



PC on a Stick: A Portable Endpoint Security Nightmare



The Security Battlefield – In the Beginning

In the early stages of the enterprise security war, solutions battled attacks at the network perimeter. The front remained a safe distance from that which security technologies were fighting to protect. However, attackers have shifted their focus to a battlefield much closer to the heart of the organization: the corporate endpoint.

Most companies realize that while fortifying the outer barriers of their networks remains a vital component to overall enterprise security efforts, it is no longer an effective last line of defense. They are equipping themselves with solutions designed to protect against attacks on PCS, laptops, servers and other endpoints.

As enterprises build their endpoint security arsenal, it is critical that they understand that endpoints are continuously shifting to facilitate today's evolving business world. The number of ways users can access sensitive corporate data is continuously increasing — especially with the proliferation of handheld devices — and organizations must establish defenses accordingly.

The Shifting Endpoint

Traditionally, the most common entry point into a corporate network was the desktop computer. Employees could only access information in a controlled environment that could be easily monitored. Some workers could also log on to server consoles, but these were mostly IT staffers who could be trusted with this privilege. However, this controlled workplace environment no longer exists and the number of corporate endpoints is drastically increasing.

With business travel and telecommuting on the rise, laptops have become a vital instrument for success. Advances in wireless technology make it possible for employees to connect to the corporate network from the unlikeliest of places. This creates an enormous security risk as a laptop could easily be stolen from a coffee house or other local Wi-Fi hot spot.

Additionally, more and more employees rely on handheld devices. Cell phones, Blackberrys, flash drives and USB memory sticks have evolved into invaluable business tools, allowing for instant, on-demand access to — and transport of — corporate data. Storage space is steadily increasing and reams of sensitive information can now be stored on a device that fits on a keychain. Just one lost or stolen memory stick could prove disastrous to the company, its employees and most importantly, its customers.



Data theft is not the only potential risk from unmanaged USB devices and removable media - these same devices are now being recognized as an entry point for malware.

Devices are also growing increasingly more complex and manufacturers will soon develop the "PC on a stick." Not only will gadgets provide mass storage capabilities, but they will contain fully functional computers with custom applications. While this innovation may someday benefit the business world, it also opens a new endpoint security concern: mobile malware. Today, it's benefit is primarily in the consumer space, and as these days become more commonly used to hold applications, we can be assured that they will be exploited by malware as new path of entry.

Hackers are finding ways to manipulate and sabotage the applications that reside on personal digital assistants (PDAs) and other devices, creating yet another security nightmare for enterprise IT administrators. If a flash drive or USB stick becomes infected, the user could plug it into the corporate network and unknowingly unleash a crippling virus. **Data theft is not the only potential risk from unmanaged USB devices and removable media - these same devices are now being recognized as an entry point for malware.**

Devices as Entry Point for Malware

1. Recently, McDonald's Japan began recalling MP3 players it offered as a prize, after discovering that the prizes were loaded with a particularly nasty strain of malware. Up to 10,000 people might have been exposed to the QQpass spyware Trojan after claiming a Flash MP3 player.
2. Apple said since September 12, a small percent of Video iPods -- pocket-sized devices that can play music files and video clips -- left its contract manufacturer carrying the virus RavMonE.exe, which affects computers running Microsoft Corp.'s Windows operating system.
3. This summer, one company conducted a "Social Engineering" experiment, in which 20 USB devices (preloaded with a Trojan that would collect passwords and then email the data to the program's creator) were planted around office buildings waiting for the unsuspecting pawns. Fifteen of these sticks were plugged into corporate machines, and ultimately compromised the individual and organization's security.

The proliferation of handheld devices within the enterprise creates a vast network of new corporate endpoints that must be secured. While some companies are able to successfully address these threats, many continue to struggle with so-called solutions that do not effectively or efficiently secure endpoints because they rely on traditional, antiquated approaches.

Caught Between a Device and a Hard Place

If you look at the latest corporate desktop releases from top makers Dell, H-P and Gateway, a single system can easily have up to eight USB ports, each representing an entry point into the corporate network. Even more troubling is the default plug-and-play



configurations of operating systems. Current systems provide seamless support for USB devices and for good reason: users want to be able to load photos, sync their PDAs or transfer music to and from their MP3 players with no hassle. What's more, devices play an important role in day-to-day business operations.

