

# Forrester Consulting

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE

*Prepared for Verdasys, Inc.*

January 31, 2005

## **The Total Economic Impact™ Of Digital Guardian Solutions From Verdasys**

**Project Director:**

Bob Cormier, Principal Consultant, TEI

FORRESTER®

FORRESTER®

**Headquarters**

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA  
Tel: +1 617/613-6000 • Fax: +1 617/613-5000 • [www.forrester.com](http://www.forrester.com)

## Table Of Contents

Executive Summary .....	3
The Organization Chooses Verdasys For Enterprise Information Security .....	5
The Organization’s High-Level Objectives With Verdasys .....	5
The Organization’s Drivers And Challenges.....	6
The Organization’s Costs.....	7
The Organization’s Benefits .....	8
The Organization’s Risks And Risk Mitigation Strategies .....	9
The Organization’s Flexibility Options .....	10
Financial Analysis — The Organization.....	10
Study Conclusions.....	11
Appendix A: Total Economic Impact™ Overview .....	12
Appendix B: Verdasys Digital Guardian Solutions.....	14
Overview — About Verdasys .....	14
Overview — About Verdasys Healthcare Solutions.....	14

© 2005 Forrester Research, Inc. Circulation or disclosure in whole or in part of this report outside the authorized recipient organization is expressly forbidden without the prior written permission of Forrester Research, Inc. Forrester, Forrester Oval Program, Forrester Wave, ForrTel, WholeView 2, Technographics, TechRankings, Total Economic Impact, and TEI are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

## Executive Summary

In January 2005, Verdasys, Inc. commissioned Forrester Research, Inc. to examine the financial impact areas and potential value that enterprises might realize by adopting Verdasys solutions within their environment. To determine the impact, Forrester examined the specific costs, benefits, flexibility, and the risk elements associated with an organization's investment in Digital Guardian solutions from Verdasys. Forrester interviewed representatives of a leading provider of healthcare and related benefits offered through the workplace predominantly in North America, which we will call the *organization*. It has chosen to remain anonymous for this study.

**Purpose:** The primary purpose of this study is to provide readers with a *framework* to evaluate the potential financial impact of Digital Guardian solutions from Verdasys within their own organizations. This study primarily should be seen as a guide to better understand and evaluate whether or not investing in Digital Guardian solutions from Verdasys is worthwhile.

**Methodology:** Verdasys selected Forrester for this project because of its industry expertise in security solutions and Forrester's Total Economic Impact™ (TEI) analysis methodology. TEI not only measures costs and cost reduction (areas that are typically accounted for within IT), but also weighs the enabling value of a technology in increasing the effectiveness of overall business processes. Forrester's TEI methodology serves an extremely useful purpose by providing a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

**Approach:** Forrester used a four-step approach for this study.

1. Forrester interviewed Verdasys marketing and sales executives to fully understand its value proposition.
2. Using input from existing Forrester research and knowledge of Digital Guardian solutions and Verdasys, Forrester representatives conducted in-depth discussions with the assistant vice president and the senior vice president of Information Protection at the *organization*.
3. Forrester constructed a financial value model representative of the data collected in the interview.
4. Forrester created this study, which examines the estimated value and represents the findings derived from the customer interview and analysis process, as well as Forrester's independent research.

**Key findings:** The table below represents a summary of the cost savings that the *organization* expects to achieve during a three-year period by using Verdasys’ Digital Guardian solutions compared to alternative application logging solutions.

**Table 1: Estimated Three-Year Costs And Savings, Net Present Value (NPV), To The Organization**

Summary financial results	Amount
Total three-year cost savings (NPV)	\$5,455,000
Total three-year costs (NPV)	\$1,771,000
Total three-year net cost savings (NPV)	\$3,684,000
Payback period	two months

Source: Forrester Research, Inc.

The total three-year net savings of \$3,684,000 represents cost avoidance of not recoding existing legacy applications to support Health Insurance Portability and Accountability Act (HIPAA) compliance and reporting. The *organization* estimated that the cost of breaking open the legacy code to add the logging functionality could range from \$100,000 to \$1 million for each of its 10 legacy applications. The *organization* experienced other benefits with Verdasys Digital Guardian solutions that it was not able to quantify in the areas HIPAA compliance and audit control and protection (for more detailed information, see the section below titled “The Organization’s Benefits”).

