

# DataArmor



## DataArmor™ is a policy-driven Full Disk Encryption solution for PCs, Laptops, Notebooks, Tablets and Smartphones

- Pre-boot authentication prevents unauthorized users from accessing data on the device
- Device wipe feature disables device
- Centralized administration and key management
- Extensive device-specific auditing and reporting

## Complete Data Protection for PCs, Notebooks, Laptops and Tablets

Mobile Armor provides comprehensive data protection for PCs, notebooks, laptops, tablets and Smartphones with DataArmor™, a centralized, policy-based full disk encryption solution. DataArmor is equipped with full AES 256-bit encryption and a robust set of authentication methods to provide organizations with unparalleled protection for data at rest, data in use and data in motion. DataArmor is also integrated with the Policy Server to provide remote management capabilities and extensive auditing and reporting features on devices deployed throughout the enterprise.

With DataArmor, unauthorized access to data on the hard drive or device is eliminated with enhanced security measures that detect and protect stolen computers and devices. The pre-boot authentication feature enforces policy-driven access control that is checked immediately when the hard drive powers up so that the device can be locked at pre-boot, preventing unauthorized users from logging on to the device. For additional layers of data security, the administrator can send a device wipe message that disables the hard drive so data on lost or stolen computers and devices cannot be accessed.

DataArmor is fault tolerant and completely transparent to end users, providing total protection of sensitive data wherever it

travels. The highly scalable solution is centrally managed from a single management console, a single management server and a single management agent, enabling security administrators to conveniently manage security policies, enforce compliance and produce management reports across multiple hardware configurations and operating systems.

DataArmor's centralized administration allows IT professionals to easily deploy the solution: Depending upon the drive size, DataArmor typically encrypts a hard drive the first time within two hours and the encryption can be performed while the computer or device is being used.

### DataArmor Features

- Centralized administration and key management via a Policy Server
- Device wipe/kill functionality
- Over the air deployment for Smartphones
- Device-specific auditing and reporting
- Supports multiple hardware configurations and operating systems, including Windows Mobile
- IPv4 and IPv6 compatible
- Pre-boot Authentication methods
  - Fixed Passwords
  - Smart Card (CAC & PIV)
  - Active Directory Domain Password
  - Color Code, PIN, RSA
- Tamper proof and fault tolerant
- Reduced sign-on capability to pass through Windows login

## Mobile Armor Validation and Industry Certifications

Mobile Armor strives to provide its customers with solutions that meet the highest standards in the industry. The superiority of Mobile Armor solutions is validated through the achievement of the most stringent certification guidelines in the industry:

Common Criteria EAL4+ (in final review)

Federal Information Processing Standard (FIPS) 140-2 Level 1 & Level 2

National Institute of Standards and Technology (NIST) certified and approved.

DARTT Validation: The US government's Data at Rest Tiger Team ("DARTT") selected Mobile Armor from over 800 vendors to be one of nine encryption providers to the U.S. government.

### Specifications

#### Hardware Requirements:

- Pentium III class (or equivalent) or above
- 256 MB memory
- 4 GB (IDE and SATA) drives
- Video card with XVESAs compliance

#### Operating Systems:

- Windows Vista
- Windows XP
- Windows 2000
- Windows Mobile

#### In Development:

- Mac OS X
- Linux – SUSE 10
- Linux – RHEL 5
- Linux – RHEL 5

#### System Requirements:

- Microsoft® .NET Framework 2.0 SP1 or higher installed

### Management Server Features and Benefits

- Highly scalable and easy to deploy - Enables large-scale deployments and live, operational rapid deployment capability; lowers total cost of ownership.
- Centralized administration and key management - Administrators manage all users and devices through a single management interface using Microsoft Management Console.
- Extensive auditing and reporting - Provides audit trail, compliance, and system metric reports to management that help define and facilitate regulatory requirements.
- Simplified password management - Offers several password reset choices for users to change password securely without administrator intervention.
- Enhanced security - Offers pre-boot authentication that prevents unauthorized data access; security measures detect and protect stolen devices.
- Service Oriented Architecture (SOAP/XML) - Features Active Directory Integration, administrator hierarchy and no Schema Change.



Mobile Armor provides the most comprehensive Data Protection Solution to ensure that sensitive and confidential data is secure and protected at all times. Entirely built in the USA, Mobile Armor's Data Protection Suite protects sensitive data on PCs, Laptops, Notebooks, Internal Hard Drives, External Hard Drives, Blackberrys, Smartphones, Removable Storage Devices and PDAs, and provides extensive auditing and compliance reporting. Mobile Armor's solutions are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe. **Your Data. Secure. Anywhere. Anytime.**