GuardWare Suite facilitates Defence Data Strategy

The GuardWare suite of products has the potential to be a force multiplier tool for the Australian Government to achieve the vision set out in the recent Defence Data Strategy. A mapping of the functionality of the products to the five pillars (Govern, Trust, Discover, Use, Share) is provided below.

GuardWare INTEL - Affordable and unobtrusive visibility & control of data usage for compliance.

- Discover / initiative 1 - Monitors all movements and user interactions with sensitive data. Provides alerts in case of possible breaches.
- Govern - Helps organisations conform to ISO/IEC 27001, DISP, ITAR, NIST 800-171, ACSC ISM and CMMC.

GuardWare PROTECT – Tagging and protection of any type of data (raw data, xml, txt, source code, design files etc) within organisations.

- Trust / initiative 1 - Enables classification and meta data to be added to file types that do not natively support meta data, such as txt, csv, source code and xml files. This meta data follows the file wherever it is stored, when in use and when transferred.
- Trust / initiative 3 - Protects against leaks by defence acceptable level encryption. Provides identity assurance of end-users who are accessing the encrypted files.
- Trust / initiative 4 – Disposal of data at end of life through removal of access to file encryption keys.
- Discover / initiative 1 - Automatically discovers, classifies and encrypts all types of files. Supports ad-hoc classification and encryption of files by users via 'right-click encrypt' options.
- Use / initiative 5 - Encryption is file-type and file-size agnostic, so can protect all files used by Defence including engineering files, large sensor data files, email archives, project files, office files, videos, source code, etc. Files do not need to be decrypted before use by data processing applications.
- Use / initiative 5 - Online and Offline modes of encryption. Online mode enables real-time control over user access to encrypted files. Offline mode provides time limited control over access to encrypted files but allows files to be opened or protected even when accessed on air-gapped pcs and networks.
- Govern - Provides full visibility on the location and usage of protected files, including tracking of changes and copies of the files.

GuardWare OVERSIGHT - Visibility and control over the usage and generation of unstructured data of any type (raw data, design files, xml, txt, sourcecode etc) throughout the Defence supply chain.

- Discover / initiative 1 - Automatically discovers, classifies and encrypts files of any type across the supply chain. Including new data being created as part of the project.
- Share / initiative 2 – Files can be shared securely with other organisations in the supply chain. All parties have independent visibility and control over the shared data.

- Trust / initiative 3 – Ability to control access of protected data of any type across the entire supply chain.
- Trust / initiative 4 - Enables data disposal of all copies of encrypted files across the supply chain at the end of a project
- Use / initiative 5 – Files can be shared for processing across the supply chain whilst remaining secure.
- Govern - Provides full visibility on the location and usage of protected unstructured data, including tracking of changes and copies across the entire supply chain.

Reference: https://www.defence.gov.au/about/publications/defence-data-strategy-2021-2023