



DeviceWall White Paper:

Taking control of removable media device usage

A guide to successful endpoint security



Revision 1
March 2006

1.0 Overview

For years, the major risk to IT systems was deemed to be hackers outside the organization trying to break into the corporate network. To protect against this threat, organizations invested millions of dollars in firewalls, content filtering, anti-virus and intrusion prevention solutions.

But the advent of local high-speed data (most notably USB) ports, together with the proliferation of tiny, yet high-capacity portable storage devices, has changed the IT security challenge facing organizations around the world. While the vast majority of users will have the best intentions when using these portable storage media in the workplace, there are three significant security risks to be considered:

- i) the device being used is probably not company property, and therefore not under the organization's control, yet is capable of storing sensitive company files
- ii) there is no possible way to ensure that the device will not be stolen or mislaid with sensitive company data still in place
- iii) there is an increased risk that devices brought in from outside the network could be infected with dangerous virus or malware applications – bypassing the detection and prevention solutions already in place

With less scrupulous computer users, the problem is further compounded as it has never been easier to get large amounts of sensitive data out of the office, or unwanted content onto the network, by bypassing existing perimeter security defenses.

A simple PC-level transaction can render millions of dollars in IT security investment useless.

The challenge facing IT security professionals today is threefold:

- 1) How to manage the connection of removable media devices to the corporate network via PCs and Laptops, so that only authorized staff with legitimate needs can use these devices, while unauthorized users are automatically blocked.
- 2) How to ensure that only devices owned (or specifically approved) by the company are used to connect to the corporate network, blocking any personally owned devices or unauthorized devices.
- 3) Where an employee has the right to copy sensitive data to a portable storage device, how can the integrity and security of that data be ensured – even if the device is lost or stolen?

With documented cases of extensive data loss using removable media all around the world, the fact is clear that

internal security breaches are on the rise. And with the average security incident now costing around \$200,000, what can be done to combat these threats before your organization, staff and customers fall victim?

2.0 Identifying and categorizing risks

While many of the portable devices that are increasingly turning up in the office may appear to be entirely innocent, the fact is that any device with storage capacity is a risk to your IT systems and data. Indeed, recent research showed that 90% of IT staff connect a PDA or USB stick to their work PC at least once a week.

Whether it's a 30GB iPod, a 2GB USB flash drive, a cell phone with a removable SD card or even a digital camera with flash memory – these devices can each be used to carry sensitive information away from the corporate network. Although they are marketed as being ideal for a particular data type (music, photos etc.) they can all hold any form of data you choose to load onto them – Word® documents, Excel® spreadsheets, databases etc.

What's more, the threat isn't just outbound. Any of these devices can be used to bring unwanted, inappropriate and malicious content *onto* the network.

So while many IT managers rush to configure their firewalls and content management solutions to prevent computer users downloading spyware applications from the internet, nothing is stopping these files from being uploaded locally from infected devices.

2.1 Addressing the risk

Perhaps the simplest response to this threat would be a wholesale ban on the use of removable media devices on company PCs. Simple, yes, but also highly ineffective for the following reasons:

- 1) You can't physically stop these devices coming into the office
- 2) You can't lock down USB ports in Windows without a negative effect on productivity (how would you like to lose the use of your mouse, keyboard or printer?)
- 3) A small number of users in the business will have a legitimate need to use some form of removable media device

So instead, companies need a more intelligent way to manage the devices on the network and protect the data that is legitimately copied to a removable media device.

2.2 Understanding the current levels of risk

One-size fits all is not a concept that works when it comes to IT security. What constitutes an acceptable risk for one organization almost certainly won't work for another. As such, each firm must make its own call when it comes to what devices should be used by which users – and which should be blocked by default.

The first step towards making this judgment is to understand the current level of device activity on company-owned PCs. How often are iPods[®] connected to the network? Who uses USB sticks the most?

By establishing who is using what kinds of devices and why, the organization can have more confidence that it is accurately identifying legitimate business uses (as well as many more unnecessary uses) which can be supported later – thus avoiding any productivity issues.

Using a product like DeviceWall from Centennial Software, organizations can quickly establish the current (and historical) usage levels of different types of devices by computer users across the entire network. DeviceWall automatically records the connection of removable media, including key information such as: device type, user, PC, date and time of connection and whether the connection was allowed or blocked.

2.3 Managing device connections

Only when managers understand the current levels of device usage in the organization can they then create the right security policies. Here, the policy owner needs to balance the organization's culture, industry, regulatory obligations, productivity and security concerns into a single, enforceable policy.

This means that while the organization may adopt a 'standard' security policy for device usage across the network, in reality different users will need a variety of access privileges based on legitimate business needs.

