Digital Guardian

Proven

Revolutionary

Innovative

Companies Serious About
Information Protection Choose

VERDASYS™

VERDASYS
GLOBAL DATA SECURITY

THE INFORMATION PROTECTION CHALLENGE

Your security perimeter is no longer defined by your firewalls, network gateways or other externally facing machine or devices. This protection model does not take into account either the business or technology changes of the last 15 years. Today, businesses must mitigate the risk of sharing sensitive data to enhance collaboration across geographically dispersed organizations, global distribution networks, integrated supply chains and outsourcing environments. These are just a few of the mainstream business models that reduce a traditional security perimeter to irrelevance.

New technologies such as high powered laptops with CD burners, Blackberries, multi-gigabyte USB devices, web based email and unlimited wireless access enable data to move beyond the corporate network so quickly and efficiently that traditional infrastructure security is almost always blind to its movement. Infrastructure-centric approaches to data security have been tactical in nature, utilizing disparate "point products" which introduce administrative complexity, raise IT costs and increase risk. Once sensitive data begins moving into an uncontrolled environment (off of a corporate network, for example), it is effectively compromised.

For companies to substantially reduce the risk of information loss, they need to take a strategic, risk based approach to data security by implementing an integrated solution that enables:

- Data discovery & classification
- Central policy management
- Risk-appropriate responses to policy violations
- Automated controls
- Actionable alerting and reporting
- Global visibility into the information location and usage

CIGNA

"Digital Guardian is a business enabler For example, we wouldn't be able to achieve the significant business benefit outsourcing offers without it."

Craig Shumard,
CISO
CIGNA

BROADCOM.

"Digital Guardian's unique capabilities to centrally monitor and control, at point of use, our high value corporate data and intellectual property across our global operations, including engineering, business and manufacturing processes integral to our supply chain, makes it an ideal solution."

Ken Venner,
CIO **Broadcom**

The Verdasys Digital Guardian Platform

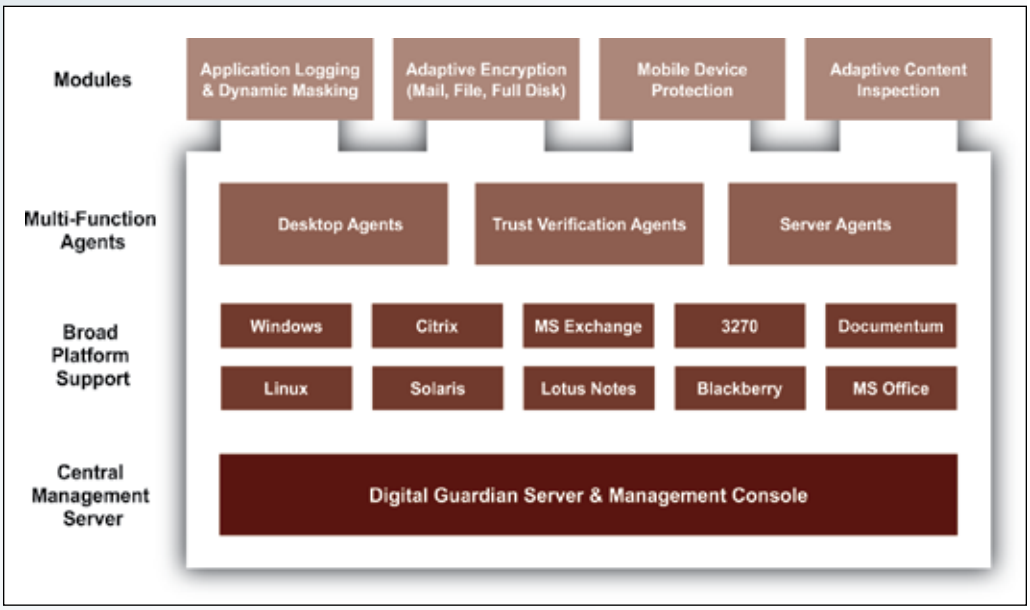
Verdasys Digital Guardian is a comprehensive information risk management solution that serves as the foundation for enterprise-wide information protection. Digital Guardian's unique and proven architecture makes it possible to implement a data-centric approach that acts at the point of use to make real-time decisions about data protection.

