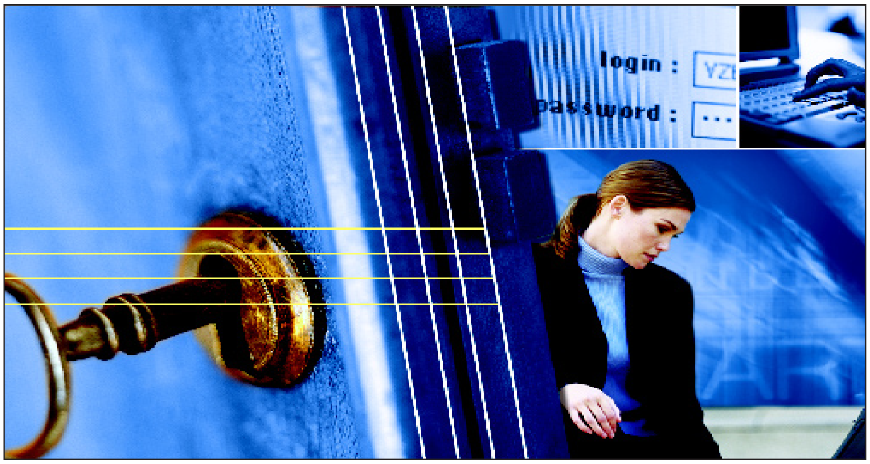
Automating policy enforcement to prevent endpoint data loss

IBM Data Security Services for endpoint data protection—endpoint data loss prevention solution



Highlights

- ***Facilitate policy-based enforcement of data protection policy***
- ***Automate discovery of sensitive content to protect business value***
- ***Consistently enforce required corporate and regulatory security policies while raising user awareness and voluntary compliance of policies***
- ***Leverage market-leading endpoint data loss prevention technologies, services expertise and proven methodologies to deploy, support and manage a complete integrated security solution***
- ***Benefit from lower total cost of ownership and accelerated deployments using an extensible platform and scalable solutions***
- ***Ensure optimized protection through professional security services, managed security services and support desk***

Protecting your business value from growing data losses

Today, global business trends in worker mobility, data sharing and collaboration, driven by new technologies, contribute to strong growth in some of the world's most profitable companies. But, increased growth comes with increased risk and cost to companies as associated data losses, misuse and business-process compromises become a growing problem.

Publicly embarrassing corporate data losses and dramatic data privacy breaches as well as rising information-related crime—such as corporate IP theft and online identity-based fraud—demonstrate the limitations of traditional information security strategy and technology. To address these incidents, companies now need to protect their critical data at the "point-of-use"—employee PCs, laptops, USB-attached storage devices and other endpoint devices. IBM offers an endpoint data loss prevention solution that represents an evolutionary combination of technologies and services to help companies discover and classify sensitive data, monitor data usage and control and block high-risk activities. IBM Data Security Services ensure that your organization benefits from the latest endpoint data loss prevention technologies—to detect and mitigate the risks associated with sharing sensitive data while enhancing collaboration and business agility.

Reducing risk—and enhancing business processes—through the endpoint

Unprotected endpoint devices are like open doors into your sensitive information. You need to guard the data on those devices—whether the data is at rest, in use or in motion. You need to protect data in every stage of its lifecycle—from creation and modification to distribution and archiving. And you have to secure data no matter what form it takes or where it is stored. Endpoint data loss prevention enables you to make information more readily accessible to authorized users, to help ensure consistent collaboration while encouraging and enforcing the responsible use of corporate data to improve compliance with regulations and policies.

Endpoint data security gives you wide coverage in terms of geographical range, modification of end user behavior and visibility into data usage. It offers strong preventative control without interfering with business processes. Endpoint data loss prevention enables you to encrypt sensitive data files on the endpoint internal hard disk or different externally attached media to protect data on lost or stolen devices. And, it allows you to perform forensics for investigative purposes. Ultimately, endpoint security reduces the risk of data loss more directly than security at any other point.

Delivering end-to-end integrated security solutions for endpoint data protection

Data generates new value when it is used. Although usage creates risk, appropriate manipulation increases the value contribution of an organization's most valuable asset—data.

IBM can create a security framework to help secure your information throughout the extended enterprise. IBM also provides application integration for ease-of-compliance reporting and policy administration. The resulting solution ensures that you can collaborate while mitigating risk associated with data transfer and usage.

IBM designs endpoint data loss prevention solutions with your needs in mind to:

- *Establish an enterprise data loss prevention framework for your organization*
- *Deploy market-leading technology using a proven implementation methodology*
- *Translate and enforce corporate data classification and management policies*
- *Discover sensitive data at rest across endpoints including laptops, desktops, file servers and more*
- *Monitor data usage, configure application controls and block unauthorized behavior*
- *Define and deliver reliable management and support services*

IBM Data Security Services address the challenges associated with deploying a comprehensive solution by managing cost and scope, accelerating implementation, leveraging IBM information security expertise and eliminating the need for additional headcount.

