

Digital Guardian

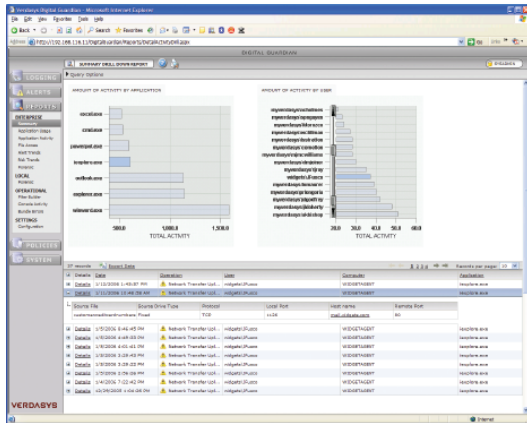
GLOBAL DATA SECURITY

COMPREHENSIVE GLOBAL DATA SECURITY

Verdasys Digital Guardian is a comprehensive and proven data security solution for protecting and tracking the flow of critical data anywhere in the world. Whether on PCs, laptops, or servers...inside or outside the organization... Verdasys Digital Guardian is there to monitor, log, and, if necessary, block prohibited actions by trusted end-users. With a central server console to deploy and monitor intelligent agents, Digital Guardian logs user data transactions and applies pre-defined rules to ensure that end-users are using applications and data properly. It also assures that data is being used in accordance with established company best practices and government regulations for handling confidential and private information. All without modifying your existing business processes.

PROVIDES CENTRAL VISIBILITY AND AUDIT CAPABILITY

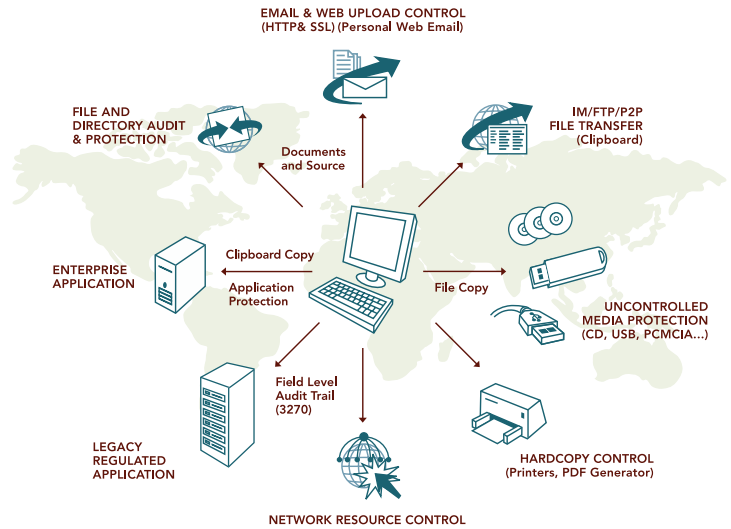
Digital Guardian complements its extensive control and monitoring functions with a comprehensive set of analytics capabilities, producing detailed drilldown reports and offering a complete audit trail of data usage transactions. Intelligent automated alerts and policy violation warnings are generated to administrators and end-users, reinforcing organization policies for the use of sensitive or private information.



Detailed Query and Summarization Reporting for All Alerts and User Transactions

PREVENT DATA LOSS AT THE POINT OF USE

Digital Guardian protects against the loss of data as a result of "hard to detect" user actions such as: illicit copying to CD (or USB device), printing, network transfer, or the personal e-mailing of sensitive files and other data. Because it oversees transactions at the "point of use", or host, Digital Guardian is uniquely capable of protecting data *simultaneously across applications, devices and channels of communication* from a single console – anywhere in the world.



Access, Flow and Utilization Monitoring: Gives total visibility to data access, flow, and utilization by end-users across a global enterprise in near real-time.

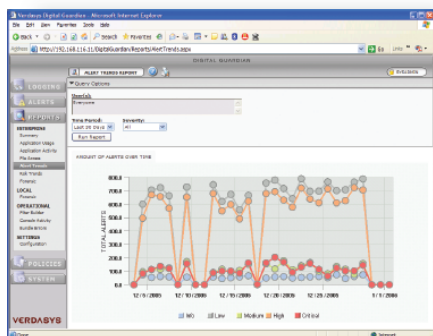
Control: Prevents unauthorized actions by users such as copying to CD (or USB device), printing, network transfer, data transfer via personal e-mail, clipboard cut/paste, print screen, and/or other operations.

Analytics and Reporting: Analyzes user actions and automatically prepares a suite of exportable drilldown reports, charts and use summaries, making it easy to centrally monitor and/or audit data usage across a distributed organization.

SCALABLE ENTERPRISE ARCHITECTURE

The Digital Guardian platform employs a scalable architecture composed of a central server and control console to communicate with remote device agents deployed to all desktops, laptops and servers where data needs protection. Digital Guardian Management Console continually monitors and reports on data usage on these devices, blocking forbidden access, copying, printing, network file transfer, and/or other user actions. Deployed Digital Guardian agents (small footprint, highly tamper-resistant, low-overhead controls) operate silently at the kernel level of the operating system. Agents monitor data usage and report rules violations, *continuing to operate even when a device is removed from the network*. The management of agent installation (also installable via third party tools, such as SMS and Marimba), security settings (Active Directory-integrated), rule definition, reporting and auditing all occur via a web-based interface to the Digital Guardian Control Console.

ALERTS AND RISK TRENDS



Automatic generation of risk trend analysis and alert summaries

SYSTEM REQUIREMENTS

Digital Guardian Server

Oracle or SQL Server

Digital Guardian Agent – Host

Desktop

- Windows XP – SP1, SP2
- Windows 2000 Workstation – SP4a

Server Operating Systems

- Windows 2000 Server – SP4a
- Windows 2003 Server – SP1

Verdasys

950 Winter Street
Waltham, MA 02451
781-788-8180

www.verdasys.com

FEATURE SUMMARY

Control of High-Level User Actions

Prohibits unauthorized file operations including: access, copy and modification of sensitive files.

Halts unauthorized network transfer of sensitive information including: FTP, and file upload via browser applications and private web mail.

Denies hidden sharing of sensitive information via file share operations, and the execution of unapproved applications.

Prevents unauthorized copying of sensitive information to devices such as: Printers, USB, Firewire, PCMCIA, Bluetooth, Wireless (802.11 a/b/g).

Stops unauthorized removal of sensitive data via clipboard operations (i.e., Cut/Paste, Copy) and Print Screen.

Rules-Based Policy Management and Control

- Enables the creation of rules based on corporate information policy.
- Rules can prevent users from performing prohibited operations that violate policy.
- Rules can trigger screen warnings to users, and email alerts to administrators upon policy violation (via SMTP).
- Rules can require users to justify their actions before allowing (Soft Blocking).

Detailed Analytics and Reporting Capabilities

- Provides detailed summarization of application usage and information flow.
- Creates drilldown summaries of the end user actions and use of data.
- Report query capability allows for detailed auditing across the enterprise.
- Automatically generates graphical analysis and history of all warnings and alerts.
- Automatically analyzes risk trends and threats involving data usage.

ABOUT VERDASYS

Verdasys is leading the industry in providing global data security solutions based on innovative “point of use” technologies. Our Digital Guardian platform is in use by government agencies, and by leaders in financial, pharmaceutical, insurance, healthcare, manufacturing, entertainment, and other industries around the world. Verdasys customers use Digital Guardian to complement their existing security technologies in order to comprehensively protect data wherever it's used.

VERDASYS
GLOBAL DATA SECURITY SOLUTIONS