

reflex
magnetics



DISKNETPRO4

reflex



DISKNETPRO4

FLOPPY DISKS/ZIP/JAZZ DRIVES

USB FLASH MEMORY/MEMORY STICKS

PDAS

BLUETOOTH/FIREWIRE

DIGITAL CAMERAS

Your existing anti-virus scanners and firewalls may offer little or no protection against the latest form of computer attacks that come via removable media devices, unauthorised file types or unauthorised access.

Device Management

The Reflex Disknet Pro Device Manager (DM) controls access to both known and unknown devices. Using kernel mode filter technology Device Manager supports both 'Black List' and 'White List' security controls. Device access is controlled on a user/group/machine basis and dependent on device type and/or model and brand of device. Irrespective of connection protocol, Device Manager can manage access to all ports including USB, Firewire and Bluetooth.

Granular I/O device management

White and Black List security support

Transparent data encryption

Seamless content and anti-virus integration

Configurable messaging

Filtered audit capability

DATA SECURITY THROUGH DEVICE MANAGEMENT

Would USB flash media be so terrifying if you could harness its business advantage while ensuring network integrity and data security?

The business needs from Information Technology have changed. While simply blocking access to I/O devices is no longer a viable solution, enabling portable storage to be used freely can potentially place an organisation's data at risk.

THE CHALLENGE WE FACE...

Hardware and software strategy that promote plug-and-play media, coupled with international compliance such as ISO17799, HIPPA and Sarbanes-Oxley that demand accountability, present a real dilemma for those striving to maintain network security.

In our quest to provide the ability to share data securely, Reflex Magnetics Ltd recognise the business need to exchange data while ensuring the highest level of data integrity at all times.

Reflex Disknet Pro enables IT management to enforce security policy while providing your end users the ability to use technology in a controlled and managed fashion. Content and virus checking coupled with transparent data encryption and filtered auditing ensures that only authorised devices are used to support your business flexibility.

