

Chapter

Pointsec Protector Overview

1

Recent proliferation of USB ports and CD/DVD writers on laptops and PCs, has dramatically increased the occurrence of data leak events within enterprises. USB flash drives, iPods, Bluetooth devices and removable media allow users to extract data in an instant, making all enterprise computers vulnerable. The ability to copy or move sensitive data onto these personal devices undetected places your organization at serious risk of untraceable data leaks. This chapter will discuss applying Pointsec Protector in a corporate environment, and includes installing the Pointsec Protector Server.

Objectives:

- Apply Pointsec Protector in a corporate environment where appropriate, based on Protector's use and methodology.
- Given your corporate network's structure and security policies, select the Pointsec Protector components best suited to address security requirements.
- Given corporate requirements, install and configure Pointsec Protector Server.

Key Terms:

- Removable Media Manager (RMM)
- Program Security Guard (PSG)
- Device Manager (DM)
- Encryption Policy Manager (EPM)

The Threats

Mobile workers — known in some circles as road warriors — increasingly are becoming important players in today’s fast-paced world of business. They are the people who are always on the go — the ones who spend at least half of their work weeks away from their regular offices. Because these women and men are out of the office so often, they have to use laptop computers, personal digital assistants (PDAs), and portable memory devices to exchange and transport business-critical data. In many cases, the security of this data hinges on the physical safety of the devices. Simply put, when mobile devices are lost, so is the data.



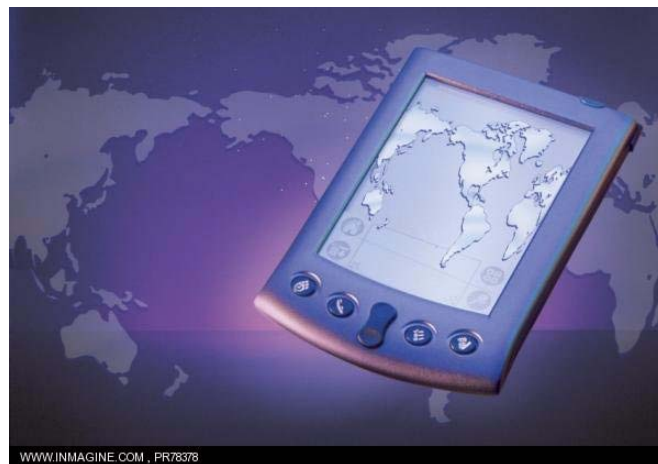
Figure 1-1: “Road Warrior” Using a PDA

Today, most laptops and PCs have some sort of antivirus and personal firewall software to prevent data hijacking. But what happens when a computer is stolen or when an overtired road warrior leaves her PDA in a cab?

A 2006 global study by market research firm Gartner indicates that while 25 percent of information theft is linked to network intrusion, 60 percent of data breaches can be attributed to lost or stolen mobile devices. With this in mind, it is critical for organizations to bolster defenses by encrypting data across the board.

Headlines from any newspaper or news Web site around the world put data security vulnerabilities due to physical loss of devices into perspective. In the United States (U.S.), the Transportation Security Administration (TSA) reported that a stolen computer exposed more than 100,000 personal records. In the United Kingdom, a laptop storing personal data on 11,000 children was stolen from a Nottinghamshire hospital. Finally, the 2006 asset audit of the New Zealand Inland Revenue Department (IRD) showed that the IRD has no clue as to the whereabouts of 106 of its computers or their contents.

Because they are much smaller than laptops, devices such as Bluetooth, USB flash or thumb drives, iPods and PDAs are easier to lose in hotels, taxis, airplanes, restaurants, and other locations frequented by business travelers.



