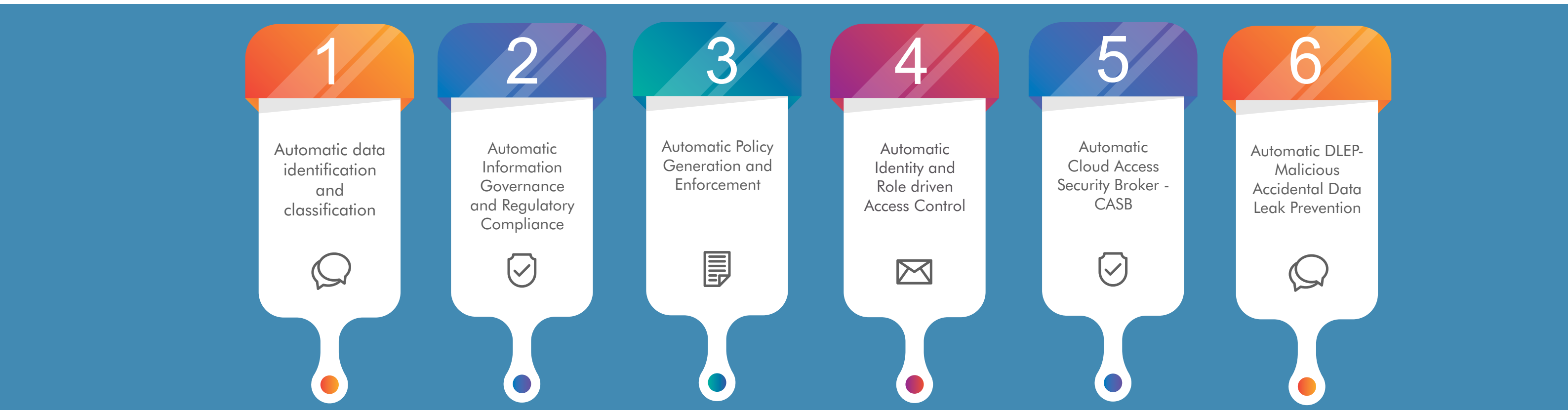
Product Brief

Pioneering the 4th Generation DLEP Accidental and Malicious Data Leak Prevention Platform

Ghangor Cloud

GhangorCloud Information Security Enforcer - Version 3

GhangorCloud's Information Security Enforcer (ISE) is a Fourth Generation Data Leak Prevention (DLP) solution that enables robust security and compliance enforcement against both 'Malicious' and 'Inadvertent' disclosure and/or theft of sensitive and confidential information. The solution could be provided as on-premise, too.



1 Automatic data identification and classification

2 Automatic Information Governance and Regulatory Compliance

3 Automatic Policy Generation and Enforcement

4 Automatic Identity and Role driven Access Control

5 Automatic Cloud Access Security Broker - CASB

6 Automatic DLEP-Malicious Accidental Data Leak Prevention

Auto-Classification of Data & Content

Automatically classifies data in real-time without any manual intervention or manual tagging of data or files. GhangorCloud's unique patented technology protects confidential information, including structured, semi- structured and unstructured data. Automated Identification and Classification of confidential and sensitive data/information is performed - even for newly created "Virgin" data/information.

Automated Policy Synthesis and Enforcement

ISE incorporates GhangorCloud's unique patented Automated Policy Synthesis technology which automatically synthesizes relevant policies, reducing the complexity and cost of laborious and error prone policy definition processes. ISE evaluates the security-based significance of the data/information and invokes the corresponding security policy; preventing data leak and/or extrusion in real-time.

Identity & Role-based Data Leak Prevention Paradigm

ISE delivers a unique Identity and Role-based DLP Paradigm. End-user and employee actions are automatically evaluated and only permitted based upon their authorized roles within the enterprise, enforcing risk- based compliance to corporate policies and procedures.

