UxV Data Sheet

Problem Statement

UxV store and collect sensitive and classified data including applications, algorithms, mission, and target data stored for and captured during the mission.

UxV mission parameters guarantee many will be recovered by adversaries.

Unauthorized access to UxV data will have significant consequences. An adversary may gain unauthorized access to algorithms compromising UxV efficacy and access sensitive mission information including location, tactics, targets, and capability data.

UxV data is not being adequately protected. Manufacturers lack expertise in data protection with the widespread use of an insecure mobile device platform.

Mission requirements increase the complexity of protecting UxV data as they will be operating in extreme environments, require seamless experience for operators, and support autonomous operations.

Protection of UxV data must cover the full lifecycle of data including mobile workstations analyzing field telemetry and developing new algorithms, external media used to transfer data to UxV management systems and the UxV devices.

Cigent Capabilities

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** 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.
- **Seamless Operations** Protection is delivered without impacting operations or user experience. This is accomplished through integration with existing user workflows and automated authentication enabled by existing system components and user credentials.

- **Insider Threat Mitigation** Reducing the risk of insider threat requires controlling access and monitoring activity. Separate partitions provide for the segmentation of data and controlling access to required personnel. Data access logs provide an uncompromised record of activity that can be exported for analysis and for event forensics.
- **Data Destruction.** UxV operations make data destruction an essential element of each mission. Cigent implements erasure in seconds via cryptowipe, full block-level erasure, and firmware-based verification ensuring UxV with remote and automated execution capabilities.
- **Maintenance and Updates.** UxV will regularly be updated with mission requirements, algorithms, and new applications. To ensure data remains protected throughout the update and data lifecycle process, an ecosystem of secure storage for rugged laptops, tablets, and external media.

Portfolio

Cigent solutions include multiple secure storage form factors that meet extreme temperature environments. Portfolio includes M.2 2230, Embedded SSD BGA, SD Cards, and Micro SD Cards.

Additionally, Cigent provides secure storage options for the UxV ecosystem including PCs, Enterprise Storage, and External Media solutions.

CIGENT AlwaysPROTECTED™

Cigent provides unparalleled technology, ecosystem, and expertise to ensure your sensitive data is protected no matter what your mission. Partnering with leading UxV manufacturers, Cigent has developed technology and processes to support the unique nature of UxV operations.

The United States-based organization includes cleared personnel (TS/SCI) with extensive operational experience. Cigent can provide off-the-shelf capabilities or support custom projects.

Book a Demo