

# Port and Device Control in Windows

*By Jeremy Moskowitz*

*This white paper sponsored by DeviceLock<sup>®</sup>*

# Port and Device Control in Windows

*By Jeremy Moskowitz*

**Executive Summary** There are a number of threats to your data. Many of them are the result of the portability of data. The common practice of storing sensitive data on insecure devices, such as USB drives or floppy disks, exposes your sensitive data to a myriad of threats. These threats can be mitigated by implementing a port-control solution that prevents the data from being stored on unauthorized devices while balancing usability concerns to ensure continued user productivity. Although there are a variety of solutions to this problem, there is no single comprehensive solution. Instead, I recommend using a hybrid approach that implements both software and hardware controls.

## Business Need

The personal computer exists in virtually every industry and business. From small restaurant chains that track orders and restock based on computerized inventory to large enterprises that base their business on data processing, computers and computerized data touch almost every business today.

As computer use expands, so does its ease of use. Just a few years ago, computers were complex devices whose inner operations were only understood by well-educated specialists in higher education and specialty jobs. Today's average computer user is much more sophisticated, often having significant understanding of computer operations—only steps behind the IT staff.

This means that today's "average users" become tomorrow's potential attackers. The CSI/FBI Computer Crime and Security Survey data (available from [http://www.gocsi.com/forms/fbi/csi\\_fbi\\_survey.jhtml](http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml)) supports this conclusion and shows a clear trend of increasing insider attacks year after year. In 2006, almost 40 percent of the survey's respondents estimated that company insiders were responsible for over 20 percent of their losses and 7 percent of those companies surveyed estimated that over 80 percent of their organization's information losses were due to insider activities. This increase in insider attacks and the increasing computer expertise of the average user indicate that in the future more attacks will come from inside sources and that these attacks will increase in their sophistication.

There are two main problems that you need to address in order to keep your network as safe as possible and your business data secure. You need to stop data theft and prevent the introduction of malicious software.

## ***Data Theft and Loss***

Data is the key asset for your company. And, indeed, it's your number one job to manage that data and keep it confidential. This data could include:

- Unpublished financial reports
- Unfiled patents
- Trade secrets
- Payroll data
- Source code
- Healthcare records

Many industries are now affected by laws mandating data privacy and secrecy, such as Sarbanes-Oxley, HIPAA, and GLBA. These laws are intended to help prevent sensitive data from being compromised as well as to provide a method for auditing information-protection systems. But even if your company is not controlled by these regulations, controlling access to the data is important.

There are three types of attackers involved in data theft: trusted, untrusted, and opportunists.

- *Trusted attackers* are often called "inside" or "internal attackers." They are your employees or other people who have a legitimate reason to access some systems and data (hence the level of trust we permit them). Often, these attacks consist of someone accessing data that they shouldn't have the ability to, such as an employee in the human resources department accessing secret engineering plans.
- *Untrusted attackers* are external attackers that have no authorization to access your systems. They can attack remotely over the Internet or use physical force to steal data. They also frequently manipulate other people to attain their goal.
- *Opportunists* can be either trusted or untrusted attackers, but they are different in that they have no initial intention of stealing data. They might find a USB drive on a park bench that contains sensitive data that can be used for extortion. Although they didn't commit data theft, they now have your confidential information.

As far as industry regulations and shareholder lawsuits are concerned, it doesn't matter who got the data, or how. Your company is still liable for the loss. Unfortunately, until recently, most security controls have only focused on preventing data theft by untrusted attackers. With trusted attackers and opportunists becoming more of a concern, this leaves a security gap for most companies.

## ***Introduction of Malicious Software***

We're all familiar with malicious software (or malware)—virus, worms, rootkits, and so on. The 2006 CSI/FBI Computer Crime and Security Survey states that 97 percent of respondents have some type of anti-virus system in place. Yet viruses still continue to plague our systems. Part of the reason lies in how the malware defense systems are deployed. There are two main categories of malware defense: host-based and perimeter.

- *Host-based malware defense* means that each computer has some type of malware scanner and remover. When malware reaches the computer, it should be detected and removed before it can cause damage. Nothing prevents the malware from getting to the computer.
- *Perimeter malware defense* prevents the malware from getting to the computer. It is normally implemented at perimeter ingress/egress points such as firewalls, proxy servers, and email servers. When malware is detected at the perimeter it is blocked, preventing it from ever getting to any computers on your network.

