

The Leader in Endpoint Data Protection

Data Protection Platform

Today more than ever, organizations need to guard against the risks of loss and leakage of critical mobile data. Not only have laws requiring companies to protect personal and private information gained teeth, but also a more mobile workforce and growing use of removable storage increase the danger of exposing personal data, IP and other critical information on endpoints. The GuardianEdge™ Data Protection Platform provides a common management platform for implementing a complete array of endpoint data protection controls. It enables optimal use of existing infrastructure, fast rollouts, and low training and support costs.

The GuardianEdge Data Protection Platform solves the practical problems associated with protecting mobile data. Specifically tailored to the needs of enterprises, it provides both the safeguards and the centrally managed flexibility that enterprises require for successfully deploying an endpoint data protection solution.

In the event a device is physically lost or stolen, industry-leading GuardianEdge encryption for PC hard disks, removable storage and smartphones provides an essential first line of defense against data loss. Device, port and file type controls further prevent data leakage by giving organizations the tools needed to implement appropriate policy-based controls required to reduce the risk of unauthorized transfer of information. The platform's best-in-class implementation results in minimal impact on end users while also protecting data even during initial deployment.

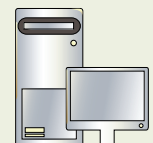
At the core of the GuardianEdge Data Platform is an enterprise-class management environment that provides administration and management of GuardianEdge products via a single console. This management environment is natively integrated with Microsoft® Active Directory® as an MMC snap-in, allowing deployment and management with existing infrastructure, fast rollouts, and low training and support costs. The platform also extends to support not only Novell eDirectory™ but also endpoints that are not a member of a network domain, making it possible to support endpoint security services for any endpoint in the enterprise from a single console.

Finally, consistent management of data security policies and detailed reporting across these environments—and across data protection applications—ensures that critical data on mobile endpoints remains protected.

The Most Cost-effective Protection for Critical Mobile Data



Laptops



Desktops

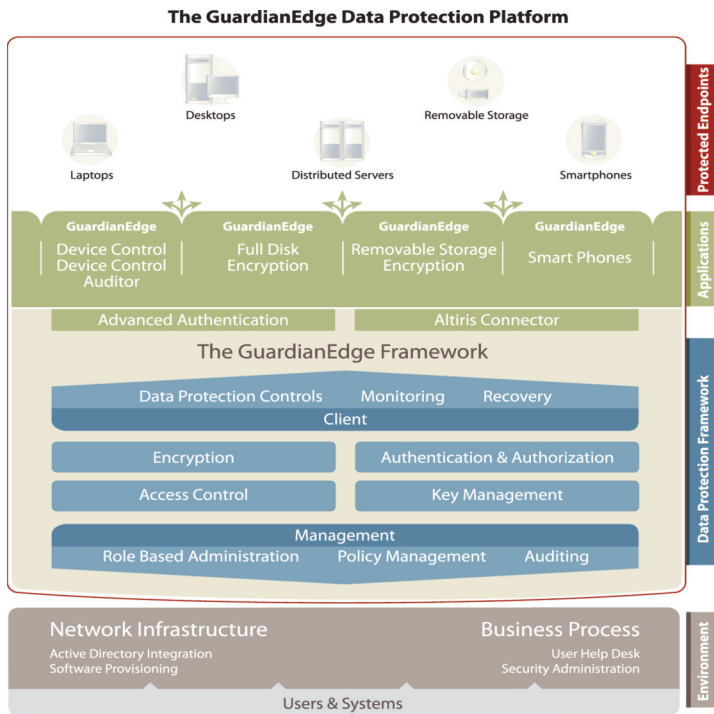


Smartphones



Removable Media

Unified Administrative Environment and Common Services



The GuardianEdge Data Protection Platform gives IT administrators a common set of security and management services for deploying, managing, and monitoring multiple endpoint data protection solutions.