In addition, the *organization* believes that its initial investment in Verdasys solutions has created future “optional” benefits in using the flexibility of the Digital Guardian “agent” to perform other security functions such as file encryption, application data redaction, and data visualization. Although the *organization* was not able to quantify these future benefits, they are described in the section below, “The Organization’s Flexibility Options.”

The objective of this study is not to illustrate common savings that other organizations can obtain by deploying Verdasys solutions, but rather to identify savings experienced by the interviewed *organization*. These results should be used as a guide to allow other organizations to determine the appropriate benefits for its particular environment.

**Disclosures:** The reader should be aware of the following disclosures associated with this study:

- The study is commissioned by Verdasys and delivered by the Forrester Consulting group.
- Verdasys reviewed and provided feedback to Forrester, but Forrester maintained editorial control over the study and its findings and did not accept changes to the study that contradict Forrester’s findings or obscures the meaning of the study.
- The customer names for the interviews were provided by Verdasys.
- Forrester makes no assumptions as to the potential value that other organizations will receive within their own environment. Forrester strongly advises that the reader should use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Verdasys Digital Guardian solutions.
- This study is not an endorsement by Forrester of Digital Guardian or Verdasys.
- The study is not a competitive product analysis.

## **The Organization Chooses Verdasys For Enterprise Information Security**

Early in 2004 the *organization* signed a multiyear licensing agreement for the enterprisewide deployment of the Verdasys Digital Guardian Information Security Platform. As of January 2005, Digital Guardian has been deployed on several hundred desktops of highly trusted users with elevated privileges and third-party contractors in the United States and offshore. According to the *organization's* chief information security officer (CISO), the plan is to roll out Digital Guardian to 24,000 employees by the end of 2005. The expectation is that Digital Guardian, as one of a number of tools in the *organization's* overall compliance strategy, will help to ensure compliance with HIPAA privacy and security directives through a creative approach to logging and controlling protected healthcare information.

Although return on investment (ROI) was not a driver of this initiative, the *organization* believes that of the alternatives it researched, Digital Guardian provided compliance security solutions at a lower cost and lower risk for new and legacy applications.

According to the CISO, the *organization* initially deployed Digital Guardian to control and protect its outsourced development center. Currently, the *organization* is in the process of deploying Digital Guardian functionality for HIPAA compliance application remediation and the general protection of sensitive corporate information.

## **The Organization's High-Level Objectives With Verdasys**

The *organization's* information security team is responsible for setting enterprisewide standards as well as assessing and acquiring IT security products throughout the enterprise. The team evaluates all IT risks, decides which risks are acceptable, and determines controls to be implemented to mitigate unacceptable risks.

The *organization's* information security team constantly reviews and assesses new technologies and vendors to find the most effective ways to mitigate IT risks; these introduced them to Verdasys in mid-2003. After careful review, the *organization* decided to invest in the Digital Guardian product as one of several tools in its suite of security solutions companywide.

The *organization* has four high-level business objectives that it is hoping to satisfy with Digital Guardian solutions, including:

1. HIPAA compliance — to determine the most cost-effective approach to ensure compliance with HIPAA privacy and security directives, and reporting requirements.
2. The *organization* needed tools to help it understand compliance levels and policy enforcement for its high-privileged users, for both healthcare (HIPAA) and financial (Sarbanes-Oxley) regulations.
3. Provide adequate security solutions for its offshore development center and third-party application service providers (ASPs).
4. Invest in an extensible platform that expands to cover a broad range of information security needs for its 24,000 employees.

