

Gain visibility and control of data to help protect critical information on endpoints from loss and misuse



## IBM Data Security Services for endpoint data protection – Digital Guardian software from Verdasys

---

### Highlights

---

- **Identifies and manages information risk to help secure data on the endpoint against loss**
- **Helps prevent unauthorized use of data by monitoring, controlling, and, if necessary, blocking activities**
- **Reduces the need for in-house data loss prevention experts during initial planning, implementation, and ongoing operations**

### Protecting sensitive data while enabling collaboration

Data can move beyond the corporate network and without detection using high-powered laptops with CD and DVD burners, Blackberries, multi-gigabyte USB devices, Web-based e-mail and unlimited wireless access. Once sensitive data moves to an uncontrolled environment, it can be compromised. You need visibility into information and how it is handled in order to protect sensitive data on endpoints against loss and unauthorized access.

IBM understands these concerns and now delivers a best-in-class data loss prevention solution for the endpoint that combines the Verdasys Digital Guardian Integrated Data Security Platform from Verdasys, Inc., with purpose-built IBM Data Security Services. Digital Guardian software from Verdasys provides a comprehensive solution

designed to automatically discover and classify sensitive data on desktops and servers and monitor the data as it is exchanged and used, applying automated security controls as necessary to secure it. The solution helps enforce corporate security policies in realtime and reduce the risk of data loss.

### Consistently enforce corporate and regulatory security policy

For companies to prevent the loss of sensitive data, they need a strategic, risk-based approach to endpoint data loss prevention (DLP) and an integrated solution that enables:

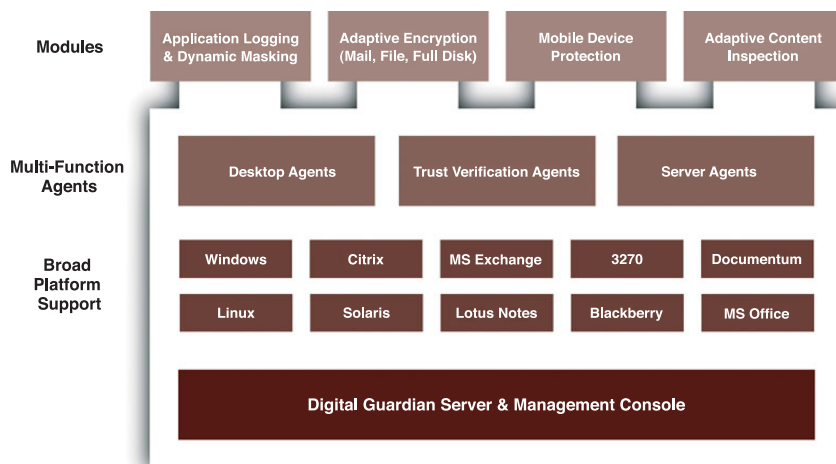
- *Data discovery and classification*
- *Central policy management*
- *Risk-appropriate responses to policy violations*
- *Automated controls*
- *Actionable alerting and reporting*
- *Global visibility of information use and location*

## Implementing a data-centric approach to information protection

The IBM endpoint DLP solution helps track and secure the flow of critical data across the enterprise. Digital Guardian software acts at the point of use to make real-time decisions about data protection. With IBM, you can implement a data-centric endpoint security platform that business and IT managers can use to:

- *Discover and classify sensitive data by context and content with visibility of employees, contractors, partners and outsourcers*
- *Assess the risk of sharing sensitive data to inform business decisions and policy design*
- *Apply policy-driven endpoint data protection to drive accountability to the end user and increase voluntary compliance and risk-aware behavior*
- *Help prevent damaging data loss without impeding business collaboration and information exchange*

Whether on PCs, laptops, or servers (inside or outside of the organization), the IBM endpoint DLP solution can monitor, log, warn, encrypt and, if necessary, block prohibited actions by trusted end users.



