World's Leading Engineering Design Automation (EDA) Firm Protects Intellectual Property with Information Security Enforcer

A leading Engineering Design Automation (EDA) firm headquartered in San Jose, California and with multiple world-wide locations, experienced serious incidents of intellectual property leakage outside of the company. The company creates large amount of confidential intellectual property including Design Documents, Design Schematics, Source Code, Product Specifications and other proprietary technical information for its marquee clients in the hi-tech space. The company is contractually and legally required to provide appropriate safeguards against any violation of its clients' intellectual property. As such the company needed to implement strong vigilance over the use, sharing, transfer and communication of any intellectual property related data and information within and outside of the company. Since the intellectual property is created and shared between multiple sites (the company has 17 sites around the globe), it is critical for the company to differentiate between permissible/authorized versus impermissible/unauthorized sharing and/or disclosure of intellectual property related information across the company and its outside partners.

The company needed to be able to enforce stringent controls on access to proprietary intellectual property information within their own infrastructure as well as during the transfer and sharing of this information with outside partners via web collaboration tools over multiple protocols.

Industry's "First and Only" Malicious DLP solution protects intellectual property from Accidental & Malicious leakage in "Real-time" – monitors large scale network, myriad of applications and data repositories.

Furthermore, the company's large corpus of intellectual property offers a large Attack Surface and as such is a prime potential target for Data Exfiltration attacks via APTs (Advanced Persistent Threats). Thus, the company needed a robust high fidelity solution for protection against Insider Malicious Data Leak (Industrial Espionage) as well as targeted Data Exfiltration Attacks (via APTs).

The company required advanced DLP features to obviate Manual Processing of Data and Manual Definition of Policies so that human errors and any malicious intent can be eliminated. The ability to Automatically Identify, Classify, and enforce Access Control and Policy in Real-time on a large evolving corpus without performance degradation was mandatory requirement.

Industry:
Hi-Technology

Product Key Capabilities:

- 4th Generation Sophisticated DLP Features
- Auto-Identification & Classification of Data
- Automated Policy Synthesis
- Identity & Role based Data Leak Prevention
- Real-time GRC Enforcement
- Malicious Data Leak Prevention

Key Benefits

- Accurate Identification and Classification of confidential information
- Ubiquitous protection – enables DLP throughout the enterprise and the cloud rather than a few select documents
- Rapid deployment – lowers the cost and administrative burdens for compliance
- Reduced TCO – eliminates the cost due to hundreds and thousands of hours of manual tagging of documents
- Real-time enforcement – immediate "actionable" information and remediation, reduced compliance overhead burden
- Detailed Reports and Forensic Analytics on Incidents and Violations

Why GhangorCloud?

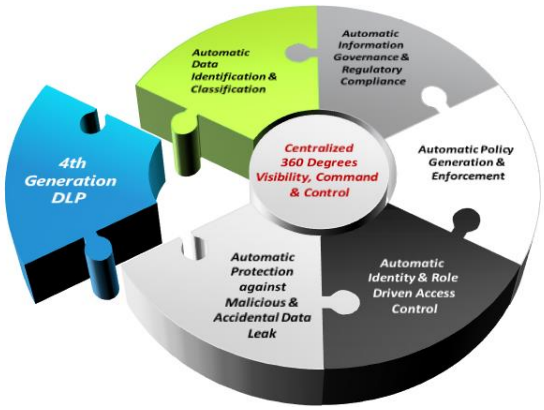
- High Efficacy against Malicious & Accidental Data Leak
- Accuracy and Reliability of DLP
- Easy Deployment and Lower TCO
- B2B Data Leak Prevention

GhangorCloud Information Security Enforcer for Intellectual Property Protection:

The company had previously deployed a leading 3rd Generation DLP solution. However, it was conclusively determined that the 3rd Generation DLP solution was mostly ineffective and had grossly failed to detect Data Leaks resulting in serious compromise of important intellectual property.

The key reasons why the company selected GhangorCloud's 4th Generation DLP solution (Information Security Enforcer) to *REPLACE* the previously deployed DLP solution were as follows;

GhangorCloud Solution Key Features



Automatic Classification of Sensitive Data: GhangorCloud's DLP solution completely eliminates any manual interference in the identification and classification of sensitive data. It provided the company the ability to Automatically Identify and Classify sensitive intellectual property information (both structured and unstructured) without any manual tagging or pre-processing. Using built-in auto-classification tools, ontologies can be created to support identification and control of customer specific proprietary intellectual property information. Furthermore, out-of-the-box pre-built ontologies (for PCI, PII and HR) enabled the company to enforce other regulatory and compliance requirements.

Automatic Generation of Policy: GhangorCloud's DLP solution completely eliminates any manual intervention in the Policy Synthesis process. It provided the company the ability to Automatically Synthesize Policies hence eliminating the chances of incorrect policies due to human error and malicious intent. Based on company's business logic and classification of critical information, the Information Security Enforcer automatically synthesizes and applies correct policies to all critical information transmissions.

Advanced Role-based Access Control: GhangorCloud's DLP solution Automatically Enforces Segmentation of Duty principles to drive a highly granular access control scheme for bi-directional checking of information access. Using the company's business logic to determine who should have access to what, it enabled the company to set sophisticated Access Control at multiple levels of granularity from documents to individual words.

Real-time Detection and Control of Exfiltration Attempts: GhangorCloud's DLP solution identifies and prevents data leaks in real time. It correlates Actors-Operations-Information to discriminate between legitimate communications versus misuse of the company's intellectual property.

Built-in Workflow and Forensic Analysis: GhangorCLoud's DLP solution provided the company a real-time dashboard for its IT Staff and Information Security personnel to control and monitor compliance and DLP enforcement. It captures and retains all relevant information about each security incident including: source, destination, transmission method and specific content which triggered the incident.

How to get started:

GhangorCloud understands that every enterprise has its own unique data security needs. GhangorCloud's team of Data Loss Prevention experts and its Value-Added Distributors will work with you to understand your unique data security requirements and priorities.

Please contact GhangorCloud to get started: email info@GhangorCloud.com.