FIND.
FIX.
DEFEND.

altiris®

Enforceable System Security

Best Practices for Managing and Enforcing USB Security

Five Questions You Should Ask About Universal Serial Bus (USB) Security

White Paper

June 22, 2006

ABOUT ALTIRIS

Altiris, Inc. is a leading provider of service-oriented management software that enables IT organizations to easily manage, secure and service heterogeneous IT assets. Flexible solutions from Altiris help IT align services to drive business objectives, deliver audit-ready security, automate tasks, and reduce the cost and complexity of management. For more information, visit www.altiris.com.

Altiris, Inc.
588 West 400 South
Lindon, UT 84042
Phone: (801) 226-8500
Fax: (801) 226-8506

CONTENTS

Introduction **1**
Janitor in Disguise 1
The Rising USB Threat 2
FIve Questions You Should Ask **4**
Won't my existing security solutions protect against UBS security breaches? 4
Can I secure USB ports without hampering the productivity of my employees? 4
Can I enforce USB security without overburdening my IT staff? 5
What capabilities should I look for in a USB security solution? 5
Is the USB solution part of a broader, holistic security approach? 6
Removable Storage-Device Security from Altiris **8**
Conclusion **9**

INTRODUCTION

Many companies live in fear of the day when someone steals their sensitive corporate data. That's why companies deploy firewalls, manage wireless connectivity, control network-access privileges, and install antivirus software. But these solutions focus on the front door and can leave the back door wide open to a new kind of security breach.

Like Trojan horses, USB and other removable storage devices such as Apple iPods, BlackBerrys and flash drives enter the corporate environment and attach to computing assets without arousing suspicion or triggering security alerts. Characterized by ever-increasing storage capacity, these devices can be used to surreptitiously download larger and larger amounts of sensitive corporate data.

As corporations determine the most appropriate method for handling this new threat, there are five questions you need to ask when considering a USB security solution.

Janitor in Disguise

About a year ago, a security professional conducted an experiment to demonstrate how easy it is to steal corporate data. Disguised as a janitor, he walked into an office with an iPod. In plain sight, he connected the iPod to a corporate computer's USB port and proceeded to download thousands of sensitive documents, executable files and unlicensed software to the iPod, bypassing the normal startup process of the machine with a specialized CD-ROM designed to circumvent traditional security mechanisms. The whole operation took two minutes.

Had the theft been real, those two minutes might have changed the entire course of the company.

Data theft costs corporations more than $50 billion a year. Seventy percent of data theft involves downloads to removable storage devices such as flash drives, DVDs and CD-ROMs. Companies realize that data loss not only could generate ugly headlines and put them at a competitive disadvantage; it could also place them in legal jeopardy for violating state, local and federal privacy regulations. That's why these companies deploy firewalls, manage wireless connectivity, control network-access privileges, and install spam and antivirus software.

These security solutions are the equivalent of locking the front door, installing extra deadbolts and placing a heavy table behind the door to prevent a burglar from entering. Traditionally, companies focus on the front door and often times leave the back door unlocked. As the janitor in disguise demonstrated, removable storage devices are the fastest-growing corporate security threats. These benign-looking devices can be used to download lots of sensitive corporate data without arousing suspicion or triggering security alerts.

USB drives, CDs, and iPods are becoming the modern-day equivalent of Trojan horses for corporate data theft.

The Rising USB Threat

Two converging trends have recently escalated the data-security threat: The explosion in the number of high-capacity storage devices and the growing mobility of the workforce.

The increasing number of removable devices, coupled with ever-increasing storage capacity, continue to reduce the cost and make these devices as commonplace as a set of car keys. Today, the estimated number of devices with external, removable storage in use by consumer is in the billions. Audio devices, MP3 and other media players, for example, are phenomenally popular. Apple's iPod alone has sold more than 25 million units worldwide since its debut, putting gigabytes of storage in the palm of any hand. USB flash drives and memory cards found in cameras, mobile phones and personal digital assistants (PDAs) can also download gigabytes of information from any PC or notebook without requiring special software. With the new devices on the technology horizon, the threat will continue to escalate.

With more and more employees bringing these kinds of devices to work, potential thieves don't have to hide the portable devices in pockets or purses. They can use them in the open, pretending to be listening to music or downloading pictures while they steal company data.

But corporate data theft doesn't always happen inside the four walls of the office. A second emerging trend—the growing mobility of the workforce—means that sensitive corporate data can often be found on notebooks and other mobile devices. Experts say that more than 40 percent of work today happens away from the office. People work from home, hotels, coffee shops and airports. Because of this mobility, the majority of the latest corporate data—two-thirds by one estimate—resides on endpoint devices such as desktops, notebooks and PDAs. The data is easily accessed.

Thieves can gain access to this data in several ways: by surreptitiously connecting USB devices to the devices of distracted users; by stealing laptops altogether; or by gaining access to computer files via wireless eavesdropping.

