

The Leader in Endpoint Data Protection

Hard Disk Encryption

In addition to the danger of losing critical IP and customer or competitive information, data stored in an unprotected state on your laptop and desktop PCs puts your organization at risk of becoming the next data breach headline. The only sure way to counter these threats is with strong encryption of all data on hard disks, which also provides a “safe harbor” from the high-profile public disclosures and costly remediation mandated by privacy laws.

GuardianEdge Hard Disk Encryption provides exceptionally manageable, policy-controlled protection against loss or theft of data on laptop and desktop PCs. This mature solution builds on over 13 years of experience in creating and deploying hard disk encryption products. It delivers strong encryption as well as transparent operation to end users, pre-boot authentication, single sign-on integration, multiple user/administrator support, and a rich administrative and management environment. When combined with GuardianEdge Advanced Authentication, it also provides extensive token card and reader support for extended access security with multi-factor authentication.

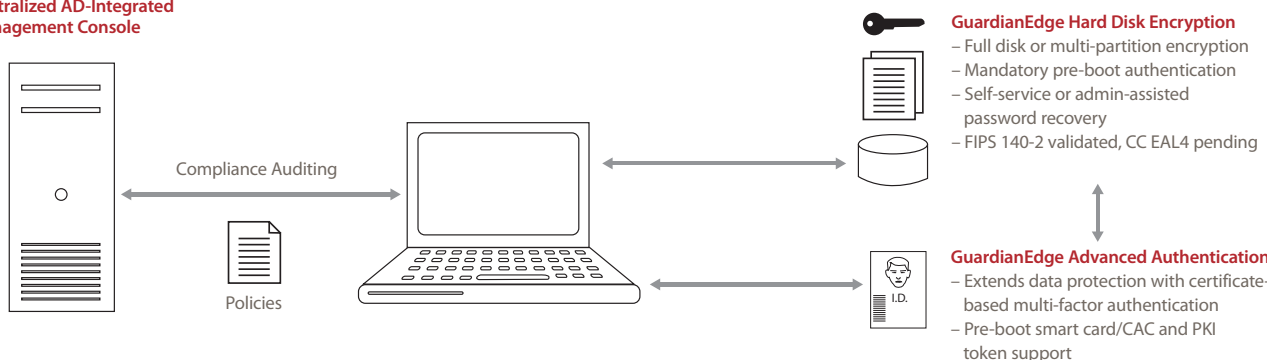
As a key component of the GuardianEdge Data Protection Platform, GuardianEdge Hard Disk Encryption delivers enterprise-grade manageability with fully integrated data protection controls and close integration with Microsoft® Active Directory®.

Key features

- True full disk or multi-partition encryption
- Mandatory pre-boot authentication
- Superior admin-assisted or self-service Authenti-Check™ password recovery
- Microsoft Active Directory-integrated enterprise management console
- Multi-factor authentication available when combined with GuardianEdge Advanced Authentication

Enterprise-Class Protection Against Data Loss

Centralized AD-Integrated Management Console



Technology Overview

GuardianEdge Hard Disk Encryption delivers an enterprise-class software solution designed to safeguard sensitive, private and legally protected data against loss from laptop and desktop PCs.

Close integration with Microsoft Active Directory means policies are easily managed and deployed via GPO, and can be granularly applied against groups, domains, organizational units and other Active Directory management structures. Software deployment and updates are performed with standard system tools (SMS, Active directory GPO, etc.).

The GuardianEdge management console provides a simple-to-use and familiar administrative interface that makes it easy for security and network administrators to create and deploy policies, monitor the status of machines, and assist users in recovering forgotten passwords.

Technical Information

Client Environment

- No additional log-in required (integrated with Microsoft Single Sign-On)
- Negligible performance impact
- Secure client/server communications
- Power failure protection for computers without a battery or backup power source during initial encryption

Pre-boot Authentication

- Microsoft Single Sign-on integration
- Password authentication
- Wake on LAN capability for seamless operation with enterprise patch and update management tools
- Lockout on maximum time-since-last-check-in exceeded (configurable)
- Password entry delay on failed password attempt threshold (configurable)
- Multiple user and administrator accounts (50 each)

Encryption

- Full disk or multi-partition including: master boot record, OS and system files, swap/hibernation files
- 256- or 128-bit AES
- FIPS 140-2 validated cryptographic library
- Common Criteria EAL4 pending

Key/Password Administration and Recovery

- Secure, self-service GuardianEdge Authenti-Check™ or administrator-assisted password recovery
- Recovery of encrypted data in the event of lost tokens or passwords

Administrative tools

- MMC management snap in architecture
- GPO policy deployment extensions
- Capability to remotely disable authentication of a targeted user
- Hard drive access tool to allow OS repair
- Integrated with forensic data recovery tools to retrieve data from crashed or evidential hard drives
- Remote, one-time password capability
- Integration with enterprise-grade deployment tools such as SMS, Tivoli, Altiris
- Real-time audit logging: policy changes, user actions (succeeded/failed authentication, attempts to uninstall the product, password recovery, change of password)

GuardianEdge Data Protection Platform

- **Single Management Console** – Provides a single, Active Directory integrated management console for administering the GuardianEdge suite of endpoint data protection controls
- **Shared Services** – Shared security and management services across data protection applications
- **Auditing and Reporting** – Unified auditing and reporting environment

Active Directory Integrated Administration and Management

- Tightly integrated with Active Directory, enabling GPO-based policy deployment
- Role-based policy administration
- Detailed audit records to verify policy enforcement
- Role-based control over security policies and recovery of encrypted disks and data

Client Computers

- Microsoft Windows™ XP Professional, Windows XP Tablet Edition, Windows 2000, Windows Vista

GuardianEdge Management Server

- Microsoft Server 2003 Standard or Enterprise
- Microsoft XP Professional

GuardianEdge Server

- Microsoft Server 2003 Standard or Enterprise for Active Directory Application Management module

GuardianEdge Advanced Authentication Integration

Extend data protection with certificate-based multi-factor user authentication by combining GuardianEdge Hard Disk Encryption with GuardianEdge Advanced Authentication.

Key features enabled by this combination:

- Pre-boot environment multi-factor authentication
- Smart card/common access card (CAC) support
- Extensive support for readers and tokens
- PKI environment support

Corporate Headquarters

475 Brannan St., Suite 400
San Francisco, California
94107-5421

t. +1.800.440.0419

t. +1.415.683.2200

f. +1.415.683.2349

www.GuardianEdge.com

GuardianEdge and Authenti-Check are trademarks of GuardianEdge Technologies Inc. All other products and services mentioned are the trademarks of their respective companies.