record of activity that can be exported for analysis and for event forensics.
Data Destruction	Crypto and block erasure, and patented firmware-based verification destroys data in seconds. Remote and automated execution capabilities.
Maintenance & Updates	To ensure data remains protected throughout the update and data lifecycle process, an ecosystem of secure storage for rugged laptops, tablets, and external media.

Contact Us
Phone: 669-400-8127 | Email: info@cigent.com

CIGENT