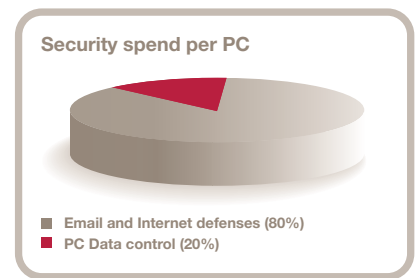
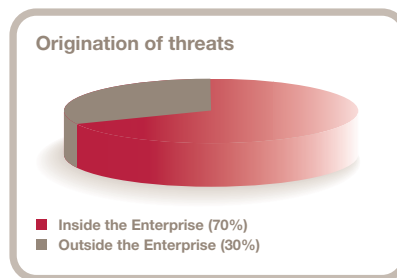


Redefining Boundaries – Intelligent Media Access Control

While organizations have made significant investments in perimeter security solutions (such as firewalls, anti-virus and content filtering), industry analysts believe that over 70% of security incidents actually occur within the network itself.

By focusing primarily on defending against external attacks, organizations are failing to address the security issues that occur inside the network, whether by accident or intent.

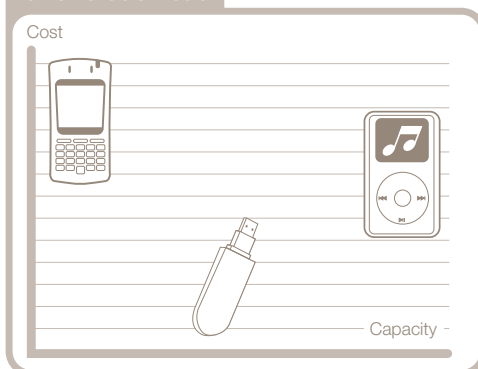
The proliferation of low cost, high capacity portable storage devices in the guise of lifestyle accessories (e.g. PDAs, iPods, USB Memory Sticks etc.) pose a real and present threat to corporate networks by blurring the boundaries between personal and corporate IT.



By not controlling the connection of removable media devices to corporate owned desktops and laptops, firms leave themselves open to serious security breaches which include:

- ⊖ Identity theft through removal or copying of customer personal information
- ⊖ Loss of company confidential files (e.g. customer database, research data etc)
- ⊖ Disruption caused by the introduction of viruses and malware
- ⊖ Legal liability for copyright-protected and inappropriate content on the network
- ⊖ Vicarious liability of the company over the actions of its employees

Calculating the risk of removable media



DeviceWall[®] from Centennial Software dramatically reduces these risks by actively managing PC users' ability to access all common removable media devices.

DeviceWall is not a PC lockdown tool; it supports full business productivity by allowing the use of selected devices by authorized staff, while actively guarding against the removal of data or the introduction of potentially harmful content onto the network.

How DeviceWall works

DeviceWall is a policy-based Windows PC security solution, which allows or blocks access to selected classes of removable media according to users' legitimate needs. The solution uses a small client agent (automatically deployed from a central server) which enforces the organization's security policy according to the current user's privileges.

To ensure that each PC carries a copy of the latest policy, DeviceWall agents automatically check for server updates at log-on and at configurable intervals thereafter. DeviceWall works both when the PC is on the corporate network and when it is offline, ensuring that security levels remain constant.

Both at log-in and when a user attempts to connect a restricted device, DeviceWall can automatically display an admin-configurable message to notify the user of the company policy and to confirm that they do not have the necessary privileges to access the device.



DeviceWall key features

'Intelligent' device identification

DeviceWall will only block devices that are considered a threat to the network; it will not affect mice, keyboards and other human interface devices.

Deployment

DeviceWall can be deployed from a single central server to the entire organization by a variety of mechanisms. It can utilize Active Directory where available.

User based policies

Security privileges are allocated to the user, not the PC. This means that users take their privileges with them wherever they go on the corporate network.

User experience

DeviceWall supports the acceptance of policy by reminding users which devices they do not have permission to access both when logging on to the network or on attempted policy breach. Administrators can choose to present these messages or operate in a silent mode. All messages are configurable to the company's own requirements.

Automatic policy checking

Clients automatically check for policy updates at log-on and configurable time periods, ensuring that all PCs are running the current version of the security policy.

Scalability & performance

Small client agents and a central application server make DeviceWall scalable to networks with tens of thousands of PCs.

Temporary access

Inevitably, circumstances arise whereby temporary access needs to be granted for a specific user to a specific class of device whether they are connected to the network at the time or not. DeviceWall is the only device management solution to offer both online and offline users the ability to gain access to a device for the current windows session. This means that security does not get in the way of business productivity. Any such access is documented in the audit log.

NT / Active Directory support

While other solutions only work with Windows 2000 or later, DeviceWall enables organizations running NT domains to still benefit from automatic policy updates and mapped user group privileges.

Audit log & status

Any changes to the policy are formally documented in the audit log and DeviceWall allows administrators to make a record of all temporary access exceptions.

Administrators can view the current deployment status of the policy both in terms of the client version and the actual policy. If required they can force an update to connected users.

System requirements

Client Service

MS Windows NT/2000/2003/XP Operating systems

Control Centre

• MS Windows 2000/2003/XP • MS IIS 5 or later

Supported (NOT Required)

Active Directory

Hardware Requirements

DeviceWall supports any hardware specification that runs the operating systems above

Client File Size

The typical size of a client agent is just 70Kb
Subsequent policy updates are usually less than 1Kb

Supported device types

Plug & Play Storage

USB sticks and drives
CompactFlash cards
Digital Cameras etc.

Multimedia Devices

iPods & other MP3 players

PDA's & Smartphones

Palm OS PDAs
Win CE PDAs
Blackberry, Treo & other smartphones

Disk Drives

Diskette drives
CD & DVD drives
ZIP drives
External hard drives & storage devices

Supported connectivity

- USB
- Firewire
- LPT
- COM
- Bluetooth
- IrDA
- PCMCIA
- IDE



CENTENNIAL
software

© 2005 Centennial Software Limited
DeviceWall is a registered trademark of Centennial Software Limited
All other trademarks acknowledged

www.devicewall.com

UK 01793 344055 · Australia 2 9973 4151 · Germany 0 6047 6281