Financial Sector Data Sheet

SecureIslands TECHNOLOGIES

Proven in the Financial Sector

- Already deployed in major financial institutions worldwide
- Ensures client data confidentiality
- Creates competitive advantage
- Unique data-centric approach
- Delivers cross-border protection
- Offers full segregation of duties
- Creates Chinese Walls for regulatory compliance

Client Data Security – 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 like yours are asking tough questions about how exactly you secure their sensitive data and privacy.

In fact, a recent survey by a Big Four auditing firm found that nearly 50% of prospective clients actively enquire about data security measures prior to conducting business with an institution.

This growing client 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:

• **Client Data Confidentiality** – Your clients need to understand that every single item of personal data is secured throughout its lifecycle - from creation, through collaboration and including storage. 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 new 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 clients.

• **Separation of Duties –** Both your clients and regulators need to clearly understand that sensitive data is accessible only to authorized users, according to their specific job function. This means that privileged users or IT administrators must be strictly and demonstratively prevented from accessing or viewing personal or financial data – without impairing their efficiency and control.

• **Chinese Walls –** Investment organizations need to maintain and demonstrate a strict “Chinese Wall” of separation between corporate advisory and brokering functions to avoid exposing the company to regulatory sanctions and litigation.

Secure Islands Solutions

Already deployed in major financial institutions worldwide, Secure Islands leverages a unique data-centric approach to data protection that Gartner recently called "visionary." With no impact on archiving, eDiscovery or other enterprise services, solutions from Secure Islands protect sensitive financial data from its source and throughout its life cycle – at rest, in motion, and in use.

Based on flexibly-defined parameters, Secure Islands 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 enterprise-wide.

Secure Islands provides solutions that measurably enhance:

Client Data Security

No matter what the origin of the data – database, application, or file - Secure Islands first identifies and classifies sensitive client 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 electronically or physically, or in storage. Because Secure Islands is a data-centric solution, even data leakage cannot expose sensitive client information.

Cross Border Protection

Since Secure Islands embeds protection within the data itself, the system can recognize not only who accesses the data, but also where it is accessed. Using secure and tamper-proof geo-location technology, Secure Islands 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

Secure Islands 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.

Chinese Walls

Secure Islands establishes and constantly maintains a segregation of duties between advisory and brokering functions, creating the strictly-enforced Chinese Walls that regulations demand.

About Secure Islands

Secure Islands Technologies provides advanced and innovative Information Protection and Control (IPC) solutions, incorporating intelligent and patent-pending data-centric security technology. The company's comprehensive, classification-driven security solutions for protection of sensitive enterprise data work seamlessly with existing business processes and IT infrastructure. Founded in 2006, with offices in Jerusalem, Israel, the company's solutions are deployed in top-tier Fortune 500 firms and government agencies worldwide. For more information, please visit www.secureislands.com.

Secure Islands Technologies Ltd.
High-Tech Village, Givat Ram Campus
The Hebrew University of Jerusalem
PO Box 39158, Jerusalem, Israel 91391

Tel. +972-2-6522941
Fax: +972-2-5661881
info@secureislands.com
www.secureislands.com

Secure Islands TECHNOLOGIES