Enabling endpoint data loss prevention as part of a holistic solution

The IBM approach to data loss prevention is to disperse control across three main areas of the IT environment. By dispersing encryption, content inspection, user monitoring and access control management functionalities throughout the infrastructure, IBM can help identify and deploy mitigating controls for greater data protection across the extended enterprise at a lower total cost.

IBM data loss prevention solutions are designed to help you achieve your company goals while protecting against sophisticated and complex IT and privileged user threats that can lead to the loss of business value.

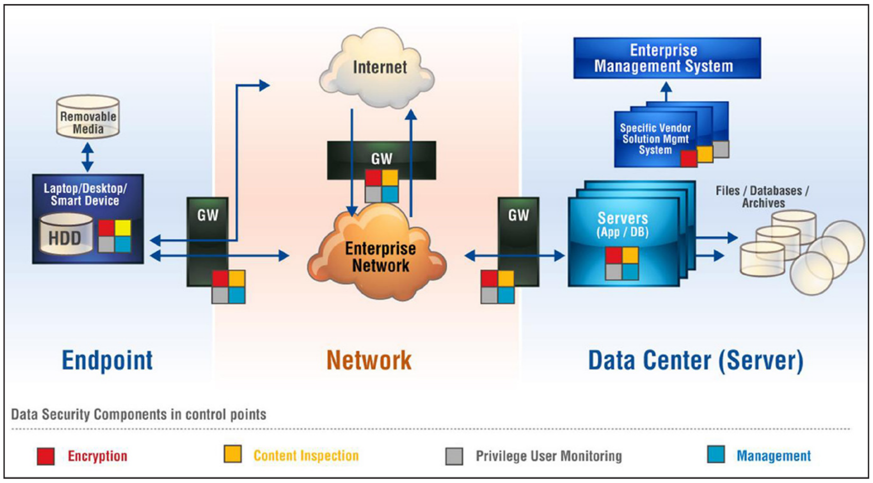

Internet
GW
Enterprise Network
Enterprise Management System
Specific Vendor Solution Mgmt System
Files / Databases / Archives
Servers (App / DB)
GW
Removable Media
Laptop/Desktop/ Smart Device
HDD
GW
Endpoint
Network
Data Center (Server)
Data Security Components in control points
🟥 Encryption
🟨 Content Inspection
⬜ Privilege User Monitoring
🟦 Management

Figure 1: The IBM approach to data loss prevention disperses control across three main areas in the IT environment.

Leveraging endpoint technology to address a broad set of information security risks

IBM's data-centric approach to endpoint security is specifically designed to prevent data from leaving the enterprise through three possible paths of exit—via devices, applications or network connections. In cases where corporate policy or regulations require encryption of all mobile data, the solution can transparently encrypt data files and/or e-mail to bring information transfer into compliance automatically. The IBM endpoint security process is designed to:

- *Establish a secure virtual perimeter around an enterprise*
- *Discover and classify sensitive data*
- *Gain visibility to how sensitive data is used by employees, contractors, partners and outsourcers*
- *Assess the risk associated with the sharing of sensitive data and define effective data security policies*
- *Implement automated data security policies uniformly across the enterprise*
- *Build out and deploy preventative warnings and justifications enforced by policies to train and deter end users before they take risky actions*
- *Deploy alert and block controls and audit collections of high-risk behavior, ultimately preventing costly and damaging data loss incidents*

IBM partners with Verdasys Inc., combining professional and managed security services with comprehensive technology to provide an integrated endpoint data loss prevention solution. This partnership ensures that every step of the solution lifecycle is backed by both proven experience and market-leading technology.

Reducing your management headache and optimizing your technology investment

IBM uses Verdasys Digital Guardian technology to power its endpoint data loss prevention solution. An integrated framework and multi-function unified agent enables companies to intelligently and adaptively address the broadest set of information risk challenges in today's highly collaborative and mobile business environment.