## The Organization's Drivers And Challenges

The *organization* had four specific drivers, challenges or issues it was hoping to remedy by investing in Verdasys Digital Guardian solutions:

1. Its No. 1 issue was security and compliance associated with the trusted or high-privileged users or administrators; the “insider” threat that employees may misuse their responsibilities. The *organization* cited industry sources suggesting that 80% of risks/issues originate from employees/contractors that have already been given authority. The *organization* recognizes that doing pre-employment background checks does not guarantee security and compliance in the workforce.
2. The second driver was potential “data leakage” with their offshore partners. The *organization* was starting a third-party offshore development center to outsource application development, maintenance, and production support of its health care applications. The *organization* understood both the benefits and risks associated with this approach and decided to put the necessary controls in place to ensure that offshore users could only access application “code” and not subscriber data. The goal was to put “security agents” on each offshore machine to ensure that users were adhering with the *organization's* (and HIPAA's) compliance policy and guidelines. The *organization* was confident that by placing Digital Guardian “agents” on these user machines, it would provide the necessary security and compliance protection to keep data or information from being downloaded and/or moved to offline media.
3. The next driver was the creative and cost-effective way Digital Guardian will address HIPAA compliance with application logging procedures. HIPAA regulations include the requirement to track user activity and report on unusual activity on a proactive basis. Therefore, the *organization's* applications would have to be “enabled” to perform application logging of adds, updates, deletes, etc., and store this data in a centralized place and report on it. The *organization's* alternative was a significantly more costly one: to recode its existing legacy applications, requiring investments in capital (hardware and software), building a centralized service to do logging, and creating a repository to store the logging data and reporting systems. The *organization* interviewees reported that this alternative would be a very complex and expensive solution possibly costing up to \$10 million.

Adding to the complexity of this alternative was the *organization's* “nTier” environment where data moves through a Web Server which moves to an application server and to a CICS gateway and then back to legacy claims mainframe systems. It was difficult for the *organization* to control and determine who had access to secure data and what they were accessing. By implementing logging at the client workstation they knew who the user was and what data they were accessing because the Digital Guardian agent resides on the clients' machines.

Hence, Digital Guardian is being used to help the *organization* meet HIPAA-mandated reporting requirements without recoding its existing applications.

4. And fourth, the *organization* wanted to reduce costs by using an ASP to manage some applications. However, most ASPs did not want to accommodate its strict security measures by altering their environment with multiple performance degrading security tools and negatively impacting their host applications. Instead, the *organization* had the ASP install Digital Guardian agents on their desktops to satisfy its security requirements.

For more information about Verdasys Digital Guardian Solutions, see Exhibit B.

## **The Organization's Costs**

The *organization's* cost experience may have been atypical (higher) because as an early adopter it took the opportunity to collaborate with Verdasys on enhancements in the Digital Guardian product; hence, the *organization* believes it used more pre-implementation resources than a current or future Verdasys customer would incur.

During the implementation of Digital Guardian, the *organization* incurred costs in the following categories:

- Verdasys Digital Guardian license fees (up to 24,000 agents)
- Verdasys support and maintenance (year one)
- Internal staff to plan and deploy — According to the *organization*, the time and effort associated with a Digital Guardian implementation was comparable to deploying software from Sygate or Symantec (which it also uses). With its Digital Guardian deployment, actual time and effort varied with the number of policies and their granularity.
- Implementation tasks totaled one year's worth of effort of four individuals (one full-time employee total effort), and these tasks included: building the Digital Guardian server, deployment of agents to end users' clients overnight using BMC Software's Marimba tool, lab testing, costs associated with the distribution group that builds software packages, and product/vendor management.

Ongoing annual costs categories associated with Digital Guardian solutions are as follows:

- Verdasys support and maintenance
- Staff (existing) to maintain Digital Guardian, i.e., policy management, reading reports relating to the several hundred existing Digital Guardian seats. (No incremental staff was needed for the current implementation level.)

## **The Organization's Future Plans With Digital Guardian**

During 2005 the *organization* will expand the deployment to 24,000 users. The CISO indicates that it has laid most of the groundwork in its existing deployment to push the Digital Guardian software agents to the remaining 24,000 users. He estimates the incremental cost of software distribution and desktop maintenance to be minimal. Other incremental cost categories include server expansion for 24,000 users, application masking and logging consisting of two days' worth of effort per application for the 10 applications affected.

## **The Organization's Benefits**

The *organization* reported realizing benefits with Verdasys Digital Guardian solution in the following categories.