- Discover and classify sensitive data as well as gain visibility to how it is used by employees, contractors, partners and outsourcers
- Assess the risk associated with the sharing of sensitive information, make informed business decisions and create effective data security policies
- Use policy driven data security to drive accountability down to the end-user and increase voluntary compliance and risk aware behavior
- Prevent damaging data loss incidents without impairing business process by detecting high risk behavior and applying risk appropriate responses

COMPREHENSIVE INTEGRATED FRAMEWORK

Digital Guardian, through its integrated framework and multi-function agent, is the only information protection solution that eliminates multiple point products, simplifies the overall control and management of sensitive information across the enterprise and enables:

- Policy enforcement that leverages not only identity and activity, but also data classification, context, and content analysis at the point of use
- Risk appropriate responses to user activities including warnings, blocks and policy driven automated file and email encryption
- Enterprise-wide visibility into sensitive information location and usage
- Actionable data classification that enables policies to be enforced efficiently and effectivly based on sensitivity across the content management lifecycle



HUMANA
Guidance when you need it most

"Verdasys' solution offers us an opportunity to not only better protect customer privacy, but give us greater insight into how our own processes really work."

Paul Ratner,
VP, IT Operations
Humana

TOYOTA

"Digital Guardian assures comprehensive data security throughout our global information supply chain."

Jim Naruo,
GM Information Technologies
Toyota

Revolutionary

Secure Outsourcing

VERDASYS
GLOBAL DATA SECURITY

POWERFUL DATA

Actionable Data Discovery and Classification

Digital Guardian includes both "context" and "content" based data discovery, analysis and classification. Data classification polices are created and enforced by Digital Guardian Agents. Context classification allows you to discover and classify files based on over 106 variables including source application, server, path, file type and user identity. Content based classification allows you to discover and classify files based on keyword, REGEX, pattern matching, dictionary and document similarity. Classification tagging can be both non-persistent or persistent which includes classification inheritance for any content moved into a new document.

Policy Enforcement

Digital Guardian protects data through flexible policies delivered from the central server. Policies can be configured from broad to discrete, and enable full control over data at the "point of use" both on and off line. Digital Guardian rules act as data management controls alerting or blocking users from taking risky activities or violating policies before action is taken; driving accountability to the user and offering alternative choices without interrupting business processes. Policy violations trigger notifications to appropriate administrators, and all related activities are logged.

