DATA SHEET

KEY CAPABILITIES

Discover
Understand where all the sensitive data of the organization resides that could lead to compromise

Analyze
Evaluate every piece of data being sent out by employees through various channels

Detect
Ascertain and monitor sensitive data that could be sent to unsolicited users outside the organization

Control
Lock down specific channels or activities, in case of any data exfiltration

INFORMATION SECURITY ENFORCER

ENDPOINT SECURITY

ISE ENDPOINT DLP

VERSION 6.0

Designed for medium and large enterprises, GhangorCloud's Endpoint Data Leak Protection offers powerful features in order to control, monitor and enforce Endpoint Security. It is a comprehensive data leak prevention solution designed to control and monitor usage of all portable storage and to keep track of what data users are taking from and to their work computers on any kind of portable storage device.

It enables fast access to controlling computer, devices and user behavior in a large network system. It also offers several ways to track any kind of activity registered on the system. A detailed report including timestamps, file names, action(s) taken, logged user, etc. allows for pin-pointing malicious behavior and malevolent users.

Data security administrators can monitor and report what data is introduced into the corporate network from a portable storage device such as prohibited materials (MP3s, movies or games) or harmful data like a virus that could jeopardize the networks integrity.

GhangorCloud's Endpoint DLP Agent creates an audit trail that shows the use and activity of portable storage devices in corporate networks. Thus, administrators have the ability to trace and track file transfers through endpoints and then use the audit trail as legal evidence for data theft.

GhangorCloud's Endpoint DLP Agent allows authorized use of "Trusted Devices" such as companies' own USB Flash Drives to handle and transfer confidential data. To ensure the protection of data carried by users on "Trusted Devices", it allows users to copy work data to a password protected and encrypted area of a "Trusted Device" only, so that confidential corporate data is protected in case of hardware loss. It supports a wide range of device types which represent key sources of security breaches.

These devices can be authorized which makes it possible for the users to view, create or modify their content and for administrators to view the data transferred to and from the authorized devices, such as removable Storage Devices, Normal USB Flash Drives, U3 and Auto run Drives, Disk on Key, Wireless USB, COM/Serial ports and LPT/Parallel ports.

By controlling the Serial and Parallel ports of a PC using GhangorCloud's Endpoint DLP Agent, the network administrator can deny or allow users access to storage devices connected to these ports.

256 bit AES CBC-mode encryption ensures security for all files exported to USB. Centralized key management allows global control of all content exported to USB devices. Hard drive sector encryption can be added for additional security.

OPERATING SYSTEMS SUPPORT

GhangorCloud's Endpoint DLP supports a wide variety of Operating Systems and Platforms including Windows, Mac OS X, Unix/Linux etc.

KEY BUSINESS BENEFITS

- **Executive Dashboard with Comprehensive Reports**
- **Works Realtime**
- **Warns Proactively**
- **Controls Everywhere (Users, Devices, Content)**
- **Enforces Compliances**
- **Capex & Opex Savings**

KEY FEATURES & SPECIFICATIONS

MANAGEMENT & CONTROL

Centralized Web Based Management & Provisioning	Browser based Centralized Management & Provisioning System for Remote Monitoring and Control of all Authorized End-point Hosts.
Network End-point Monitoring	Control, Track and Authorize the use of Devices. Allowing network to stay secure while monitoring activity via computer End-point inferences.
Trusted devices	Certify that all endpoint devices are not only authorized and controlled via DLP Agent software but also certified for protection of sensitive and confidential data.

REAL-TIME REPORTING & FORENSIC ANALYSIS

Real-time Incident Monitoring Dashboard	Instantaneous Reporting of any violation in Centralized & Consolidated Dashboard. Drill down into DLP incidents
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 and 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 REPORTING & FORENSIC ANALYSIS

Unstructured Data	Identify and protect Unstructured Data, such as text, memos, spreadsheets, emails, power-points, documents, images, Intellectual Property, etc. in real-time

Structured Data (Regular Expressions)	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
Enforced Encryption	In the event a device is stolen or lost all data pertaining to the device is encrypted and not accessible for other parties
Easily Extensible	Customize and extend as new patterns and threats arise without re-deployment
Data Types/Format Monitored	Over 48+ content format decoders including Txt, MS-Word, PDF, PPT, XLS, XML, Images, Design Documents, etc.

FILE MONITORING & TRACING

File Tracing / File Shadowing	Tracks all data copied to and from previously authorized devices. Shadowing features saves a copy of all files including the deleted files that were used in connection with controlled devices.
File Whitelisting	Allows only previously authorized devices to be copied to portable devices.
Security Policy Provisioning	No Manual Policy Provisioning required – All Policies generated and provisioned automatically
Automated Security Policy Enforcement	Easy enforcement and maintenance of latest security policies across the network.
Group-wise Policy Settings	Simplified device management policies with customizable templates for User Groups.
Automated Real-time Policy Update	Policy updates can be dispatched and enforced instantaneously in Real-time without interruption

PROTOCOLS & APPLICATIONS

Applications Types Monitored	Databases, Email, Web-Mail, MS-Exchange, Office-365, BOX, DROPBOX, Accellion, Google-Drive, Sharepoint, OneDrive, etc.
Cloud Access Control	Centralized Access Control of Web Applications and Web Services. Whitelisting or Blacklisting of Web Applications and Web Services
Enterprise Repositories	Active Directory and LDAP
Chat	Skype Chat, Google Chat Monitoring

DEPLOYMENT PROTECTION MODES

Enterprise Network Deployment	On Premise Enterprise Network Deployment
Client Uninstall Protection	Password based solution prevents users from uninstalling the End-point DLP Agent, thus insuring continuous data protection.
Client Stop Protection	Prevents the user from stopping the End-point DLP Agent at any time.
Device Activity Logging	Keeps a record of all clients, devices and actions producing history reports for future audits.

DISCOVERY, USER, DEVICE & CONTENT CONTROL

Content Search	Data Discovery, Access Control etc.
User Behavior Analytics	Search Activity Monitoring, Screenshot of activities, Event based monitoring, Employee Productivity Monitoring etc.
Content Control	User Control, Content Filtering, Applications Control, Browser Control, Fingerprinting, Remediation Workflow, Machine Learning etc.
Device Control	Granural control on USB and its content, CD-DVD access control, Control of access to Smartphones, USB Storage Encryption, Full Disk Encryption, Printer control, Screen control etc.

GhangorCloud, Inc. | 2001, Gateway Place, Ste: 710 West Tower, San Jose, CA-95110, USA
www.GhangorCloud.com