

Defining a Data Security Program

In 2007, this top five global technology company recognized a significant and growing threat to their corporation. Their Chinese and Indian labs, started several years ago, had grown to become successful and strategic components of their global operations. As that strategic importance grew, so did the amount of critical corporate IP flowing overseas to countries known for weak IP protection laws. Offshore software architects received requirements documents from onshore analysts. The offshore architects in China would work with both US and offshore development leads in China to develop sensitive functional specifications, which would be shared with quality assurance personnel in Indian QA labs, who would share test plans they'd develop with partners in Russian labs. To compound matters, peer to peer file sharing and other rogue applications ran rampant on the company's local offshore networks, representing data breach risk and wasted network bandwidth. To address both issues, the company implemented an offshore information risk management initiative with the primary objectives of:

- Enhancing data security's reach to a global footprint to protect sensitive IP in a risky area of the world where opportunities abound
- Assessing risk and controlling the threat vector presented by peer to peer and other rogue applications
- Establishing lines of trusted communication between remote labs and corporate headquarters

The strategic aim was to enable secure growth into a critically important, yet highly risky environment. The Chinese and Indian markets hold huge promise of lower cost hardware and software development for many companies. Design, development and quality assurance costs are inherently lower, but quality of output can suffer if the proper information is not shared efficiently and freely. But this is not without risks, especially in China, where a lack of traditional notions of ownership of IP is compounded by tacit approval of IP compromise by the government, leaving little legal recourse for a company that suffers a loss. With the stakes so high, this company needed a comprehensive data security strategy.

Solution Use Cases

- IP Protection and Privileged User Management
- Multi-tiered Classification
- Context and Content Analysis
- Application Management and Blacklisting
- Software License Compliance

Company Snapshot

- Top five global technology company
- Workforce of over 50,000
- Rapidly growing offshore labs with 1,800+ employees
- Global operations relies on shared ownership of sensitive design and other IP
- IP protection in India and China is one of several federated deployments of Digital Guardian at this customer

Deploying a Data Security Program

The software company started by assessing their critical data. The result was a data risk classification taxonomy. They broke sensitive data into three tiers – internal (e.g. meeting notes), confidential (e.g. quality test plans) and strictly confidential (e.g. product roadmap documents, source code, chip specifications). The team inventoried network storage locations and developed a context classification scheme based on the location of the data being accessed. Highly sensitive source code repositories, for example, warranted a higher risk score than the employee directory. They prescribed a set of risk appropriate controls for each classification of data. This risk optimized taxonomy allowed the organization to apply the appropriate level of control to each data security. Critical to the success of the program included:

- The ability to securing organizational data assets by monitoring file related activity on the laptops of all 1,500+ offshore employees
- Classifying data in real-time based on content and context, and apply it to the organizational data risk taxonomy
- Enabling central administration of organizational data security policy, allowing for risk appropriate action (e.g. blocking, warning, logging) based on classification of incident
- Enabling content inspection of critical files in multiple languages, including English, Hindi and Chinese
- Establishing a comprehensive data security approach that deals with multiple threat vectors, including rogue applications and peer to peer software

The challenge would be in demonstrating that to the enormous organization.

A Comprehensive Enterprise Platform

The team recognized the need to do careful monitoring and to define escalation workflow for identified infractions in a unified fashion across three continents. They specified a set of reporting requirements that would allow the team to monitor the state of data security according to their data taxonomy. This allowed the team to track specific events according to risk level, and to act upon them appropriately. The process is therefore continuous, and provides the ability to stay ahead of new and unknown threats. The team also recognized that this process could not be achieved without investing in a data security technology platform that would become its foundation, being able to meet all critical program requirements, scale to the global enterprise and be flexible enough to meet new and unknown threats in the future.

Rather than implement a host of disparate point solutions, the team decided they required a single management platform. The risk level in this new environment was too high to rely on disjointed and siloed reporting and workflow mechanisms. The company was already a corporate user of Verdasys Digital Guardian, and were pleased to learn that their existing technology solution would satisfy all of the new requirements introduced by this new project.

Deployment and Program Rollout

The Digital Guardian solution was initially deployed to 5% of the desktops, laptops and workstations used to support their Chinese technology development operations. This early deployment enabled the data security team to begin monitoring the flow and usage of data across all of the newly protected end points. This provided the team with significant insight into the flow of confidential data throughout their organization, and provided them with valuable intelligence to use to refine their IP protection plan. Thus, they were already realizing their vision of a continuous improvement model. This deployment model was then repeated for the development center in India with the same successful results.

After existing security policies were updated, agents were deployed to the remaining 95% of hosts in both locations. The team used the monitoring and logging capabilities of Digital Guardian to compile valuable intelligence on sensitive data usage patterns, and then to easily roll-up reporting according to risk levels. They utilized this aggregate reporting in executive presentations, and as a result were able to easily make the business case to begin to utilize additional risk-appropriate controls such as warning, blocking and/or requiring justification for high risk activities.

Once the additional risk-appropriate controls were put into place, they served to increase end-user accountability, and as a result training and behavioral influence was pushed in real-time to users as data processing activities occurred. The outcome was a real and tangible reduction in risky activity, that is easily reported on in an on-demand fashion using the Digital Guardian Management Console.

The Digital Guardian Solution

Digital Guardian, through its integrated framework and multi-function 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.

“Verdasys’ solution is uniquely able to handle our global environment including distributed data security controls in 4 countries and in three languages.”

Director, Information Security

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