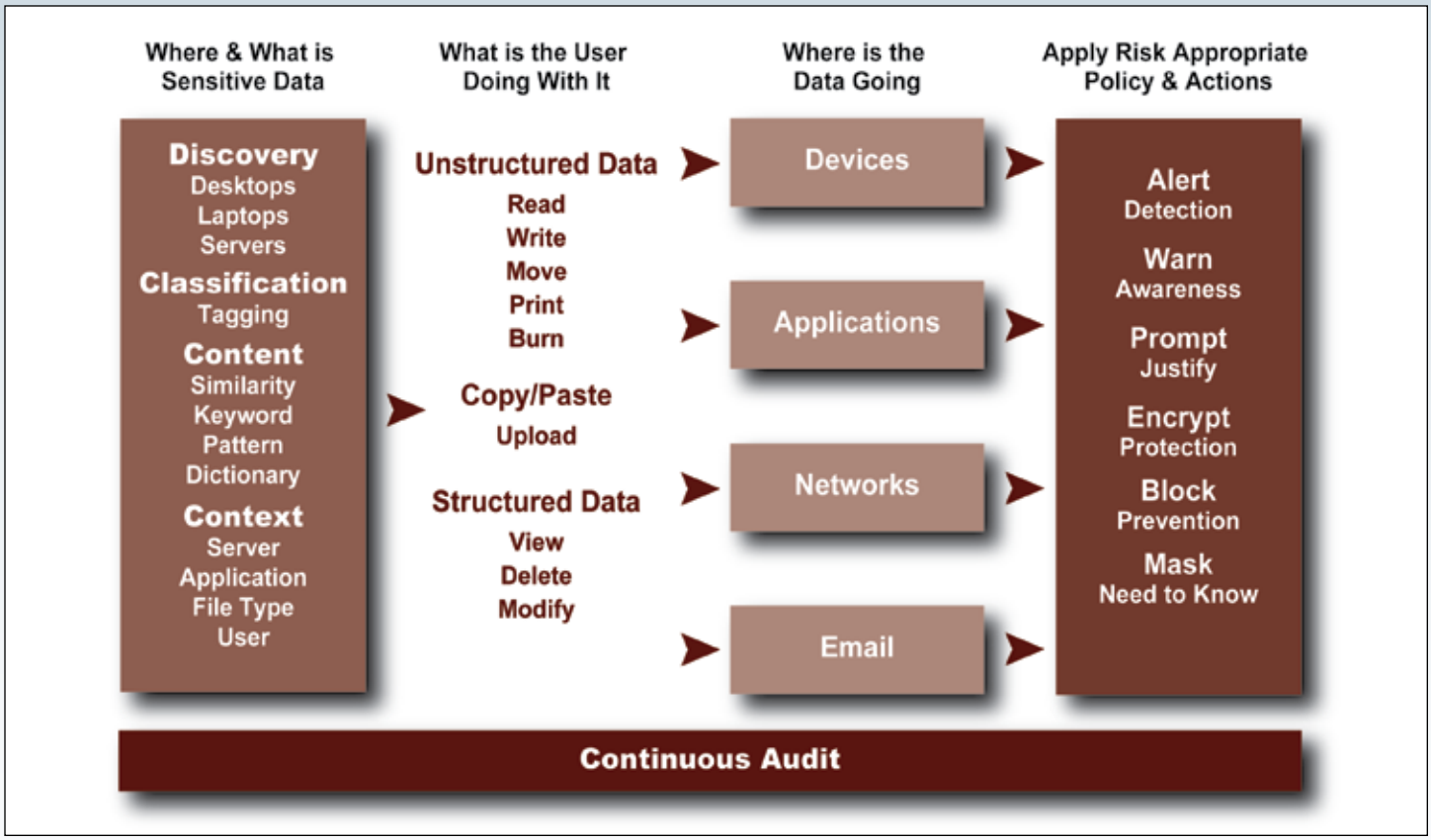
Risk Appropriate Policy Driven Controls Including Integrated Encryption

Digital Guardian offers policy driven, automated data controls designed to achieve optimal business value by allowing for the maximum amount of collaboration balanced against the inherent risk of an activity. Data controls include: incident alerting, training, prompting, justification, blocking and unified encryption. Encryption controls are fully integrated, policy driven, and cover full disk, mobile device, email and data level encryption. This control flexibility eliminates the need for companies to deploy disparate products like NAC, USB device control as well as whole disk, file and email encryption.

Innovative

FEATURE	DESCRIPTION	BENEFIT
Context Based Data Management	Discover, classify, monitor and enforce data security policies based on: source, destination, time, file type and name, connection awareness, active applications, user role, activity and name.	Powerful IP and Trade Secret data protection model for undefined data structures like software code and scientific equations.
Content Based Data Management	Discover, classify, monitor and enforce security policies based on data content in over 300 file formats and 90 languages across servers, Citrix gateways, desktops and laptops.	Protection for defined sensitive data like PHI and credit cards. Integration with Context Monitoring to virtually eliminate false positives and improve accuracy and efficiency.
eDiscovery and Forensic Reporting	Generate aggregated usage reports from across the enterprise including off-line, contractor and partner activities. Drill-down discovery to the individual users.	Efficiently move through aggregated log and audit information, focus on meaningful data. Reduce the cost and time of analyzing information and creating effective reports.
Reporting for Audit and Decision Support	Comprehensive reporting for high-level aggregate views of group and user activity. Drill down to granular views. Easy query enables creation of custom reports. Trending and behavior analysis to identify abnormal patterns.	Actionable reporting on the state of data risk across the entire organization. Drill-down offers visibility to data movement and usage.