Verdasys Digital Guardian Integrated Data Security Platform

### Governing and controlling the use of sensitive information

Verdasys Digital Guardian software enables access to sensitive information while governing, controlling and auditing its use. The solution provides:

- *Comprehensive information protection coverage, fully functional on or off the corporate network*
- *Enterprise-wide visibility into sensitive data location and usage with actionable decision support*
- *Centralized policy definition and enforcement that leverages not only identity and activity, but also data classification, context and content analysis*
- *Risk-appropriate responses to user activities including policy-driven warnings, blocking and alerting, as well as automated file and e-mail encryption*

### Protecting data at the point of use

Together, IBM and Verdasys Digital Guardian software protect against the misuse, compromise or loss of data across the enterprise with:

- *Actionable Data Discovery and Classification—Data classification policies are created and enforced by hardened and invisible endpoint agents using a combination of context and content-based classification.*
- *Monitoring Data Movement and User Activity—Agents utilize integrated context and content monitoring to record all user activity related to system operations that interact with the file, networking, clipboard, printing, and CD subsystems.*

- *Apply automated risk appropriate controls—Agents, based on classification and data activity will apply risk-appropriate controls including warning, prompting, required justification, automated encryption and outright blocking before the end user completes the data transaction and puts sensitive information at risk.*
- *File Encryption—Delivers automatic, policy-driven encryption of sensitive files located on or copied to local drives on laptops, desktops, or external devices and CD/DVD.*
- *E-mail Encryption—Provides patented, policy-driven encryption of e-mail content and attachments; operates transparently and includes automatic key management. Integrated e-mail encryption enforces security policy on network and Web mail systems both on or offline.*
- *Application Logging and Masking—Enforces field-level access control through data masking and meets regulatory requirements through audit logging for legacy (3270 terminal emulators), client server and Web-based applications.*
- *Reporting for Audit and Decision Support—Provides comprehensive reporting capabilities that include aggregated views of enterprise data usage, trend reporting, group or individual reporting, data-at-rest reports, compliance reports and operational reports.*
- *eDiscovery and Forensic Reporting—Generates aggregated case reports that include data usage from across the enterprise including offline, contractor and partner activities. Efficiently moves through aggregated log and audit information to focus on meaningful data, reducing the cost and time of analyzing information and creating effective forensic reports.*
- **Discovery Assessment** *to define your data loss prevention policies and deployment priorities for implementation and testing*
- **Implementation and Policy Design Services** *to provide project planning, architecture and design, policy design, component testing, pre-production testing, deployment assistance, help desk enablement and skills transfer during project deployment phase*

#### **Why IBM and Verdasys?**

IBM and Verdasys, Inc. come together to bring an end-to-end, trusted, and transparent endpoint data protection solution to market. Clients can confidently deploy Verdasys Digital Guardian software by leveraging IBM Global Services' experience, reach and scale. The IBM endpoint data protection solution, powered by Verdasys, includes industry-leading technology, strategic consulting and risk analysis, deployment services and solution management.

#### **Realizing the full value of an endpoint DLP investment**

IBM services can help you realize the full value of an endpoint DLP investment. We address the challenges associated with deploying a comprehensive solution by managing cost and scope, accelerating implementation, and reducing the need for additional headcount. Our services include:

- **Requirements and Planning Workshop** *to identify sensitive data and risky applications, and determine business impact when data is lost or exposed*



### For more information

To learn more about IBM Data Security Services for endpoint data protection – Digital Guardian software from Verdasys, please contact your IBM representative or IBM Business Partner, or visit the following Web site: [ibm.com/services](http://ibm.com/services).

Additionally, IBM Global Financing can tailor financing solutions to your specific IT needs. For more information on great rates, flexible payment plans and loans, and asset buyback and disposal, visit: [ibm.com/financing](http://ibm.com/financing).

© Copyright IBM Corporation 2009

IBM Global Services  
Route 100  
Somers, NY 10589 U.S.A.

Produced in the United States of America  
April 2009  
All Rights Reserved

IBM, the IBM logo, [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Other company, product or service names may be trademarks or service marks of others. References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



Recyclable, please recycle.

SED03062-USEN-00