

GuardianEdge Hard Disk Encryption

Comprehensive Mobile Data Loss Protection

GuardianEdge Hard Disk Encryption—a key component of the GuardianEdge Data Protection Platform—allows enterprises to maximize the productivity of mobile computing while avoiding loss of confidential data and resulting mandatory disclosure law costs. As the first full-disk encryption software solution developed specifically for the enterprise, it combines strong encryption and access control in a managed environment that delivers comprehensive protection for laptop, desktop and tablet PCs.

By deploying GuardianEdge Hard Disk Encryption, organizations can:

- » **Prevent** data loss due to theft or accidental loss of laptop computers
- » **Assure** that data stored on laptops and desktops is accessible only to authorized users
- » **Leverage** a common enterprise-grade management and monitoring platform across multiple data protection controls
- » **Protect** trade secrets, intellectual property, and sensitive customer and employee information.

Benefits

- » Gain a competitive advantage by optimizing the benefits of mobile computing
- » Eliminate the legal liability, customer service costs and other ramifications of data breach disclosures
- » Reduce the cost of meeting regulatory compliance requirements for data security and privacy by leveraging existing IT infrastructure
- » Strengthen investor confidence and prevent brand erosion

Protection from the High Costs of Security Breaches

Laptop computers are more expensive than they look. When you add the value of the intellectual property and other sensitive data stored on the hard disk, the value of the data on a typical enterprise machine may exceed a million dollars.

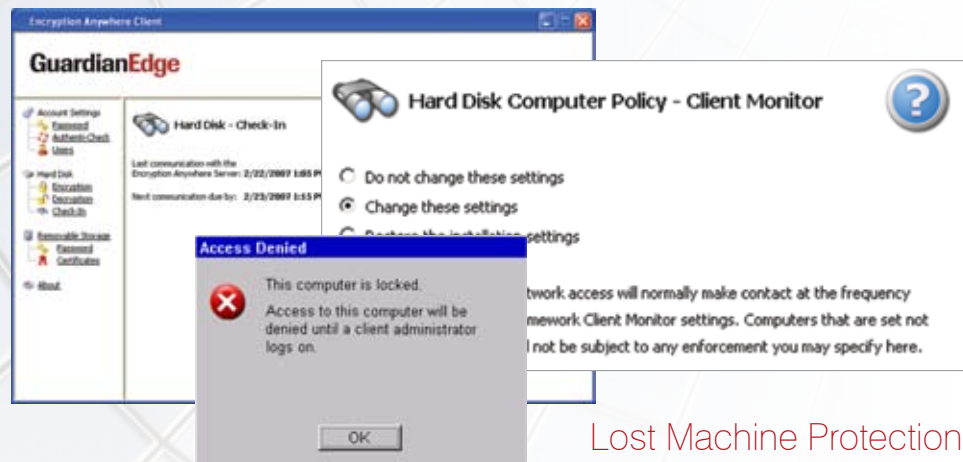
Now, consider the fact laptop theft accounted for one-third of all consumer records breached last year, and it is easy to see why organizations are increasingly concerned about protecting laptop data. In addition to compliance fines and legal expenses resulting from these losses of sensitive or legally protected information, organizations must bear the soft costs associated with the required public disclosure—such as hotline staffing, credit monitoring service subscriptions, loss of intellectual property, and erosion of the corporate brand.

GuardianEdge Hard Disk Encryption protects enterprises from the high cost of security breaches, while preventing damage to the brand and helping to promote a stronger corporate image. The first full-disk encryption software solution developed specifically for the enterprise, it avoids the risk of mobile data loss by encrypting all data stored on the hard drive—including documents, empty space, and temporary data such as the hibernation file. As an integral part of the GuardianEdge Data Protection Platform, it also leverages existing infrastructure such as directory services and software provisioning tools to reduce cost and complexity. In addition, advanced capabilities such as self-service and one-time password key recovery significantly reduce help desk cost by leveraging existing business processes.

Technology Overview

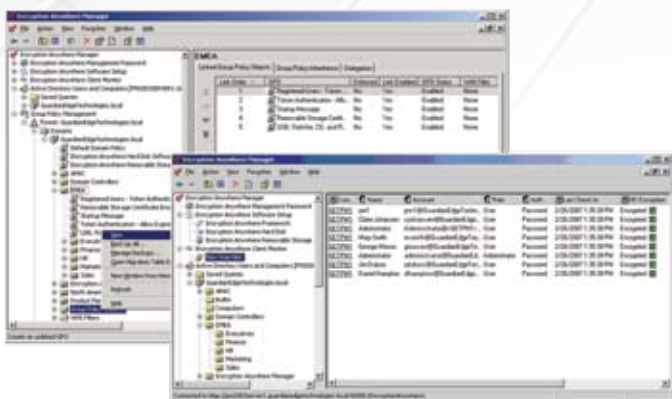
GuardianEdge Hard Disk Encryption is a full-disk encryption solution designed to protect all data on the hard drive of a Microsoft Windows-based machine.

