



Ensuring Data Privacy with Ingrian Networks

An Introduction to Ingrian and its Solutions

Ingrian Networks

475 Broadway, Redwood City, CA 94063

Phone 650.261.2400

Toll-free 866.INGRIAN (866.464.7426)

Fax 650.261.2401

www.ingrian.com

Executive Summary

Ingrian™ Networks secures sensitive data throughout the enterprise. Ingrian DataSecure™ Platforms ensure that sensitive information is impervious to attacks, whether data is at rest, in transit, or in use. Ingrian DataSecure Platforms offer intelligent, granular control of which data to protect, they adhere to open standards and are cost effective to deploy, and they deliver comprehensive security capabilities.

Company Background

Ingrian is a privately held company backed by such investors as American Express (NYSE:AXP), Globespan Capital Partners (formerly JAFCO Ventures), Partech International, and Prism Venture Partners. Ingrian primarily serves global financial institutions, e-commerce businesses, healthcare organizations, and government agencies.

Ingrian was founded in 2000 with an investment from leading technologists, venture capital firms, and security experts. Backers of Ingrian include Bill Joy and Andreas Bechtolsheim, co-founders of Sun Microsystems, and Dr. Martin Hellman and Dr. Dan Boneh, leading pioneers in cryptography and professors at Stanford University. The company holds over twenty security-related patents and maintains a world-class engineering team.

Solution Overview

Ingrian's data privacy solutions are delivered on dedicated hardware platforms that feature patent-pending cryptography software. Ingrian DataSecure Platforms are designed to provide a suite of cryptographic functions to all required systems on your network from a centralized, highly available, and hardened security platform. Ingrian offers a comprehensive way to encrypt, integrity check, fingerprint, and digitally sign sensitive data—and protect it at all times, throughout the enterprise. DataSecure protects information in all these phases:

- Data at rest—while it sits in storage devices, whether they are directly attached to systems or in a SAN/NAS environment.
- Data in transit—while information is moving between servers, databases, and storage devices.
- Data in use—while it is being accessed or processed by applications and databases.

The Result: Sensitive data—whether a credit card number, social security number, or sensitive file—is protected at all times, from the time it enters the network to the time it is saved onto the storage subsystem.

Industry Drivers

Enterprises worldwide are spending approximately \$20 billion per year on IT security, yet very costly breaches continue to occur. While the specific nature of these breaches vary, one of the central security flaws being exposed is one of focus: in large part, security efforts have been focused on network security, building and strengthening a network perimeter, rather than data privacy—taking steps to ensure data is secured within the enterprise. Traditional technologies like firewalls and intrusion detection systems are a critical part of protecting an enterprise's network perimeter, but they are only part of a complete security picture. Following are a few reasons:

- According to Gartner, 75% of external-based attacks are tunneling through applications—and so go undetected by a range of perimeter security mechanisms.
- The ongoing battle of patching known exploits is being lost: According to a study by Symantec, in 2003, 70% of all security vulnerabilities were simple for attackers to manage, and this number grew 10% over the previous year.
- Most estimates cite that now over 50% of security breaches are perpetrated by internal staff.
- Even with a fortified network perimeter, databases and applications can be compromised, storage systems can be breached, and storage management interfaces and physical devices can be stolen.

Failure to implement a data privacy solution can have a disastrous effect on an organization. For years now, the price organizations have paid when breaches become public has been catastrophic. One estimate states that compromised firms lose, on average, 2.1% of their market values within 2 days of a breach, which translates into an average of \$1.65 billion loss in market capitalization per incident¹. This is on top of very real, but harder to quantify, losses that stem from damaged brands and diminished consumer trust. Not coincidentally, many firms do whatever they can to keep these breaches from going public. In fact, recent estimates state that only 30% of all security breaches get reported at all².

Whether organizations want it to or not, this will have to change. A range of policies and legislative mandates are dictating a more data-centric approach, and, further, are requiring the disclosure of any breaches. These mandates are coming in a range of forms:

- **Regional legislation.** Europe's Data Privacy Act, Canada's Personal Information Protection and Electronic Document Act (PIPEDA), California's Database Security Breach Notification Act, SB 1386, and many others all dictate encryption in some fashion, and that any victims of breaches are notified.
- **Industry-specific legislation.** In health care, the Health Insurance Portability & Accountability Act (HIPAA); and the Gramm-Leach-Bliley Act (GLBA) in financial

1. "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers," Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan, The University of Texas at Dallas School of Management February 2002

2. CSI/FBI Computer Crime and Security Survey, 2003

services have provided comprehensive guidelines for safeguarding patient and consumer data respectively.

