

Digital Guardian

APPLICATION LOGGING

DIGITAL GUARDIAN'S APPLICATION LOGGING MODULE

Digital Guardian's Application Logging Module (*optional*) extends the powerful control, monitoring and reporting capabilities of the core Digital Guardian solution to protect data delivered by enterprise applications to desktops and laptops via 3270 terminal emulators, web-based applications, and client-server applications. Using Application Logging, a company can, for the first time, gain "field-level visibility" into the usage of discrete data handled directly by end-users while accessing their remote applications (including the recording of login, view, creation, change, and deletion actions by end-users). In the past, this information has proven to be particularly difficult to log, monitor and protect because of the heavy integration and extensive re-programming work necessary to modify legacy programs and databases to incorporate logging and security features. The Application Logging Module now makes it possible to protect the data handled by enterprise applications, *without the need for expensive recoding or modification of the applications themselves.*

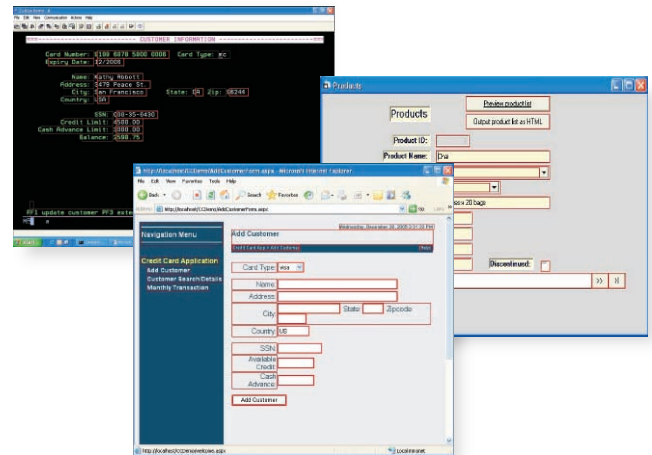
PROTECT MULTIPLE APPLICATIONS SIMULTANEOUSLY

When users access applications monitored by the Application Logging Module, Digital Guardian automatically recognizes "profiled" data fields of the application, and begins to log and monitor not only the data touched by the end-user, but also what users are doing with the data. The Application Logging Module also makes it possible to *oversee multiple applications simultaneously, creating a single repository and audit trail of user transactions and data flow across the enterprise.*

PROVIDES INTEGRATED VISIBILITY

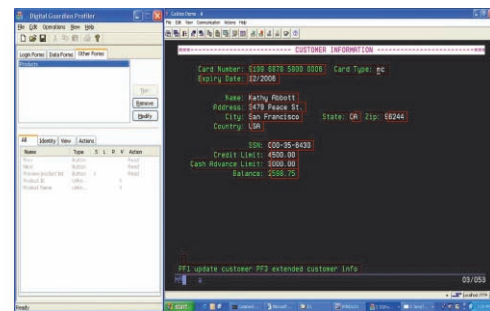
Digital Guardian's Application Logging functionality is tightly integrated with the extensive analytics and drilldown reporting capabilities of the Digital Guardian's Console Server. Application Logging captures all "profiled" data items accessed by an end-user of a corporate application, and maintains a detailed record of what is subsequently done with that data. This gives systems administrators and auditors top level, as well as granular, visibility into transactions by users, *and the data they touch, across applications.* It also gives them the ability to protect sensitive corporate data and comply with policies and regulations governing its use.

PROTECT LEGACY, WEB, AND CLIENT-SERVER DATA



Protects Data Delivered By Legacy 3270, Web and Client-Server Applications Without the Need to Recode These Applications

PROFILE APPLICATIONS TO MONITOR FIELDS AND RECORDS



Digital Guardian's Application Profiler Tool Makes It Easy to "Profile" Applications and Select Exactly Which Data Fields Are to Be Monitored by the Application Logging Module

3270 Applications: Monitor data usage across legacy applications delivered to end-users via 3270 emulators, *without the need to modify these applications.*

Web-Based Applications: Track usage of sensitive data contained in Web-based enterprise applications.

Client-Server Applications: Log the use of data delivered to the desktop via client-server applications and database front ends.

DIGITAL GUARDIAN'S APPLICATION PROFILER – For Legacy, Web, and Client-Server Applications

Digital Guardian's Application Logging Profiler tool makes it simple and easy to "profile" existing applications so that they can be monitored and protected by Digital Guardian's core capabilities. The Application Logging Profiler (included with the Digital Guardian Application Logging Module) is an easy-to-use Windows application that requires no modification or recoding of an existing application in order to be used. Using the Profiler simply requires "selecting" which pages, forms and data fields should be protected by Digital Guardian for each application requiring coverage. The Profiler then automatically configures Digital Guardian to monitor the application's screens, and applies any rules governing the use of "profiled" fields. The Profiler is tightly integrated with Digital Guardian's other control, monitoring, reporting and auditing capabilities and works with most common legacy 3270 emulated, web-based (standard HTML), or client-server applications.

OPTIONAL – FIELD-LEVEL DATA REDACTION – Hide and Protect Sensitive or Private Data

Digital Guardian's Application Logging Module includes *as an option* the capability to redact (hide or black out) data, or portions of data, so that it is unreadable by users who are not authorized to see it. This gives organizations the ability to comply with the demands of emerging privacy requirements and regulations, without the need to undertake expensive modification of their existing applications. *Note – Redaction available for 3270 applications only.*

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

FEATURE SUMMARY (When Deployed with Digital Guardian)

Control of High-Level User Actions

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

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

Hides private data, or portions of data, by providing field-level redaction (*optional*).

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.

Verdasys

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

www.verdasys.com

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