

## Next Generation Data Protection

Cyber Reliant's data protection stays with data to keep information safe and industries thriving. We transform critical data to become completely unusable so it remains safe.

### Security that Stays with the Data

Data is protected when the device is powered off, on, and at runtime.

### Groundbreaking Technology

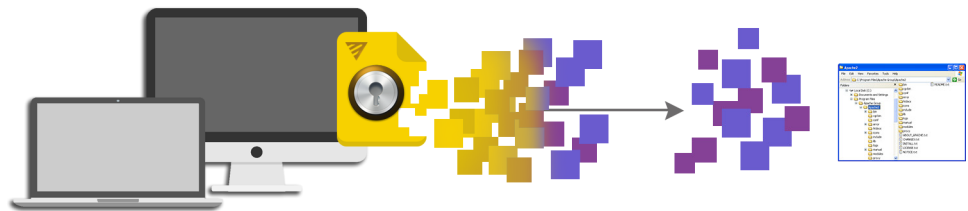
Encryption and shredding for secure storage prevents unauthorized users from accessing data on the device

### Easy to Configure; Seamless to Use

Scalable Deployments from individual device to the enterprise

## EdgeGuard for Windows

Through Cyber Reliant's leading-edge encryption and file shredding technology, EdgeGuard enables users to securely store data on their devices running Microsoft Windows to ensure critical data remains secure in the file system. EdgeGuard integrates seamlessly and complements existing security technologies.



Devices accessing critical data

Store Secure Shreds

**1**  
**Encrypts**  
files as they are saved to disc

**2**  
**Shreds**  
the encrypted files for storage

**3**  
**Stores**  
the shreds across the device file directory

**4**  
**Recombine**  
the shreds and decrypt for authorized user



### Protect at the File Level

Our solution captures data from desired applications and file types, encrypts and shreds the information, and disperses those data shreds across the system's persistent memory. This prevents exploitation of the data by exfiltration software.



### Distributed Across Storage

The data shreds of each file are dispersed utilizing a randomized information dispersal algorithm (IDA) after it has been encrypted. This ensures the data is not stored as a whole and eliminates the possibilities of recombining identifiable data.



### Strength of Security

Cyber Reliant offers defense-in-depth through multiple layers of cascading encryption keys, which are shredded along with the files. Our separate authentication serves as an additional countermeasure against hackers attempting to gain access at the file level.



### Security Stays with the Data

Whether an end-user device is powered off, on, or operating at runtime, Cyber Reliant provides highly transparent data protection for users, with no discernible latency.



## Cyber Reliant Architecture

**1** The **Management Service** centrally configures and manages the solution, as well as authenticates the user.

**2** EdgeGuard is installed on the device, it intercepts specified file types and application data. It then sends them to the encryption engine to be split and saved in a specialized file system.

**3** The **File System** is centrally managed and allows for the storage of encrypted and shredded data.



## Benefits

- Layered data protection
- Highly transparent to end-user
- Flexible licensing options
- Keeps PII and PHI data compliant, meets HIPAA, GDPR, PCI DSS, ISO 27000 series data protection requirements
- Obfuscation for tamper resistant code
- Multi-tenant support; each user has a unique keyset
- No modifications necessary to existing applications

## Features

- High-performance file I/O and cryptography
- FIPS 140-2 certified encryption module
- Randomized IDA with file shredding combined with AES 256 bit encryption
- Flexible configuration options to manage encryption rules
  - Directories, applications, file types
  - Folder Vault
- Robust data protection architecture, utilizing three layers of cascading encryption keys
- Obfuscates file shreds from the operating system
- Separate layer of user authentication required in addition to native device log-on
- File level fault tolerance to ensure data integrity

## Supported Platforms:



Windows 8.1 & 10

## About Cyber Reliant Corp

Founded in 2010, Cyber Reliant's next generation data protection stays with data to keep information safe and industries thriving. Cyber Reliant supports the classified or sensitive data protection needs of Government agencies (DoD and Intelligence communities) and companies in regulated markets, such as Healthcare and Financial Services.