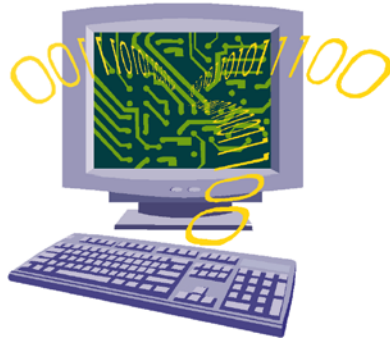
The threats to enterprise security from mobile devices include:

- Unauthorized access.
- Unauthorized media use.
- Theft of company data.
- Introduction of unauthorized files.
- Introduction of unlicensed software.
- Maintaining PC integrity.
- No control of data-flow into and out of the company.

Without taking measures for network-wide auditing, Security Administrators will be unaware of the type of traffic moving in and out of the network. Organizations need to monitor what is being introduced into the network to determine the potential for unwanted traffic such as spyware or viruses.



In addition, careful consideration must be made for data leaving a company's protected network. Should this information be available outside the corporate network, and if so, is the data secure?



Moreover, though a firewall protects intruders from the outside world, what protects data from unauthorized use from within the corporate network? Little known to the general public is that 80% of security breaches are caused by insiders. A USB flash drive in the wrong hands makes the firewall ineffectual. Their size and shape make them easy to lose and often hard to see. One 80 GB iPod allows someone to copy 2,500,000 word documents in under 15 minutes. Introducing malicious code in the corporate network via a mobile device such as a flash drive is also a serious threat.

We can expect the use of new mobile devices to increase as prices decrease.

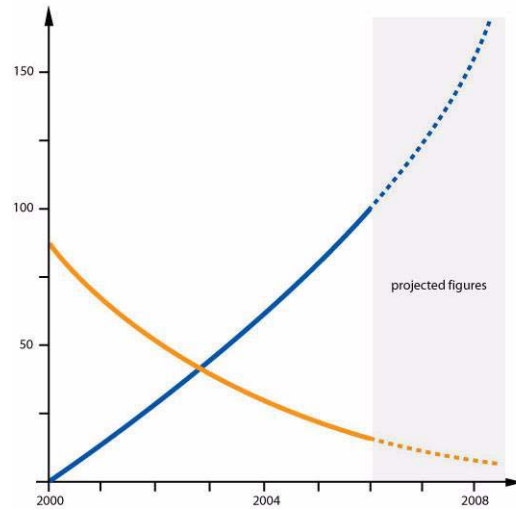


Figure 1-2: Mobile Device Use Compared to Cost

Given their cost and time savings with regards to conducting business transactions remotely or in-person, stopping their adoption is both impractical and ludicrous. However, policies must be enforced to enable devices to be used securely; therefore, restrictive but flexible.

About Pointsec Protector

Pointsec Protector enables the ability to secure devices without impeding employee throughput and productivity, whether travelling, at home or at the office. It is a unique corporate solution that provides a policy-driven mechanism of securing an organization's information and ensures data integrity across all end points.

Protector prevents unauthorized copying of sensitive data by combining port and device management, and provides content filtering and centralized auditing with robust media encryption. Based on market-leading Pointsec technologies, Pointsec Protector plugs potential leak points and logs data movement to and from any plug and play device, providing comprehensive control of security policies.

Pointsec Protector:

- Transparently encrypts removable media including USB Flash Drives and Removable Hard Disks using a 128-bit AES algorithm.
- Is independently certified.
- Deploys quickly, which meets compliance objectives and conserves resources.
- Controls input and output on all connection ports.
- Centrally manages devices individually by type, brand, or model.
- Scales to meet the needs of any size enterprise or government agency.
- Provides complete audit of device usage.
- Integrates transparently with Windows 2000/2003 Active Directory and Novell eDirectory.
- Maintains high productivity because the application runs transparently to users.