### **HIPAA Compliance**

Verdasys helped the *organization* meet its HIPAA compliance goals through an information security solution that actively enforces HIPAA policies across an enterprise. The *organization's* CISO is not aware of any other solution that would satisfy the risk of a high-privileged user downloading or transferring sensitive data.

### **Audit Control And Protection**

Verdasys provides the *organization* with a solution for the audit, control, and protection of regulated, proprietary, and sensitive data, at the point of use, across its current deployment (offshore, onshore, and ASP environments), preventing intentional and accidental actions that could put sensitive data at risk. The *organization* is also reducing risk and experiencing savings by installing Digital Guardian agents on the computers of its ASP for the hosting of some applications.

Digital Guardian automates the analysis of risks to sensitive data by tracking all application, file, and network use and flow. Summary and trend reports track the many unmanaged conduits of desktop information loss, such as USB flash drives, CD-ROMs, and tunneled peer-to-peer networks. In one instance, Digital Guardian “caught” an offshore employee downloading data onto a digital camera memory stick in an innocent attempt to bring some extra work home. Digital Guardian can also generate a prompt notice to an employee who is either consciously or inadvertently committing a compliance infraction.

### **Savings From Application Logging Alternatives**

The most significant cost savings was in the area of application logging. The *organization* understood that recoding existing applications to support HIPAA compliance and reporting was both risky and expensive. It estimated that the cost of breaking open the legacy code to add the logging functionality could range from \$100,000 to \$1 million for each of its 10 legacy applications. In addition, a few of these applications are scheduled for retirement in the next few years, so the *organization* avoided investing up to \$1 million in a short-term asset. While saving millions, the *organization* also avoids the risks associated with recoding and recertifying these legacy applications, as well as avoids negatively impacting its business applications. In addition, existing resources can be directed toward more beneficial activities.

The alternative chosen was Digital Guardian, which the *organization* concluded was a very cost-effective alternative for application logging and HIPAA compliance. Digital Guardian will allow the *organization* to limit access to information without breaking open legacy applications and reworking the code.

## **The Organization's Risks And Risk Mitigation Strategies**

There are two aspects of risk and risk mitigation discussed in this study, project and business risk:

### **Project Risk And Mitigation**

The risks associated with IT projects in general and specific risks cited by the *organization* related to Digital Guardian solutions.

At the time of its investment in Digital Guardian, the *organization* knew Verdasys did not have a portfolio of companies experienced in using the solution. As an early adopter, the *organization's* risk mitigation strategy was to take a more deliberate, "hands-on" approach to the product selection decision and implementation. The *organization* wanted to completely understand Digital Guardian's features, functionality and planned future enhancements, and to establish a close partnership relationship with Verdasys' employees. A large organization with the technical abilities of the *organization* could afford to assume the risk of a relatively new vendor and its product. A year later, the *organization's* Chief Information Security Officer reports that he and his staff are impressed by the technical and business people at Verdasys. The Digital Guardian solution was delivered as promised, and continues to meet and in some cases exceed the *organization's* expectations.

### **Business Risk And Mitigation**

The *organization* invested in Digital Guardian solutions to mitigate the risks associated with non-compliance to government regulations, primarily HIPAA and secondarily Sarbanes Oxley. The *organization* does not associate ROI with security solutions, but rather views these products as risk mitigation and risk avoidance tools used to ensure sensitive information is protected and regulation compliance is ensured.

In investing in Digital Guardian solutions, the *organization's* primary objectives related to business risk mitigation in the following areas:

- Maintain the *organization's* "public" reputation for excellent overall business controls.
- Ensure compliance with HIPAA privacy and security directives and reporting requirements.
- To understand compliance levels and policy enforcement for its high-privileged users, both healthcare (HIPAA) and financial (Sarbanes-Oxley).
- Provide security solutions for offshore development centers and third-party ASPs.

With the benefit of hindsight, the *organization* believes that its investment in Verdasys Digital Guardian solutions carried a relatively low level of risk for the *organization* when compared to alternative solutions such as changing the legacy code of its mission-critical applications.