CENTRIC SECURITY



FEATURE	DESCRIPTION	BENEFIT
Unified Adaptive Encryption	Patented, classification driven automatic encryption of data through its entire lifecycle, across full disk, files, to portable media and across email.	Eliminate the need for multiple encryption tools, enforce data security policy consistently, and mitigate data loss risk from stolen laptops.
Mobile Device Protection	Govern, control and audit the flow of sensitive information sent using handheld mobile devices in your organization.	Extend effective control perimeter to workers on mobile devices. Empower higher mobile productivity while maintaining security.
Trust Verification Agents	Establish a secure “community of trust” among the data owner, provider and user ensuring sensitive data is accessed only by trusted machines and is subject to appropriate security policies.	Create a “virtual” network access control solution across the extended enterprise. Enforce data security policy to offshore locations, suppliers, and outsource providers.
Application Logging and Masking	Enforce field level access control through data masking, and audit logging for legacy (3270 terminal emulators), client server and web based applications.	Extend data security to applications that lack native data access and logging capabilities necessary to protect data and assure regulatory compliance.

EXTENSIVE USE CASE COVERAGE

Digital Guardian enables customers to address the broadest set of expanding information risk challenges economically, intelligently and adaptively in today's highly collaborative and mobile business environment.

Personal Data Protection

Reduce the risk of PHI or PII data loss through unified policy enforcement. Create a risk aware culture and remove voluntary compliance through warnings and prompts to end-users and blocking if required. Secure personal information across all employee and contractor desktops, laptops, file servers, Linux servers and Citrix servers.

Secure Messaging & Mobile Data Protection

Define policies that automatically encrypt files or emails based on context, classification or sensitive content. Eliminate the need for separate encryption tools while sharing sensitive data in emails and on network drives with your partners, suppliers, contractors, outsourcers – on and offline.

Data Discovery & Classification

Utilize both content and context based data awareness; run both background and real-time data discovery programs. Apply policy based actionable classifications to all sensitive data across the enterprise.

Secure Outsourcing & Third Party Collaboration

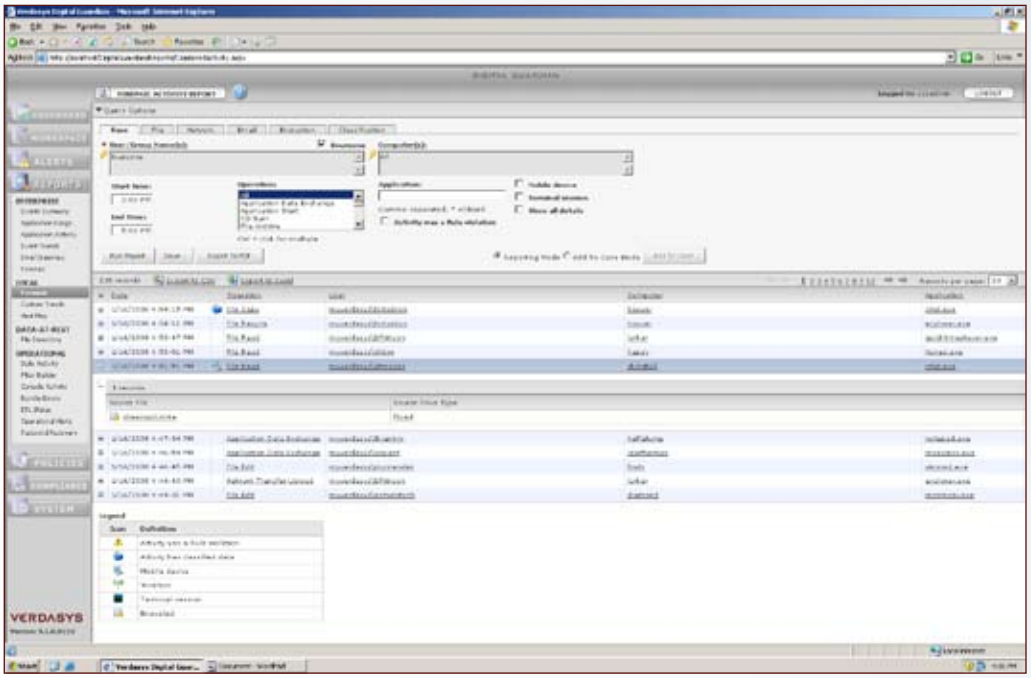
Enable greater cross enterprise collaboration and data sharing while minimizing the risk of sensitive information compromise. Digital Guardian's flexible host architecture secures intellectual property and trade secrets from being misused by privileged users at partner and outsourced sites around the globe.