Some companies employ a hybrid solution where they use both perimeter and host-based malware defense. That's the start of a good defense. But very often companies invest heavily in only one solution based on limited funds or management resources (because both solutions need to be regularly maintained to be effective). When that investment is made primarily in perimeter-based malware defense, a significant risk of infection from portable storage devices is exacerbated.

For example, a study was done in London recently and the stunning results were presented at a private security conference. Steve Stasiukonis of Secure Network Technologies wanted to find out how often people would pick up and use a portable USB drive without knowing what was on it. He purchased twelve 32MB portable USB drives. He then placed a file on each drive that, when executed, would contact his research computer to report that the file had been executed (meaning the USB drive had been inserted in a computer) and some basic information about the computer it was executed on. The researcher then placed these USB drives where he felt they'd be picked up by office workers on their way to work—the subway during morning rush-hour, smoking lounges near large buildings, and so on. At the end of the day, more than 50 percent of the drives had been inserted and the file had been run. Of that 50 percent of inserted USB drives, 100

percent were run on business computers connected to a company's network.

The USB drive illustrated in the study could easily have contained malicious software (viruses or Trojan horses) or could have been an act of industrial espionage (containing keyloggers or monitoring software). The fact that the victims were able to insert a foreign USB drive into their computer and execute code on that drive means that:

1. There were few or no security controls against this type of attack.
2. The users were not aware that they should not introduce unauthorized hardware or run unauthorized software at work.

Because of these two significant threats, most businesses should consider protecting ports that allow unauthorized data into and out of secured networks. Protecting these ports would significantly limit the likelihood and effectiveness of such attacks.

## **Common Methods for Protecting Ports**

There is no single best method to completely protect all ports in every situation. Some of the controls are expensive or difficult to implement, some require extensive setup, and some actually damage the systems they're implemented on. Many of the controls we'll talk about significantly reduce all-around usability, which usually results in less-tangible, long-term productivity loss and in angry users. Here, we'll describe and discuss many of these controls and help you understand the various options available to you.

There are three categories for port control that are broken down by implementation: physical locks, software methods, and user education. For each category we'll discuss how the control works, what benefits it provides, and what drawbacks are associated with implementation.

### ***Simple Locking Mechanisms***

The most direct method to control port access is to control access to the hardware. There are several controls in this category that range from simple to complex and from useful to marginally effective.

Note that most of these security controls require that the computer case be physically locked shut in order to be effective. Some of these controls can be reversed by a skilled user who has access to the system cabling and motherboard connectors. A user could also add new hardware to an unlocked device, thereby rendering the existing locked hardware ineffective. You might think to yourself: "My users aren't sophisticated enough for that sort of thing." Even if it's true today, tomorrow's employee could be different.

Most new business computers come with a hardware lock. So there is little initial cost for locking the hardware. But the cost of maintaining the keys,

tracking the computer and key locations, and opening lost-key computers can be significant over time. In addition, there are very few variances between the keys, often resulting in one key opening numerous computers. The weak protection and significant cost are why very few large companies lock all (if any) of their desktop computers.

One exception to the locked hardware control (which needs to be managed) is laptop computers. Because of the complexity and specialized nature of a laptop chassis, only skilled professionals can open them effectively. This inadvertently adds a thin extra level of security, specific to laptop computers. So even though laptops do not generally have lockable cases, the fact that they are complex to open means they are ever-so-slightly more secure than desktop computers (and, only then, in some cases.)

In general, while port-locking hardware solutions may initially seem like an effective solution due to their inexpensive cost and their very visible display, in the long run, their total cost of ownership can be quite high. They can take a toll on user productivity by significantly reducing the usability of computer systems. And hardware-based port-locking solutions can inflate system administration costs as IT staff is called on to physically lock and unlock computers for the countless number of exceptional cases bound to arise.

## **Epoxy**

One of the most widely publicized controls for ports today is the judicious application of epoxy, glue, or caulk to a computer's unused ports. This is implemented just like it sounds: An administrator identifies which ports are necessary for the normal use of the computer and then applies one of these substances to all other ports.