While organizations scramble to turn off the data spigot with no guarantee that software or PC manufacturers will do anything to stop default USB access, things are only going to get worse. Several trends will continue to feed this security dilemma, including:

- ▣ **Pop culture:** iPods, digital cameras, PDAs and other gadgets will continue to see rapid adoption among consumers and business users. With no configuration at all, an employee can plug a USB keychain with a gigabyte of storage into the back of a corporate PC. Employees already bring digital cameras to work to download photos as desktop wallpaper or screensavers. These devices spend most of their lives plugged into far less-secure home computers, making it incredibly easy for someone to unintentionally download a nasty virus or destructive code onto an enterprise machine.
- ▣ **Malicious code meets device:** Wireless LANs and laptop computers are the current hot vectors for malicious code infections, but the recent appearance of malicious code in portable and personal devices does not bode well for security administrators. Infected PDAs syncing to a corporate computer could conceivably offer a scenario where malcode is passed from device to machine to corporate network. It is also conceivable that future malware will seek out portable media solely for the purpose of proliferation.
- ▣ **Storage device meets mouse:** The convergence of different computer components and technology could present the ultimate dilemma for security personnel. Mice, keyboards and other components that are intrinsic to everyday computing—combined with storage capabilities—is the potential Swiss army knife for data thieves and insiders, or yet another threat vector for malicious code exploits.

The mass proliferation of handheld devices presents a dilemma for organizations in all industries. On one hand, devices are invaluable business tools that employees need to perform their day-to-day tasks. On the other hand, they represent a serious security risk to sensitive company and customer information. Companies must implement solutions that allow users access to business-critical devices while protecting corporate assets. Effective strategies begin with establishing a clear written policy and are supported with an enforcement technology.



In a perfect world, written corporate policy would be enough to dictate what devices employees can and cannot use on company PCs and laptops. In reality, even the most stringent policies need a solution to support and enforce them. The fact is, it only takes one instance in which an employee steals information or unleashes a crippling virus to make the policy obsolete.

The best solutions to match the best policies will emphasize a number of things, including technology better suited to the distributed nature of today's enterprise, as well as better configuration of existing systems. However, perhaps the best solution is to take what organizations already know and simply reverse it.

Denial by Default

When it comes to IT security, most companies continue to rely on a blacklist approach. Firewall, anti-virus software and intrusion detection systems require the constant updating of a blacklist of known threats that should remain barricaded outside the network. Many companies take the same approach to device use, denying access to unauthorized devices. The problem, however, is that with the sheer number of new devices coming to market every day, maintaining an accurate blacklist is next to impossible.

The opposite of blacklisting is whitelisting. This involves setting a pre-defined list of devices or applications that are allowed to run on corporate machines while blocking everything else by default. The whitelisting concept shelters administrators from the laborious task of maintaining blacklists of all known devices.

While blacklisting only accounts for devices that a company knows it wants to deny, the whitelist approach prevents even unknown devices from harming the network. With a blacklist-based solution, any device that is not specifically listed as a threat will be able to connect to the network, allowing users to pilfer data or inject malware into the systems.

The whitelist approach places control of corporate policy squarely in the hands of the IT administration staff. Only devices that are authorized as having a viable business use will work on corporate endpoints. This supports company policy because it gives the IT staff the means to enforce its written list of allowed devices. For example, if policy excluded iPods from use on company computers, the IT administrator would simply not include iPods on the whitelist and they would not work on corporate endpoints."



Lumension Security Sanctuary[®]: Secure the Known. Protect Against the Unknown

Lumension Security Sanctuary provides policy-based application and device control that proactively secures your organization from data threats, including data leakage, malware and spyware.

By employing a whitelist approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC – facilitating security and systems management, while providing necessary flexibility to the organization.

