

## **USB Lock RP** (Remote Protect)

### **Don't Just Lock it Down - Lock it Up!**

**If you answer yes to these questions, this is for you.**

- Do you have 10 or more workstations connected to your Network?
- Do any of your workstations have CD/WR, USB Ports or Bluetooth?

#### **Contents**

- What is insider threat?
- Business Impact - Top 5 Threats
- Legal issues - Are you promoting piracy?
- Disabling USB - How practical is it?
- Endpoint Security with USB Lock RP
- USB Lock RP - Top 5 Features
- USB Aware - Detailed reports of files copied
- Make USB device READ ONLY!
- Advanced Monitoring - Get e-mail alerts
- Contact

### **What is Insider Threat?**

Most organizations take time, energy and money to build enterprise security but leave out the single largest factor for data theft and compromise. - Insider Threat

According to a 2005 FBI Computer Crime Survey, 44% of organizations have reported network intrusions from within their own organizations. Technology analyst Gartner warns that portable devices containing a USB or FireWire connection are a serious new threat to businesses. In their report, Gartner named portable storage devices as a significant security risk in the workplace and advised that these can be used both to download confidential data, and also to introduce a virus into the company network.

Some of the Top reasons for Insider threat include:

- Internal Politics
- Love interest
- No Promotion
- Humiliation
- Bad Manager
- Personal grudge
- Money

### **Business Impact - Top 5 Threats**

Every day, USB devices are making a huge progress in manner of size and capability. Today we have the following concerns when we speak of USB as a future threat:

1. Viruses – Users can either bring in infected documents from home, or take home a business document to an infected PC, update it, and return it to a corporate file server. Unless your antivirus policies are very aggressive, and you actively scan all files stored on your network, Flash Drives can present a new vector for computer viruses that is nearly impossible to defend against.

2. Data theft - Corporate espionage is a largely underreported problem in India and in many cases these are crimes of opportunity. Disgruntled employees can take home client lists, sales forecasts, or research data in a few minutes. (At 1/Mb per second, a user can copy a 120Mb file to a flash drive in 2 minutes.)

3. I-pod / MP3 Players– Sharing, downloading and listening to music on company premises during work hours affects the overall performance of a team and its approach towards professional work.

4. External USB CD/DVD Writers – People, on pretext of working overtime can bring in external writers to attach on USB. This means entire data on the network can be written on DVD's for as little as 8 minutes for 4.5 GB of data.

5. Portable applications – Are you aware that there are many applications like Nero Burning Rom, hacker related tools for compromising data and even an Entire OS based on Linux for stealing server passwords available that work from a single USB device?

## **Possible Legal Issues –**

Are you promoting piracy? Why leave the possibility open?

Do you want people to use your resources and company work hours uploading and downloading music?

Would you like your employees to share music and movies freely within your network thereby inviting piracy and possible legal issues?

Controlling USB use goes a long way in curbing external legal threats.

### **Disabling USB –**

How practical is it?

Most Administrators think of blocking USB access at the Hardware level. How practical is it to control the USB port in this manner? What are the issues you will face doing it this way?

1. Most modern keyboards and Mouse come with USB interface
2. All printers / Scanners come by default with an USB interface
3. Web Cams operate via USB only
4. Modern Wireless LAN cards come with USB interface
5. Most data-cables connect to other devices Via USB

It is simply not effective to block USB ports at the hardware level. What is required is a smart solution, a solution that can control what you need and allow essential devices to operate smoothly with the USB port when needed.

### **Endpoint client security**

Control your enterprise endpoint client security with USB Lock RP. Now you have the solution! Control who can access USB ports for copying data! Unless a password is entered, a user will not be able to access the USB port / CDROM Drive / CD-DVD Writer or Bluetooth Devices.

Centralize Administration of all client computers in your Network. From a centralized control interface, you can now Block or Allow access to USB Ports / CD-DVDR/ RW/floppy and Bluetooth devices! You can also view log files, shutdown and restart remote machines.

### **USB Lock RP - Top 5 Features**

1. Agent installs as service to give complete endpoint security
2. Remotely control access to USB Ports / CD-DVD-R/RW and Bluetooth
3. Client logs "Blocked" attempts to USB on a shared network path
4. It is smart enough to NOT block Mouse / keyboard / printer and webcam on USB.

5. WORKS WITHOUT ACTIVE DIRECTORY.

### USB-Aware

Can I allow the operation of the USB ports but keep a watch on what files are being copied from my company to the USB storage device?

Yes, With USB-Aware, a unique way to monitor the USB access, we can give you detailed reports of what data is exactly being copied from your organization. This is an optional pack you can buy as an add-on.

USB Aware – provides:

1. Detailed reports of files copied.
2. Make a USB device READ-ONLY.
3. Now you can also make your USB just READ ONLY. You can deny WRITE access to the USB network or per client wide to ensure hassle-free security.
4. Get Email alerts whenever someone tries to access USB in any of your secured locations.

With Alert notifications, you can always focus on your work without getting worried who is trying to steal your data! Get hourly notifications from all the machines you manage. With detailed or short reports.

### FAQ's

What if a user kills the process via task manager?

*He cannot. If a user attempts to kill the process, the machine gets automatically locked for 15 seconds and the user is warned of unauthorized access.*

What if a user tries to connect a Pen/flash/mp3/iPod type drive?

*The machine will immediately give a locked black screen and a 15 second timer will start. If the user does not remove the pen drive, in 15 seconds the machine*

*will shutdown, preventing theft effectively. If the user removes the pen drive within 15 seconds, the machine resumes to its normal state.*

What about CD-ROM drives and CD/DVD-Writers?

*USB Lock RP can remotely block CD-ROMs and DVD Writers. You can enable access to the same on a per need basis from the control center.*

Can I actually know when a user is trying to use a USB storage device silently?

*Yes, USB Lock RP will automatically detect the attempt, Log it on a network shared folder and enabling a log monitoring tool to send you instant SMS or E-mail Alert.*

Additional benefits:

1. Protection History reports
2. Global security reports
3. Capable of shutting down and restarting client machines
4. Average consumption 0% CPU/3,980 Kb
5. Permanent use license – non transferable

### **Contact :**

US Diversified Tech, LLC  
PO Box 599  
Nashua, NH 03061

1-888-361-8718 Phone  
1-603-484-1942 Local  
1-603-484-2698 Fax

**Visit :** <http://www.LaptopSecuritySolutions.com>

**E-mail :** [support@LaptopSecuritySolutions.com](mailto:support@LaptopSecuritySolutions.com)

Representing: Advanced Systems International S.A.C. Peru