Intellectual Property Protection

Increase innovation and reduce time to market through collaboration across design and development teams including partners and contractors. Digital Guardian secures intellectual property and trade secrets from being misused by privileged employees, contractors and third parties around the globe.

Privileged User Monitoring, Segregation of Duties

"Police the policeman." Monitor and record all activities of privileged users including system administrators and senior executives, apply appropriate security polices. Log all activities through Digital Guardian's operating system independent of existing security models.



Intellectual Property Protection

eDiscovery & Forensics

Proven

Information Governance, Risk & Compliance

Architect and deploy transparent, automated and actionable data protection policies and controls across information risk disciplines and external mandates such as HIPAA, GLBA, PCI, PIPEDA, CA SB 1386 and the EU Data Directive.

Unified Enterprise Encryption

Adaptive, risk appropriate and centrally managed file, mail and full disk encryption. Drastically simplified key management through patented technology. Painless enrollment and recovery scenarios.

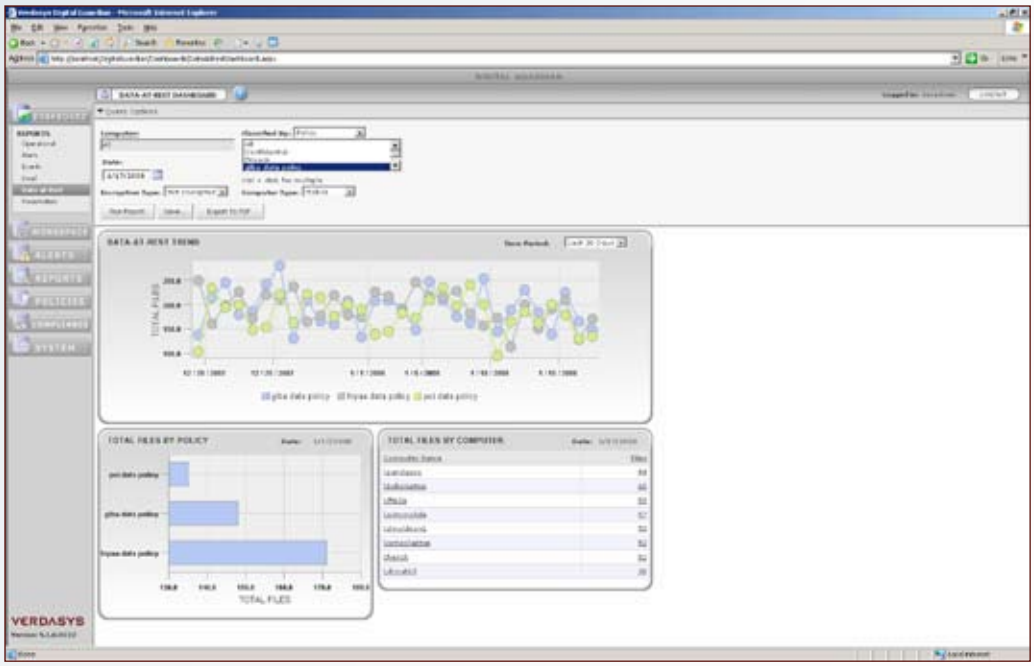
Application Management & Compliance

Utilize application management to control downloads and executables, white, black and gray list applications by type and version, maintain gold images, prevent malware downloads and reduce operational support complexity. Extend to legacy and custom applications that lack native access and logging, controls necessary to protect data saving millions of in re-coding costs. Ensure regulatory compliance with mandates including HIPAA, GLBA, PCI and other privacy regulations.

eDiscovery & Data Forensics

Reduce the time and cost of conducting forensic investigations. Generate aggregated discovery reports for all user activities and data usage across the enterprise including offline activities. Prove the positive and the negative (e.g. one user copied a file to an external drive and no one else did).

