

GuardianEdge Smartphone Protection

Smartphone Data Loss and Data Leakage Prevention for Enterprises

Your data is more mobile now than ever, it's no longer just executives taking their data on the road with a Palm, Windows Mobile or other Smartphone, it's everyone in your organization – The administrator responding to email on the train, the salesman corresponding with customers in an airport, the accountant on-site at a project working on an audit. And if they're connected via email, or other application, chances are that sensitive, private and legally protected information is on those devices.

The problem is that these smaller devices are more at risk for loss, and increasingly targets of more sophisticated criminal attacks to get this valuable data. When data is lost or leaked organizations can be liable for substantial customer service costs, damage to image and brand equity, and other significant legal, financial and business costs or could lose trade secrets, source code, formulas or other key IP.

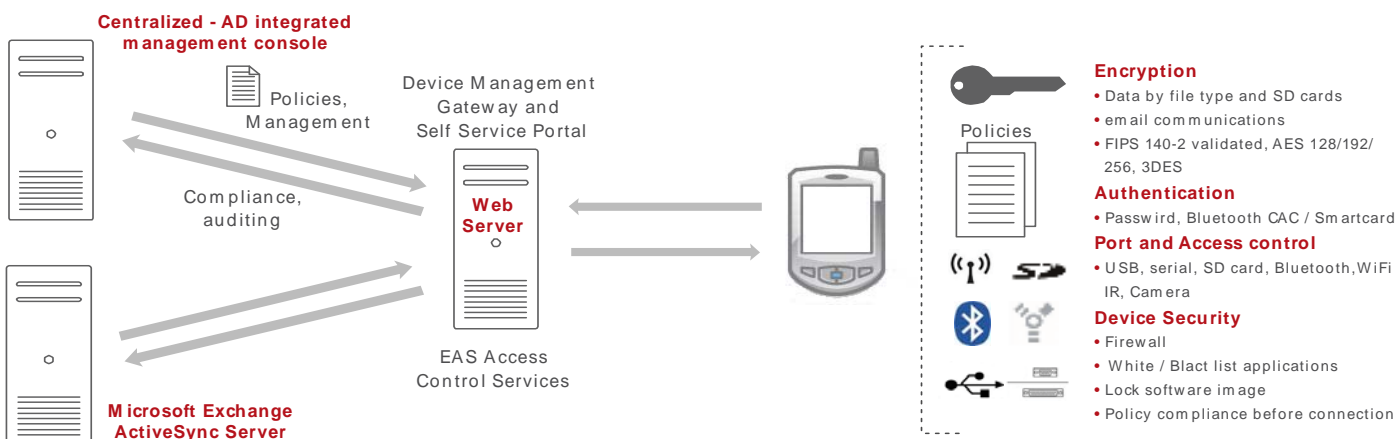
To avoid these negative impacts, and still enable productivity, Smartphones require enterprise class, manageable solutions that include both data loss and data leakage protection.

Smartphone Protection

GuardianEdge Smartphone Protection provides a complete integrated solution to safeguarding the data on smartphones. Data loss protection with strong, central policy controlled encryption for data on the phone or on connected storage devices. Data leakage protection with comprehensive port and device connection control, combined with WiFi / NAC control. Extended defense against traditional security threats with firewall, application control and policy based connection control for Microsoft Exchange ActiveSync adds an additional layer of defense. And a strong, Active Directory integrated central management and support environment that enables enterprises to use policy to control security, without adding a high cost of management completes the solution

Key Features

- Comprehensive port, device and WiFi NAC policy based connection control
- Microsoft Exchange ActiveSync access control
- FIPS 140-2 validated encryption – AES 128, 192, 256 bit
- OTA policy updates, self-provisioning, reporting, software update / deployment



Technology Overview

GuardianEdge Smartphone protection secures the data on enterprise connected smartphones from loss or leakage and provides extended security for additional protection. Integrated with Microsoft® Active Directory™, policies are easily managed and deployed from the Enterprise Management Console. Extensive over the air (OTA) services enable reporting, policy compliance and update, initial provisioning and software updates to the connected smartphone while strong on-device security provides enforcement of encryption, configuration, connection and other policies. To complete the solution, a device management gateway and user self-service portal enforce connection requirements and provide services that streamline the support and IT management process.

Encryption

- FIPS 140-2 validated encryption (AES 128/196/256 and Triple DES)
- Administrator configured, policy controlled encryption by data types: Outlook (email, contacts, tasks, calendar), Word, Excel, PDF, Docs to go
- Data on the phone
- Data on SD cards
- Shared key encryption option for groups available
- Digitally encrypt and sign email messages

Authentication

- Controlled by policy
- Password based
- Two factor authentication based: Bluetooth smartcard, CAC Bluetooth

Device, port and access control

- Port control: USB, serial, SD card
- Access control: Bluetooth, WiFi enable / disable, WiFi NAC control, Infrared, Camera
- Resource access control: IR, Camera, Voice recording

Device security

- Trusted application architecture prohibits unauthorized application from accessing data
- Blacklist prohibits execution of specific applications
- Firewall control: IP traffic, email, IM, web-browsing, SMS / MMS
- Lock application profile on device
- Data wipe by device inactivity time and password failure threshold (also OTA from console)
- Application specific passwords

User self-service portal

- Self-service password recovery

Exchange ActiveSync (EAS) access server

- Allow synchronization only with registered, approved and compliant devices
- Required by policy before connection allowed to Exchange ActiveSync
- Authentication
- Registration
- Pass policy compliance

Device management gateway

- Over the air (OTA) policy update deployment
- OTA reporting
- OTA software updates and deployments
- OTA remediation for devices not meeting compliance policy requirements
- OTA self-provisioning for new devices

Enterprise management console

- Help desk assisted password recovery
- Policy management
- Remote wipe, unlock, device decommission
- Reporting for device compliance and activity
- Systems management and administration
- 80+ policy customizations
- Best practice profiles
- Assign on-device security policies to specific Active Directory groups
- Support for security compliance and IT audits

Supported smartphone OS versions

- Windows Mobile® 5
- Windows Mobile 5 Smartphone
- Windows Mobile 6
- Palm OS® 5.x
- PocketPC 2003
- Symbian

Server requirements for: Enterprise Console, Compliance Server, Self Service Portal and Device Management Gateway

- All four components may be installed on one server
- Microsoft Windows 2003 server standard, SP1, .NET Framework 2.0, IIS
- Dual CPU, 2.8GHz or greater, 2GB RAM, 10GB free disk space, Ethernet adapter

Database

- Microsoft SQL server 2000, SP4

EAS access manager server requirements

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

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

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

©2007 GuardianEdge Technologies Inc.