The benefits to this approach are in simplicity and cost effectiveness. Most administrators can easily figure out how to glue a USB port shut—you just jam the tube in and squeeze a little out. This control happens to be somewhat effective because it is very direct and absolute. A user cannot copy data to a USB thumb drive if there's caulk in all the USB ports. The solution can be applied to all unused ports—FireWire/1394, serial, parallel, USB, and so on. And epoxy and caulk are extremely cheap. If a tube of silicon caulk costs \$5.00 and you can protect 20 computers with it, at \$0.25 per computer there are few cheaper solutions.

However, there are numerous drawbacks to this approach. They include:

- Long-term devaluation of the computer
- Risk of electrical short or fire
- Limitation of later system expansion
- Permanency of the solution
- Labor intensive deployment

## USB Blanker Plate

This variant of the Epoxy solution is implemented by attaching a specially made plastic or metal plate over the computer's unused USB ports. This prevents physical access while still allowing some future use of the ports. The benefits are very similar to the Epoxy solution. However, there are fewer drawbacks to this approach: The blanker plates normally only cover USB ports and are only available for some specific-model computers. But at least the risk of fire and long-term devaluation are mitigated.

While there may be some value in this solution in the future, its limited availability and specialized nature currently limit its effectiveness.

## USB Port Locker



Figure 1: USB Port

As a kind of hybrid of the Epoxy and Blanker Plate solutions, there is an emerging market for specialty port-locking hardware. These are appearing as devices that are inserted into USB ports and prevent any device from being inserted. They can only be removed with a special key that the administrator retains.

There is some benefit to this solution in that it prevents USB device insertion without destroying or modifying the computer. It also allows the administrator flexibility in removing the locks temporarily when necessary. And, most importantly, USB port locking does address the principle method for data theft today—the USB ports themselves where users can attach “thumb drives” or even larger devices.

Unfortunately these locking devices don't scale to large businesses very well. Applying locks to each USB port throughout a large company is a nearly impossible task, and managing those installed devices is even more daunting. IT staff would need to be dispatched every time a user obtained an authorized PDA or switched to a USB mouse. Key management would certainly be impossible unless a very limited number of keys were used, but that would significantly lower the security of the deployment. All this trouble and the solution can only lock USB ports.

## Physical Disk Locker

Overall, USB port lockers could be useful in small or specialized deployments. But they simply don't scale well and are prohibitively expensive today at about \$5.00 per port.



Figure 2: Physical Disk Locker

Yet another physical control is the device locker. This takes the form of a physical device that prevents the insertion or removal of removable media, for example, a floppy disk. Once it's inserted, it prevents any other disks from being inserted and can only be removed with a special key. There are also general-purpose drive-bay lockers that can lock out a variety of media, such as the one shown here.

The benefits and drawbacks of physical disk lockers are similar to those of port-locking devices. They are simply an extension of the same type of physical security control. However, physical disk lockers are even less scalable due to their bulk and expense, with some costing \$40.00 per unit or more.

## **Cabling Changes**

One of the easiest and least destructive methods for preventing access to ports is to disconnect the cable connections *inside* the computer. If a computer's USB front and rear panel cables are removed from the motherboard, a device simply cannot make a connection to the computer. This type of strategy also works on other ports and removable media devices such as CD-ROMs and floppy drives.

One important benefit is that it's relatively easy to implement this control. Simply unplug the ports or devices during deployment, before the user gets the computer. This sets the user's expectations that the ports do not work and ensures that the computer is not compromised before any other security controls can be implemented.

Positive aspects about this solution are its simplicity and its cost. The only cost involved is the labor required to remove the connections and then lock the computer's case. Additionally, it is exceptionally difficult for a user to circumvent this security control without breaking into the computer's locked case.

Unfortunately there's a fairly major drawback: This security doesn't work on laptops. Most laptops are not user serviceable and only highly skilled technicians understand how to open and manage the hardware. So you cannot disconnect cables inside the case yourself—you need to pay someone to do it properly.

Another major drawback of this security control is the effect on usability. If an authorized user cannot use any of their ports, it may impact their productivity.

## **Software Controls**

There are several firmware and software controls available today to help block ports. These controls can help improve the effectiveness of the hardware controls in the previous section. But, as you'll see, none of those sampled here prove to be the ultimate panacea. Most can be circumvented with little or no trouble and require no specialized knowledge to defeat.

For large networks encompassing more than one hundred endpoints, these controls have some flexibility and efficiency advantages over the hardware controls in the previous section.

