

IQProtector Custom Data Interceptor

Customizable Versatility for any Data Source



Data is most effectively classified and protected right at the source – at the point of creation or first access – before it can be exposed. To immunize data immediately at the point of creation, Secure Islands offers scalable and seamless IQProtector data interceptors for applications running in the private or public cloud. Data interceptors for popular and complex applications like Exchange, SharePoint and OpenText, and for application servers, automatically identify data in need of classification and protection based on content and context, and managed centrally according to enterprise policies. They automatically immunize the data at the source of creation or first access and throughout its lifecycle independent of users or devices.

In some cases, enterprises work with special data sources where our data interceptors cannot handle data used by the application before it is written to a file-store. These can be:

- Applications that handle data with no file-system involvement
- Applications that receive information from one source and deliver it to another (transaction)
- Applications that run on non-Windows platforms like Linux
- Applications that save file properties separately from the file itself and where this information must be considered for classifying the document

To enable automatic classification and protection for such applications and services, Secure Islands offers a Custom Data Interceptor Software Development Kit (SDK). With the SDK, enterprises are able to extend data classification and protection to any type or use of data for any service or application including:

- Enterprise Content Management (ECM)
- Document Management Systems (DMS)
- Mail or relay servers
- Cloud services
- Report servers
- Archive servers

Highlights

IQProtector Custom Interceptor enables the creation of Server interceptors for detection, capture, classification and protection of data on-premise, as well as cloud-based interceptors that extend security coverage for applications and data stores in the cloud.

Benefits

- Complete, next-generation data-loss prevention from the moment of data creation
- Effective protection against insider threats
- Compliance with industry and government regulations regarding data security and confidentiality
- Accurate mapping of all information assets and pinpointing of risk – where information is created, used, stored and with whom it is shared
- Establishment, management and control of information-protection policy via a central management console
- Comprehensive auditing and forensics capabilities detect anomalies and analyze threats

VISIT US AT:

www.secureislands.com
info@secureislands.com



IQProtector Custom Data Interceptor

How does it work?

The Secure Islands Classification & Protection (C&P) Server is installed at the enterprise. This server can receive a file stream or a file location from the custom interceptor via Web services or RESTful API. Then, it classifies and protects the file based on enterprise policies and returns it to the original application. Through API commands, the C&P Server can also return properties about the file such as how it is classified.

A custom interceptor can be developed to intercept all data inside the target application and then communicate with the C&P Server through its APIs to classify and protect the file.

Just like Secure Islands' data interceptors in the IQProtector Product Suite, custom data interceptors integrate with:

- The IQProtector Management Console that ensures that a single classification and protection policy is maintained and enforced throughout the enterprise. The Management Console additionally provides predefined and customizable reports on data creation, storage, usage and sharing trends to enable powerful data tracking and auditing.
- IQProtector Analytics to map information assets and understand where information is created, used, stored and shared both within and beyond the perimeter. Leveraging big-data analytics, Secure Islands IQProtector utilizes sophisticated online analytical processing (OLAP), real-time forensic-level analysis, and behavioral anomaly detection to keep organizational security policy in line with real-world usage.

Professional Services

Enterprises wishing to take advantage of Secure Islands' experience can order custom data interceptors from Secure Islands Professional Services.

Key Features

- Automatic and 100% accurate information classification and protection for information created in or in transfer between application servers and services
- Supports any kind of application or service on any OS, even if it saves metadata separately
- Goes beyond files and works with data and transactions
- Protection of data from any source
- File encryption and rights-management enforcement based on Microsoft RMS
- Persistent protection and enforcement of usage rights for files in native applications
- Central Web-based management for policy distribution
- Real-time event logs reveal where information is created and who is accessing it
- Usable with other IQProtector products

ABOUT SECURE ISLANDS

Secure Islands develops and markets advanced Information Protection and Control (IPC) solutions for the borderless enterprise. Our policy-driven technology immunizes data at the point of creation, applying classification and protection that persist throughout the entire data lifecycle.

