Ingrian® DataSecure™ Platforms provide an intelligent, cost-effective way to encrypt critical data in applications and databases. As a result, organizations can better ensure they are compliant with legislative and policy mandates for security, and mitigate the risks of data thefts.
Today’s Mandate: Secure Sensitive Data

Enterprises have become adept at harnessing their vast information repositories to become more informed, more responsive, and more successful. In today’s climate, however, the success of a business hinges just as much on how well it protects its data as how well it utilizes that data. Here are a few reasons:

- Devastating security breaches continue to make headlines—frequently with corporate databases being exposed by internal staff as well as external attackers.
- Consumer decisions are increasingly dictated by concerns for privacy protection and fears of identity theft; organizations need to establish and maintain trust or customers will go elsewhere.
- Organizations must contend with an onslaught of privacy legislation and security mandates that cut across industries and geographies.

Securing sensitive data has never been more vital, yet, in spite of the billions spent each year on IT security, data theft remains alarmingly common and shows no signs of abating. Why? While traditional, network security mechanisms—firewalls, IDSs, and other products—remain vital, they’re not foolproof, and they’re not designed to address many of the threats that confront organizations today.

To ensure that sensitive data remains secure, both from internal and external threats, many organizations are taking a proactive approach to ensure data privacy—and turning to Ingrian Networks to achieve this objective. Ingrian DataSecure Platforms deliver sophisticated capabilities for encrypting sensitive data in databases and applications. These products feature granular encryption, seamless integration, and centralized security management—enabling organizations to eliminate an array of critical security threats, with unparalleled ease and cost effectiveness.

Advantages of the DataSecure platform include:

- **Robust security.** Addresses a broad range of threats with capabilities for granular encryption, secure policy and key management, sophisticated administration, segregation of duties, strong AAA support, and more.
- **Streamlined implementation.** Integration is automated and transparent to applications; administration is intuitive; and because all keys and policies are managed on a centralized appliance, ongoing maintenance is streamlined.
- **Scalability and reliability.** Offloads processing-intensive cryptographic functions from servers, and offers throughput and high availability for even the most demanding environments.
- **Flexible, multi-tier integration.** Can be integrated in heterogeneous environments and be deployed at the Web, application, and/or database layer.
Robust Security Platform

DataSecure platforms offer granular, column- or field-level encryption of sensitive data in Web servers, application servers, and databases. DataSecure enables organizations to protect only the sensitive data that poses a business or liability risk—whether credit card numbers, social security numbers, email addresses, account numbers, or other sensitive information. Further, by implementing encryption with Ingrain, organizations can ensure that sensitive data is secured...

- at rest in databases and servers, and
- as it is saved to storage systems, including network-attached storage and storage area networks.

As a result, sensitive data is never readable by unauthorized users, thus minimizing the risk of information theft from internal or external attacks.

A Dedicated Security Appliance

By centralizing all cryptographic processing, key management, logging and auditing, and security policies on a single, hardened appliance, DataSecure delivers benefits in administration, performance, and, most importantly, security. For example, the cryptographic keys needed to decrypt sensitive data never leave the DataSecure appliance. Also, the appliance can be configured with a variety of administrative safeguards to ensure only appropriate administrators can access the device. DataSecure features:

- **Centralized key management**, offering both physical and administrative safeguards—including a FIPS 140-2 Level 3 compliant hardware security module for tamper-resistant protection of cryptographic keys.
- **Capabilities for segregating administrative duties** so key controls are shared among multiple administrators.
- **Secure, multi-factor authentication and access control** between databases and servers and the DataSecure platform.
- **Granular authorization capabilities** that enable constraints to be placed on user operations based on specific key permissions.
- **Active alerting capabilities** so that, if attempts to breach protected data occur, mechanisms are employed to alert administrators.
- **Comprehensive, secure, and centralized logging and auditing** of all cryptographic functions and access.

Streamlined Implementation

DataSecure addresses the challenges of making encryption work in large-scale enterprises, offering flexible, cost-effective implementation options so organizations can deploy in a way that makes sense for their specific security and business requirements.

Automated Integration

With its automated database integration capabilities, DataSecure can be implemented with complete application transparency, dramatically reducing the time and costs normally associated with encrypting data in the enterprise. With DataSecure, administrators can, via an intuitive graphical user interface, make initial configuration settings, then harness capabilities that automate:

- Database schema changes.
- Migration of selected fields from cleartext to ciphertext.
- Installation of triggers and views for application transparency.
- Key rotation to adhere to defined security policies.

In addition, DataSecure can be integrated with bulk load utilities to handle large batch processing and existing data import/export processes.

Ease of Administration

The DataSecure platform delivers unrivaled features for streamlining and reducing the costs of ongoing administration—particularly compared to server-based cryptography and key management. This is achieved through the following:

- Easy-to-use, intuitive management via a graphical user interface.
- Centralized management of all policies, users, and cryptographic keys.
- Automated replication between Ingrain products.

Scalability and Reliability

DataSecure centralizes all cryptographic processing on a highly specialized appliance that delivers performance robust enough for the most demanding batch processing and online transaction processing environments. A single platform can handle over 12,000 cryptographic requests per second, and Ingrain makes it easy, through load balancing capabilities, to add additional appliances and boost scalability as performance needs dictate.