These controls include:

- BIOS Port Locking
- Floplock.exe
- Windows Group Policy Alone
- Add-on End-point Device Security Solutions

Let's talk about those solutions now and explore how each one can help address the problem.

**BIOS Port Locking** The computer's BIOS (sometimes called CMOS) is the software portion of the interface between the higher-level operating system and the physical devices on the computer. Most current BIOS versions have extensive controls for configuring and disabling all ports on the computer. BIOS software can be used to disable all of the common built-in ports and drives, including:

- Floppy disks
- CD-ROM and DVD drives
- Serial ports
- Parallel ports
- USB ports
- 1394 ports

The following screenshot from a recent BIOS version shows a basic USB configuration screen. Note that the USB is disabled.

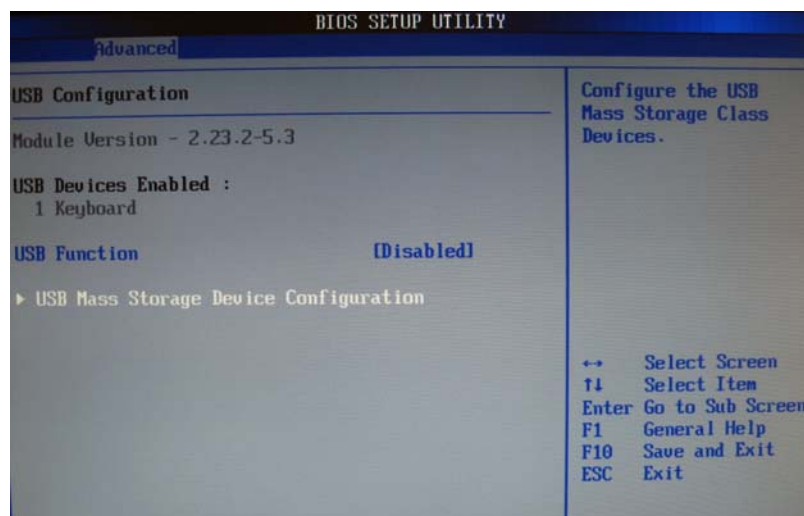


Figure 3: BIOS Port Locking

The next screenshot from the same BIOS shows the configuration of other ports such as parallel, serial, and 1394. Each of these can be configured independently.

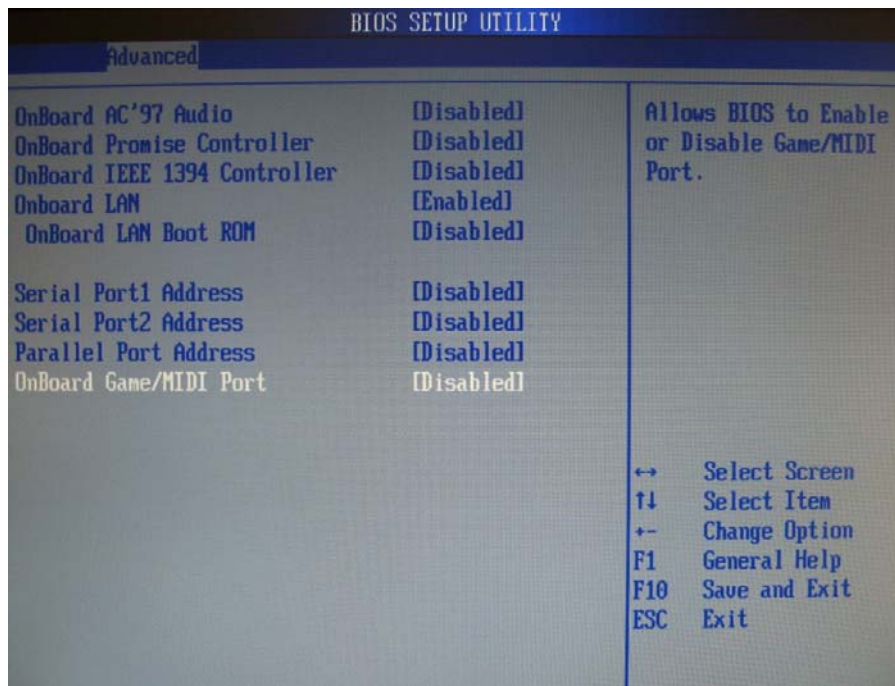


Figure 4: BIOS Port Locking cont...

