

# Insider Threat Protection

## COMMERCIAL SOLUTIONS DATASHEET

### PROTECTION FROM INSIDER THREATS

Preventing data misuse by trusted users is the hardest information protection challenge to solve. More than ever, the growing need for “anytime, anywhere” data collaboration to support business strategy and increase competitiveness creates new opportunities for privileged insiders to compromise classified information as their access to sensitive data increases. Traditional IT security measures which simply control unauthorized network or application access are ineffective, as insiders already have full authorization to the data. A more powerful security approach is required to defend against the Insider Threat.

### VERDASYS DIGITAL GUARDIAN

Verdasys Digital Guardian is the only proven solution for insider threat **detection, deterrence, and prevention** at enterprise scale in both physical and virtual environments. The Digital Guardian platform addresses insider threats by monitoring and controlling both user access and usage rights to data. Digital Guardian continuously logs and controls the handling of sensitive information by privileged users without preventing authorized activity; it intervenes only when a policy violation is detected.

### INFRASTRUCTURE AGNOSTIC SECURITY

Digital Guardian is ideally designed to secure critical information like Intellectual Property (IP), trade secrets, PII, PHI and proprietary data across global operations. Digital Guardian is an autonomous, host-based security system that works equally in physical or virtual environments to monitor and control file, application, and system operations independent of user privileges.

### RISK-BASED POLICY ENFORCEMENT

Digital Guardian’s advanced security sensors operate in-between the user and data to achieve real time situational and risk awareness. Agents autonomously confirm insider threats defined by policy, and determine the correct enforcement response, with rules-based logic based on the user’s identity and privilege to complete the data transaction.

### SUPPORTS USER, APPLICATION, AND FILE-LEVEL CONTROLS

Once users are authorized to access protected data, Digital Guardian allows them to perform a wide range of file and application-level operations based on their policy rights, ranging from copy/move/save as to removable media; upload; email; print; burn to CD/DVD; copy and paste, etc.

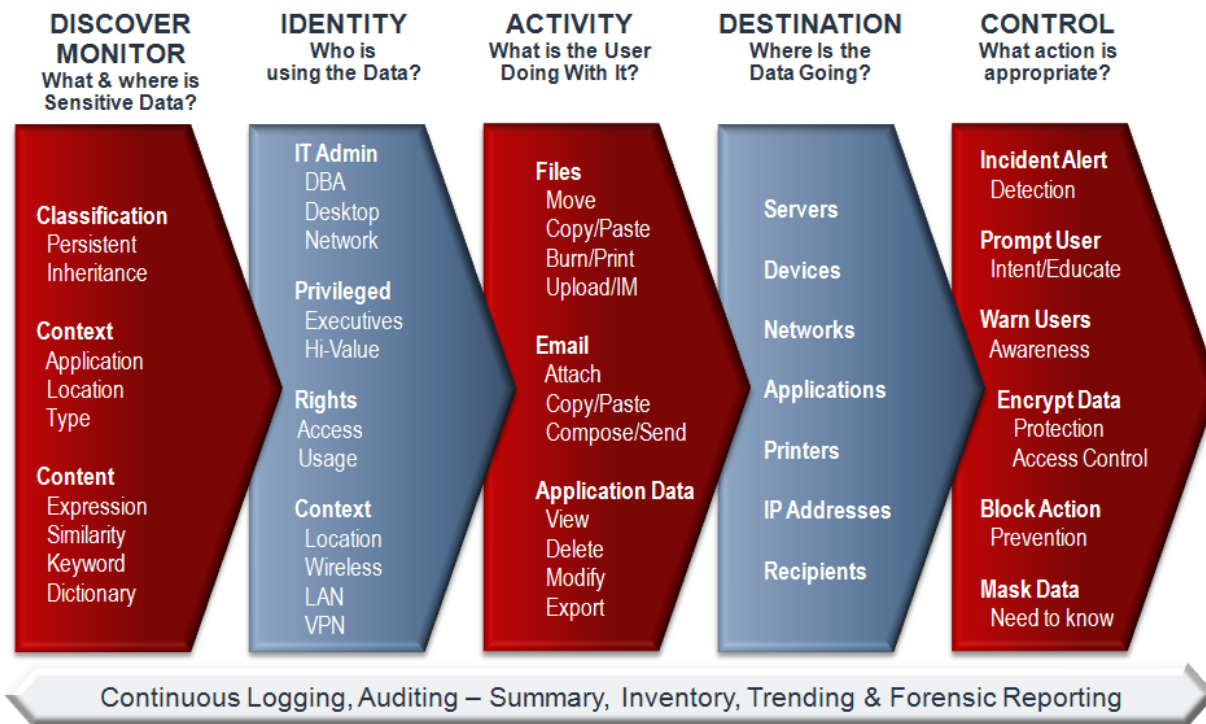
### COMPLEMENTS EXISTING INVESTIGATIVE TOOLS AND ADDRESSES INCIDENT RESPONSE NEEDS

