Major National Security Agency Protects Sensitive Data with GhangorCloud Information Security Enforcer (ISE)

GhangorCloud's customer, a modern sophisticated National Security Agency in a leading South East Asian country has recently commissioned a state of the art National Cyber Coordination & Command Center – herein referred to as "The Cyber Security Agency (CSA)". The primary objective of the CSA is to provide a high fidelity means for real-time monitoring and surveillance of the key high security Cyber Infrastructure. The CSA is designed to closely monitor all electronic communication, electronic exchange and transfer of sensitive documents and information of high national security value, and to monitor the cyber behavior of government employees, agents, contractors, partners, etc. The CSA is located in a custom built high security building and incorporates a centralized Command & Control Situation Room.

The CSA needed "cutting-edge" data leak prevention mechanisms to safeguard sensitive national security information, financial transaction information and other confidential mission critical information. The CSA deployed GhangorCloud's Information Security & Compliance (ISE) line of product to "Automatically" identify, protect and monitor sensitive information/data, block unauthorized transfers and/or downloads of sensitive information (including PCI, PII data, national security related information, secret military & intelligence communications, government communique, and other secret information), and to enforce a sophisticated workflow for monitoring and delegating decision making authorities to different actors and elements.

4th Generation Information Security & Compliance solution monitors "National Cyber Coordination & Command Center", myriad of applications and data repositories, and protects important data in "Real-time".

The CSA is a prime target for Data Exfiltration Cyber Attacks and hence posed several key requirements from a DLP solution including (a) Real-time Centralized Command & Control ability to accurately detect and pre-emptively block any violation of sensitive data, (b) Automated Identification & Classification of mission critical data "without human intervention", (c) Automated Policy Synthesis without "human intervention", (d) Advanced Access Control for confidential data & information, and (e) Real-time Enforcement of all Policy Settings.

The CSA also required a very high efficacy index against "Malicious Data Leak Scenarios" and a "robust ability" to perform surveillance against Advanced Persistent Threat (APT) based Data Exfiltration Cyber Attacks.

Industry:
National Security & Defense

Product – Information Security Enforcer (ISE)

- Real-time Cyber Command Control Collaboration & Intelligence – C4I
- Cyber Exfiltration Attack & Data Leak Prevention
- Auto-Identification & Classification of Data
- Automated Policy Synthesis
- Identity & Role based Data Leak Prevention
- Automated Governance & Regulatory Compliance (GRC) Enforcement
- **Malicious Data Leak Prevention**

Key Benefits

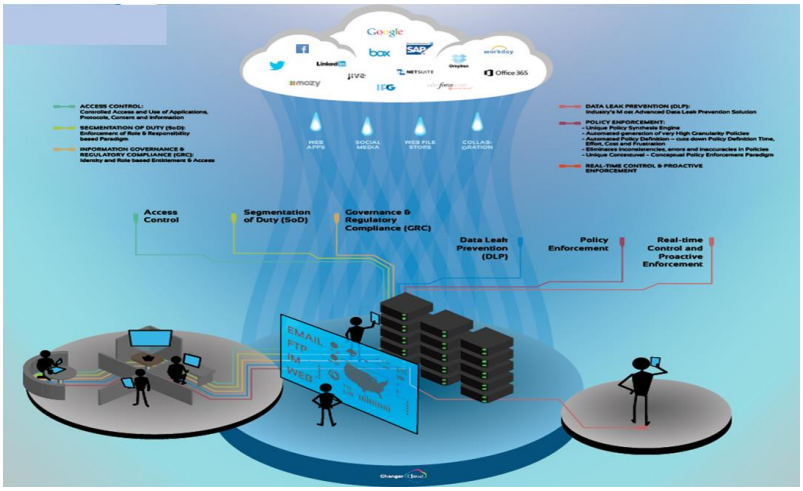
- Military Grade Accuracy and Reliability of DLP
- Protection from APT based Data Exfiltration Attacks
- Accurate Identification & Classification of sensitive Data & Information
- Automated Rapid deployment – lowers the cost and administrative burdens for compliance
- Ubiquitous protection – enables DLP penetration throughout the critical corpus rather than a few select documents
- Real-time enforcement – immediate "actionable" information and remediation, reduced compliance overhead burden
- Detailed Reports and Forensic Analytics on Incidents and Violations

GhangorCloud Information Security Enforcer for Malicious DLP & Data Exfiltration Cyber Security:

The CSA rigorously evaluated several leading 3rd Generation DLP solutions and concluded that the 3rd Generation DLP solutions were mostly ineffective as they failed to meet advanced DLP and Data Exfiltration security requirements. The CSA required the capability to protect against Insider Malicious DLP Attacks as well as External Data Exfiltration Attacks.

The key reasons why the CSA selected GhangorCloud's 4th Generation Malicious Data Leak Prevention solution were as follows;

GhangorCloud 4th Generation Solution – Malicious DLP & Exfiltration Cyber Defense



Centralized Command & Control System: GhangorCloud's ISE solution incorporates robust C4I (Centralized Command Control Collaboration and Intelligence) system that offers "Military Style" centralized command and control over all DLP and Exfiltration Cyber Attack Prevention features. This Centralized Command & Control eliminates possibility of unauthorized or "Malicious" alteration of Data Classification precepts, Policy definitions, Security Profile of Actors or Access Controls by any unscrupulous actor inside the CSA. It also embodies sophisticated Real-time Dashboard that ergonomically presents a cohesive and centralized view of 'State & Status' of Incidents as they are detected in real-time. It provides powerful Analytics capability for real-time correlation as well for detailed Forensic Analysis.

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 CSA the ability to Automatically Identify and Classify sensitive 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 sensitive information. The Ontology driven Auto-Classification helps the CSA eliminate human errors as well as any possibility of "Purposeful Evasion" by unscrupulous actors inside the CSA.

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

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 CSA's operational guidelines to determine who should have access to what, it enabled the CSA to set sophisticated Access Control at multiple levels of granularity.

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 permissible legitimate communications versus Exfiltration of the CSA's sensitive information.

How to get started:

GhangorCloud understands that every security organization 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.