- **Commerce policies.** Credit card issuers like Visa, MasterCard, and American Express all have delivered comprehensive guidelines that provide an edict for both best security practices, including data encryption for example, as well as mandating consumer notification of breaches.

The bottom line to all this is that organizations need to address data privacy in a comprehensive fashion. Those that don't, and wait for a legislative mandate, or, worse, a security breach, before they do so, will ultimately be taking chances that can put an entire business at risk.

It's no wonder that in a recent Gartner survey of Chief Information Officers around the world, data privacy moved up to number three on the list of top priorities from number ten a year ago, with security remaining the top concern.

Historically, the challenge in achieving data privacy has been that many of the options available to organization have been lacking, either in terms of delivering true security, or in terms of prohibitive cost or complexity. Ingrian Networks offers solutions that enable data privacy throughout an enterprise, while overcoming these traditional shortcomings. With Ingrian DataSecure Platforms, companies can effectively address today's most critical security threats—data left unprotected within applications, databases, or storage systems.

Technology Overview

Ingrian Networks provides a comprehensive solution for ensuring data privacy. The solution consists of a rack-mounted, hardened platform coupled with intelligent software connectors that reside on applications and/or databases and communicate with the Ingrian platform securely.

Ingrian's data privacy solutions offer the following capabilities:

- Strong encryption of selected data in storage and transit—DataSecure platforms offer a wide-range of standard high-security cryptographic algorithms, including 3DES, AES, and RSA, to secure your sensitive data at rest. High-performance SSL is available to protect data as it traverses the network.
- Robust authentication and fine-grained access control—Ingrian delivers comprehensive capabilities for managing client and administrative access to the DataSecure platform. Access to keys and cryptographic functions are defined using an easy-to-manage, role-based access system. Responsibilities can be delegated to multiple administrators using smart cards.
- Secure key management and logging—Ingrian products can include a FIPS 140-2 Level 3-compliant hardware security module for the storage of key material, which supports

- U.S. government requirements for tamper resistance. Centrally managed and signed audit logs are also offered.
- Data Integrity Checking—Ingrian can perform an integrity check on important data that is also encrypted via DataSecure, or on data that does not need to be encrypted, but must be protected—such as a product price list, which must never be modified without permission. In this case, Ingrian uses the HmacSHA1-based algorithm to create a Message Authentication Code (MAC) equivalent of the price list, which is then returned to the server and stored with the original price list file. Then, when the price list is requested by a user, the solution can perform an integrity check to ensure the file still matches the MAC equivalent.
 - Data Fingerprinting—Ingrian can perform a similar identity-checking function on data such as user passwords. It can apply a keyed hash to the password when the user registers with the server. The result is a unique password-equivalent “fingerprint,” which is stored in an appropriate location. Then when the user logs on a second time, the same steps are performed and the result is compared with the stored fingerprint to ensure that there is a match. Offline dictionary attacks and other brute force techniques to recover the passwords for the system will be ineffective with a key used to create the fingerprint, and the key is stored securely on the Ingrian platform.

Solution Components

The Ingrian data privacy solution is comprised of three components:

- The DataSecure platform, a dedicated hardware appliance,
- The Network-Attached Encryption™ (NAE) Server, which runs on the DataSecure platform, and the
- Ingrian NAE Connector.

Ingrian DataSecure Platform

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

Network-Attached Encryption Server

The Network-Attached Encryption (NAE) server is a combination of the software architecture and components for executing highly specialized cryptographic activities. The NAE server