## The Organization’s Flexibility Options

Flexibility, as defined by Forrester’s TEI methodology, represents investing in additional capacity or agility today that can be turned into business benefits later, at some additional cost. The *organization* believes that its initial investment in Verdasys solutions has created the “option” to use the flexibility of the Digital Guardian “agent” to perform other security functions such as file encryption, application data redaction, and data visualization. Digital Guardian may provide the following future benefits to the *organization*:

- Support the goal of reducing the amount of software deployed at the *organization*.
- Reduces costs associated with the redundancy and complexity of a multi-product/vendor security environment.
- Avoid the costs associated with testing, deploying, and upgrading of multiple agents. The Digital Guardian agent is already approved from the standpoint of the network.
- Supports the *organization*’s goal of making security robust but non-intrusive to the users. The *organization* knows that multiple agents can negatively impact desktops and the productivity of people working on them.

Additional future flexibility options that the *organization* attributes to Digital Guardian include the ability to expand its business process outsourcing initiatives, move work to other more cost-effective locations, and exposing more applications to third parties, all with the same level of confidence that they have with their own internal security.

## Financial Analysis — The Organization

The table below (repeated from the Executive Summary) represents a summary of the savings that the organization expects to achieve during the next three years by using Verdasys’ Digital Guardian solutions compared to alternative application logging solutions.

**Table 1: Estimated Three-Year Costs And Savings, Net Present Value (NPV), To The Organization**

Summary financial results	Amount
Total three-year cost savings (NPV)	\$5,455,000
Total three-year costs (NPV)	\$1,771,000
Total three-year net cost savings (NPV)	\$3,684,000
Payback period	two months

Source: Forrester Research, Inc.

## Study Conclusions

Based on our in-depth discussions with the *organization*, Forrester and the *organization* estimate the NPV of its three-year savings will be \$3,684,000 based on using Verdasys Digital Guardian solutions instead of incurring the extensive costs of recoding existing legacy applications to support HIPAA compliance and reporting.

Although not quantified for this study, the *organization* outlined additional benefits in the following areas:

- **HIPAA compliance:** Verdasys helped the *organization* meet its HIPAA compliance goals through an information security solution that actively enforces HIPAA policies across an enterprise.
- **Audit control and prevention:** Verdasys provides the *organization* with a solution for the audit, control, and protection of regulated, proprietary, and sensitive data at the point of use, across its current deployment (offshore, onshore and ASP environments), preventing intentional and accidental actions that could put sensitive data at risk.
- **Future flexibility options:** Digital Guardian may provide the following future benefits to the *organization*:
  - Support the goal of reducing the amount of software deployed.
  - Reduce costs associated with the redundancy and complexity of a multi-product/vendor security environment.
  - Avoid the costs associated with testing, deploying, and upgrading of multiple agents. The Digital Guardian agent is already approved from the standpoint of the network.
  - Supports the *organization's* goal of making security robust but non-intrusive to the users. The *organization* knows that multiple agents can negatively impact desktops and the productivity of people working on them.

For the *organization*, using Verdasys products carries a relatively low level of risk when compared to alternative solutions described above, and positive and immediate net benefits in the amount of \$3,684,000.

## **Appendix A: Total Economic Impact™ Overview**

Total Economic Impact™ is a methodology developed by Forrester Research, Inc. that enhances an organization's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI™ methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

The TEI methodology consists of four components to evaluate investment value: benefits, cost, flexibility, and risk.

### **Benefits**

Benefits represent the *value* delivered to the user-organization – IT and/or business units – by the proposed product or project. Oftentimes product or project justification exercises focus just on IT cost and cost reduction, leaving little room for analysis of the impact of the technology to the entire organization. The TEI methodology and resulting financial model places equal weight of the measure of benefits to that of costs, allowing for a full examination of the impact of the technology on the entire organization. Calculation of benefit estimates involves a clear dialogue between the user-organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

### **Cost**

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs. These may be in the form of fully burdened labor, subcontractors or materials. Costs consider all the investment and expenses necessary to deliver the value proposed. In addition, the cost category within TEI captures the any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

### **Flexibility**

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point in time. However, having the ability to capture that benefit has a present value that can be estimated. The flexibility component of TEI captures that value using real options.

