



## **Preventing Data Leakage and Malicious Code Intrusion**

*Securing removable storage, mobile device and wireless data pathways without impacting productivity or convenience*

### **GuardianEdge Device Control And the GuardianEdge Data Protection Platform**

**A GuardianEdge White Paper**

April 27, 2007

## ***Productivity, Convenience & Security Risks***

Today there are a myriad of options for the transport and distribution of data and the portability of data is no longer dependent upon Internet connectivity. Never before has such convenience been available. Removable storage, mobile devices and wireless access technologies boost employee productivity by opening up easy and fast methods for capturing and transferring data from one place to another. Members of organizations take advantage of USB, FireWire, CD/DVD, WiFi, and Bluetooth technologies every day to work remotely and to share data with external partners.

While convenient and productivity-enhancing, these data transfers pathways also represent enormous security risks. According to Vista research, 70% of IT security breaches occur internal to the organization. Organizations use firewalls and other security schemes to protect their sensitive data; however, removable, mobile and wireless pathways are often forgotten open doors to precious internal data and systems.

These “open doors” make it easy for organizations to lose intellectual property, customer records, employee data and other valuable and sensitive information. These “open doors” also leave the way wide open for malicious code to get into an otherwise secure internal data environment; malicious code that could wreak costly damage to an exposed enterprise. Worse yet, there is usually no evidence of where precious data exited, or dangerous code entered the enterprise data environment if one of these pathways is used. The Economist estimated that U.S. companies alone lost \$50 billion in 2006 due to data that leaked from the company via an internal data breach.

### **The way forward: Device access control for enterprise endpoints**

GuardianEdge Device Control offers enterprises a way to control access to removable, mobile or wireless ports on enterprise PCs. This solution provides network administrators granular control that is easily manageable and massively scalable. With GuardianEdge Device Control, enterprises can stop sensitive data from leaking out of the company and prevent malicious code from coming into the data environment through open peripheral ports within the network security perimeter.

GuardianEdge Device Control is a key component of the GuardianEdge Data Protection Platform, a highly scalable software solution for protecting data at the endpoints in an enterprise. The GuardianEdge Data Protection Platform significantly differentiates GuardianEdge solutions from other endpoint security products. The platform provides enterprise-grade deployment and management capabilities for endpoint data protection, scaling to the largest enterprises while retaining flexibility and providing granular control of devices and policies. It achieves this by leveraging the directory services enterprise infrastructure already in use by most organizations.

## ***Peripheral Ports are Vulnerable to Data Loss & Intrusion***

### **Data Leakage**

Data represents a critical asset for organizations. The loss of intellectual property, customer information or employee data can be very damaging to a company's financial health, competitiveness and reputation. Unfortunately, it is only too easy for data to slip out of an organization via physical and wireless peripherals.

The productivity enhancements that come with removable, mobile and wireless devices are undeniable but these devices also represent open, unmonitored ports into what may otherwise be a secured data environment. Sensitive data is easily leaked out via these pathways without being detected by firewalls, IDS or other network-based mechanism. Enterprises can suffer a critical loss of data without having any way of tracking it.

The challenge lies in **appropriately securing these ports without hampering the productivity of employees who need access to these devices**. All the ports on some computers can be blocked as unnecessary for access but clearly this would create problems and degrade productivity if this was done on all computers across the board. A method for selectively allowing access or limited access to these device pathways is needed. There can be thousands of these ports in an enterprise so the solution must also be scalable and easily manageable.

### **Malicious Code Intrusion**

These peripheral ports also represent a pathway for malicious code to get into a PC and from there to spread within a corporate network. These open ports are not protected by the firewalls, intrusion detection systems and antivirus measures typically employed to prevent malicious code from infiltrating the network via other electronic means. Malicious code such as a virus or worm successfully infiltrating a corporate system or network can wreak havoc on an enterprise.

## ***The GuardianEdge Solution: Centrally Managed Device Control***

GuardianEdge enables enterprises to effectively manage these risks by controlling access to selective peripheral devices from a central location without hampering the productivity of employees who have a legitimate need to use portable media.

