DATA SECURITY FOR THE FINANCIAL SECTOR

Protecting Client Data - A Competitive Advantage

With daily news of damaging cyber attacks, data leakage, tightening regulatory restrictions, and increased sensitivity to reporting liabilities - clients of financial organizations are asking tough questions about how exactly to secure their sensitive data and privacy.

This growing customer awareness has changed client data security from an industry necessity and regulatory imperative into an actual competitive differentiator.

FINANCIAL SECTOR DATA SECURITY CHALLENGES

To alleviate client fears about data security threats and demonstrate regulatory compliance, financial services organizations need to demonstrate comprehensive and laser-targeted security solutions for:

- **Customer Data Confidentiality** - Failing to protect personally identifiable information (PII) and client identifying data (CID) can cause serious damage to your firm's reputation, and consequently - its business. Your clients need to understand that every single item of personal data is secured. They need to know that even if leakage occurs - from targeted or persistent threats, human error, or even malicious internal sources – their data is securely encrypted and inaccessible to unauthorized users.
- **Cross Border Protection** - Some national regulations forbid export of sensitive financial information. Despite the complexity involved, financial institutions need to demonstrate strict compliance with these laws to both regulators and customers.
- **Separation of Duties** - Both your clients and regulators expect that sensitive data is accessible only to authorized users, according to their specific job function. This means that privileged users such as IT administrators must be strictly and demonstratively prevented from accessing or viewing personal or financial data - while not impairing their efficiency and control.
- **Ethical Walls** - Investment organizations need to maintain and demonstrate a strict "Ethical Wall" of separation between corporate advisory and brokering functions to avoid exposing the company to regulatory sanctions and litigation.

BENEFITS:

- Fully protect customer data confidentiality
- Apply cross-border protection; segregation of duties and Ethical Walls
- Full visibility and tracking of all sensitive data across the organization
- Automatic encryption of sensitive information from any source
- Assess risks and measure success using big-data analytics

FIELD PROVEN SOLUTION:

Fully deployed in major financial institutions worldwide at scales of over 50k production devices

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 life-cycle.

VISIT US AT:

www.secureislands.com
info@secureislands.com

secure islands

Secure Islands Technologies Inc. 79 Madison Ave. New York, NY 10016 | Tel: +1 (646) 313 3798
Secure Islands Technologies Ltd. 5 Menachem Begin Ave., Beit Dagan, Israel 50250 | +972 (3) 729 9899

DATA SECURITY FOR THE FINANCIAL SECTOR

SECURE ISLANDS' SOLUTION

Already deployed in major financial institutions worldwide, Secure Islands' IQProtector (IQP) leverages a unique data-centric approach to data classification and protection. With no impact on archiving, eDiscovery or other enterprise services, Secure Islands' IQProtector protects sensitive financial data from its source and throughout its life cycle - at rest, in motion, and in use.

Based on flexibly-defined parameters, IQProtector classifies in real-time sensitive data from any source - users, applications, file repositories or directories. Then, leveraging existing IRM and encryption frameworks, Secure Islands intelligently generates, applies and enforces encryption policies across the entire enterprise.

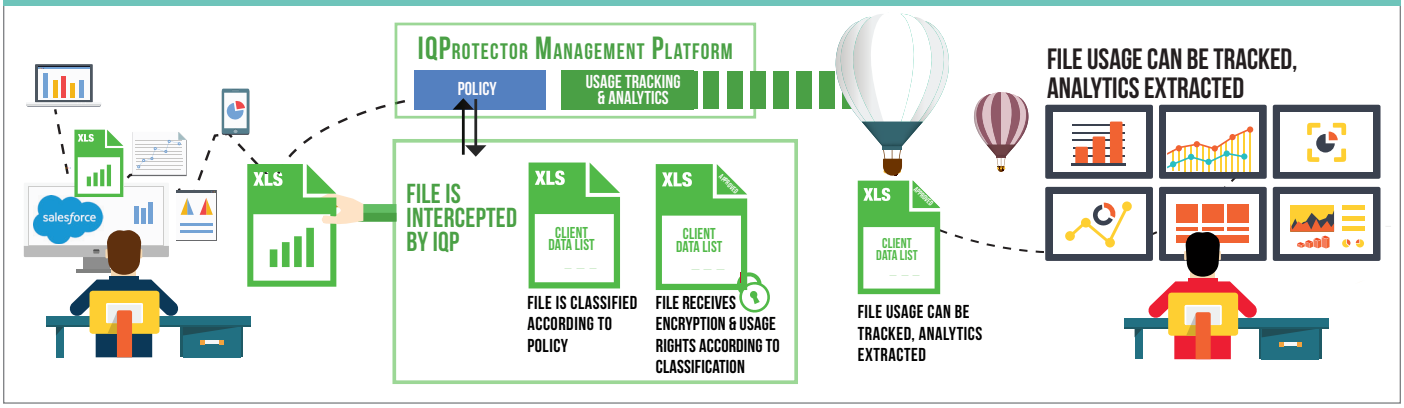
ENHANCING SECURITY

- **Customer Data Security** - No matter what the origin of the data - database, application, or any file type - IQProtector first identifies and classifies sensitive customer data, and then embeds protection within the data itself. Once classified and tagged as sensitive, this data is persistently protected - whether in use by an authorized user, in transit, or in storage. Because IQProtector is a data-centric solution, even data leakage - malicious or benign - does not expose sensitive customer information.
- **Cross Border Protection** - IQProtector allows the system to recognize not only who accesses the data, but also where it is accessed. Using secure and tamper-proof geo-location technology, IQProtector enables access to sensitive data within national borders, but can block access in other locations - delivering demonstrable data border protection, together with a full audit trail.
- **Segregation of Duties** - IQProtector creates and enforces enterprise-wide entitlements which are constantly updated, infrastructure-agnostic, and enforced transparently. This creates a strict and documentable segregation of duties for each individual piece of data, which is applied to both privileged and regular users - enabling complete and centrally-governed visibility over sensitive data usage.
- **Ethical Walls** - Secure Islands establishes and constantly maintains a segregation of duties between advisory and brokering functions, creating the strictly-enforced Ethical Walls that regulations demand.

FEATURES

- Intercept data at creation from any data source:
  - **PC:** outlook and office, web download and upload, data access and change by applications and processes, file move between folders
  - **Data Interceptors:** classification and protection - independent of platforms: for exchange, open text and cloud services
- Classification based on content and context: patterns, phrases, location, users, groups, custom properties
- Classification spectrum: Fully automatic classification, system recommendation and user-manual classification
- Visible content marking
- Encrypt any file format and enforce usage rights when files are used & shared over native applications
- Bridge - for seamless assimilation with IT environment and business processes (indexers, AV & DLP scanners, email archivers, and home-grown processes)
- Scanner - for classifying and protecting pre-existing data
- Central management, reporting and big-data analytics

PERSISTENT, ACTIVE DATA IMMUNIZATION



Secure Islands Technologies Inc. 79 Madison Ave. New York, NY 10016 | Tel: +1 (646) 313 3798
Secure Islands Technologies Ltd. 5 Menachem Begin Ave., Beit Dagan, Israel 50250 | +972 (3) 729 9899