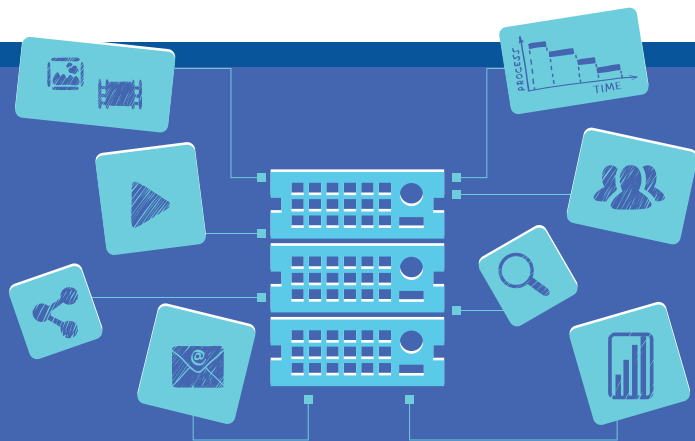


# IQProtector Scanner for File Stores



## Information protection for data at rest

Enterprises have been creating vast quantities of critical data since long before modern information security methods like classification, encryption and DLP were invented. Legacy data stored in repositories can contain critical product, marketing and accounting information. It can include financial data, intellectual property, patient records, drug trials, HR records and other information that is perpetually subject to data-confidentiality regulations or other needs. Misuse of legacy data by unauthorized personnel or power users, such as administrators, can put the enterprise at risk.

But what IT department has the time to undertake the daunting task of sifting through millions of data files to discover information that needs to be classified and protected? What enterprise has budget to painstakingly map its legacy data and verify compliance with industry and government regulations?

IQProtector Scanner applies Secure Islands' breakthrough active, persistent, data immunization technology to data repositories. It enables enterprises to automatically classify, tag and protect their legacy data and be in compliance retroactively and permanently.

## Complete immunization of legacy data and more

IQProtector Scanner crawls through legacy data files of any file type on network shares and file stores such as NAS, SAN, SharePoint, and more, identifying, classifying and protecting valuable data automatically, based on content and context, and according to enterprise policy. It is able to scan the entire data repository, delivering quick and significant value from pre-existing information.

IQProtector Scanner can act as an additional layer for information created and uploaded to file stores, ensuring that all new data is immunized according to enterprise policy.

## Highlights

IQProtector Scanner applies Secure Islands' breakthrough active, persistent, data immunization technology to data repositories, enabling enterprises to classify and protect their legacy data automatically – even data created long ago – and be in compliance retroactively and permanently.

## Benefits

- Applies enterprise policy to accurately classify and protect all data at rest including legacy data
- Provides complete classification data at the enterprise: on NAS, SAN, on premise and off premise
- Accurately maps information assets
- Alleviates IT resources
- Assures compliance with industry and government data-security and confidentiality regulations regarding data created in the past

## VISIT US AT

[www.secureislands.com](http://www.secureislands.com)  
[info@secureislands.com](mailto:info@secureislands.com)



# IQProtector Scanner for File Stores

## Complying with data security regulations

To meet compliance and industry data security regulations, organizations must be able to identify sensitive information and protect it. IQProtector Scanner inspects file content in all data stores and maps it in order to ensure that all the information is classified and protected, and that the enterprise fully complies with regulatory requirements.

## Automatic without tying up IT resources

IQProtector Scanner works automatically, freeing up IT resources. It goes to work in the background making legacy data as classified and protected as data created today.

## Central management, comprehensive reporting and analytics

IQProtector Scanner is managed centrally via the IQProtector Management Console. Unified management ensures that a single classification and protection policy is maintained and enforced throughout the organization. Real-time event logs created by IQProtector Scanner are sent to the Management Console and provide security experts with real-time clarity and visibility over all sensitive information across and beyond the enterprise. The Management Console additionally provides predefined and customizable reports on data creation, storage, usage and sharing trends.

## Key Features

- Crawls through vast volumes and repositories of data in network folders and file stores in the background: NAS, SAN, SharePoint, and more through CIFS, WebDAV and AFS protocols
- Automatically immunizes information according to enterprise policy, managed from a central server
- Applies classification, visual tagging, file encryption and rights-management enforcement based on Microsoft RMS
- Maps legacy data
- Processes all file types
- Central management provides a unified policy, reporting, and analytics
- Usable with other products from the IQProtector suite



## 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.