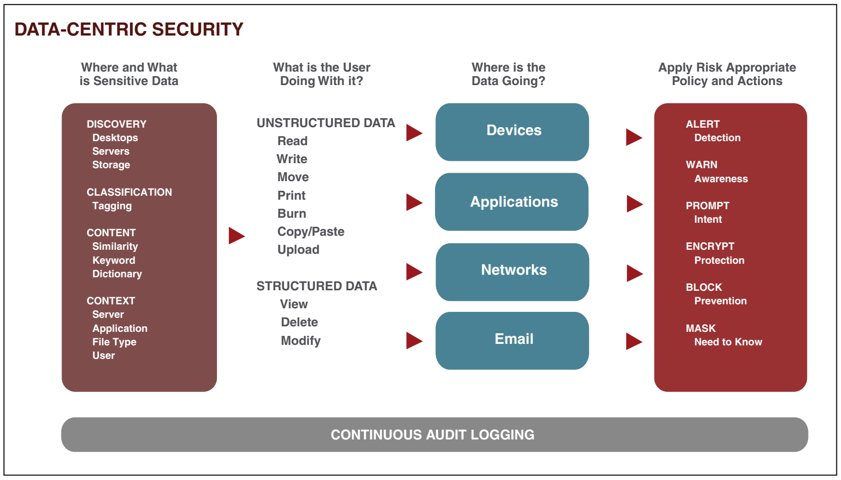


Figure 2: IBM Data Security Services uses proven technology and services to secure data throughout its lifecycle.

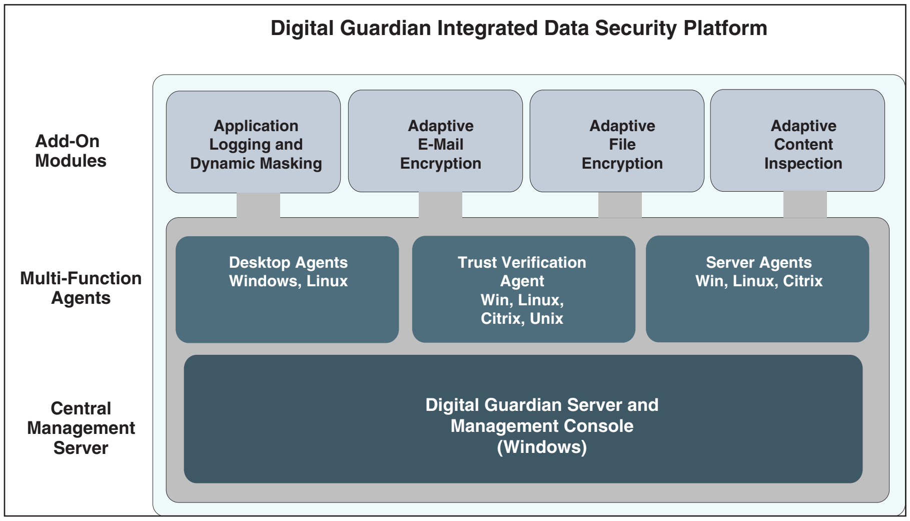

Digital Guardian Integrated Data Security Platform
Add-On Modules
Application Logging and Dynamic Masking
Adaptive E-Mail Encryption
Adaptive File Encryption
Adaptive Content Inspection
Multi-Function Agents
Desktop Agents Windows, Linux
Trust Verification Agent Win, Linux, Citrix, Unix
Server Agents Win, Linux, Citrix
Central Management Server
Digital Guardian Server and Management Console (Windows)

Figure 3: Verdasys Digital Guardian Integrated Data Security Platform

Digital Guardian ensures that data, applications and usage of information are governed, controlled, audited and, when necessary, automatically encrypted across infrastructure and business process boundaries through the following capabilities:

- **Actionable Data Discovery and Classification**–*Data classification polices are created and enforced by hardened and invisible endpoint agents. Context-based classification allows you to discover and classify files based on source application, server, path, file type and user identity. Content-based classification allows you to discover and classify files based on keyword or entity content pattern matching and document similarity.*

- **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, offering complete visibility into data activity, location and movement.*

- **Policy Enforcement**–*Protect your data through configurable policies delivered from the central server. Policies can vary from broad to discrete and enable full control over data usage at the "point of use" both on- and offline. Rules are subsets of policies and warn users of impending high-risk activities and policy violations before action is taken, giving users the ability to alter their behavior without interrupting business processes. Rules can also block user actions outright when policy violations are repeated or severe. Administrators are automatically alerted to policy violations, and all activities are logged.*

- **File Encryption**–*Delivers automatic, policy-driven encryption of sensitive files located on or copied to local drives on laptops, desktops, or external devices and CDs/DVD. File encryption eliminates the need for multiple encryption tools to consistently enforce data security policy, reduce the risk of data loss from stolen laptops and increase regulatory compliance.*

- **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. This eliminates the need for separate mail encryption tools, while enforcing consistent security policies across the enterprise and beyond to your partners, suppliers, contractors and outsourcers.*

- **Trust Verification Agents (TVA)**–*Establish a secure community of trust between the data owner, provider and user. It helps ensure that sensitive data is accessed only by trusted machines and is subject to corporate security policies. TVA creates a "virtual" network access control solution across your extended enterprise without requiring the redefinition of networks and servers. The community-of-trust solution enables organizations to enforce data security policy across offshore locations, suppliers and outsource providers.*