The BIOS can also control the boot order of the computer to ensure that only trusted devices such as the hard drive are bootable. Most computers can have a password added to the BIOS so that it only allows modification by approved administrators. All of these benefits are included in the system at no extra cost—it's just part of the basic computer operation.

While editing the BIOS is a more flexible method of port locking than epoxy fill and cabling changes, it still shares most of the same weaknesses. The relatively low cost of initial deployment is soon superseded by a high total cost of ownership because there is no provision for centralized management. Additionally, there is no flexibility with regard to applying user- or device-specific policies. As a result, the BIOS method of port locking is somewhat better than the above-mentioned destructive methods, but still not sufficiently flexible and ultimately an expensive way to go.

## Floplock.exe

High-speed storage and transfer devices like USB and 1394 devices have not always been the best method for transporting data. Not too long ago, floppy disks were the only ubiquitous, portable media available. They were cheap, easy to use, the drives were installed on virtually every computer produced, and in their time, they stored enough data to be useful.

Because of the known threats of data theft and malware introduction, Microsoft decided to provide some preventative software for its Windows products. They released Floplock, a tool available for download or included in the Windows NT Resource Kit.

Once this tool was installed, only an administrator could access the floppy disk drive from Windows.

While the tool itself was useful for those who needed it, its actual implementation proved difficult. And, floppy drive popularity is waning—most computers don't even come equipped with a floppy drive anymore.

There are several tools of this type besides Floplock. They are all much the same thing—specialized operating-system-level software that prevents access to a specific device. But most of them have limited functionality and some even destabilize the environment due to their incomplete and untrusted nature. You should avoid this type of software if there is an alternative available, which fortunately there is.

## Windows Group Policy

Microsoft Windows has used different types of policy-based control throughout Windows NT, Windows 2000, Windows XP, and Windows Server 2003. Windows has more-specialized settings that let an administrator make specific configuration changes to computers and user environments.

Currently, there are several built-in Group Policy controls that can help an administrator control some access to removable media and restrict the installation of new removable devices. They include:

- User Configuration | Administrative Templates | Windows Components | Windows Explorer | **Hide these specified drives in My Computer**
- User Configuration | Administrative Templates | Windows Components | Windows Explorer | **Prevent access to drives from My Computer**
- Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options | **Devices: Allowed to format and eject removable media**
- Computer Configuration | Windows Settings | Security Settings | Local Policies | User Rights | **Load and unload device drivers**

Although these policy settings are more comprehensive today than in the past, they still fall well short of what you might consider a true port-locking security control. They only control certain aspects of port usage and do not offer a comprehensive protection scheme, which would include elements of intelligent device authorization to provide both flexibility and security. In addition, while Group Policy is an effective configuration control, it should not be solely relied upon for critical security controls, as aspects of Group Policy can be defeated with expert knowledge.

## Add-on End-point Device Security Solutions

But the tools in the box only go so far. Ideally, you'd want to manage end-point security controls for all plug-and-play ports, drives, and removable devices on Windows computers. A solution like this should be able to address the following concerns:

- Simple and flexible roll-out and ongoing management across many hundreds and even tens of thousands of endpoints
- Highly granular setting of security policy permissions to allow intelligent device authorization
- Robust data auditing and shadowing options.

One example is DeviceLock<sup>®</sup> from SmartLine Inc. DeviceLock<sup>®</sup> administrators have precise control over which users and groups have which level of access to which devices on which computers and when that access is allowed. DeviceLock<sup>®</sup> can discretely manage any physical Windows port or drive with its layered security architecture and White List options, while ensuring that even local computer administrators cannot tamper with its enforcement.

DeviceLock<sup>®</sup> provides a fully-integrated Group Policy Management MMC console that snaps into the Active Directory (AD) Group Policy Editor to directly create native Group Policy Objects for distributing peripheral port and device security settings. This allows DeviceLock<sup>®</sup> to be as scalable as any AD environment and to efficiently manage hundreds of thousands of Windows desktops with a tool that is familiar to all Windows administrators. DeviceLock<sup>®</sup> can also manage any LDAP network of Windows computers (Novell, OpenLDAP, etc.), including mixed-network operating system environments.