Protector Requirements

The following tables detail the Pointsec Protector System Requirements:

System Requirements

Disk and Memory Space

Component:	Space required:
Pointsec Protector Enterprise Server	30MB+ SQL
Pointsec Protector Client	7MB

Operating Systems and Software

On the:	Operating system and software
User's PC	MS Windows Vista 32-bits MS Windows 2000 Professional/Server/Advanced Server MS Windows XP Professional MS Windows 2003 Server
Administrator's PC	MS Windows 2000 Professional/Server/Advanced Server MS Windows XP Professional MS Windows 2003 Server

Figure 1-3: Protector System Requirements

Pointsec Protector Elements and Features

Pointsec Protector is comprised of two basic elements:

- Pointsec Protector Server
- Pointsec Protector Client

Comprised in each of these elements are the following features, allowing the Administrator to match the organization's security policies:

Removable Media Management

By centrally controlling access to removable media/IO devices, a system administrator can control user access to floppy disks, memory sticks, PDAs, flash memory, Zip/Jazz drives, digital cameras, etc. (CDs, CDRs, DVDs can be protected by using Device Manager). The **Removable Media Manager (RMM)** controls device access on all available ports including USB and Firewire.

All removable media/IO devices must be authorized before use is granted. Authorization can be centrally managed or users can authorize their own devices providing certain rules are met (see “Program Security” on page 18). A digital signature is written to a device to mark it as authorized. The digital signature is automatically updated during file transfers within the protected environment. If changes to the media are permitted outside of the organization, the device will require re-authorization before it can be used again within the protected environment.

The system enforces that all devices are virus-free, prevents illegal importing of data and more importantly, it can prevent the unauthorized exporting of data. This system will also stop users gaining access to any unauthorized hot-swap and plug-and-play devices.

Program Security

Pointsec Protector provides profile-based file management using the **Program Security Guard (PSG)**. For example, users can be prevented from creating defined file types on the local workstation and network drives.

File types are specified by extension and can be used to prevent the introduction of unlicensed software (i.e., **.exe**, **.com**, **.dll**), malicious file types (i.e., **.vbs**, **.scr**), or simply unwanted file types (i.e., **.mpg**, **.mp3**, **.jpg**).

Protection is provided from any external source including e-mail attachments and Web downloads. PSG also provides unrivalled protection against new and unknown virus attacks. For example, both W32/MSBlast and W32/SoBig would be automatically blocked from infecting the system simply by preventing the creation of unauthorized executable files.

Content Management

PSG is a data authorization module, which is integrated within the media authorization process. Employing this module, users can be given the right to authorize their own media providing the device contains

only permitted file types. PSG can be configured to allow the authorization of data-only files. Any executable/unapproved code will be rejected even if renamed or hidden. This provides an additional layer of generic active code protection.

Device Management

Pointsec Protector allows an administrator to control user access to devices through all PC ports using the **Device Manager (DM)**. Access to IrDA, COM, USB, Firewire and LPT ports can be controlled. By applying security permissions to devices, it is also possible to manage access to all removable media, such as CD/DVD drives, PDAs, WiFi, Blackberries, Bluetooth and unauthorized hard disks. This feature also prevents users from connecting unauthorized devices to the PC ports including hardware such as a modem and provides On/Off/read-only protection as opposed to the more granular approach offered by Removable Media Manager detailed above (see “Removable Media Management” on page 17). The Device Manager includes a predefined list of devices in which to permit or disallow. However, it is also possible to define new devices depending on corporate requirements.

Centralized Management

Pointsec Protector is centrally administered. A familiar Microsoft Management Console (MMC) interface is provided to control user profiles, real-time monitoring, and extensive auditing. User profile management and configuration is all stored within a SQL database.

Centralized Auditing and Alerts

Pointsec Protector provides detailed auditing of attempted security breaches. All events are centrally logged in a SQL database with the ability to create structured queries and detailed reports.

For example, Pointsec Protector enables the Administrator to centrally audit all file operations on all removable storage including CDs/DVDs.

The Administrator can configure the auditing of certain events to produce e-mail alerts to defined addresses.

Detailed Reporting

The Pointsec Protector auditing provides extensive tracking of user behavior and system security. To simplify audit analysis, fully “configurable” HTML reports can be generated from within the management console detailing summary information across all audit events.