Data Protection Applications

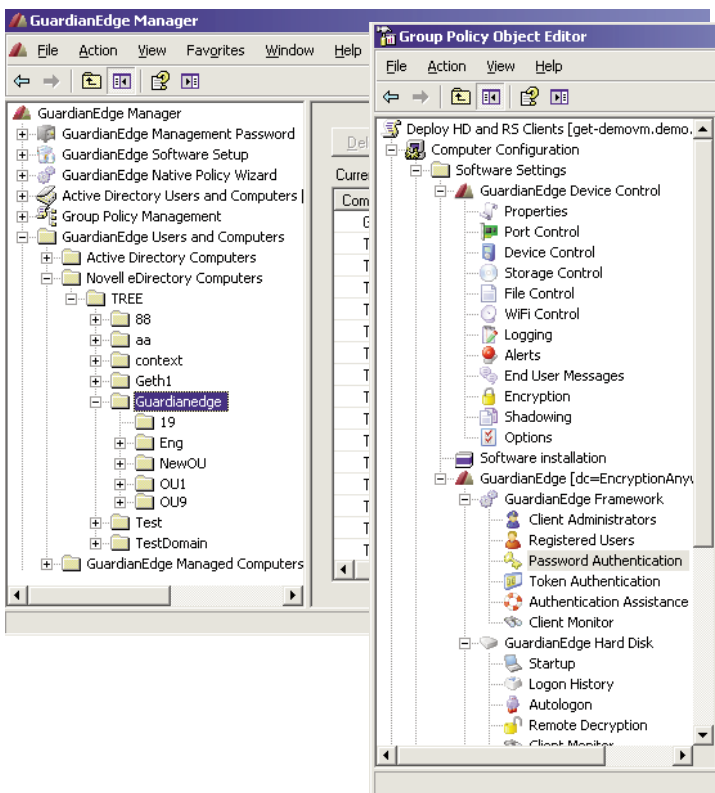
The GuardianEdge Data Protection Platform combines an enabling framework of common management and administrative services with a comprehensive set of endpoint data protection applications:

- **GuardianEdge Hard Disk Encryption**—Protects data on desktop and laptop PCs from physical loss or theft
- **GuardianEdge Device Control**—Prevents unauthorized transfer of sensitive information to devices or wireless networks
- **GuardianEdge Removable Storage Encryption**—Shields data on USB flash drives, CD/DVDs, floppies, MP3 players, and other removable storage from physical loss or theft of the device or media
- **GuardianEdge Smartphone Protection**—Provides a complete solution for protecting data on smartphones
- **GuardianEdge Advanced Authentication**—Enables deployment of strong multi-factor authentication for enhanced protection of data encrypted with GuardianEdge Hard Disk Encryption and Removable Storage Encryption
- **GuardianEdge Altiris Connector**—Integrates with the Altiris® Notification Server™ for a more complete, single console solution that combines the rich Altiris asset, configuration and other management functionality with endpoint data protection controls, management and reporting.

Native Active Directory Integration

The GuardianEdge Data Protection Platform is natively integrated with Active Directory, allowing enterprises to make direct use of existing Active Directory infrastructure investments in servers, scaling, replication, management and failover.

This integration includes using an MMC snap-in for deployment, management, policy, and reporting within Active Directory, allowing administrators to use this familiar interface to implement endpoint data protection—and with minimal training. Implementation of policies is performed using standard Microsoft GPOs (Group Policy Objects) for Active Directory domain machines, and through the same configuration interface for Novell or non-domain endpoints. Existing groupings for users, machines, administrators and security policies are directly supported, without requiring synchronization or operation with other management consoles.



Single Console Management

For Hard Disk Encryption, Removable Storage Encryption and Device Control applications

In addition to directory services integration, enterprises also require common administration for data protection solutions. GuardianEdge addresses this need with a single combined console for data protection applications, which is closely integrated with directory services. This approach enables common policy management, reporting, role-based administration, help desk support, key management, and other administrative actions for GuardianEdge Hard Disk Encryption, Removable Storage Encryption, and Device Control.