DeviceLock<sup>®</sup> gives administrators comprehensive control of device access permissions by individual users or groups. Administrators can set permissions for a wide range of devices including CD-ROMs, DVD-ROMs, and floppy disks; serial, parallel, infrared, USB, FireWire ports and devices; WiFi (802.11), Bluetooth, and MP3 devices; and the ports/memory cards for digital cameras, phones, and PDAs. System administrators can assign access privileges by class (for example, "all USB Storage devices") or by individual device model or port (such as allowing a specific user to only use a particular USB removable drive on specified computers). Administrators can also specify that read-write devices such as removable floppy, CD, and Zip drives be accessed in read-only mode. Optionally, administrators can populate a White List permission database of authorized USB and FireWire device models or serialized devices, such that they are unlocked on specific computers or for assigned users or groups.

## ***Behavioral Controls***

We've discussed numerous technical hardware and software controls to help protect ports from unauthorized access. These controls are all useful to some degree in helping prevent data theft and malware infection. But there are some very important people- and policy-centric controls that should also be put in place to help prevent the same events from occurring. Implemented alone, without any technology enforcement, these non-technical controls are not dependable. They deliver unpredictable and unreliable results because they're largely based on human implementation, and people are unpredictable and unreliable (both unintentionally and deliberately). Yet, strong training efforts and policy statements with regard to the proper use of computer resources are essential to ensure the security of a company's data and the health of its networks.

## **User Education**

The impact of the human element in maintaining or compromising security cannot be overstated. People can make or break *any* security scheme. In fact, if people weren't part of the security equation we wouldn't need to have any in-depth discussion, since there would be no such thing as the connection of an unauthorized device to an unprotected port. While your company's staff is not the sole cause of computer security breaches their actions (or inactions) certainly do contribute to your organization's overall computer security.

A significant threat to any organization is *social engineering*, which is the act of manipulating people for a nefarious purpose. Because people are more variable than physical or logical controls, there's a higher likelihood of an individual or group of users being the weak link in IT security. For example, a recent study was conducted by the organizers of *Infosecurity Europe 2004* to determine how many users would give their password to a stranger. The stranger posed as a survey taker and interviewed people outside their company headquarters. This survey included generic security questions but always focused on getting users to disclose their corporate password. There were two shocking statistics from this survey:

- 34 percent of participants gave their password to the surveyor immediately
- 70 percent gave up their password after being offered an incentive to participate in the form of a bar of chocolate

The participants didn't know what the surveyor would do with their password and relied on the good nature of the surveyor. In this case the surveyor was just gathering statistical information and didn't use the data to attack the organizations affected. But the same technique could easily be used by an attacker with similar success (as long as they had a sufficient supply of chocolate bars).

For more information on this study, read the report at:

<http://www.net-security.org/secworld.php?id=2075>

Luckily, people can usually be taught the difference between right and wrong behavior, and between acceptable and unacceptable actions. A strong user education program can be very effective in preventing a large number of security breaches. Users can be taught a few simple concepts relating to the security risks of data loss and malware introduction, including:

- **Proper data handling procedures**—What data they can copy, where they can copy it to, and how to handle its disposal when they're finished with it.
- **Corporate policy for removable storage devices**—What storage devices can be used (if any) and what the policy is for their use. For example, some companies forbid any type of removable media from entering or leaving their premises. Other companies allow only certain types of devices that have built-in security safeguards to help prevent data loss in case of theft.
- **How malware infects and spreads between computers**—The potential downside of copying files from the Internet and bringing them to work. Most users don't understand the effect that "just one file" can have on their organization, and would happily stop this behavior if they understood the ramifications.

User education is often expensive in terms of lost productivity, because you need to take people away from their primary jobs to attend training. It is also a recurring cost, because training must be periodically updated and repeated to ensure that people remember it and remain vigilant. There is a significant up-front cost in obtaining training material, classrooms, instructors, and so forth. And even with all this investment, people can still decide on their own that they will not follow the security instructions that they've been given. People often circumvent or disregard security controls that they don't agree with or see value in, and there's very little you can do about that. Despite these drawbacks, user education is a critical element of any broad security plan. Employees are often the most important security control at your disposal, so it's usually worth investing some time and effort in this area. But it's simply impossible to rely solely on people to prevent security incidents from occurring. Even if everyone at the company truly tried to "do the right thing", it would still be impossible.

## **Restricting Possession of Disallowed Devices**

One way to stop an attacker from inserting an unauthorized device into a port is to ensure that such devices never enter the building in the first place. With this plan, you can be mostly certain that even if port locking hardware and software controls fail the attacker will still have no way to exploit the weakness. This sounds like a great idea, but is it reasonable?

