

The Data Forensics Challenge

The Verdasys Digital Guardian platform offers a complete data forensic and eDiscovery solution and is the only data security solution that has been used in multiple successful data loss prosecutions. Data forensics and eDiscovery are critical components of a “defense in depth” security program and an imperative part of any data security strategy. Forensic information is often critical evidence in many types of criminal and civil litigation including fraud, theft or misappropriation of trade secrets and other internal or confidential information.

Digital Guardian Forensics & eDiscovery

Digital Guardian increases the efficiency and accuracy of investigative work by providing complete, real-time visibility into the actual data usage of all investigative targets. Digital Guardian offers enterprise wide comprehensive, forensic-level analysis of all data located on protected applications, servers, workstations, desktops and laptops across the enterprise. Digital Guardian’s flexible reporting capabilities and integrated “case management” tool are specifically designed to meet investigative and discovery requirements as well as protection of evidence. As a platform data security solution, Digital Guardian uniquely offers the ability to :

- Securely investigate/analyze data on any Digital Guardian protected machine
- Collect, aggregate and format all data related activities in a forensically sound manner
- Reduce incident impact and eliminate system downtime during investigations
- Efficiently analyze only potentially relevant data upon investigation requests
- Identify data security events and employee integrity issues wherever they are taking place on or offline without alerting the target
- Monitor and audit all privileged users actions including investigative activities once a case has been opened
- Download all audit information to third party case tools as needed

Multiple Verdasys customers have successfully utilized Digital Guardian’s forensic information in litigation against sensitive data and IP loss including Broadcom and Ferrari. Broadcom utilized Digital Guardian forensic data to prosecute an individual after

Planning & Identification	Collection & Preservation	Analysis & Reporting
<ul style="list-style-type: none"> • Case planning • System target definition • Data discovery planning • User or Group investigation • Downtime reduction 	<ul style="list-style-type: none"> • Aggregated data collection • Enterprise data usage • Enterprise data discovery • Offline usage evidence • Evidence preservation 	<ul style="list-style-type: none"> • Aggregated reports • Drill down by user • Deep usage reports • Evidence protection • Third party integration

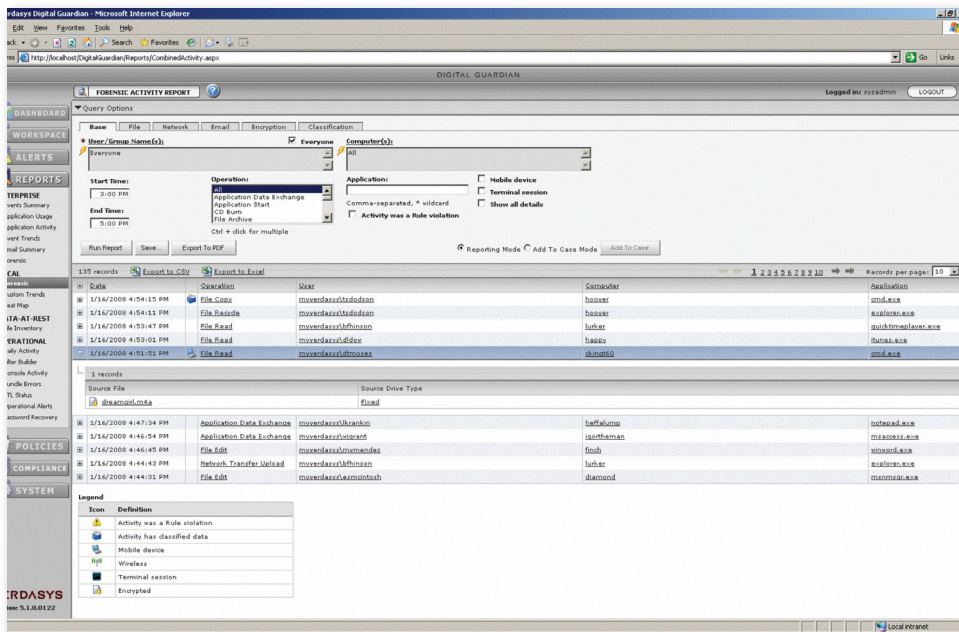
they left the company with sensitive chip design data. Digital Guardian enabled Broadcom to prove the individual in question downloaded sensitive IP onto non-company devices and that this was the only employee to do so. Ferrari utilized Digital Guardian to prove a former employee printed large amounts of sensitive design data which was later found at a competitor site. The Digital Guardian’s reports of misuse were successful in proving fault by the competitor who received a \$100 million dollar fine. The information is currently being used in litigation against the employee. Digital Guardian’s fully integrated data forensic capabilities increase the efficiency of investigative work maintaining the “proper” forensic data collection and protection requirements.

Forensic and Discovery Technology

The Digital Guardian Case Management Tools enables forensic investigators to build and manage a forensic trail of evidence to establish proof of malicious activity. Forensic cases and evidentiary collection can be created from alerts and events that demonstrate that a specific policy violation or event occurred. Configurable case management views are created with fully integrated access rights for different levels of investigators. Digital Guardian can automate ongoing investigation evidence collection as well as enable analysis of historic archived evidences.

Unified Forensic Reporting and Analytics

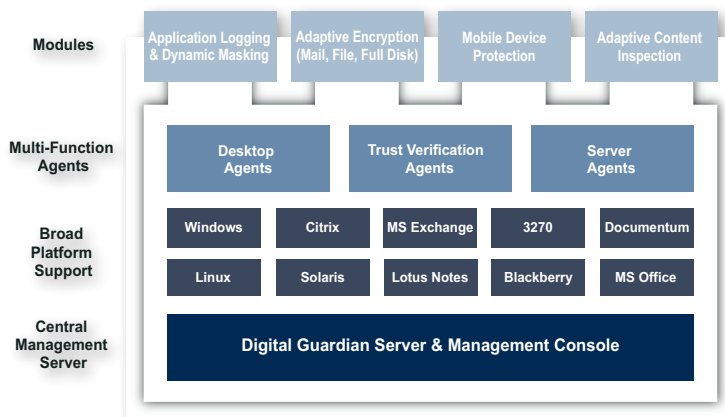
Digital Guardian's comprehensive reporting capabilities provide high-level aggregate views of group and user activity, with drill-down to granular views necessary for investigative intelligence. Easily created custom queries enable custom investigative reports. The benefit to investigators is faster time to value and richer context, driving efficiency and value.



Digital Guardian

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



Verdasys provides enterprise software solutions that are the foundation of our customers' 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, USA, with offices in London, Munich, Rome, Madrid, Athens, Tel Aviv, Tokyo, Osaka, Taipei, Singapore and Shanghai.

© 2008 Verdasys, Inc. All Rights Reserved. Verdasys, the Verdasys logo, Digital Guardian, and the Digital Guardian logo are trademarks of Verdasys, Inc. All other logos are the property of their respective owners. The content of this document is subject to change without notice. V5.0 09-29-08

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

WWW.VERDASYS.COM