Computing Security
Secure systems, secure data, secure people, secure business

NEWS
OPINION
INDUSTRY
COMMENT
CASE STUDIES
PRODUCT REVIEWS

Information Security Enforcer (ISE^{TM}) from GhangorCloud

Editorial: Review. **Date:** 2016-11-01. **Views:** 2632. **PDF Version:**
Tags: Networking, Cloud, Cloud-based Security, Security, Data Leakage, Data Loss Prevention, GhangorCloud, Information Security Enforcer

It's generally accepted that first lines of defence such as firewalls do not prevent data exfiltration

Effective DLP has realistically been beyond reach because of a dependence on manually created policies and categorisation. GhangorCloud has now tackled this head-on by creating a next generation platform, the Information Security Enforcer (ISE), that enhances visibility and data exfiltration control.

ISE, a Data Leak Protection platform, operates in real-time with no need for manual tagging and policy creation. It additionally provides automated Governance and Compliance services, taking data protection out of the silo.

ISE builds on four core functions: the Semantic (topical and security) classification of data; Policy Automation reducing administration overhead and, eventually, false positives to zero; content control by Segmentation of Duty using the identity and role of the Actor - a person, machine or process - and lastly, Compliance enforcement to actively prevent data violations using industry regulation or local policy once data movement is detected.

We logged into our ISE appliance as Super Administrator with full access. Security Administrator or Security Manager logins provide subset functionality.

The Security Operations-style dashboard offers Dashboard, Reports, Actor Administration, Policy, Classification and System services. Underneath, unpopulated graphs show Extrusion (data leak) incidents, the incident rate and a pie chart showing severity. The Extrusion graph shows incidents per protocol monitored - FTP, Email, Web Services, IM, Exchange, etc. - while other grids detail Extrude resources, top Extrusion sources (Actors) and Most Recent Events.

We added our AD/LDAP server to the Server Directory on the System tab. There may be multiple ISE servers in a distributed Enterprise whose setup is automatically propagated. Our Exchange server and the other protocols that we wished to monitor were also added.

From Global settings we could choose Silent Mode, Journaling and Active mode, which enables incident escalation. For example to block an attachment and refer it to a manager, if required, over two levels.

Computing Security
Secure systems, secure data, secure people, secure business
NEWS
OPINION
INDUSTRY
COMMENT
CASE STUDIES
PRODUCT REVIEWS

Next, Actor Administration and Import from Directory Server quickly populated ISE. We viewed Source (sending) and Destination (receiving) security levels for each Actor alongside their business function and Job title. Security Clearance levels are applied using Guest, Limited, Confidential, Privileged and Absolute. This business logic is part of initial configuration, a service bundled with the license cost. It's extremely granular and delineates precisely the information an individual can send and receive.

With send/receive clearance levels set, a right click on that group rapidly generated Policy rules. To verify this, the Policy Tab presented a grid displaying, by rule, the Actor, Security Clearance, allowable Operations, the direction and associated action. The ability to be specific about Direction (send/receive) is useful. Imagine an employee monitoring an email account who is allowed to read incoming data but not send sensitive data.

A right click on any policy rule produces a 7-field information screen that readily articulates its function. Should there be a false positive the rule can be easily tweaked, and the system will learn and self-correct.

Classification automatically classifies structured and unstructured data using advanced semantic analysis. There are built-in ontologies for vertical compliance requirements which help automatically classify unstructured data. It's language agnostic and neat, and according to GhangorCloud totally unique.

ISE has extensive built-in reporting, including automatic regular reports showing incidents, breach and compliance posture, top incidents, extruded resources by protocol and powerful custom reports.

Data loss is the number one problem for organisations, and it can literally be life threatening. Running this solution in Silent Mode articulates existing problems in detail: in Active Mode the organisation will be protected and can focus on doing business instead of industrial scale production and management of polices and classification. ISE works in real time to detect, prevent, and record data exfiltration. NC

Product: Information Security Enforcer
Supplier: GC Cybersecurity
Web site: www.gccybersecurity.ai
Sales: sales@ghangorcloud.com
Price: Starts at $19,995 USD
Phone: + 1 408 713 3303Tel: +1 408 713 3303

About GC Cybersecurity, (former branded as GhangorCloud)

GC Cybersecurity is an award-winning provider of next-generation Advanced Data Protection solutions. GC Cybersecurity's Information Security Enforcer (ISETM) platform protects data based on its contextual and conceptual significance, using a powerful Deep-AI engine and deterministic security algorithms to automatically identify, classify, and protect large volumes of information in real-time with unprecedented accuracy. The company is founded by Silicon Valley security veterans that include leading authorities from companies like Symantec, McAfee, Trend Micro, Cisco, Juniper, Alteon and Array Networks. For more information see. http://www.gccybersecurity.ai/.

About GC Cybersecurity Inc. https://www.gccybersecurity.ai
Located in Silicon Valley, GC Cybersecurity is a leading provider of advanced data protection solutions.

2001, Gateway Place, 710 West Tower
San Jose, CA-95110 United States of America
Main: (408) 713-3303 Sales: (408) 713-3303 x108