In practice it is nearly impossible to implement. Only enterprises with the most sensitive data can begin to implement such a tight security control. Even then, only the highest security areas have this type of control in place. Consider the cost of searching every employee on arrival and departure, examining every briefcase, folio, and package (and even each wristwatch and ballpoint pen) as it enters and leaves the property, checking the garbage to ensure that data doesn't leave that way, and so on. In the recent movie *The Recruit*, one fictional character, Bridget Moynahan, smuggled data out of a secure area by hiding a USB drive in the base of her coffee cup. "Being sneaky" isn't an unusual way to circumvent such stringent security controls.

**Progressive Methods for Protecting Ports** The immediate future is showing great promise for an increase in the number and effectiveness of port-locking controls. Fueled by current demand for some type of comprehensive security control, many software solution vendors are taking a critical look at how they can provide value in this area. Their major value is primarily based on the complexity of using several redundant current controls versus using fewer, less expensive, and more effective tools in the future.

Two strong examples of progress in this area are the security features built into Windows Vista and the latest version of DeviceLock<sup>®</sup>. Like the physical controls described earlier, these software solutions can be used independently or combined to provide an even stronger solution.

**Windows Vista** At the time of this writing, Windows Vista is just about in final production with an anticipated launch of January 2007. Vista (Longhorn) Server is scheduled for release in the 2nd half of 2007. Vista is the next generation of Microsoft Windows client operating systems built on the sturdy Windows NT platform. As expected, Vista includes a number of security enhancements, one of which directly addresses port locking.

Device Management and Installation (DMI) is a new feature of Windows Vista. It's designed to provide an administrator with granular control over the types of portable devices that are recognized by the system. It works by watching the computer bus for device insertion.

When a new device is detected, DMI uses administrator-configured rules to determine whether the device is allowed or disallowed. These rules include (the names are paraphrased here for readability):

- Default behavior for device installation (allow or disallow)
- Prevent devices that match a class ID or device class from installing
- Allow devices that match a class ID or device class to install
- Exempt the administrator from these rules

If the device is allowed, the device driver is loaded and the user can use the device. If the device is disallowed, DMI displays a message indicating that the administrator has disallowed this device and the device driver is not loaded. This prevents the device from being recognized by the operating system.

The DMI rules are policy-based and will normally be deployed to Vista computers through Group Policy settings available when Vista releases. Once the administrator creates the rules, they can be deployed like any other policy.

Microsoft has categorized the use of DMI into three main scenarios.

- **Prevent installation of all devices.** In this case, only an administrator can install devices.
- **Allow installation of only authorized devices.** Only devices identified by the policy are installed.
- **Prevent installation of only prohibited devices.** Only devices identified by the policy are disallowed.

As stated, the main benefit of DMI is that it is rule-based and can be deployed to Vista (and, presumably codename Longhorn Servers) via Group Policy. And, it's undeniably convenient to have a feature built right into the operating system.

However, DMI lacks a few key features that may be important to you. Primary among these is simple configuration. To configure DMI, you need to follow a cumbersome process of inserting allowed or disallowed devices, using a tool to read their device classes and device IDs (long alphanumeric strings), and copying those IDs into a Group Policy Object. This process requires you to have at least one of each device class or device ID.

Additionally, very little flexibility is available with DMI. You can either exempt the administrator or not, and then allow or disallow installation. There is no conditional or intelligence-based decision. In this respect it works almost identically to Microsoft's Software Restriction Policy (SRP).

It is also possible to have data theft occur directly from your servers. To prevent this kind of attack, only the DMI features built-in to codename Longhorn server will help. There is no such protection for Windows Server 2003. Therefore, as a total security stance, a Windows environment would only begin to see protection with both Windows Vista on all desktops/laptops and Longhorn server on all servers.

## ***Future Device and Port Management with Auditing***

As computing resources, connections, and media-equipped devices become more numerous around your company, the need to intelligently authorize devices will only increase.

The explosive popularity of USB Flash drives, PDAs, smartphones, MP3 players, and other mobile devices is a powerful end-user force that your security staff needs to address. It will be nearly impossible to enforce a complete prohibition of non-threatening devices (such as USB-connected keyboards, mice, and printers) or to lock out sanctioned portable storage devices that have password protection and encryption. Add-on solutions like DeviceLock® provide the necessary flexibility and granularity—right down to efficient handling of special cases, such as allowing a specific serial-numbered device and/or issuing temporary access to a drive or port in an emergency while offline or via remote consoles.

