Armor Persistent Data Encryption

COMPLIANT ENCRYPTION SERVICES

Role-Based Encryption for the Cloud

Maintain peace of mind and exceed regulatory compliance requirements for sensitive data with Armor persistent data encryption.

Traditional logical encryption protects your organization from the unlikely physical theft of your data, or encrypts data while in an "off" state. This approach is inadequate when data lives in an always-on cloud environment.

Armor's role-based encryption protects your data at the file and folder levels while at rest and in an off state. Ensure data remains secure even if threat actors gain access.

Meet FIPS 140-2 Requirements

Armor delivers FIPS 140-2-level encryption with granular access control. This safeguards your organization from both physical and online threats in a manner that isn't available via simple whole-disk encryption. Granular access controls and permissions are simple to manage via an easy-to-use online interface.

Centralized Key & Policy Management

Leverage a centralized key and policy management system across your entire secure cloud infrastructure through a Data Security Manager (DSM).

An encryption agent is installed on each server and communicates with the central DSM to enforce granular policies and encryption keys. Create, store and manage encryption keys that protect your most sensitive data.

Safe & Compliant

Meet Safe Harbor requirements via file- and folder-based data encryption to protect your organization from data breach disclosure ramifications.

The solution is also compliant with PCI, HIPAA and SOX encryption requirements, and boasts a 100 percent success rate for compliance audits when configured properly.

What is FIPS 140-2?

The Federal Information Processing Standard, or FIPS, is a U.S. government computer security standard used to accredit cryptographic modules. Publication 140-2 defines its four standard security levels.

ONLY AVAILABLE FOR

Armor | Complete

ARMOR™

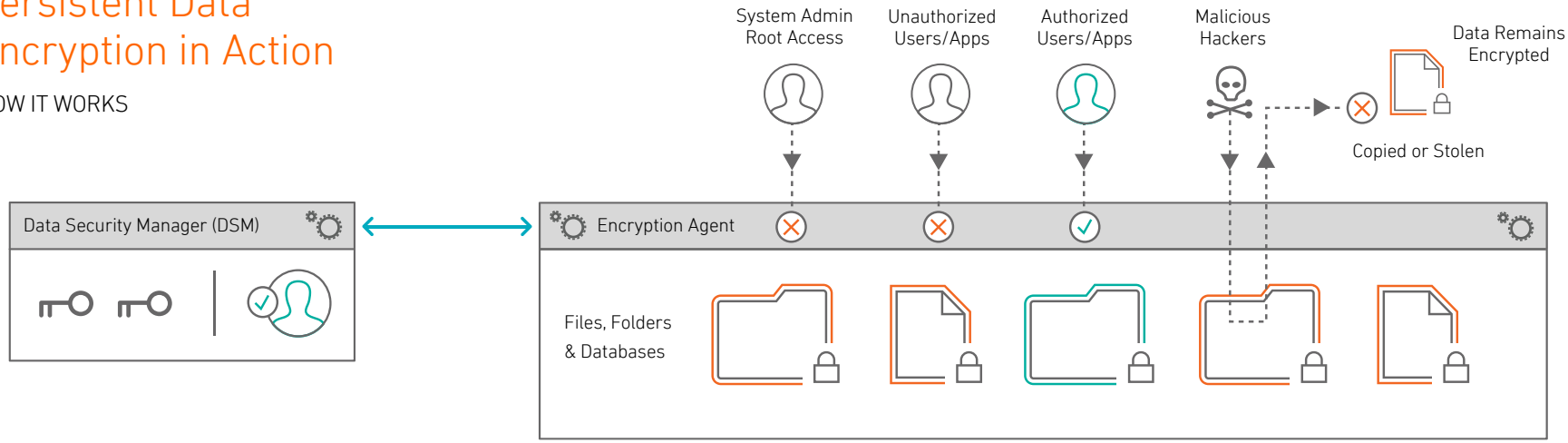
armor.com (US)+1 844 682 2858 (UK)+44 800 500 3167 @armor

Armor Persistent Data Encryption

COMPLIANT ENCRYPTION SERVICES

Persistent Data Encryption in Action

HOW IT WORKS



Manage Access Controls

Armor persistant data encryption includes granular access controls to ensure only authorized accounts may access decrypted data. The solution also guarantees that all data remains encrypted — even if it's removed from the original disk. Regulatory compliance auditors prefer this method of persistent encryption as opposed to whole-disk encryption methods.

- MEETS FIPS 140-2 STANDARD
- 100% COMPLIANT
- SAFE HARBOR PROTECTION
- ZERO-TOUCH INSTALLATION

ONLY AVAILABLE FOR

Armor | Complete

armor.com (US)+1 844 682 2858 (UK)+44 800 500 3167 @armor