Digital Guardian’s tamper-resistant agents record situationally-aware and causal event logs with admissibility and weight precedence as primary forensic evidence in criminal and civil cases, both domestically and internationally. Digital Guardian ensures a secure, complete, and accurate audit trail of privileged user access and activity – on or offline – over the entire data lifecycle with minimal storage, CPU and network overhead.

Digital Guardian’s highly tamper-resistant architecture supports deterrence, prevention, training, investigative, and prosecutorial requirements out-of-the-box, including:

- Continuous, rules-based logging of user, file, application, network, and system event forensics
- Advanced analytics to prove intent and chain-of-custody
- Data discovery & persistent file tagging, disk inventory, and classification inheritance from source to destination file
- Transparent data-at-rest, data-in-use, and data-in-motion encryption (AES 256-bit), with automated key management and recovery
- Removable media logging, control and encryption
- Policy-based access control and usage entitlement of files by data categorization, user identity, and clearance
- Policy-based, real-time prompting to train or alert users exceeding their data-handling privileges
- Automated sensitive data leak detection and prevention, e.g. unstructured data moved from a secure database to removable media
- Integrated Advanced Persistent Threat (APT) live memory forensics detects and protects classified information from targeted external attacks

Autonomous Data Controls	✓
Automated Data Discovery & Categorization	✓
Data Content & Context Analysis	✓
Offline Policy Alerts & Enforcement	✓
Removable Media & CD/DVD Management	✓
File-based AES 256 bit Encryption	✓
Logical Data Segregation	✓
Complements Investigative and Incident Response Tools	✓
Continuous, Rules-based Forensic Logging	✓
VDI & Citrix Support	✓



### COMPREHENSIVE INSIGHT AND CONTROL CAPABILITIES

- Integrated software platform for insider threat monitoring, detection, deterrence, and prevention
- Provides continuous, rules-based capture of system activity as sequenced, compressed, hashed, signed, and encrypted log events
- Proven to scale beyond 500,000 agents reporting continuously to a single backend server
- Multi-tier reporting supports tactical or centralized threat analysis, and segregated administrator access
- Low load on network (50-200KB per user/per day of log data); agents report to the management server via secure messaging from anywhere in the world
- Tamper-resistant agent sources own forensic data with kernel, user mode, and application-agnostic visibility
- Hardened agent with configurable stealth and tamper resistance

- User-level data access and usage controls enable secure “anytime, anywhere” data collaboration
- Provides data transfer auditing and user accountability by monitoring and controlling all policy layers of the transactions (privilege, access, application, data, and activity)
- Centralized anomaly detection and precise incident drill down of policy violations across hundreds of thousands of transactions
- Integrated, on-board AES 256-bit encryption for transparent or password-based file transfers; includes automated key management and recovery
- Infrastructure agnostic, operates in physical or Citrix/VDI environments
- Integrates with existing DR, HA, and data warehousing infrastructure
- Archived log data can be replayed for forensic, investigative or evidentiary purposes

### CLEAR LEADER IN INSIDER THREAT SOLUTIONS

Verdasys has been successfully delivering innovative enterprise-class software in the insider threat market for over seven years to the world’s largest and most security-conscious organizations. Our unique product and service offerings combined with our execution success at the world’s leading companies make Verdasys the de facto leader in the Enterprise Information Protection (EIP) market space.

### SUPPORT

Digital Guardian software runs on Windows 2000, XP, Vista, Windows 7 (32 and 64 bit); Windows 2000 Server, Server 2003, Server 2008 as well as Red Hat Enterprise Linux 4 or 5; SuSE Enterprise Linux 9, 10 or 11; and Fedora 10.

## VERDASYS

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

[www.verdasys.com](http://www.verdasys.com)

### ABOUT VERDASYS

Founded in 2003, Verdasys provides insider threat solutions that are the cornerstone of our customer’s global data security strategy. With more than 2 million security agents deployed at over 200 of the world’s leading organizations and Federal agencies, our solutions and services provide a strategic and comprehensive approach to information risk management.