INSIDER THREAT PROTECTION

VERDASYS

Verdasys Digital Guardian provides insider threat detection, deterrence and prevention with the ability to scale from hundreds to millions of users. Digital Guardian captures forensically-rich intelligence and ensures total operational awareness and control over the use of classified data across all clearance levels with minimal storage, CPU and network utilization.

Protect and Deter Insider Threats: Federal agencies have been required to evolve very quickly from "need-to-know" into "share-to-win" or "need-to-share" requirements for classified information. Although the advantages of cross-service access are manifest for missions requiring on-demand intelligence, the opportunities for privileged users to compromise classified information rises exponentially. It is no longer sufficient to monitor and control who has access to data; insiders have all the credentials and entitlements to access protected data. A different paradigm in information protection is necessary to ensure authorized users cannot access or mishandle classified information outside of the mission scope.

Infrastructure Agnostic Security: Digital Guardian is ideally designed to support classified information security within complex operating restrictions. It is an autonomous, host-based security system that works equally well in physical and virtual environments to monitor *and* control file, application, and system operations independent of user status.

Risk-based policy enforcement: Digital Guardian's advanced security sensors operate in kernel and user-modes simultaneously for precise situational and threat awareness. Agents autonomously confirm potential threats defined by policy – and determine the correct enforcement response – using on-board logic relating user identity, clearance level, file classification, and mission scope.

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 operations based on file classification and user clearance, ranging from copy/move/save as to removable media, upload, email, print, burn to CD, copy and paste, etc. Verdasys Digital Guardian Insider Threat solutions support "share-to-win" policies out-of-the-box by monitoring and controlling user-level access to data, while also protecting and deterring unauthorized uses once a file has been accessed.

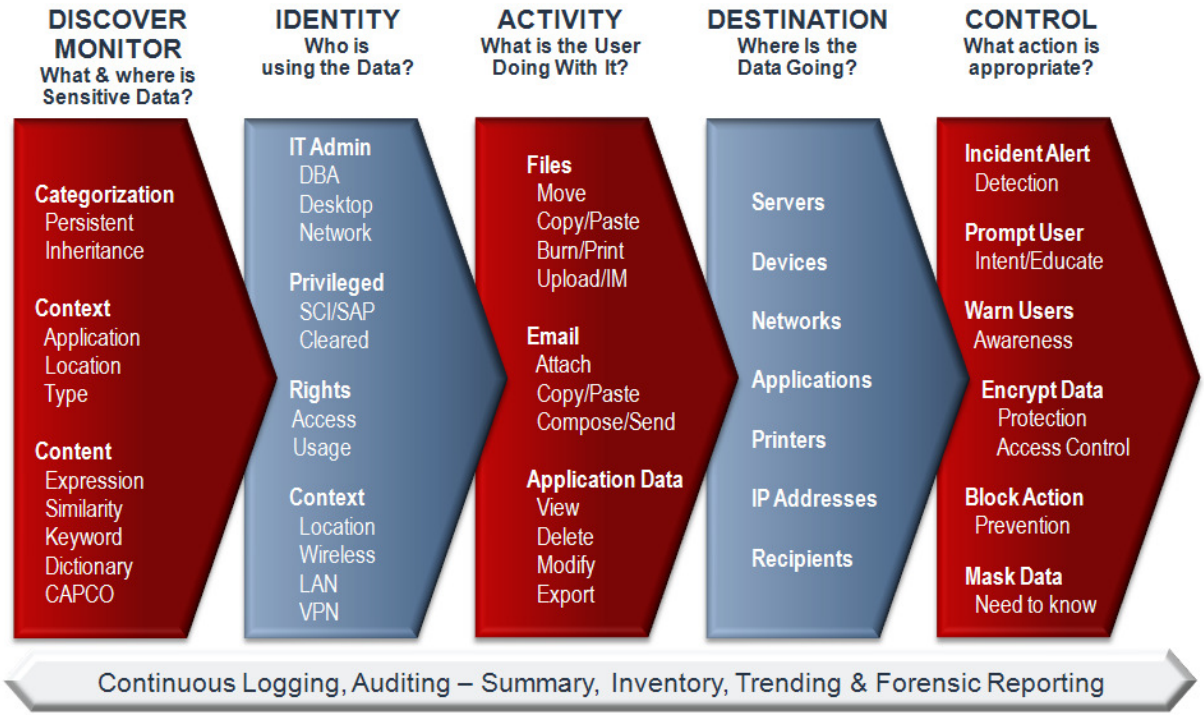
Complements existing IA/CND tools and addresses LE/CI needs: Digital Guardian's tamper-resistant agents record situationally-aware and causal event logs with admissibility and weight precedence as primary forensic evidence in criminal and civil cases, both domestically and internationally.

Automated Data Controls	✓
Automated Data Discovery & Categorization	✓
Data Content & Context Analysis	✓
Offline Policy Alerts & Enforcement	✓
Removable Media Management	✓
AES 256 bit Enterprise Encryption	✓
Logical Data Segregation	✓
Complements IA/CND with LE/CI needs	✓
Continuous, Rules-based Forensic Logging	✓

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 at rest discovery, disk inventory, and persistent file tagging/categorization
- Automated data-at-rest, data-in-use, and data-in-motion encryption (AES 256-bit)
- Removable media logging, control and encryption
- Policy-based access control and usage entitlement of files by data categorization, user identity, and clearance
- Tactical, real-time awareness prompting when users exceed privilege or scope
- Automated classified data spill detection, remediation, e.g. data from classified to unclassified using removable media
- Organizational Conflict of Interest (OCI) detection, monitoring and control
- Integrated Advanced Persistent Threat (APT) live memory forensics detects and protects classified information from targeted attacks

INSIDER THREAT PROTECTION



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 CND analysis, and restricted LE/CI access
- Low load on network (50-200KB per user/per day of log data); communicates from anywhere in the world on any port over HTTP(S)
- Tamper-resistant agent sources own forensic data with kernel, user mode, and application layer visibility
- Hardened agent with configurable stealth and tamper resistance
- Data usage and movement monitoring and control addresses “share-to-win” requirements
- Provides cross-domain data transfer assurance and accountability through monitoring and controlling transmit and receive points
- User anomaly detection with statistical analytics and optimized OLTP data warehouse
- Integrated, on-board AES 256-bit encryption for transparent or password-based file transfers; includes automated key management and recovery
- FIPS 140-2 certified cryptography
- Infrastructure agnostic, operates in physical or virtual/VDI environments
- 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: Verdasys 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.

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.

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

WWW.VERDASYS.COM