- » A pre-boot password or smartcard based authentication ensures that only authorized individuals will have access to the computer's data
- » Supports Single-Sign-On to the network domain
- » Supports multiple users and administrators on individual machines
- » Provides extensive logging of the status and activity of the hard disk encryption application
- » Protection operates transparently to users—even if they create new partitions—with negligible impact on performance



Lost Machine Protection

All software deployments, updates, and policy implementations are done using Group Policy Objects (GPO) within an Active Directory environment. The GuardianEdge management console provides a simple-to-use and familiar administrative interface that allows security and network administrators to create and deploy policies, monitor the status of machines, and assist users in recovering forgotten passwords.



Centralized Administration and Monitoring

Category

Features

Full-volume encryption protects all data	<ul style="list-style-type: none"> » Ensures regulatory compliance with several state and federal laws, including California SB 1386, FISMA, HIPAA and SOX » Eliminates costs associated with consumer data loss » Protects all confidential data, including trade secrets and intellectual property » Ensures new partitions are automatically encrypted
Most secure method to protect the confidentiality of data	<ul style="list-style-type: none"> » 256-bit AES encryption » Public key infrastructure » Mandatory pre-boot authentication » Remotely disable authentication of a targeted user » Periodic check-in can disable authentication and lock down a lost computer » Real-time audit logging includes policy changes and user actions, both successes and failures (e.g. failed authentication attempts, attempts to uninstall the product, password recovery, change of password)
Convenience for the end user	<ul style="list-style-type: none"> » Single sign-on avoids the need to remember and enter multiple passwords » End-user transparency of data encryption/decryption » Little or no noticeable impact to performance » GuardianEdge Authenti-Check® self-service password recovery without the hassle of long recovery codes or backup keys » Power failure protection for computers without a battery or backup power source during initial encryption
Scales to large, distributed, multi-national enterprise deployments	<ul style="list-style-type: none"> » One Time Password for helpdesk assistance to recover passwords » Multiple accounts per computer (50 Users and 50 Admins) » Auto-logon support for Wake-On-LAN services » Integration with Verdasys Digital Guardian and enterprise-grade deployment tools such as SMS, Tivoli, Altiris » Unique integration with Microsoft Active Directory for Group Policy Object based policy management » Role-based control over who sets security policies or recovers encrypted disks and data » Standard management console (MMC Snap-in)
Meets government directives and regulations	<ul style="list-style-type: none"> » FIPS 140-2 validated » Common Criteria EAL-4 certification pending » Multi-factor authentication using tokens and smart cards

Type

Token

Software

Card Readers

RSA	RSA SID800	RSA Authenticator Utility	N/A
Smart Card	Axalto Cyberflex 64K v1	Axalto 5.0	Axalto Reflex USB v2 & v3 Axalto Reflex 20 PCMCIA v2 & v3 Dell keyboard w/Smart Card reader Any CCID compliant USB reader
Smart Card	Axalto Cyberflex 64K v2c	ActivCard Gold 3.0 Feature Pack 2	Axalto Reflex USB v2 & v3 Axalto Reflex 20 PCMCIA v2 & v3 Dell keyboard w/Smart Card reader Any CCID compliant USB reader
CAC	Axalto Access 64K v1 Axalto Access 64K v2 Gemplus GemXpresso 64K v2 Oberthur CosmopolIC v4 32K Schulmberger Access 32K v2	ActivCard Gold 3.0 Feature Pack 2	ActivIdentity USB v2 ActivIdentity PCMCIA

Supported Client Systems

Windows 2000 Professional SP4

Windows XP Tablet Edition

Windows XP Professional SP1 and SP2

Windows Vista coming in Q2-2007

GuardianEdge Corporate Headquarters

475 Brannan Street, Suite 400
San Francisco, CA
94107-5421

Tel: +1-415-683-2200
Fax: +1-415-683-2349

GuardianEdge EMEA Office

2 Sheraton Street
Soho, London
W1F 8BH UK

Tel: +44 (0)870 366 6772
Fax: +44 (0)871 433 7356

www.guardianedge.com