Non-Disruptive to End Users

For successful deployment and operation, endpoint data protection solutions must protect data on devices while ensuring the productive use of PCs, removable storage and other connected devices. Key to striking this balance are minimal user adoption requirements and implementations that allow users to continue working with their systems as they have in the past.

GuardianEdge Data Protection Platform applications have been designed to achieve this balance of protection and workflow for end users as a basic requirement.

- The platform provides integration with Microsoft and Novell Single Sign-on so that users only need to log-in to their systems once, and do so with the same credentials that they use across the enterprise network
- Built-in user registration processes—which are either simple to use or automatic—are non-intrusive or minimally intrusive into user operation
- Initial encryption takes place in the background and works properly even when power is unplugged during initial encryption of hard disks or other storage, to prevent failures during the initial encryption process
- Encryption occurs on the fly and in a background operation mode to ensure minimal impact on the speed users perceive when reading and writing data (typically an overhead of 3% or less).
- Group removable storage usage can be configured to enable common use of storage devices—without the need to enter passwords when data is stored or read, while protecting critical data with encryption
- Policies control whether an Access Utility is also written to a removable storage device when encrypted data is written. Consequently, users who have taken work home will not discover they have encrypted data that they cannot use

Novell eDirectory Support and Non-Domain Computer Support

The GuardianEdge Data Protection Platform supports Novell eDirectory registered PCs from the same management console as Active Directory machines. The GuardianEdge management console automatically synchronizes with changes to Novell directory, and can seamlessly allow machines to migrate from AD and Novell directory structures without loss of endpoint data protection or reporting.

This common management environment also extends to PCs that are not part of a domain organization. Typically, these “unregistered” machines are the home PCs of employees that are used to access the network via VPN, or contractors’ computers that are directly connected to the network. As a result, any PC in a network, whether registered with a domain or not, can be protected and managed from this common management environment.

- Messages (which are configurable by the administrator) warn users whenever policy controls for reading or writing data and attaching devices are violated. These help users understand that the action was prevented by policy, and not by some failure of their machine or device
- Background operation can capture file transfer information or complete data files for detailed auditing without user awareness or impact
- Systems management tools work on PCs protected with hard disk encryption to update configurations, patches and other settings just as they do with unprotected PCs

Integration with Systems Management Frameworks

GuardianEdge Altiris Connector makes crucial management and reporting functionality available directly from the Altiris® Notification Server™. The result is a more comprehensive, single-console solution that combines the rich Altiris asset, configuration and other management functionality with endpoint data protection controls, management, and reporting.

Role-based Administration

Managing data protection software in an enterprise environment requires effective coordination between administrators, with a clear chain of command across multiple departmental units and geographic locations. The GuardianEdge Data Protection Platform supports this requirement with direct use of Active Directory's administrative roles and groupings—enabling a flexible multi-tiered administration system with effective, efficient delegation of access rights and responsibilities.

Recovery from lost passwords

GuardianEdge provides the industry's most comprehensive and scalable administrative support services for end-user assistance. GuardianEdge Authenti-Check™ enables administrators to deploy a self-service capability for recovery of forgotten passwords to GuardianEdge Hard Disk Encryption users. Authenti-Check is a challenge-response process (local on the endpoint) that eliminates the need for administrative interaction with end users.

Help Desk support is also available through the GuardianEdge One Time Password (OTP) service. OTP enables remote Help Desk personnel to create single-use passwords for end users, allowing them to securely access locked machines. Administrators have local access—managed centrally through policies—to protected machines, enabling seamless integration of hard disk encryption with Standard IT support processes. For data encrypted on removable media, the platform provides a central data recovery process delivered through strong administrator public/private key pairs and tokens.

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.