Anti-Virus Scanner Integration

Pointsec Protector automatically detects and integrates with compatible anti-virus scanners. Anti-virus scanners can be used to enforce that all removable media are virus-free before access is granted as part of the authorization process.

Remote/Offline User Support

Pointsec Protector supports remote and standalone workstations. Remote workstations (i.e., laptops and desktops) often pose a greater security risk as conventional anti-virus and security techniques are often hard to enforce.

Pointsec Protector provides valuable generic protection against malicious code and can be fully managed just like networked workstations. A remote worker can be dynamically controlled if connected to the Internet via a VPN or RAS connection. In addition, Pointsec Protector can be configured to assign different access rights when machines are on and off the network. This may be particularly desirable for laptop users where different access rights are required. For example, disabling WiFi access when the laptop is on the network and enabling it when offline.

Pointsec Protector empowers businesses to manage and secure their data across both networked and standalone workstations. Being user-based and centrally managed, it presents the minimum of administrator overhead while affording the maximum level of security aimed at your internal threats.

Removable Media Encryption

Pointsec Protector is supplied with the **Encryption Policy Manager (EPM)**. The greatest threat when granting access to removable media

storage devices is the loss of sensitive or proprietary information. The EPM can be configured so that data can only be accessed by authorized staff on authorized systems.

EPM provides transparent encryption of removable media storage devices. This feature includes the encryption of CD/DVDs when using the built-in software on the protected workstations. Unlike any other solution on the market, offline access can be granted to trusted users. Users will be able to access secure devices without the need to install any software onto third party systems using secure password authentication. This component will allow access on third-party systems even with just basic user rights.

Pointsec Protector Architecture

This section details the various options and architectures available when installing and managing Pointsec Protector on medium to large network infrastructures. Typically on a large network (i.e., over 20,000 workstations), you would need the ability to distribute Pointsec Protector functionality across multiple servers. This is made easy due to the modular approach of the Pointsec Protector Server installation.

Each Pointsec Protector Server installation is comprised of three separate components:

- Pointsec Protector Database

This is the MS-SQL database that stores all Pointsec Protector users, groups and profile settings.

- Pointsec Protector File Server

This is the main Pointsec Protector service. This provides communication between the management console and the database, and handles the client connections.

- Management console

This is the MMC-based interface for managing the Pointsec Protector database. As mentioned above, this component communicates with

the Pointsec Protector file server, which in turn communicates with the Pointsec Protector Database.

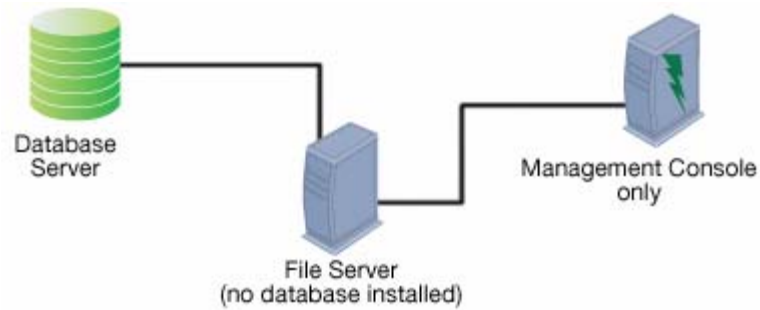


Figure 1-4: Pointsec Protector Network

All of the components communicate using secure encrypted TCP/IP sockets. This allows each of the components to be installed on different machines on the network.

Using this technique, you can install multiple Pointsec Protector file servers on a network all connecting and sharing the same Pointsec Protector database. It is recommended that one of these is used as an administrator server containing the management console, and the others for client connections.