Cloud Access Security Broker - CASB

ISE performs secure access control for data moving from the enterprise to the cloud. Blocks transfer of sensitive data to web-based applications based on security status of content and actor. Provides detailed reports on exfiltration attempts based on actor, content and intended web destinations.

Advanced Workflow for Monitoring and Policy Enforcement

With intuitive workflow built-in for Security Administrators, Business managers and Employees/End-Users, ISE alerts the relevant parties of suspected violations, allows users to cancel their inadvertent actions, and blocks malicious users from leaking information. All incidents are motored in real-time and logged for compliance reporting. Adaptive Architecture for Enterprise On-Prem, Hybrid Cloud and Public Cloud Deployment

ISE is designed to be flexible and adapt to any deployment topology e.g. on-prem, hybrid cloud or public cloud based architecture. It is deployed on the corporate network between employees and data/information repositories and analyzes real-time data transmissions over any communication channel e.g. Email, Webmail, Web Applications, FTP, I nstant Messaging, etc.

Adaptive Architecture for Enterprise On-Prem, Hybrid Cloud and Public Cloud Deployment

ISE is designed to be flexible and adapt to any deployment topology e.g. on-prem, hybrid cloud or public cloud based architecture. It is deployed on the corporate network between employees and data/information repositories and analyzes real-time data transmissions over any communication channel e.g. Email, Webmail, Web Applications, FTP, I nstant Messaging, etc.

Headquartered in Silicon Valley, GhangorCloud is a leading provider of next-generation Information Security and Compliance solutions.

GhangorCloud, Inc.
2001, Gateway Place
Ste: 710 West Tower
San Jose, CA-95110
United States of America
Main: (408) 713-3303
Technical Support: (408) 713-3303 x105
US Sales: (408) 713-3303 x108

Key Features and Specifications

C4i System - Real-time Centralized Command-Control-Collaboration and Intelligence Dashboard

Key Features	Specifications
Centralized Command Control System	Browser based Centralized Command & Control System, using any browser e.g.Internet Explorer, Google Chrome, Firefox, Mozilla and others
Real-time Incident Monitoring Dashboard	Instantaneous Reporting of any violation in Centralized & Consolidated Dashboard.
Forensic Analysis	Detailed Forensic Analysis Tools, Analysis of preventative measures taken
Incident Reporting & Logging	Extensive set of Predefined Reports, Detailed Reports generated based on a variety of Filters and Criteria
Reporting Formats	Open Formats for export into other reporting systems e.g. Crystal Report, Actuate, Tivoli, SQL based Reporting Tools – Export to PDF, CSV formats
User-Friendly Security Administration	Central Management System interface for the creation, monitoring and management of system configurations, multiple security administrator's accounts, end-user privilege settings

Real-time Governance and Regulatory Compliance Enforcement

GRC based DLP Paradigm	Built-in Segmentation of Duty (SoD) Definition and Enforcement
Identity and Role-based Access Control	Unique 3-D Correlation Technology Correlates three dimensions: "Actors~Operations~Information," in real-time. Performs sophisticated correlation to automatically create an abstraction of enterprise "Organization Structure" and enforce Access Control based on SoD Principles.
Pre-defined Templates for Compliance	PII, PCI DSS, HIPAA, GLBA, SOX, NERC, FISMA, European Union Directive on Data Protection, PDPA, and most United States Data Privacy Laws including SB-1386

Key Features and Specifications

(Continued...)

Key Features	Specifications
User defined Compliance Criteria	Templates can be customized and filters can be defined easily to adapt to new compliance and security needs
Compliance Monitoring	Compliance violations sent as real-time alerts to employees, business managers and security administrators for corrective measures - Incidents are logged in realtime and archived to demonstrate compliance
Auto Classification of Data and Content	
Automated Semantic Analysis based Data Classification	Unique Intelligent Semantic Analysis based Classification system to perform Categorization & Classification without human intervention – No pre-tagging required.
Unstructured Data	Unique Security-based Semantic Analysis of Unstructured data with minimal or no human intervention required. Identify and protect Unstructured Data, such as text, memos, spreadsheets, emails, power-points, documents, images, Intellectual Property, etc. in real-time
Structured Date (regular expression)	High performance Regular Expressions (Reg-Exes) matching algorithms for data such as Credit Cards, Social Security Numbers, Account No., Bar Codes, etc. – Expressions can be combined with wildcards and defined constructs
Pattern Matching & Analysis	Full support of Logical and Pattern-based occurrence analysis methodologies – Goes beyond traditional Statistical or Bayesian methods
Semi-Structured Data	Full keyword & phrase matching capabilities identify known data types

Key Features and Specifications

(Continued...)