Sanctuary is comprised of two modules to secure your endpoints:

- ▣ **Sanctuary Application Control:** Provides policy-based enforcement of application use to secure endpoints from malware, spyware and unwanted or unlicensed software.
- ▣ **Sanctuary Device Control:** Provides policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints.

Sanctuary validates applications and removable devices as they are used within an enterprise. Applications or devices that are not authorized are simply not allowed to execute.

Through a central console, application and device control policies are quickly established and enforced through two simple steps: Identification and Assignment. Since Sanctuary works with devices and applications, it enables agencies to develop granular use policies - working with the devices and applications rather than simply enabling or disabling them. Sanctuary policies are managed per user or user group as well as per computer. For devices, policies are enforced by time constraints, encryption, volume of data, data transfer and much more criteria. Linking application and device policies to user and user-group information stored in Microsoft[®] Windows[®] Active Directory[™] or Novell[®] eDirectory[™], Sanctuary enables the immediate association of user groups to devices and applications on the fly - dramatically simplifying the management of endpoint application and device resources.

Sanctuary can also encrypt removable media so that it can be safely used and transported without the fear of exposing your confidential data to unauthorized users. Users can have access to their encrypted data even in computers that do not have Sanctuary client software installed. Centralized and decentralized encryption schemas provide the Sanctuary administrator with the flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and, more importantly, enforce the use of that encrypted media.



Providing the ultimate flexibility, Sanctuary enables administrators to allow trusted users to authorize their own applications. This option provides the best of both worlds - flexibility to users and control for administrators through notifications of activity. Auditing and reporting enable systems administrators to precisely track how devices and applications are used, by whom and how. They can also see when un-authorized device and application usage are attempted and track that as well.

Sanctuary combines the proven capabilities of its application and device control modules, providing organizations with the most comprehensive solution for endpoint security management – all from one console. Sanctuary removes the risk of data leakage, malware and spyware, improves IT security and network bandwidth, reduces the effort and cost associated with supporting endpoint technologies and assures regulatory compliance.

Sanctuary:

- ▣ Prevents data leakage via removable media, malware or spyware
- ▣ Protects against malware, viruses and spyware
- ▣ Safeguards against zero-day threats
- ▣ Controls proliferation of unwanted applications and devices
- ▣ Assures and proves compliance with regulations governing privacy and accountability
- ▣ Maximizes benefits of new technologies and minimizes risk

Summary

The traditional definition of a corporate “endpoint” is clearly evolving. For millions of employees, portable mass media represents the next generation of endpoints, shifting from simply PCs and laptops. Because of this evolution, enterprise endpoint security must also grow to address the increasing concerns. Ultimately, this shifting corporate endpoint exposes a new threat vector that IT professionals must confront and secure.

To win the war against mobile malware and information theft, organizations must develop clear, in-depth policies regarding the use of devices within the enterprise. They must also deploy proactive solutions, such as Lumension Security Sanctuary to support these policies. While the enterprise security war will continue to be long and trying, enterprises can gain a decisive advantage by taking an offensive approach to protecting their corporate endpoints, no matter how frequently they evolve. A “PC on a stick” should improve business processes, not impede them.



About the Author

Dennis Szerszen, VP Marketing and Corporate Development

Dennis has over 20 years of product management, marketing and business development experience working for IBM where he was responsible for introducing new systems management and security software and services offerings. While at IBM, he played a key role in helping IBM acquire Tivoli Systems. In recent years, Dennis directed Hurwitz Group's security practice where he had the opportunity to work with some of the most innovative and influential companies in the IT security and systems management markets. He also served as President and Chief Strategy Officer for a Swedish security vendor. Most recently, Dennis worked as an independent consultant, helping software startups bring their products to market. He joined Lumension Security in 2004 as VP of Business Development. Dennis is CISSP and ISO certified security specialist.

About Lumension Security™, Inc.

Lumension Security, a company formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a recognized, global security management company, providing unified protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Positive Security Model, Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes automated asset discovery, vulnerability assessment, remediation and validation; application and device control; extensive policy compliance reporting; and integration with leading network access control solutions. Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore. PatchLink, now Lumension, was founded in 1991 by Sean Moshir. More information can be found at www.lumension.com.