- **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. It saves millions of dollars in recoding costs while extending data security to applications that lack the native data access and logging capabilities necessary to protect data and ensure regulatory compliance.*

- **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. All report types offer high-level views and granular details. The reporting engine includes an easy query interface for the creation of custom reports. Digital Guardian's actionable reporting offers visibility into the state of data risk across the entire organization. Drill-down capabilities offer visibility to data movement and usage at an individual level. Compliance reports include predefined data usage reports for PCI, HIPAA, GLB and SOX regulations.*

- **eDiscovery and Forensic Reporting**–*Generates aggregated case reports that include data usage from across the enterprise including: offline, contractor and partner activities. It can drill down through your case reports to discover file, network, classification, user activity, time and environmental information for individual or group activity. Efficiently move through aggregated log and audit information to focus on meaningful data, reducing the cost and time of analyzing information and creating effective forensic reports.*

The IBM endpoint data loss prevention solution can help prevent the loss of sensitive information, applications and processes essential to maintaining market value, proprietary assets, intellectual property and the reputation and process integrity of your global enterprise.

Deploying your endpoint data loss prevention solution—IBM understands data security at the enterprise level. Our consultants and specialists have experience with a wide range of industry solutions and IT architectures to help you adopt an endpoint data loss prevention solution. Our professional support services can help you:

- *Conduct a* **Requirements and Planning Workshop** *to help you define your environment, business, compliance and IT requirements, prepare for implementation of controls and help you develop an all encompassing approach for planning and implementing a data loss prevention solution.*

- *Assess and discover sensitive data and user actions associated with this data on endpoint devices through a* **Discovery Assessment**.

- *Create your* **Policy Design** *by working with you to define your data loss prevention policies and deployment priorities for implementation and testing. IBM will also utilize a number of predefined rules and policies to help accelerate solution deployment throughout large enterprises.*

- *Implement all components of a solution in your environment successfully by providing the following* **Implementation Services***:*

  - *Implementation planning and project management*
  - *Solution architecture and design*
  - *Installation of primary components*
  - *Testing of primary components*
  - *Pilot deployments to test in your live environment*
  - *Product roll-out of controls to all endpoints*
  - *Project documentation*
  - *Help desk deployment assistance*
  - *Technical training and transfer skills*
  - *Project close-out and hand-off*

- *Provide a single point of contact for your support needs with a global* **Support Desk**–*which will provide support for all Verdasys products licensed and deployed in the solution with escalation to Verdasys for break/fix or insolvable issues. The IBM support desk will own and help manage, track and resolve problems related to the data loss prevention solution.*

Ongoing endpoint data loss prevention with IBM Managed Security Services

IBM provides ongoing managed services to help you manage your solution:

- **Ongoing remediation and policy enforcement** *for day-to-day operational support from an IBM hosting center that runs and manages your deployed data loss prevention solution. Our services include:*
  - *Policy design, implementation and enforcement*
  - *Implementation, configuration and maintenance of server and endpoint agent components*
  - *Single point of contact for support desk*

- **Ongoing monitoring, response and reporting** *for day-to-day monitoring and response to critical events and policy violations. IBM will deliver periodic reports on policy compliance, enforcement status and end-user violations. In the case of a serious event, based on defined procedures and service level agreements, IBM will escalate the issues. IBM would then propose adjustments and refinements to your policy to help accommodate new requirements and minimize false positives.*

IBM combines refined methods and extensive skills to help you realize the full value of your technology investment. Our services are designed to help optimize productivity, manageability and cost-effectiveness within your IT organization.

Why IBM and Verdasys?

Together IBM and Verdasys combine their technology, experience and expertise to deliver a complete endpoint data loss prevention solution. Verdasys software is designed to identify and mitigate the risk of sharing critical information across the extended enterprise through automated discovery, classification and monitoring of sensitive data utilizing an optimized mix of context and content analysis. Verdasys software enables the creation and management of centrally defined data security rules that automatically enforce corporate security policies at the endpoint, helping prevent unauthorized use of data through control and block activities and preventing data loss through CD burning, copying/pasting, printing, writing to USB drives, network transfers, file sharing and use of unapproved applications

With IBM Global Services' experience, global reach and scale, you can confidently deploy Verdasys' best-in-class software. IBM solutions, powered by Verdasys, provide you with an end-to-end integrated endpoint data loss prevention solution to manage your information security through its entire lifecycle—creation through ongoing management.

With IBM and Verdasys, knowledgeable practitioners, proven methodologies and innovative software and services help you rapidly implement and support a comprehensive solution to protect your market value at less risk than your internal staff and most other service providers.

For more information

To learn more about IBM Data Security Services for endpoint data loss prevention, contact your IBM representative or visit:

ibm.com/services

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
04-08

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.