

Strategic Risk Management and Compliance Program

In 2005, one of the largest US health insurance providers undertook a seemingly impossible task. Concurrently, they sought to:

- Drive down data risk
- Meet PHI regulatory compliance
- Decrease the number of point products deployed
- Reduce administrative costs

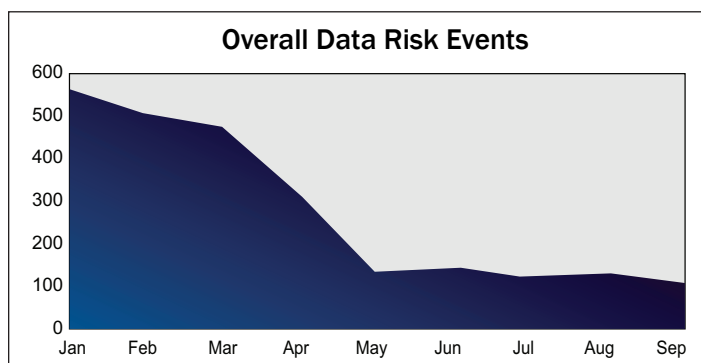
And accomplish this with minimal operating impact to the business. The results exceeded all expectations, thanks to a solid mix of technology and integrated business and security processes. The initiative went on to solve unforeseen risks and meet emerging security threats. Results included:

- 82% drop in risky user behavior after 6 months
- Operational staff requirements reduced from 12 to 3 FTEs
- Average annual return on investment of 92x

The overwhelmingly positive outcome was the result of excellent program management and creative thinking by a mixed business and security team, with the cornerstone of the program being Verdasys Digital Guardian.

A New Approach to Data Security

What began as a DLP compliance initiative to resolve a HIPAA audit weakness ended as an entirely new, comprehensive data security strategy. The compliance weakness was found in the way the company's 10,000 home-based customer service workers interacted with sensitive personal healthcare information (PHI). These workers required the ability to access and email sensitive customer PHI in order to complete required business tasks. The remote nature of these workers represented a significant cost savings to the company which provided a unique competitive advantage. At the same time, that advantage introduced significant risk of PHI data loss which became apparent during an internal audit.



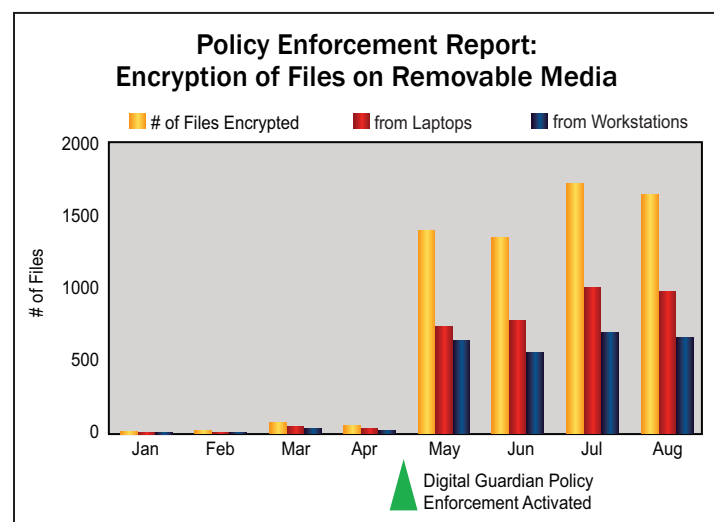
Deployment Snapshot

- Heavy regulatory PII/PHI requirements
- HIPAA Compliance
- Extensive network of outsourced and affiliate providers
- 40K systems protected
- 82% risk reduction
- 92x average yearly ROI

The audit results concluded that the home workforce required special monitoring and controls around protecting PHI that was accessed and processed outside the corporate network. Home users would only be able to access PHI after they had connected to the corporate network through a prescribed VPN, and that no alternative means could be opened to transfer data or files including FTP or Web environments. Requirements also mandated that every action involving PHI would be monitored and controlled in a risk appropriate fashion.

Digital Guardian Flexibility Became Key

Digital Guardian's unique and highly flexible architecture proved to be the ideal solution for controlling the flow of sensitive customer information beyond the corporate network and enable the company to utilize its cost saving home workforce. Digital Guardian's ability to offer holistic visibility and control on the end point enabled the security team to create policies that enforced all of the controls required by the audit finding. But the organization would be shocked when they learned how much more it would accomplish.



Digital Guardian Flexibility Delivers Comprehensive Data Security Use Case Coverage

Through its flexible and fully integrated platform, Digital Guardian mitigated risks related to a wide variety of data security related use cases including:

PII & PHI Data Management and Compliance: Risk based automated controls and reporting for all compliance related data

Remote PC Connection Control: Ensure home/mobile internet connections are on a single network, eliminating dual homing and providing safer operating environments

Malware Protection: Alert security to and block downloads of extensions from firing or being copied including; exe, bat, cmd, vbs, and more from the Internet, USB devices and other removable media

VPN Usage Enforcement: Security controls require VPN activation before any internet browser or data transfer can occur forcing all remote data movement through the corporate security infrastructure. Mitigates the risk of internet usage at home and at Wi-Fi hotspots while utilizing existing security investments for greater defense and depth

Actionable Data Classification: Automation of a data risk taxonomy, classifying files and emails in real time based on file context and content (using complex Bayesian analysis and regular expressions)

Email & Webmail Data Management: Risk appropriate controls over webmail content and attachments including justification, encryption and blocking based on risk classification

Data Usage Compliance and Awareness: Just in time end user training, driving voluntary user compliance with information usage policies in real time, saving training costs and mitigating risky behavior

Application Usage Control: Ensure only approved applications and application versions are loaded, report non-compliance, reduce administrative costs and security risks

Building a Unified Approach to Information Protection

Building on the success of the initial deployment to meet home worker security requirements, the organization quickly formed a task force to identify additional data risk vectors across the company. The Digital Guardian Solution offered unprecedented visibility and advanced analytics to help measure known risks as well as identify and measure previously unknown risks. The security team was able to prioritize these risks and offer senior executives real visibility and understanding of what the risks were and how to mitigate them. In most cases, the team utilized Digital Guardian to implement controls to mitigate these risk or employed existing technology investments while using Digital Guardian to measure results. The data security program quickly expanded across the enterprise with Digital Guardian executing policies and implement controls to resolve ten significant data security use cases in the first year. The company continues to rely on Digital Guardian as the cornerstone of its strategic information protection program identify and mitigating new risks as technologies and business environments change.

The Digital Guardian Solution

Through its integrated framework and superior, fifth generation agent, Digital Guardian is the only data security solution that delivers:

- Comprehensive information protection coverage on or off the corporate network
- Real time enterprise-wide visibility into sensitive data location and usage
- Centralized policy definition and enforcement that leverages not only identity and activity, but also data classification, context and content analysis
- Flexible risk appropriate responses to user activities including warning, alerting, blocking and fully automated file, email and full disk encryption
- Proven technology and results, with 50,000+ user deployments, 1 million agents deployed and 5 years of success

Digital Guardian allows your business to put sensitive information to work, while ensuring its usage is governed, controlled and audited. Customers serious about data security choose Verdasys Digital Guardian.

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 worlds 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 01-01-08

Corporate Headquarters

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

WWW.VERDASYS.COM