Administrators can set policy-based user access controls for ports and devices. These access control policies allow organizations to restrict the transfer of data between enterprise computers and peripheral devices or to block access to these mobile devices altogether. Device access controls can be based on model, vendor, and individual serial number and tied to Organizational Units and groups within Active Directory and other directory services.

Additionally, the GuardianEdge solution provides an effective method for verifying that an enterprise has implemented the proper security controls to protect against a loss of data — an invaluable service to avoid legislative disclosure requirements if PC equipment is lost or stolen.

### **GuardianEdge Device Control**

GuardianEdge Device Control makes it possible for administrators to control access to all the input/output ports and peripheral devices on the PCs in their network, including USB, FireWire, serial, parallel, infrared, CD/DVD, floppy disk, tape, WiFi, and Bluetooth items. Specific users or classes of users may be given permission to use certain pre-defined devices or broad access controls can be enforced. Multiple levels of access control options are available; for example, certain pathways may be limited to read-only capabilities. Enterprises can monitor all activity associated with these ports including success or failure events, dates, times, device types, file names and file operations. By using data shadowing organizations can track exactly what data is transferred, even if files are renamed to something generic (e.g. 2008 Strategic Plan could be renamed to My to Do List). Extensive reporting capabilities come with this monitoring feature.

GuardianEdge Device Control is a key component of the GuardianEdge Data Protection Platform, a highly scalable software solution for protecting all the data endpoints in an enterprise.

### **GuardianEdge Data Protection Platform**

A security solution will only be successfully implemented if it is convenient to manage and does not impact the productivity of end users. The enterprise-grade GuardianEdge Data Protection Platform, a solution that simplifies deploying and managing endpoint data protection controls, meets these requirements. Designed to serve the specific needs

of enterprise IT administrators, this platform leverages the widely-used Active Directory enterprise infrastructure to provide unprecedented scalability and manageability.

The GuardianEdge Data Protection Platform minimizes the costs associated with administration and support, and reduces the potential for data security gaps through the alignment and integration of data protection policies. Whether machines are lost or stolen, or unauthorized individuals attempt to compromise data through malicious activity, the platform ensures that the organization's critical information is secure. The platform provides core enabling security and management services, including user registration and management, policy administration, client audit and reporting, and recovery mechanisms for data and encryption keys.

With the GuardianEdge solution, administrators manage endpoint data protection for potentially thousands of ports and devices using group policy objects (GPOs) or third party software tools, such as SMS, to distribute policies. This provides enterprise-grade manageability — a key requirement for a data protection solution. Plus, in the event of an incident involving the loss of a device, the platform provides administrators the ability to validate that required data protection controls are in place and operational.

The complete GuardianEdge Data Protection Platform includes GuardianEdge Hard Disk Encryption, GuardianEdge Device Control, and GuardianEdge Removable Storage Encryption. This complete solution provides the controls and applications any enterprise needs to protect its data. These three solutions can be deployed on their own or together for comprehensive endpoint data protection.

## ***Conclusion***

By deploying GuardianEdge Device Control, organizations can prevent data leakage of trade secrets, intellectual property and private customer or employee data as well as stop malware from entering their data environment. This solution prevents any unauthorized person from transferring data from a corporate PC to an unapproved peripheral device or via any unapproved input/output port.

The GuardianEdge Data Protection Platform allows enterprises to align their device access policies with their business processes and user policies. With this solution organizations centrally manage and monitor port and device access as an integrated component of their data protection strategy.

GuardianEdge provides a complete solution to enable enterprises to reduce the costs associated with meeting regulatory compliance standards for data security and privacy by leveraging their existing IT infrastructure. This solution helps to eliminate the legal liability, customer service costs and other ramifications of data breach disclosures. By facilitating extensive monitoring and reporting, the GuardianEdge solution helps enterprises meet regulatory compliance requirements for data security and in some cases provides assurance that a data leakage did not actually occur.

## ***Begin Your Evaluation Today***

For more information on protecting your organization from data leakage and malicious software intrusion via input/output ports and peripheral devices, contact GuardianEdge for an evaluation of your data endpoint security needs. Or visit [www.guardianedge.com/salesinquiry](http://www.guardianedge.com/salesinquiry) to register for your evaluation of GuardianEdge Device Control.

US: +1 415-683-2200

UK +44 (0)870 366 6772

<http://www.guardianedge.com>