

Securing Points of Risk in a Creative Environment

In the multimedia entertainment industry, protecting digital assets is essential. The theft of even a small amount of source code or the leak of an upcoming product over the internet can easily jeopardize competitive advantage and endanger millions of dollars in revenue.

In a multimedia entertainment company, one of the most vulnerable points in the infrastructure is the development studio, where terabytes of new products in various stages of development sit on dozens of servers accessible to the development team. Verdasy's is helping a leading multimedia entertainment company lock down its studio and secure its products through Digital Guardian™, a powerful information protection solution that provides continuous visibility and control over how information assets are being used by authorized users, or insiders.

By blocking unauthorized user activity in real time, Digital Guardian has enabled the company to dramatically improve the security of its information, without impacting productivity or innovation.

OUTPUT DEVICE DANGERS

Today's desktop and laptop computers present a variety of conduits over which valuable data may leave a company's confines. In particular, communications buses like USB and Firewire present a growing security challenge, especially in creative environments like multimedia development. While communications buses make it simple to connect a multitude of input devices critical to graphic development and audio design work, they make it equally simple to connect high-capacity data storage devices that can be used to inappropriately remove information.

Knowing that its written information usage policies would discourage the theft or misuse of company information but could not prevent it, the company was considering dramatic measures to ensure that its valuable data never left the development studio. By stripping all computers and servers of removable media devices and completely disabling internet access, the company could create a sealed environment where no team member would be able to move data out of the company.

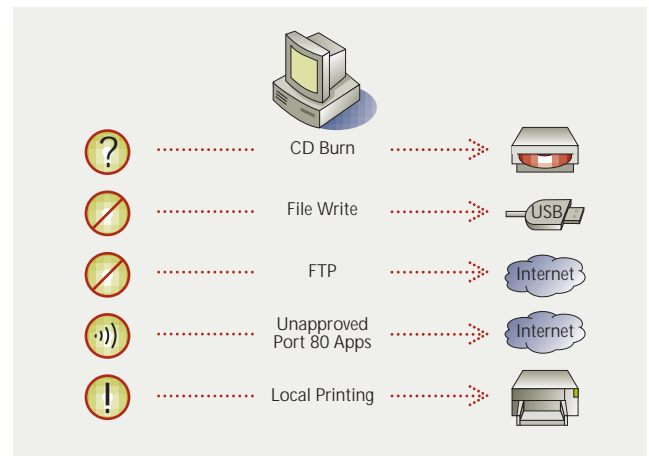
But such tight security is impractical in the world of multimedia entertainment. This approach would virtually eliminate risks to information, but would hinder collaboration and essentially cut off the development team from the Internet, an important source of creative inspiration and resources.

Digital Guardian provides the company an attractive alternative to isolating the development team and taking away critical tools. With Digital Guardian, the company can now actively enforce its information usage policies at every individual desktop by monitoring user activity and putting a stop to any user actions that place company information at risk.

DATA CONTAINMENT AT THE POINT-OF-USE

Deployed on desktops and laptops company-wide, Digital Guardian balances security with productivity by enabling the company to selectively control what information can leave a particular workstation and how it can leave it.

Digital Guardian has enabled the company to restrict the use of removable media devices such as CD-ROMs and USB flash drives. The company can easily translate its policies into a set of XML-based business rules, which can be implemented as needed at different points or at different levels across the organization. For example, one policy restricts the use of removable storage devices for nearly



Digital Guardian helps the company enforce policies by sending alerts to security staff, notifying users of policy violations, and even blocking specific user actions.

every user in the company. Digital Guardian automatically blocks users from moving information to such devices, and records any such attempt. The policy does, however, allow a limited number of product managers and QA staff to burn product CDs for testing. Digital Guardian automatically reminds these users that their actions are being recorded and prompts them for a brief note on the purpose of their activity. Their replies are sent to security staff as alerts for review.

“When insider crime inevitably occurs, compelling evidence must be found quickly. Digital Guardian is the only solution that collects real-time, digitally signed evidence of all user actions making it easy to detect, investigate and even prevent incidents.”

ED APPEL, COO, JOINT COUNCIL ON INFORMATION
AGE CRIME AND EX-FBI CYBER CRIME EXPERT

A similar set of policies restricts the use of well-known network file transfer applications. For example, one policy curbs the use of certain ports for protocols like FTP when the destination is outside of the corporate network. Another policy prevents risky tunneling applications, such as P2P applications, from executing on desktops and laptops altogether.

ENTERPRISE-SCALE FORENSICS

Digital Guardian has also provided the company with the ability to quickly respond to any security violations by making it easy to trace incidents to their source. Digital Guardian’s digital forensics capabilities were demonstrated during the company’s trial deployment phase, when a security team member assigned to monitor internet newsgroups and websites known for the distribution of copyrighted material spotted content originating from one of the company’s upcoming products.

Analysis of the content in question indicated only that the leak had come from a particular development group composed of dozens of people. Traditional firewall, network and system security logs offered no further clues. Digital Guardian, however, was able to correlate file, application and network activity at all desktops within the development group. A few simple queries through the system’s detailed activity reporting interface enabled the security team to analyze forensic-quality activity journals for the entire department.

The evidence quickly pointed to a machine running what appeared to be an http tunneling application providing file transfer capabilities, which would appear to be simple outbound web traffic to network security tools. Armed with this data, the security team was able to proceed with an investigation of the machine and user in question using additional Digital Guardian reports as well as other forensics tools.

MEANINGFUL RISK MITIGATION

Through Digital Guardian, the company has brought together security policies, automatic enforcement capabilities and forensics tools to mitigate the potential risks to corporate data presented by authorized users. By blocking dangerous activities in real time, warning users of unauthorized activities and alerting the security team to suspicious activity, Digital Guardian has enabled the company to dramatically improve the security of its information – without impacting productivity or innovation.

ABOUT DIGITAL GUARDIAN

Verdasys Digital Guardian is a unique software solution that allows companies to continuously monitor and actively control how information is used by employees, contractors and other authorized users. By actuating security policies and holding users accountable for the acceptable use of information at its point-of-use – the office desktop, the mobile laptop and the corporate file server – Digital Guardian prevents actions that jeopardize regulatory compliance, bring about proprietary information loss and compromise the integrity of information.

For more information on Digital Guardian and how it can help your organization mitigate insider threats, visit www.verdasys.com.

➤ ABOUT VERDASYS

Verdasys is dedicated to providing a new class of information security and risk management solutions focused on the largely uncountered threat from authorized internal users. Our solutions allow organizations to actively manage insider threats to information – detecting, preventing and documenting incidents of loss and misuse wherever users access, utilize or communicate sensitive and proprietary information.

VERDASYS[™]

950 Winter Street, Suite 2600 Waltham, MA 02451
781-788-8180 Tel 781-788-8188 Fax
info@verdasys.com www.verdasys.com