

The Leader in Endpoint Data Protection

## Smartphone Protection

With 75% of the US workforce expected to go mobile by the end of 2011, workers are increasingly dependent on smartphones such as the Apple iPhone™, Palm Treo™ and Windows Mobile devices. However, the benefits of this increased mobility come with growing risks. Full-time connections via email, VPN and enterprise applications combined with local storage of data on smartphones increase the potential for exposure of sensitive, confidential and legally protected data.

GuardianEdge™ Smartphone Protection shields organizations from the risks of exposing legally protected data, losing critical intellectual property, and failing to comply with government and industry regulations. It not only provides complete protection for data on smartphones but also extensive device security capabilities.

The solution combines a common, management environment across smartphone platforms—Apple iPhone, Windows Mobile and Palm OS—that operates completely over-the-air (OTA) with critical safeguards on the device. This environment delivers a number of enterprise-class capabilities:

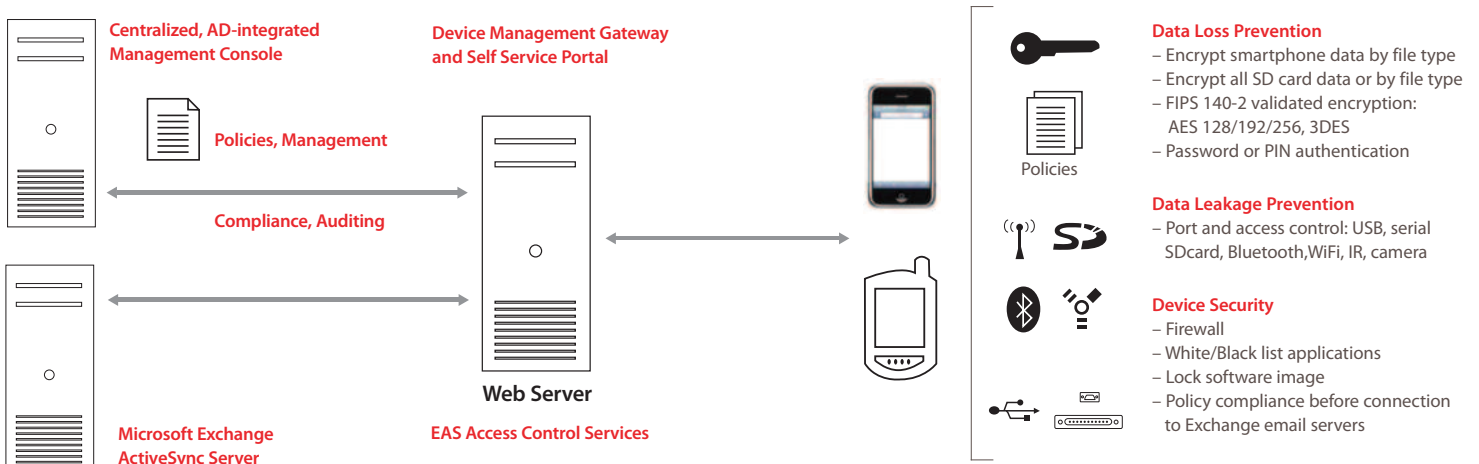
- Microsoft Exchange access controls that require compliance with security policies before connection to the email server is allowed
- Strong encryption to protect against risks associated with loss of a device or connected SD cards
- Device security features, including firewall, application controls and more

The result is the ability to support full enterprise use of smartphones without increased risks.

### Key features

- Single console management of Apple iPhone, Windows Mobile and Palm OS smartphones
- Microsoft Exchange ActiveSync access control
- FIPS 140-2 validated encryption—AES 128, 192, 256 bit
- Complete over-the-air (OTA) management environment—no requirement to connect to a PC or local network

### Enterprise-Class Smartphone Data Loss and Data Leakage Prevention



# Technology Overview

GuardianEdge Smartphone Protection safeguards enterprises from the risks posed by sensitive, private and legally protected data on smartphones by delivering a full-featured, manageable device security solution.

GuardianEdge Smartphone Protection secures enterprise-connected smartphones from data loss and device security risks, enforcing 7x24x365 protection across iPhone, Windows Mobile and Palm OS smartphones. Integration with Microsoft Active Directory® ensures that policies are easily managed and deployed. Extensive over-the-air (OTA) services further enable reporting, policy compliance and update, initial provisioning and software updates to the connected smartphone.

Strong on-device security provides enforcement of encryption, configuration, connection and other policies, while a device management gateway and user self-service portal round out the solution by enforcing connection requirements and providing services that streamline the support and IT management process.

## Technical Information

### Encryption

- FIPS 140-2 validated encryption (AES 128/196/256 and Triple DES)
- Administrator configured and policy controlled
- Encryption by data types: Outlook (email, contacts, tasks, calendar), Word, Excel, PDF, Docs To Go, etc.
- Encryption by data location: On device and attached SD card, by file path
- Shared key encryption option for groups available

### Authentication

- Controlled by policy—password or PIN

### Port and access control

- Port control: USB, serial, SD card, Bluetooth (exception allowed for hands free), WiFi enable/disable, infrared
- Resource access control: IR, camera, voice recording.

### Device security

- Trusted application architecture prohibits unauthorized applications from accessing encrypted data
- Application blacklist prohibits execution of specific applications
- Firewall control: IP address(es) and ports for both incoming and outgoing communications.
- Lock application profile on device
- Data wipe: Time since last check-in exceeded, password failure threshold exceeded OTA from self-service or administrative consoles

### User self-service portal

- Self-service password recovery
- Self-provisioning for new devices
- Remote device wipe
- Recovery of encrypted data from SD cards

### Exchange ActiveSync (EAS) access server

- Ensures that only compliant devices with current security software and policies are allowed to connect to the email server
- Supports Exchange 2003 and Exchange 2007

### Device management gateway over the air (OTA) features

- Policy update, deployment and reporting
- Software deployments and updates

### Apple iPhone support

- Single console management with Windows Mobile and Palm OS devices
- Active Directory user/group integration
- Exchange ActiveSync access control
- Password strength control
- Remote wipe from console or user portal
- Device wipe on exceeded password attempts
- Reporting - asset and inventory management report integration

### Enterprise management console

- Help desk assisted password recovery
- Policy management – Active Directory group based
- Remote wipe, unlock and device decommission
- Recovery of encrypted data from SD cards
- Extended reporting for device security compliance, activity, client versions, auditing
- Systems management and administration
- Customizable best practice profiles – 80+ policy options

### Supported smartphone OS versions

- Windows Mobile® 5 / 6 / 6.1
- Palm OS® 5.x
- Apple iPhone 2.0 and higher

### Server requirements

- Microsoft Windows 2003 Server standard (or enterprise), SP1 or higher, .NET Framework 2.0 AND .NET Framework 3.5 SP1, IIS
- Dual CPU, 2.8GHz or greater, 2GB RAM, 10GB free disk space, Ethernet adapter

### Database

- Microsoft SQL server 2000, SP4 and SQL Server 2005

### EAS access manager server requirements

- Microsoft ISA server 2004 Enterprise / 2006 Enterprise
- Microsoft Windows Server 2003 Standard, SP1 and SP2, .NET Framework 2.0 and 3.5
- Dual CPU, 2.8GHz or greater, 2GB RAM, 250MB free disk space
- Two network adaptors: Corporate LAN and Carrier Data Network (via Internet)

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](http://www.GuardianEdge.com)

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