

Defining a Data Security Program

In late 2005, a senior research scientist at this large manufacturing company left to join a competitor. In doing so, the scientist downloaded over 20,000 sensitive documents from the corporate network, and took at least 150 of those documents with him to his new employer. Once discovered, the data breach was estimated to have cost this company approximately \$400 million. This staggeringly high number illustrates the magnitude of the consequences for loss of sensitive intellectual property, and set off an initiative to introduce risk management measures to guard against an incident of this kind happening again. Critical success factors to this initiative included:

- Safeguarding critical research, engineering and manufacturing IP, whether residing in files or application databases
- Enabling secure collaboration with third party scientists, manufacturers and other business partners
- Enabling secure and streamlined communications with remote offshore manufacturing locations

The project, initially conceived as a response to a single incident and threat vector, grew to take a holistic look at data security throughout the value chain, from research and development through engineering and on to manufacturing, including sourcing and distribution. One unifying element across the organizational value chain is the use of IP libraries as a content repository. These libraries housed research records, formulas and specifications, results of trials and experiments, and would serve as the primary content repository to standardize the classification model. In effect, it was the organization's secret sauce – precisely the type of critical information that was breached. The company's competitive edge depended on ready access to this information to drive efficiency and collaboration. Due to the sheer scale and complexity of the company's operations, any slowdown of the product development lifecycle would be unacceptable. This organization was not willing to sacrifice operational efficiency for security – they absolutely needed both.

Solution Deployment

- Enterprise Deployment across 50,000 Internal Systems
- External Deployment across 7,000 Partner Systems
- Trust Verification Agents

Use Cases

- IP Protection
- Secure Outsourcing

Company Snapshot

- \$30 billion manufacturing and consumer goods company
- Workforce of 60,000
- Public data breach cost \$400 million
- Global manufacturing in India, China, Europe, and the Americas
- Reliance on third party scientists requires IP to sit outside corporate network

Comprehensive Protection across Internal and External Processes

Critical and sensitive IP flow across all points of the organization's value chain, from suppliers to manufacturing to distribution. With internal operations, research and development data is utilized by engineering and the resulting engineering data is delivered to and utilized by manufacturing. Within each step of these processes, data is being shared externally with third party scientists and engineers, further complicating the task of keeping sensitive information secure. As such, any potential risk management strategy needed to extend outside of the corporate walls and beyond the network perimeter. With so much sensitive data flowing throughout the value chain, achieving that balance of operational efficiency and information security would at first seem quite a daunting task. To achieve this balance the company needed to:

- Protect IP sourced in secure repositories and flowing through complex, internal and external communication channels
- Classify data in real-time based on content and context, and apply it to the organizational data risk taxonomy
- Centrally administer organizational data security policy, allowing for risk appropriate action (e.g. blocking, warning, encryption, logging) based on classification of incident
- Secure sensitive IP whether it resides on or off the corporate network
- Create of virtual communities of trust, that allow for free and efficient collaboration between secured parties
- Maximize operational efficiency while introducing a previously unachievable level of data security

Start with Secure Offshore Outsourcing

A new initiative to work with design partners in Taiwan was utilized for the pilot program of Verdasys Digital Guardian. The corporation was extremely worried about potential overseas IP loss, and views “trusted” external parties as a high risk egress point for confidential data. In less than two months, the team built out a full pilot deployment to safeguard corporate intellectual property. The organization deployed Digital Guardian on 25 partner workstations in the offshore facility. IP was only to be accessed or transmitted on these machines, thereby creating a secure virtual perimeter.

Taking full stock of operating environments and potential risk factors, the group crafted and through Digital Guardian made actionable risk aware information usage policies and secondary controls. Information was only allowed to reside on the 25 secured workstations, and those workstations did not have the authority or ability to transmit IP to any machine in Taiwan without a Digital Guardian Agent, and were only permitted to send information back to machines in the US corporate headquarters also secured by a Digital Guardian Agent. This created a virtual community of trust, and contained information by governing its use at the endpoint. Aggressive policies regarding device control (USB drives) and printing of confidential IP were also deployed.

Enterprise Deployment

Building on the success of their Taiwanese pilot, the team expanded their usage of Digital Guardian to 5,000 workstations in the US and China across five divisions. This expansion represented a move to safeguard IP on a global scale across three countries. The team utilized Digital Guardian’s powerful data discover capabilities and deployed the desktops in stealth monitoring mode to gain an accurate understanding of data flows within their organization.

They then monitored and logged potentially risky actions (e.g. FTP to an outside destination) over a one month period to facilitate a detailed risk analysis.

The team worked with corporate security officers to utilize the results of the risk assessment to craft a series of risk aware data security policies. The new policies made heavy use of content and contextual analysis to classify confidential data in real time, and based on that classification take risk appropriate actions. The result was a realization of the company’s dual objectives – secure data interchange with minimal end user interruption and maximum operational efficiency.

Based on the success achieved through this expanded deployment, the organization rolled out Digital Guardian enterprise wide, and today safeguards data on over 40,000 internal workstations and 4,000 partner machines. The manufacturer is currently reaping the benefits of vastly safer operations, greater data security awareness and improved collaboration from design to manufacturing.

The Digital Guardian Solution

Digital Guardian, through its integrated framework and multifunction agent, is the only data security solution that delivers:

- Real-time and background multi-function scanning and data classification of sensitive data on laptops, desktops and servers across the extended enterprise
- Enterprise-wide visibility into sensitive data location and usage
- Policy enforcement that leverages not only identity and activity, but also data classification, context and content analysis
- Risk appropriate responses to user activities including policy driven warnings, blocking and alerting, as well as automated file and email encryption

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

“Our Intellectual Property is our company and Digital Guardian, through its extremely flexible and effective security policies, forms the foundation of our data security program to protect it.”

Chief Information, Security Officer

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