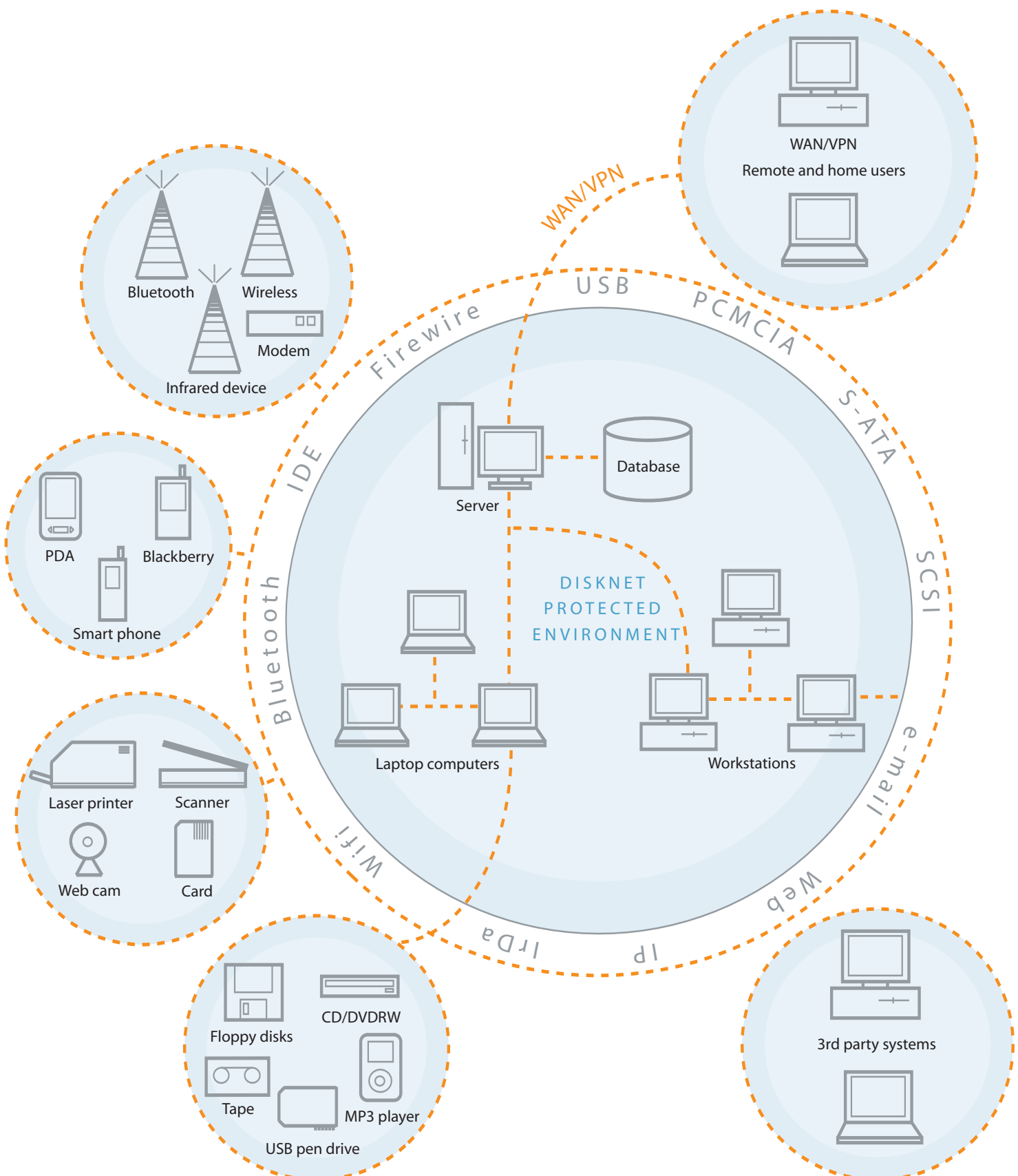
Removable Media Data Management

Additional controls can be put in place to manage data flow to removable media devices using the Removable Media Manager (RMM). The RMM enforces that all removable media devices are authorised before use is granted. A unique digital signature is written to a device to mark it as authorised and contains unique information about the device contents. The digital signature is automatically updated during file modifications/transfers within the protected environment. If changes to the media are made outside of the organisation, the device will require re-authorisation before it can be used again within the protected environment. The system can perform a complete content and virus scan using a third party anti-virus scanner of your choice.

Transparent Removable Media Encryption

The Encryption Policy Manager (EPM) provides transparent encryption of removable media storage devices including USB pen drives. Utilising AES 128/256 bit encryption EPM requires no user training and enforces that all devices are encrypted prior to any data being transferred. Encryption policy is centrally managed on a user, group or organisational unit basis. Offline access or access on trusted sites can be configured (see *Access Encrypted Media Offline* section).

DISKNETPRO4





Generic Active Code Protection

The threat from malicious code and unwanted file types (mp3, mpg, avi etc) can be controlled using Program Security Guard (PSG). PSG prevents users and untrusted sources/applications from creating/modifying and deleting defined file types. PSG ensures that only trusted staff, sources and applications can modify the system configuration. Users can be blocked from introducing unlicensed software, virus-infected files, spyware and trojans. This system is completely generic and does not rely on outdated signature-based recognition.

Centralised Administration/Auditing

Reflex Disknet Pro is centrally managed using a familiar Microsoft Management Console (MMC) interface. By transparently integrating with the MS NT Domain, 2000/3 Active Directory and Novell eDirectory user/group information, the administrator is able to assign profile based policy across an organisation. The Reflex Disknet Pro Enterprise Server is highly scalable and runs on an MS SQL back end database enabling server replication and configurable audit report generation.

Remote/mobile user support

Remote and mobile workers can be managed in the same way as network users. Reflex Disknet Pro supports VPN and RAS connections and can be secured to run in a completely standalone mode. The client software filters and securely stores essential audit information until the server is next available.