Further, by offloading CPU-intensive cryptographic processing from disparate servers and databases, DataSecure restores server and database performance to optimal levels—resulting in less waiting for information and higher resource utilization. Designed specifically for business-critical processing, DataSecure offers an array of features to ensure reliability and availability:

- **High availability**, featuring optional RAID support and redundant power supplies, fans, and processors on each appliance, DataSecure also enables the use of redundant, replicated appliances and failover configurations that ensure optimal up time.
- **Health checking**, Web servers, application servers, and databases can determine immediately if an appliance is unavailable and switch to an alternate.
- **Disaster recovery capabilities** enables a second, active site with duplicate, secure backups of critical configuration, policy, and key information—and secure recovery through Ingrain’s FIPS k-of-n smart card recovery mechanism.

Flexible, Multi-Tier Integration

DataSecure can be integrated wherever an organization’s security and business needs dictate—whether at the Web server, application server, or database layer. DataSecure offers support for leading, standards-based cryptographic algorithms: AES, 3DES, RSA, and others. Accessible via standard APIs, DataSecure can be effectively integrated with:

- All application servers, including those from BEA, IBM, Microsoft, Oracle, and Sun.
- IBM DB2; Microsoft SQL Server; and Oracle 8i, 9i, and 10g databases.
- PeopleSoft applications, including Human Capital Management, Customer Relationship Management, and Financial applications.
- All Web servers, including Apache, Tomcat, Resin, and Microsoft IIS.
- Legacy and custom environments via an XML, JCE, MS-CAPI, .Net, or PKCS#11 interface.
Platform Components
The Ingrian DataSecure Platform is comprised of three components:

- The DataSecure appliance, a dedicated hardware system,
- The Network-Attached Encryption™ (NAE) Server, which runs on the DataSecure appliance, and
- The Ingrian NAE Connector, a software provider that is installed on the Web server, application server, or database that interfaces with the DataSecure appliance.

DataSecure Appliance
The DataSecure appliance is a dedicated hardware product that is designed specifically for security and cryptographic processing. The DataSecure appliance is offered with redundant system components (including dual CPUs, power supplies, and fans), multiple NICs, and onboard options for high availability. The appliance features an optional integrated FIPS 140-2 Level 3 compliant hardware security module, providing tamper-resistant protection of cryptographic keys.

Network-Attached Encryption Server
The Network-Attached Encryption (NAE) Server provides facilities for executing a large volume of highly specialized cryptographic activities. The NAE server executes a range of security-related tasks, including processing all cryptographic requests generated by the NAE connectors residing on applications and databases, doing integrity checks to ensure critical company information and other application data has not been modified, securely storing and managing cryptographic keys, and centrally logging all cryptographic requests and activity on the appliance.

Ingrian NAE Connector
Ingrian NAE Connectors provides standards-based cryptographic interfaces that enable the protection of user-defined data within the Web server, application server, or database, allowing effective integration of security at the business logic layer. These small software components are designed to be installed on servers and databases that interface with the Ingrian appliance. All NAE connectors also have embedded logic that provides load balancing, health checking, and connection pooling among a cluster of redundant DataSecure appliances.

Product Line Overview
Ingrian offers a variety of DataSecure appliances, ensuring Ingrian customers get a solution tailored to their specific security, performance, and budget requirements. The family of DataSecure products includes the following offerings:

Ingrian i311 DataSecure Appliance
Ingrian’s entry level platform offers processing horsepower to handle a high volume of cryptographic operations and ensure optimal application performance. The i311 comes with 2GB RAM, combined single processor and ASIC architecture, and the ability to process over 12,000 cryptographic operations per second.

Ingrian i315 DataSecure Appliance
The Ingrian i315 offers the same features as the i311, and also has an integrated FIPS 140-2 Level 3 compliant hardware security module for enhanced key management. The i315 processes over 2,000 cryptographic operations per second.

Ingrian i321 DataSecure Appliance
The i321 delivers all of the features and performance found in the i311, including capabilities for processing over 12,000 cryptographic operations per second. In addition, the i321 offers dual power supplies and fans with automatic failover to ensure “always on” performance. It also offers a Gigabit Ethernet interface, enabling maximum bandwidth and throughput of application traffic.

Ingrian i325 DataSecure Appliance
The Ingrian i325 offers the same features as the i321, and also has an integrated FIPS 140-2 Level 3 compliant hardware security module for enhanced key management. The i325 processes over 2,000 cryptographic operations per second.

About Ingrian Networks
Ingrian Networks brings complete data privacy to the enterprise. With Ingrian DataSecure Platforms, organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. DataSecure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases. With its capabilities for granular encryption, seamless integration, and centralized security management, DataSecure enables organizations to guard against a range of security threats, with unparalleled ease and cost effectiveness. Ingrian is a privately held company backed by such investors as Globespan Capital Partners, HighBAR Ventures, Menlo Ventures, Partech International, and Prism Venture Partners. For more information, visit www.ingrian.com.