End-point security tool sets are also expanding to offer further forensics evidence to IT security officers. Facing the nightmare scenario of suspecting an insider has violated security policy and is systematically stealing information, the security staff has been at a loss to answer the question: “What records are at risk?”. Without the addition of third party tools like DeviceLock®, it would be virtually impossible to know what files have been copied to a removable storage device. Even if a standard logfile has been maintained on the users computer, there is always a possibility that the log has been altered or that the proprietary information has been copied anyway (but disguised by encrypting, compressing, or just by changing file names.) Therefore, removable storage and other mobile devices should be not only be under control but also under audit. Logging and auditing are becoming important aspects of corporate security and compliance enforcement.

Neither BIOS/Epoxy nor “native” Windows Group Policy solutions can provide the kinds of auditing you need to enable you to know that a potential data copy has taken place. However, software like DeviceLock® provides secure audit logs and accommodates centralized collection of shadow copies of all of the files downloaded and uploaded through peripheral PC ports and drives. The result is a non-refutable record of removable storage device activity that can be made tamper-proof for even local administrators. If a break with corporate policy is ever suspected at a certain endpoint, an IT security team would then have all the forensic evidence needed to prove or disprove the suspicion.

## Summary

Hardware locks are a cheap and efficient way of inhibiting some data loss and may work for some limited scenarios. But they're unpredictable, hinder usability, and may damage valuable assets. Some native software controls are difficult to manage and do not provide auditing or enough granular control to allow an administrator to properly control access to some devices while permitting the use of others. User education, while an effective technique, cannot be relied on as the only protection against data loss and malware introduction.

For the best flexibility and most granular device control today, consider using end-point device security software like DeviceLock® in conjunction with physical restriction policy and appropriate user education.

Remember: Technology alone is not a panacea.

## About the Author



Jeremy Moskowitz, MCSE, MCSA, is the Chief Propeller-Head for Moskowitz, inc. ([www.moskowitz-inc.com](http://www.moskowitz-inc.com)) as independent consultant and trainer for Windows technologies. He runs [GPanswers.com](http://GPanswers.com), and [WinLinAnswers.com](http://WinLinAnswers.com); two community forum for people to get their toughest Group Policy and Windows/Linux integration questions answered.

He can be found speaking at IT conferences and inside corporations all over the world. He has authored or co-authored six books, including *Teach Yourself Windows 2000 Server in 24 Hours* (SAMS) (translated into a dozen languages), the highly acclaimed *Group Policy, Profiles, and IntelliMirror* (Sybex), and *Windows 2003: Active Directory Administration Essentials* (Windows & .Net Magazine).

Since becoming one of the world's first MCSEs on both Windows NT and Windows 2000, he has performed Active Directory, Group Policy, and Windows infrastructure planning for some of the nation's largest organizations.

## About the Company

**DeviceLock®** is manufactured by **SmartLine Inc** ([www.protect-me.com](http://www.protect-me.com)), a leading developer of well-integrated, cost-effective network management software solutions. SmartLine's many customers include major technology stakeholders, large U.S. and international financial companies, telecommunications conglomerates, government agencies, classified military networks, and educational institutions.

For additional technical or purchasing information, please contact us at [sales@protect-me.com](mailto:sales@protect-me.com).

### **SmartLine Germany:**

Halskestr. 21, 40880 Ratingen  
TEL: +49 (2102) 89211-0  
FAX: +49 (2102) 89211-29

### **SmartLine Italy:**

Via Falcone 7, 20123 Milan  
TEL: +39-02-86391432  
FAX: +39-02-86391407

### **SmartLine UK:**

The 401 Centre, 302 Regent Street, London, W1B 3HH  
TEL: +44-07779-28-27-21  
FAX: +44-20-7691-7978

### **SmartLine USA:**

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583  
TEL (toll-free): +1-866-668-5625  
FAX: +1-646-349-2996

DeviceLock is a registered trademark of SmartLine Inc. Other registered trademarks are property of their respective owners. COPYRIGHT ©2006 SmartLine Inc. ALL RIGHTS RESERVED. Reproduction or copying of images is strictly prohibited.