HGC GLOBAL COMMUNICATIONS

Data loss prevention solution

Centralized management of data security

Data breach poses serious threats for organisations, as the consequences of data loss by hackers or unintended exposures through internal staff would cause company reputation damage, data breach lawsuit or even worse - loss of business.

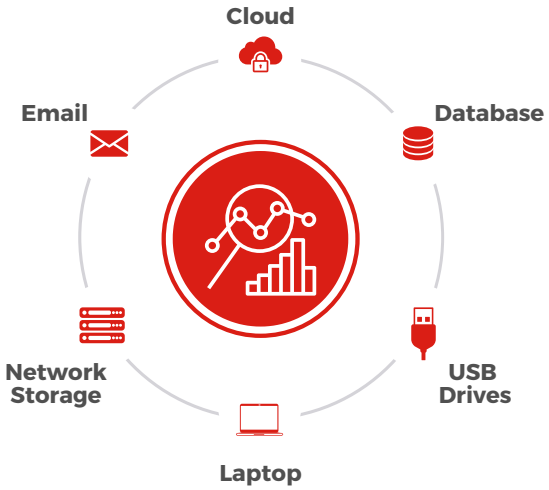
While compliance is another important topic that global enterprises are required to fulfil, how can enterprises identify, track, and secure all confidential data from dozens of applications to thousands of endpoints, according to their importance and characteristics to each staff?

HGC Data Loss Prevention Solution empowers enterprises to comply global compliance requirement easily through centralized governance of data in and out across staff and devices, by following corporate policy with a easily manageable setup.

Your Benefits

- A bird's-eye view of data visibility across employee, data media, data location, way of transfer and action associate to individual employee's access level
- Load of policy templates that help enterprises fulfil compliance regulation per international or national requirements
- Easy setup and data control from a centralized management application
- Comprehensive executive report to show analysis of risk conditions at organization and recommendations on fine-tuning security policy

Visibility & control everywhere your people work and data resides



- Discover data everywhere
- Classify data with integrations (e.g. Microsoft Azure information Protection, Boldon James, Titus
- Leverage advanced detection and forensics like fingerprinting
- Quickly build from largest policy templates available for compliance and critical intellectual property protection

Advanced detection
Deep forenisics
Discovery and classification
Human-centric analysis
SaaS app protection

Manage your compliance risks with powerful data protection

To comply with industry regulations, such as The Personal Data Protection Act (PDPA) and Singapore Technology Risks Management (TRM) Guideline, organizations have the obligation to keep personally identifiable information private.

PDPA

The Personal Data Protection Act (PDPA) provides a baseline standard of protection for personal data in Singapore. It complements sector-specific legislative and regulatory frameworks such as the Banking Act and Insurance Act.

It comprises various requirements governing the collection, use, disclosure and care of personal data in Singapore.

Singapore TRM Guideline

11.1 Data Security

- Data in motion - data that traverses a network or that is transported between sites;
- Data at rest - data in endpoint devices such as notebooks, personal computers, portable storage devices and mobile devices, as well as data in systems such as files stored on servers, databases, backup media and storage platforms (e.g. cloud);

Customer use case and scenario – A Regional Bank

Business Challenges:
How to prevent any intentional and accidental leakage of sensitive data in order to meet relevant cybersecurity regulations and compliance. There is no information about where the data are located and how they are being used.

Solutions:
Build up comprehensive data protection postures in several ways based on unique customer requirements:

- Protection on web channel
- Protection on email channel
- Protection on endpoint channel

Benefits:

- The bank seizes the strong control over PCI (Payment Card Industry Data Security Standard) and PII (Personally identifiable Information) related data.
- Control all policy management from a single pane of glass
- Full visibility of how sensitive data are distributed over endpoints.
- Comprehensive reports to identify and classify high risk users.

Start a comprehensive data security consultation

+65 6339 1203

christopher.koh@hgc-intl.com