

Introducing the 4th Generation Advanced Data Protection Platform

Information Security Enforcer ISE™



The Gold Standard for Data Protection and Information Security

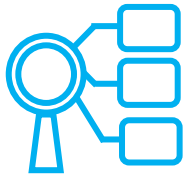
Protect and Control your Enterprise Data

With GC Cybersecurity's Information Security Enforcer (ISE™ v4.0)

ISE™ is the industry's first and only 4th Generation Advanced Data Protection platform that gives you complete control over securing your sensitive information and data assets from malicious or accidental disclosure, theft and/or exfiltration

- 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 Data Leak and Exfiltration Prevention

Real-time, Auto-Classification of Data, Information & Content

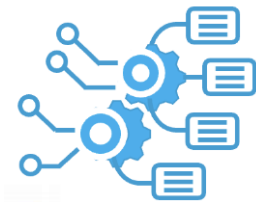


Classify Data

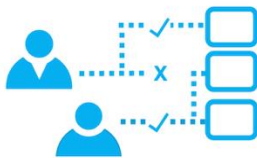
Automatically classify all your data and content at any level of granularity in real-time, without any manual intervention or tagging. GC's patented technology (e.g. Semantic DNA Vector™) classifies structured, unstructured and semi-structured data – even newly created “virgin” confidential and sensitive data & information

Automated Policy Synthesis and Enforcement

Automatically synthesize your policies and enforce them with ISE patented Automated Policy Synthesis Technology which reduces the complexity and cost of laborious and error prone manual policy definition processes. ISE evaluates the security significance of your sensitive data/information, invoking the corresponding security policy to prevent data leaks and/or exfiltration in real-time.



Synthesize Policies



Secure / Control Access

Identity & Role-Based Advanced Data Protection

Control your data at rest and enroute with ISE's role-based data protection paradigm. By defining roles for end-user/employee “actors” and the actions allowed for each role, data actions are automatically evaluated and permitted to enforce security policies and procedures in real-time.

Cloud Access Security Broker - CASB

Secure and control access for data moving from the enterprise to the cloud. Block transfer of sensitive data to web-applications based on security status of content/data or actor. Receive detailed reports on data exfiltration attempts by actor, content and attempted web destinations.



Secure Cloud Access



Monitor Workflows & Enforce Policies

Advanced Workflow Monitoring and Policy Enforcement

Security administrators, business managers and employee end-users receive alerts for suspected access violations with the ability to cancel inadvertent actions or block malicious users from leaking sensitive data and information. In real-time, ISE can notify all relevant parties based on role and log actions for compliance reporting.

Adaptive Architectural Enterprise Deployments

Deploy ISE flexibly in any topology - on-prem, in public clouds or in hybrid cloud architectures. Installed on a corporate network between employees and data and information repositories, ISE analyzes real-time data transmissions over any communication channel including e-mail, webmail, web applications, FTP, instant messaging and other unstructured content communication methods.



Flexible Deployments



Global Command & Control

Centralized Data Protection Command and Control

Control your enterprise and cloud SOC's with ISE's real-time, centralized command and control system modeled after military-grade command and control centers. Monitor data and information being transmitted between actors across global enterprise networks. Automatically block malicious and inadvertent movements of sensitive data by insiders and outsiders, or information maliciously exfiltrated by insiders with silent alerts to notify the proper security and administrative personnel to respond appropriately.

Real-time C4i System 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**Specifications (Cont'd)**

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 (Semantic DNA Vector™) 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**Specifications (Cont'd)**

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

Specifications (Cont'd)

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, GCCybersecurity is a leading provider of next-generation advanced data protection and information security solutions.

GCCybersecurity, 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

Copyright © 2019 GCCybersecurity® Inc. All rights reserved. GCCybersecurity® and certain other marks are registered trademarks of GCCybersecurity®, Inc., and other GCCybersecurity® names herein may also be registered and/or common law trademarks of GCCybersecurity. All other product or company names may be trademarks of their respective owners. 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 GCCybersecurity® and GCCybersecurity® disclaims all warranties, whether express or implied, except to the extent GCCybersecurity® enters a binding written contract, signed by GCCybersecurity®'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 GCCybersecurity®. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in GCCybersecurity's internal lab tests. GCCybersecurity disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. GCCybersecurity 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.