

Hard Disk Encryption

Data stored in an unprotected state on your laptop and desktop PCs puts your organization at risk of becoming the next data breach headline. Only strong encryption of all data on hard disks counters the threat of losing critical IP and customer or competitive information and provides a “safe harbor” from the high-profile public disclosures and costly remediation mandated by privacy laws.

To protect mobile data from the risks of loss or theft of a laptop or desktop, enterprises not only need the security provided by strong encryption but also a standards-based solution to the practical issues that organizations encounter when deploying endpoint data protection.

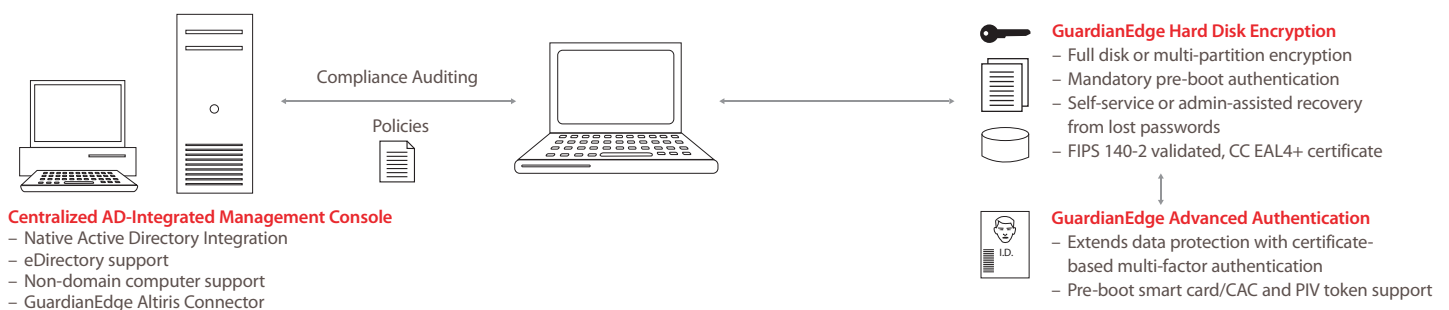
As a component of the GuardianEdge™ Data Protection Platform, GuardianEdge Hard Disk Encryption reduces management, implementation and deployment costs by allowing organizations to make maximum use of existing IT infrastructure. This includes the industry’s only native integration with Microsoft® Active Directory™ along with single console support for Active Directory, Novell eDirectory™ and non-domain endpoints integrated with management for other GuardianEdge data protection products. By leveraging industry standards, GuardianEdge makes endpoint data protection across the entire organization simple to deploy and cost-effective to manage.

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.

Key features

- True full disk or multi-partition encryption
- Full featured pre-boot authentication environment
- Standards-based for industry’s best scale and availability
- Superior admin-assisted or self-service Authenti-Check™ recovery from lost passwords
- Secure unattended wake-on-LAN administrative access
- Single sign-on integration– Microsoft and Novell
- Transparent user operation– including initial encryption and ongoing operation

Enterprise-Class Protection Against Data Loss



Technology Overview

GuardianEdge Hard Disk Encryption combines enterprise-class management and strong encryption with a complete feature set, exceptional ease of use and ease of support. The result is a comprehensive, standards-based solution for protecting data from the loss or theft of a laptop or desktop. Native Microsoft Active Directory integration results in policies that 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.). Novell eDirectory and non-domain endpoint support ensures management of endpoint security for any PC on your network from a single console shared with other data protection security services and includes the capability to seamlessly migrate across network domains with no gaps in data security administration.

Technical Information

Client Environment

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

Pre-boot Authentication

- Microsoft and Novell Single Sign-on integration
- Password authentication (multi-factor authentication available with GuardianEdge Advanced Authentication)
- Secure 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 (up to 1,024 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, CC EAL4+ certificate

Administrative tools

- 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 (Guidance EnCase Forensics)
- 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)

Recovery from lost passwords

- Simple and secure access to encrypted PCs in the event of lost passwords with self-service or admin-assisted recovery

Client Computers

- Microsoft Windows XP Pro SP2 and SP3, Windows XP Tablet Edition, Windows 2000 SP4, Windows Vista; Business, Enterprise and Ultimate

GuardianEdge Management Server

- Microsoft Server 2003 Standard or Enterprise

Database - Microsoft SQL Server 2005

- Express Edition with Advanced Services, Standard or Enterprise

Two-factor authentication

- When used with GuardianEdge Advanced Authentication. Supports an extensive set of authentication tokens, and token readers

GuardianEdge Advanced Authentication Integration

Extends data protection with certificate based user authentication

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

The Leader in Endpoint Data Protection

- **The only native Active Directory integration** – maximum use of existing infrastructure and training investments
 - Deploy and manage with existing infrastructure
 - Low training and support costs, fast rollouts
 - GPO based policy deployment, MMC snap-in architecture
 - Role based policy administration
 - Detailed auditing and reporting
- **Manage endpoint data protection for all PCs from a single console**– Also supports Novell eDirectory and non-domain PCs
- **Proven ease of operation** – Highest deployment success rates and millions of licenses deployed
- **Single console administration** – common management for Hard Disk Encryption, Removable Storage Encryption and Device Control
- **Non- disruptive to end users** – Minimally intrusive, transparent operation and deployment

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 is a trademark of GuardianEdge Technologies Inc.
All other products and services mentioned are the trademarks of their respective companies.