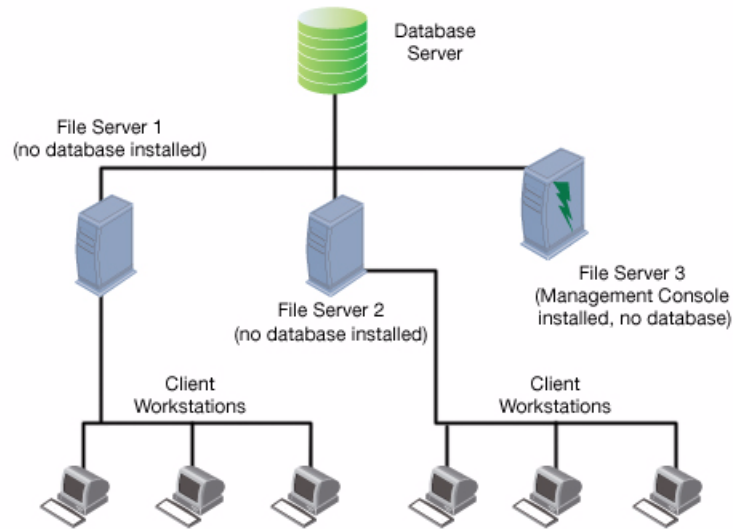


Figure 1-5: Multiple Servers Sharing One Database

Pointsec Protector Database Transaction Replication

Using MS-SQL transaction replication backup, multiple SQL servers can be installed on the network. Replication will be performed between the master and a number of slave servers.

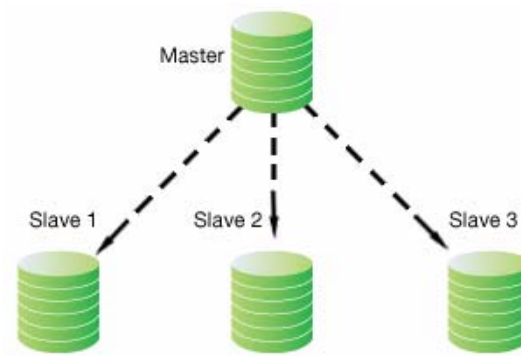


Figure 1-6: Master/Slave SQL Server Communication

As this is only a one-way replication, any changes made to the slave databases will not be replicated back to the master server. Using this system, it is possible to have backup SQL server(s) available on the network in case of failure to the main server.

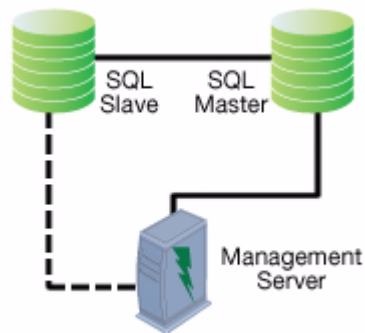


Figure 1-7: Management Server/SQL Server Communication

If the first server fails, then it moves on to the next server, etc. It is possible to have as many slave/backup servers as required, all of which will be complete clones of the master server.

Database Administration

All database administration *must* be performed on the master SQL server. This will ensure that any changes (i.e., additions or deletions) are replicated down to the slave server(s).



Figure 1-8: Management Console Communicates with the Master Database Server

This means that you cannot connect any Pointsec Protector file server to a slave SQL database unless the main SQL server has failed.

Pointsec Protector Server Merge Replication

It is also possible to have two-way replication between two master servers. Using this system, you can have two or more master SQL servers both replicating between each other. It is then possible to have separate database or profile servers for each of the master SQL servers employed by clients on the network. You can as required, have additional backup server(s) on the system.