For example, training staff might have a legitimate need to carry files from one office to another on a USB stick, while senior managers would complain if they weren't able to synchronize their PDAs.

DeviceWall can be quickly deployed to all Windows PCs in the organization, automatically enforcing the company's security policies – permitting only authorized connections and blocking all others by default. In addition, DeviceWall is able to inherit users and groups automatically from Active Directory, minimizing the set-up time for policies.

When managing the use of removable media devices, it is worth considering whether the organization should limit the use of such devices to those specifically supplied by the employer to certain employees. In DeviceWall, for example, it is easy to allow nominated staff to use only a particular brand and model of USB flash disk, automatically blocking all others. This can be

an important step in helping to change user habits and prevent the invasion of lifestyle IT devices into the workplace.

2.4 Protecting data in transit

Managing who can and cannot copy data from the network to removable media devices is a critical step to ensuring endpoint security. But it still leaves organizations with a major security gap – the safety of the data once copied to the transport device.

The media is full of stories of government employees leaving USB sticks in the back of taxis, or external auditors losing unprotected CDs on airplanes. To avoid an embarrassing and potentially disastrous exposure of confidential records, a simple yet effective step would be to encrypt any data legitimately copied from company PCs to removable media devices such as USB flash drives.

As part of its data management capabilities, DeviceWall can be configured to automatically encrypt data transferred to a USB drive using the latest AES or Blowfish 256-bit ciphers. Administrators can decide between corporate (a generic, hidden key covering all authorized users) and personal (unique to the individual user, to increase privacy) keys – ensuring that data copied from a company PC can only then be re-opened on another PC from the same organization.

Combined with effective device management, automatic data encryption dramatically reduces the risks of sensitive files being taken from the network and ending up in the wrong hands.

Why encryption is not a data leakage panacea

Encryption is an extremely valuable security measure for ensuring the safety of corporate data while it is in transit. However, encrypting a USB flash disk cannot prevent the device itself from being lost, stolen or otherwise corrupted. USB disks are by their nature very small and easy to misplace. As such, encrypted USB sticks should never be used to carry unique instances of important company documents – they should only be used as a temporary data store for duplicate files.

2.5 Protecting the desktop

Just two years ago, the majority of desktops were pre-installed with nothing more than a floppy disk and maybe a CD reader. Today, the list of standard-fit equipment extends to wireless ports, on-board modems and DVD burners. Add to that the plug and play nature of USB and Firewire ports and there is a real risk that company PCs may be deliberately or accidentally used to make unauthorized connections with a plethora of insecure networks and mobile devices.

As such, organizations need to consider the possible (mis)uses of company PCs and guard against those risks considered most likely to cause damage. This might include disabling modems, preventing Wi-Fi connections or even managing access to locally-connected printers.

To help prevent company PCs leaking data or becoming exposed to foreign networks, DeviceWall allows administrators

to centrally manage any number of internal and external devices – helping to maintain the integrity of the desktop.

2.6 Compliance needs both visibility and control

In many ways, being able to quickly and graphically report on the effectiveness of security policies is just as important as the actual enforcement itself. For organizations subject to industry regulations on data protection, the ability to demonstrate which users have and have not been using removable media devices is critical to achieving full compliance.

To this end, DeviceWall not only monitors the connection of individual devices to company PCs, but also tracks the actions of system administrators, automatically recording when new client agents are deployed, or when user privileges are changed.

DeviceWall's permanent audit trail helps organizations meet their compliance obligations and provides a solid foundation for endpoint security on the network.

3.0 Summary & Next Steps

By adopting an intelligent protected-by-default approach to device usage and desktop security in the workplace, organizations can effectively combat a gaping hole in current security measures.

Preventing the removal of sensitive files from the network, or introduction of malicious content onto company PCs is a major step towards total endpoint security.

By combining this granular level of device control with data encryption, the organization can extend security *beyond* the endpoints, effectively assuring the integrity of confidential files while in transit.

To learn more about Centennial Software's DeviceWall solution, or download a free 30-day trial of the software, visit www.devicewall.com

About Centennial Software

Founded in 1997, Centennial Software has sold over four million licenses of its IT asset management and endpoint security solutions to organizations around the world. Today, the company has offices in the UK, USA, Germany, Australia and South Africa – and its Discovery and DeviceWall solutions are sold globally by a network of over 100 professional accredited resellers. For more information about Centennial Software, visit www.centennial-software.com or contact:

UK & Intl:	+44 (0)1793 836200
USA:	1-866-355-7455
Germany:	+49 (0)6047 6281
APAC:	+61 (0)2 9025 3966
South Africa:	+27 (0)83 6040 603