Key Features	**Specifications**
Easily Extensible	Customize and extend as new patterns and threats arise without re-deployment
Content Types Monitored and Controlled	Monitors data from databases, file systems, and desktops
Data Types/Format Monitored	Over 48+ content format decoders including Txt, MS-Word, PDF, PPT, XLS, XML, Images, Design Documents, etc.
Automatic Policy Generation	
Automated Security Policy Generation	No Manual Interference or pre-tagging of security policies required – All Policies generated automatically
Automated Security Policy Enforcement & Real-time Reactivity	Automatically evaluates the significance of information and applies the appropriate policies in real-time without human intervention
Highly Granular Policy Settings	Highest level of Policy Granularity – Complex Permutation of Actor-based, Groupbased, Protocol-based, Application-based, Source & Destination-based, Contentbased, etc.
Policy Accuracy	Automatically Identifies and Prevents any Internal Policy Conflicts – No Anomalous Behavior
Policy Syntax	Unique Policy Syntax – Human Readable and Easy to Understand
Real-time Policy Update	Policy updates can be dispatched and enforced instantaneously in Real-time without interruption
Proxies and Key Cloud Applications	
Built-in Proxies	Full Reverse & Forward Proxies – HTTP/HTTPS, SSL, ICAP, SQUID, SMTP, IM, XMPP
Cloud Applications	MS-Exchange, Office-365, BOX, DROPBOX, GoogleDrive, Sharepoint, OneDrive, etc.

Key Features and Specifications

(Continued...)

Key Features	**Specifications**
Enterprise Repositories	Active Directory, LDAP – Full Duplex Mode Synchronization
Protocols and Applications	
Comprehensive Set of Network Protocols	TCP, FTP, HTTP, HTTPS, SSL, SMTP, POP3, *Mail 6073 MS-Web Exchange +773, +7736, RPC-over-HTTP, Instant Messaging IM, XMPP, ICAP, MS-Exchange 2007/2010/2013
Applications Types Monitored and Controlled	Databases, Email, Web-Mail, MS-Exchange, Office-365, BOX, DROPBOX, Google- Drive, etc
Cloud Access Security Brocker - CASB	
Cloud Access Control	Centralized Access Control of Web Applications and Web Services. Detailed reporting on exfiltration attempts to Web Applications and Web Services
Content Aware Security Broker	High Granularity Control of Data & Content Transactions to Web Services and Web Applications based upon sophisticated DLP Criteria
CASB Reports and Analytics	Comprehensive set of CASB Reports and Drilldown Analytics
Deployment Modes	
Enterprise Deployment	On Premise Enterprise Network Deployment
Hybrid Cloud	Hybrid Cloud based Deployment
Public Cloud	Large Scale Public Cloud based Deployment

Headquartered in Silicon Valley, GhangorCloud is a leading provider of next-generation Information Security and Compliance solutions.

GhangorCloud, Inc.
2001, Gateway Place
Ste: 710 West Tower
San Jose, CA-95110
United States of America
Main: (408) 713-3303
Technical Support: (408) 713-3303 x105
US Sales: (408) 713-3303 x108

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by GhangorCloud© and GhangorCloud© disclaims all warranties, whether express or implied, except to the extent GhangorCloud© enters a binding written contract, signed by GhangorCloud©'s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on GhangorCloud©. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in GhangorCloud's internal lab tests.GhangorCloud disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. GhangorCloud reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.