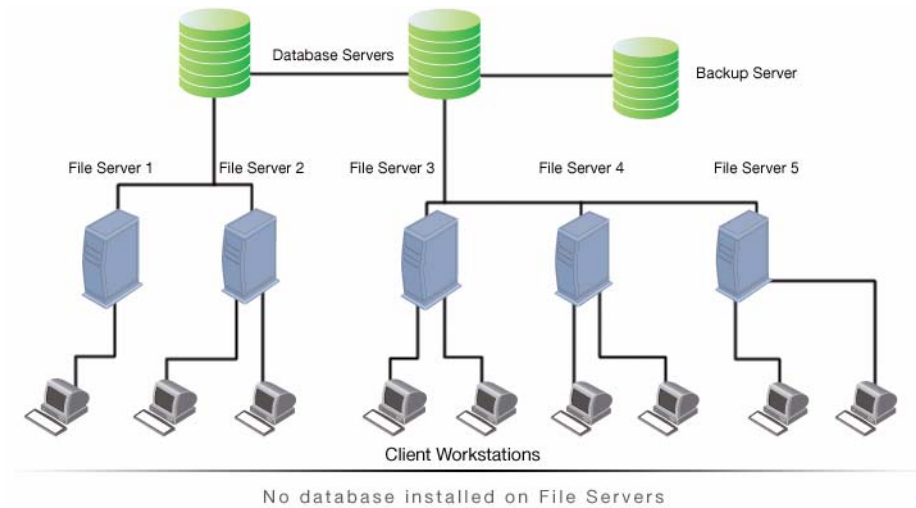


Figure 1-9: Two Master Database Servers

Client Connections

Machines running Pointsec Protector Client *must* connect to a Pointsec Protector file server that connects to a master SQL database. When the client software first starts, it registers itself with the Pointsec Protector file server. If the client was connecting to the slave database, the “computer” record would be created here and not sent to the master SQL server causing data inconsistency between the two servers.

The Pointsec Protector Clients have the ability to connect to multiple Pointsec Protector file servers to obtain a profile. This can be achieved sequentially by connecting to each server in a specified order; if the first one is unavailable, then a connection is made to the next and so on. Alternatively, random server selection can be used for load balancing across multiple servers. This is useful on a large network as a backup mechanism in case of failure to the primary Pointsec Protector file server.

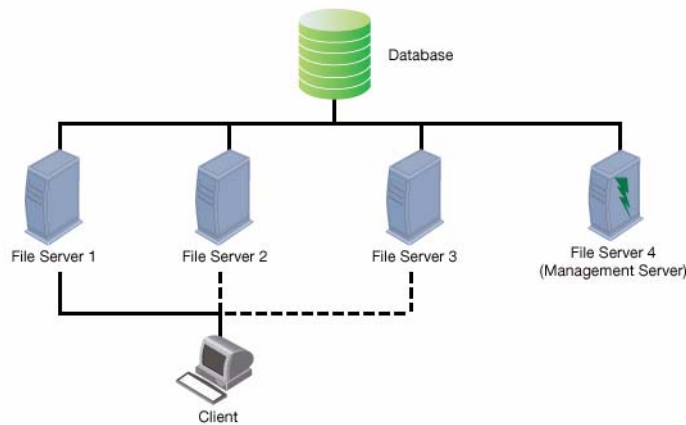


Figure 1-10: Client to Multiple Servers

License Handling

Licenses for Port Management and Media Encryption features together or for either, can be obtained from Check Point. It is possible to run some computers in a network with only Port Management enabled, other computers have only Media Encryption enabled, and others have both features enabled. Computers with a license for both Port Management and Media Encryption have access to all features in the management console.

On computers with a Port Management-only license, everything is accessible except the **Encryption** tab and the **Encrypted** column in the Device Manager, which are grayed out.

On computers with a Media Encryption-only license, only the **Encryption** tab and the **Encrypted** column in the Device Manager are accessible, the rest is grayed out.

If a user tries to install a client with both features enabled while having a license for just one of them, an alert will be displayed in the central logs.

If there are any active unlicensed computers, a warning window with details will be displayed at the startup of the management console.

It is possible to run the License Manager and install additional licenses from both the central logs and from the startup warning screen. There is no need for uninstallations or manual configurations of the clients missing valid licenses. For further information, please contact your authorized Check Point Software Technologies Ltd. partner or representative. For a list of authorized partners, please visit

**`http://partners.us.CheckPoint.com/
partnerlocator`**.