Access Encrypted Media Offline

Removable media offers great versatility for the transportation and on demand access of data anywhere. Unlike other systems available, EPM Explorer enables authorised users to access encrypted media on any system without the need to install any software and without the need for raised security permissions.

Key Features

DEVICE MANAGEMENT

- Supports both 'Black List' and 'White List' security
- Controls I/O devices/removable media on all connection ports (USB, Firewire, IDE, etc)
- Devices can be managed by type, brand, model or individual device
- Utilises kernel mode technology that can even secure against local admin attacks
- Custom devices can be added easily by the system administrator
- Retrieves unique device information
- Fully plug and play compliant

REMOVABLE MEDIA MANAGEMENT

- Uniquely identify approved devices using a digital signature
- Where permitted, detect changes performed externally from the home network and enforce a device policy verification
- Enforces a virus check of new devices by automatically integrating with most 3rd party AV systems
- Enforces a configurable content check of new devices (dependent on policy)
- Define an acceptable usage policy regarding device
- Allow only defined applications to write to removable media

TRANSPARENT ENCRYPTION

- Enforceable removable media encryption utilising AES 128/256 bit algorithm
- Centrally managed with global key encryption infrastructure
- Enables secure offline access of encrypted devices without the need to install software or local admin rights
- Provides the ability to share encrypted data on a user, group, organisation or site level
- Encrypted devices can be pre-configured and assigned by the system administrator (allows only approved devices)

- External access can be prevented where required ensuring encrypted devices are only accessible on defined networks
- Secure challenge/response system enables remote password recovery
- Supports encrypted device revocation and key recovery

AUDITING

- Detailed auditing of attempted security breaches
- Complete audit of device usage (floppy disk, CD/DVD, USB flash media, diskOnKey, etc)
- Client side filtering ensures only relevant information is sent to the server
- Fully configurable filters and audit analysis reports
- Stored in a MS SQL database
- Configurable email alerts