### **Risk**

Risk is the fourth component of the TEI methodology. Risk is a measurement of the uncertainty to benefit and cost estimates contained within the investment. Uncertainty is measured two ways: the likelihood that the cost and benefit estimates will meet the original projections as well as the likelihood that the estimates will be measured and tracked over time.

TEI applies a probability density function known as “triangular distribution” to the values entered. At minimum, three values are calculated to estimate the underlying range around each cost and benefit estimate. The expected value — the mean of the distribution — is used as the risk-adjusted cost or benefit number. The risk-adjusted costs and benefits are then summed to yield a complete risk-adjusted summary and ROI.

## **Appendix B: Verdasys Digital Guardian Solutions**

### **Overview — About Verdasys**

According to Verdasys, its information security solutions provide the executive-level visibility and control needed to:

- **Protect intellectual property**, such as patentable inventions, trade secrets, source code or lab results, from theft and unauthorized distribution.
- **Meet the expectations of customers and business partners** who have entrusted a company with sensitive information.
- **Enable compliance with regulations**, such as HIPAA and the Gramm-Leach Bliley Act (GLBA), by maintaining a higher level of data protection.
- **Provide financial auditors and regulators** with documentation proving the veracity of company financials.

Verdasys' patent-pending technology enables companies to understand risks to their data, monitor the use of files, and prevent unauthorized actions that can put information in jeopardy.

### **Overview — About Verdasys Healthcare Solutions**

According to Verdasys, Digital Guardian solutions can help insurers and healthcare providers address the information security challenge through a comprehensive platform that brings new safeguards to regulated and proprietary information in complex environments. Through real-time control over access to sensitive data across all desktops, laptops, and servers, organizations can prevent intentional and accidental actions that could put information at risk.

#### **Facilitating Enterprisewide Compliance**

Today's organizations face the task of bringing their applications, business processes, and corporate culture into line with federal legislation such as HIPAA and the GLBA, as well as state regulatory requirements. Verdasys helps companies avoid potentially costly violations or embarrassing public disclosures of policy violations, and just as importantly, maintain the trust of their customer base.

With the Verdasys solution, organizations can take a proactive approach to compliance by activating their security policies on the computer of every employee. According to Verdasys, a Digital Guardian solution makes it possible for insurers and healthcare organizations to:

- Enforce corporate compliance policies across the organization, from headquarters to satellite offices.
- Monitor all access to regulated information and prevent unauthorized access.
- Warn users when activities violate policies or prompt for business justification before allowing them to proceed with risky actions.

- Block unacceptable activities, such as pasting patient data into an email or burning customer details onto a CD-ROM.
- Customize policies on an office-by-office basis to meet the varying regulations of different states.
- Continually educate employees on compliance policies by explaining why activities were blocked.

### **Application Remediation**

Recoding existing applications to support compliance requirements can be both risky and expensive. Easily integrated with legacy, client/server, and thin client Web-based services alike, the Verdasys solution helps companies:

- Eliminate the need to “break open” and recode fragile applications.
- Maintain business continuity by ensuring application availability.
- Prevent the introduction of new security holes caused by recoding efforts.

### **Streamlined Reporting**

Regulatory directives require companies to compile and maintain extensive logs regarding access to certain data. With Verdasys, companies can reduce the cost and simplify the chore of ongoing compliance reporting through the ability to:

- Track all file and application access and attempted access, as well as storage and network activity.
- Provide definitive documentation of enterprisewide information usage through executive summaries and fine-grained reports.

### **Enabling Secure Outsourcing**

To keep new and existing customers satisfied, insurance companies and healthcare providers are driven to implement new and improved IT applications that help them maintain lower prices and provide better service than the competition. To keep costs down, many organizations are outsourcing IT development or hosting key applications with external providers.

According to Verdasys, Digital Guardian solutions can help organizations keep both regulated data and proprietary source code safe in offsite environments. By implementing the Verdasys solution on their partners’ computers, organizations can:

- Prevent access to confidential customer information that flows through hosted applications.
- Ensure that source code is not copied and distributed to third parties or leveraged for use with the partner’s other customers.
- Control which partner employees have access to data or applications.
- Remotely block select user actions that could jeopardize the security of information.