Recent headlines are filled with chilling examples of security breaches involving endpoint devices. Thieves stole sensitive personal information about 26.5 million U.S. veterans—including social-security numbers and birthdates—after a Veterans Affairs employee brought the information home on a notebook computer. Ernst & Young recently disclosed that one of its notebook PCs had been stolen. The notebook contained the personal information of current and previous IBM, Sun Microsystems, Cisco, Nokia and BP employees. Outside a U.S. military base in Bagram, Afghanistan,

removable USB storage devices containing sensitive military data were on sale at a bazaar. The data was apparently stolen from offices inside the base by Afghan staff working there.

Most of the publicity about data theft has often involved lost or stolen notebook computers. USB security breaches haven't garnered as many headlines for one, simple fact: Many companies don't even know when USB breaches happen.

FIVE QUESTIONS YOU SHOULD ASK

No wonder, then, that more and more companies are looking for USB security solutions designed specifically to prevent these stealth attacks. But not all security solutions are created equal. When considering a USB security solution, companies should ask five key questions:

1. Won't my existing security solutions protect against UBS security breaches?
2. Can I secure USB ports without hampering the productivity of my employees?
3. Can I enforce USB security without overburdening my IT staff?
4. What capabilities should I look for in a USB security solution?
5. Is the USB solution part of a broader, holistic security approach?

Let's consider these five questions.

Won't my existing security solutions protect against UBS security breaches?

Most "old-style" security measures such as firewalls are perimeter defenses designed to keep data thieves out, not protect against inside attacks. According to experts, most data and identity thefts occur inside the enterprise. Firewalls can block ports, but they are not designed to manage file-system transfers.

Most network-access controls won't prevent USB devices from attaching to endpoint devices such as PCs, either. In fact, USB downloads are typically not detectable, and they don't usually leave an audit trail.

Unless your security solution includes specific, policy-driven and location-aware protection against unauthorized use of USB ports (this issue will be discussed in more detail later in this document), your company is not protected against the fastest-growing threat to corporate security.

Can I secure USB ports without hampering the productivity of my employees?

The USB ports on endpoint devices are there for a reason: They enable workday productivity. The keyboard and mouse connect via USB ports. Workers also use USB ports to do things like synchronize computing and communications devices, transfer multi-media sales presentations, print documents and back up work.

To control the use of USB ports, companies have two choices. One extreme approach is to pour glue into the ports or otherwise disable them via hardware modifications. While this might help eliminate USB risks, it can also strangle productivity. The other option is to centrally control access to these USB ports via software, using policies that enforce when and where

the ports can be assigned one of three states: Read-only, read-write, or disabled. Central control of USB states means that employees won't have to be bothered with security options and prompts. Policy-based enforcement will happen transparently, allowing users to do their work safely without jeopardizing security.

Can I enforce USB security without overburdening my IT staff?

IT staffs are already stretched to their limits as they deploy and manage a growing number of users and devices while struggling to keep networks up and running. A USB security solution should not add to this burden.

There are ostensibly simple USB security solutions available that in reality require lots of attention from IT staff. For example, software solutions exist today that simply notify the IT staff whenever someone attaches a device to a USB port. However, the thousands of daily alerts that result will require constant monitoring. By the time a staff member investigates, a thief could be out the door.

Other USB solutions require companies to compile and manage lists of "safe" and approved devices that can attach to USB devices without compromising security. In a typical IT environment characterized by changing users and devices, these lists can be difficult and time-consuming to manage.

Also, security solutions designed to support only devices from a single manufacturer don't take into account the heterogeneous nature of today's IT environments—and they won't afford complete protection.

The kind of USB security solution that will not hamper the productivity of the IT staff will be centrally managed, via a single console, and allow IT staff to control all USB ports and access states using software tools.

What capabilities should I look for in a USB security solution?

An effective, efficient USB security solution is characterized by the following attributes.

- **Centralized and policy-based**—Automated rules that dictate the state of a USB port depending on the user's location and role within the organization should be the cornerstone of an effective USB security solution. Once granular policies are established, they can be centrally managed and pushed out to individual endpoint devices. A centralized, policy-based approach relies on automation to apply different rules to different users and devices, freeing IT staff to focus on possible breaches rather than administration.
- **Location-aware**—A policy-based solution should allow different rules to be applied to USB ports depending on location. When a notebook or other computing device is in a riskier environment such as an airport,

polices can be set to restrict all USB connections. When the device is inside the company's walls, read-write access might be permitted. In other locations, such as the user's home, read-only access might be applied.

- **Self-defending**—The solution should make it impossible for the end user to defeat the security policy by turning off the policy-enforcement engine. Avoid systems that use prompts to allow users to assign security on their own endpoint devices.
- **File-system-level operations**—Ideally, the removable storage-device security solution should operate at the file-system level to ensure control of all devices (external hard drives, CD/DVD-ROM, other forms of removable storage, etc.) that act as a file system. Meanwhile, the solution should not disable devices such as a USB mouse that do not pose a threat.
- **Auditable and trackable**—The USB security solution should keep track of policy-enforcement actions as well as attempted USB activities and suspected attacks. This kind of tracking is critical for not only tightening up defenses but also complying with data-control and privacy provisions contained in regulations such as Sarbanes-Oxley and HIPAA (Healthcare Insurance Portability and Accountability Act). Audit information—such as who transferred information to removable media, how much data was transferred, what files were transferred and what types of devices the information was transferred to—should be accessible to the administrator.