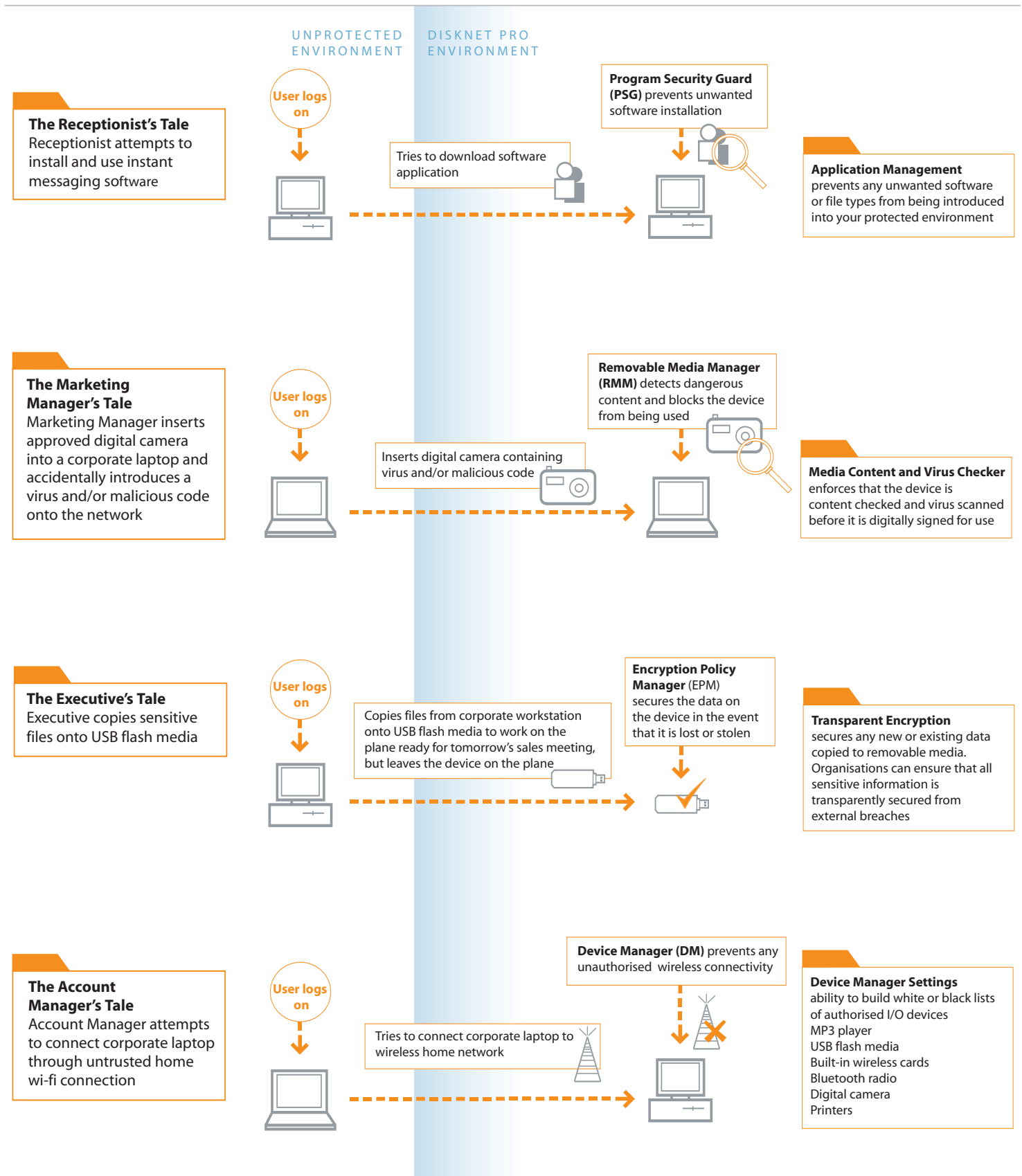
DEPLOYMENT AND SCALABILITY

- Supports MS Windows NT/2000/2003/XP
- Integrates transparently with MS Windows NT Domain, MS Windows 2000/2003 Active Directory & Novell NDS
- Highly scalable cross-platform architecture
- Customisable user messaging
- Online and offline settings enable diverse management of standalone and mobile workers
- Silent client deployment (Fully MSI enabled installer)

3RD PARTY CERTIFICATIONS

- Common Criteria certified
- FIPS certified encryption
- CSIA Claims Test Mark certified
- UK MOD (DIPCOG) certified
- Novell 'YES' certified

SECURITY TALES



The Receptionist's Tale
Receptionist attempts to install and use instant messaging software

The Marketing Manager's Tale
Marketing Manager inserts approved digital camera into a corporate laptop and accidentally introduces a virus and/or malicious code onto the network

The Executive's Tale
Executive copies sensitive files onto USB flash media

The Account Manager's Tale
Account Manager attempts to connect corporate laptop through untrusted home wi-fi connection

Application Management
prevents any unwanted software or file types from being introduced into your protected environment

Media Content and Virus Checker
enforces that the device is content checked and virus scanned before it is digitally signed for use

Transparent Encryption
secures any new or existing data copied to removable media. Organisations can ensure that all sensitive information is transparently secured from external breaches

Device Manager Settings
ability to build white or black lists of authorised I/O devices
MP3 player
USB flash media
Built-in wireless cards
Bluetooth radio
Digital camera
Printers

IT Security by Innovation

DISKNETPRO4

SYSTEM REQUIREMENTS

MS Windows NT 4 (SP6)
MS Windows 2000 (SP3+)
MS Windows 2003
MS Windows XP (SP1+)
MS Internet Explorer (5.5+)
Novell Client v4.91+

All trademarks acknowledged



TELEPHONE +44 (0)20 7372 6666

FAX +44 (0)20 7372 2507

EMAIL enquiries@reflex-magnetics.com

WEB www.reflex-magnetics.com

© Reflex Magnetics Ltd 2002/6

Designed by www.fosterandlisle.co.uk 0845 310 0855