Companies serious about Information Protection choose VERDASYS GLOBAL DATA SECURITY



Privileged User Management

Data Discovery

VERDASYS
GLOBAL DATA SECURITY

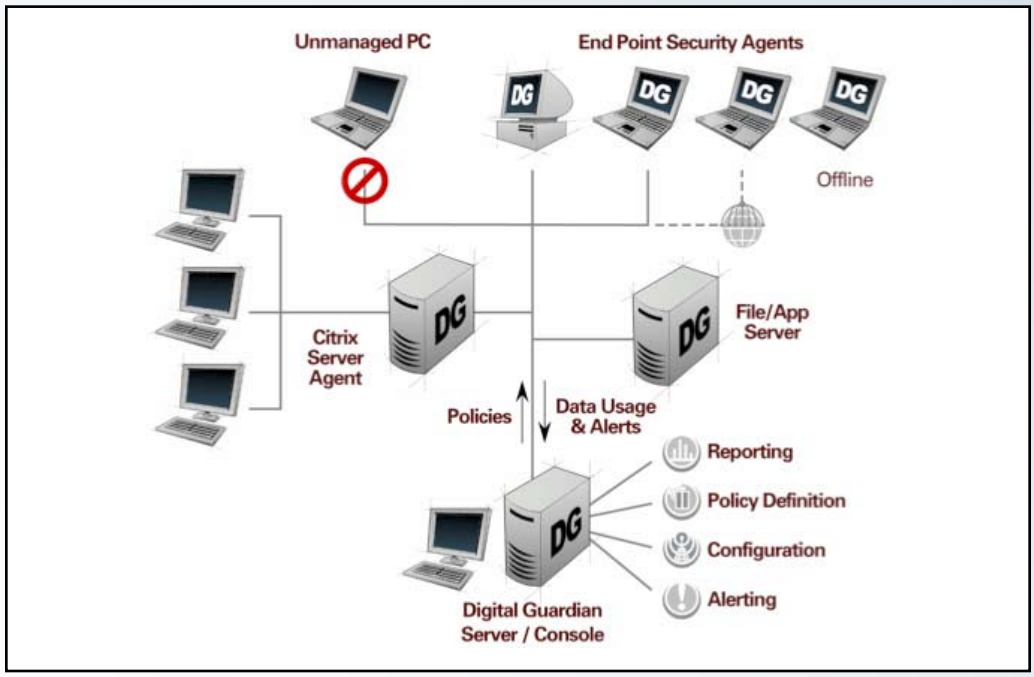
DIGITAL GUARDIAN ARCHITECTURE

Digital Guardian Multi-Function Agent

The Digital Guardian Agent is the only multi-function agent available that delivers policy driven data discovery, classification, monitoring, and control. The Digital Guardian Agent:

- Delivers fully integrated policy driven adaptive file, email and full disk encryption.
- Hardened and tamper proof, can be made invisible on the host system.

Verdasys Digital Guardian is a unique comprehensive and proven host based information protection solution for tracking and securing the flow of critical data across your extended enterprise. Whether on PCs, laptops, or servers (inside or outside the organization). Verdasys Digital Guardian is there to monitor, log, warn, encrypt and, if necessary, block prohibited actions by trusted end-users.



Digital Guardian Server

The Digital Guardian Server is a Web-based application server and console that is the command center for the Digital Guardian Platform. The Digital Guardian Server:

- Manages and monitors all Digital Guardian Agents
- Captures, aggregates and stores all user activities related to sensitive data
- Manages data security policies and distributes them to all Digital Guardian Agents for enforcement
- Enables flexible data classification frameworks and rules to be created
- Triggers administrative alerts and email notifications when security policies are violated
- Includes an easy to use reporting engine for high-level, detailed and custom report creation

About Verdasys

Verdasys provides enterprise software solutions that are the foundation of our customer's global data security strategy. With greater than 1 million security agents deployed at over 120 of the world's leading organizations, Verdasys is the proven leader of global data security solutions for information protection and compliance.

Verdasys headquarters is located in Waltham, MA, with offices in London, Munich, Rome, Madrid, Athens, Tel Aviv, Tokyo, Osaka, Taipei, Singapore and Shanghai.

Corporate Headquarters

404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

WWW.VERDASYS.COM