Is the USB solution part of a broader, holistic security approach?

Stand-alone USB solutions don't come close to addressing every kind of endpoint corporate security threat out there, nor are they designed to. Therefore, you must ensure that your USB solution is just one component of an integrated, holistic approach to endpoint security.

Look for endpoint security solutions that manage USB security as well as advanced firewall enforcement, wireless or "Wi-Fi" connectivity, endpoint integrity, removable media access and theft protection.

Firewalls integrated into the operating systems kernel can protect against network port scans, Internet Protocol (IP) spoofing, denial-of-service and other protocol-based attacks. Wi-Fi connectivity control is needed to guard against wireless snooping and attacks, whether the user is located inside the company's walls, at home, or in Wi-Fi hotspots. With endpoint integrity checking, policies can require notebooks and other computing devices to have the approved antivirus signatures and up-to-date patches before the device is allowed to communicate with the public Internet and the outside world. A holistic solution should allow policies to control the use of removable media devices such as thumb drives and writeable CD-ROMs,

and the solution should protect sensitive data if a mobile computer is lost or stolen.

For any security solution to be effective, it must be enabled and actually running on the machine. If a user or malicious code can simply shut off the security solution, the result is an ineffective defense that doesn't go much beyond good intentions. All the security functionality discussed here should be protected from being disabled or bypassed by users tampering with registry keys, deleting critical files, stopping services/processes or uninstalling the software—even if they have administrative privileges or boot into "safe mode."

Ensure that USB security is part of a broader security solution that can be managed from a central location. Otherwise, you'll be using a piecemeal approach to endpoint security that will complicate management and make it harder to identify remaining security holes.

REMOVABLE STORAGE-DEVICE SECURITY FROM ALTIRIS

Altiris has adopted a holistic, comprehensive approach to endpoint security that recognizes the current industry challenges and future technological advances on the horizon. Recognizing the growing threat of USB and removable media attacks, Altiris includes advanced removable storage control features in its Endpoint Security Solution™. Now, via one easy-to-use management console, companies can manage USB security, firewalls, Virtual Private Networks (VPNs), Wi-Fi connectivity, theft protection, and endpoint integrity.

The Altiris Endpoint Security Solution removable storage control driver sits in the kernel-level storage stack of endpoint devices, so it can control local optical media (writable CD-ROMs and DVDs) and all attached storage devices (USB thumb drives, floppy drives, flash memory cards, ZIP drives, SCSI PCMCIA cards and other removable media types). Altiris' removable storage control features are policy-based, assigning either blocked, non-blocked or read-only states depending on the user, the user's location and other parameters. Administrators control and push out policies, so end users are not involved with selecting security options.

The removable storage control features not only protect against data theft but also against the introduction of harmful files, viruses and other malicious software ("malware"). All USB and other storage-media activities are tracked and recorded for auditing purposes.

Through intelligent policy enforcement, Endpoint Security Solution enforces security policies that protect endpoint devices from misuse and malicious access. Altiris provide companies with a centrally management solution to create, distribute, manage and enforce security policies associated with endpoint security threats, such as USB devices, removable storage, Bluetooth, wireless, networking, applications and data. Endpoint Security Solution dynamically enforces security policies dependent on the location threat profile (at the office, on the road or at home).

Endpoint Security Solution is the most comprehensive endpoint security solution on the market today. Using patented technology, you can dramatically reduce the risk of data loss, simplify security management, and protect against attacks from the inside and outside without hampering the productivity of your company.

CONCLUSION

Many companies do not have the security solutions they need to ensure complete information integrity and data security. Most do not even know that they have a threat. Instead, they approach security in a reactionary manner and they seek a solution once they've actually had a problem. It's not surprising that the issue of USB security hasn't gained more recognition. The reality is that few solutions exist for this pervasive problem.

Altiris believes that companies must manage all corporate information and security policies in a manner that adapts to the current and future innovations of technology. To accomplish this, companies need to be provided with technologies that ensure security through automated and transparent methods, while proactively notifying the organization of security threats in real-time.

These modern-day Trojan horses are carried by individuals who do not always recognize the cost and risk of the information they are using. The solution to this challenge is to institute economic and flexible software and information-monitoring services that audit, control and prevent security breeches where they occur. Altiris offers comprehensive solutions with repeatable processes that address the challenges of endpoint security. Altiris provides a pro-active environment for managing corporate information assets where they live and ensures that information is "entitled" to move between removable media and USB devices. These capabilities are based around manageable and configurable policies that do not interfere with corporate productivity.

What has your company done to protect itself against USB attacks? If the answer is "very little," then it's time to evaluate endpoint security solutions. Be sure to ask the right questions, including the five questions we've explored here.

Then listen carefully to the answers. At Altiris, our approach to endpoint security will help you make the next Trojan horse a relic of ancient history.