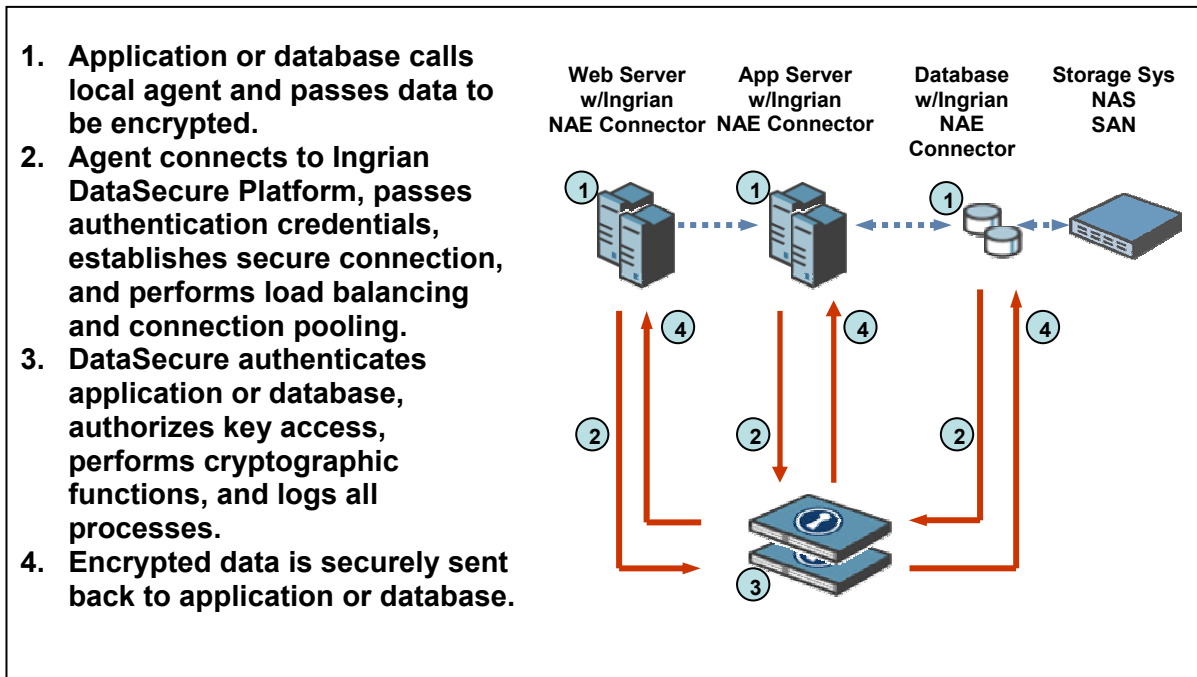
executes a range of security-related tasks, including processing all cryptographic requests generated by the software agents residing on applications and databases, doing integrity checks to ensure critical company information and other application data has not been modified, securely storing and managing cryptographic keys, and centrally logging all cryptographic requests and activity to the platform.

Ingrian NAE Connector

The Ingrian NAE Connector provides standards-based cryptographic interfaces that allow the protection of user-defined selected data within the application or database, allowing effective integration of security at the business logic layer. These small software components are designed to be installed on each application server or database that has a need to interface with the Ingrian platform. NAE Connector works seamlessly with any enterprise application server, including BEA Weblogic, IBM WebSphere, Sun ONE Application Server, Apache Tomcat, and others and can be integrated with such leading database products as Oracle, IBM DB2, and Microsoft SQL Server.

The DataSecure Process

First, the DataSecure platform enables secure connections between itself and the application server or database using SSL. This establishes a protected, encrypted tunnel for the applications and databases to use for communication of cryptographic requests. Authentication and cryptographic operation privileges are created on and controlled by the DataSecure platform for each application or database. When the Ingrian platform receives the cryptographic request, it first performs access control verification, validating the server certificates and/or application ID and password. Policies on the platform are then checked to make sure that the server has the appropriate privileges to perform the desired operation. Once this step is completed successfully, the DataSecure solution offloads the cryptographic request to dedicated hardware for processing. After the cryptographic processing, the data is then returned over the same encrypted network connection to the server. From there, encrypted data can be safely stored on the appropriate server, database, or other storage device, while the keys used to encrypt the data remain secure on the DataSecure platform.



Business Benefits

Ingrian’s standard-based software interfaces allow for the centralization of intensive cryptographic processing to the DataSecure platform, processing which traditionally would have to be performed on each server. Having individual servers or devices manage these sensitive keys and functions is a security risk and can dramatically increase the complexity and operational cost of the network. Consolidating these security services to the DataSecure platform allows for a more secure, scalable, and manageable infrastructure. This allows for savings in the following areas:

- Lowered operational and management costs—Enterprises are demanding a high degree of integration between operational systems for security and network performance management. Requiring network and security managers to examine the performance and configuration of individual elements from multiple different vendors when an event occurs is inefficient and costly. An integrated, centralized solution with easy-to-use to administer and management provides much greater operational effectiveness and reduces management costs.
- Capital cost efficiency—Most current network infrastructures were not optimized for the kind of security requirements that companies face today. In order to implement real security while maintaining the value of existing equipment, IT managers need products that are specifically designed to overlay security into existing infrastructures. Ingrian’s DataSecure platform provides a network-based service that can be leverage by existing system components, without retrofitting or upgrading hardware to meet new security

and performance targets. Additionally, data protection services are offloaded to a dedicated device, thereby freeing valuable server resource to service applications.

- Improved scalability and performance—The DataSecure platform has been designed to scale horizontally to meet processing needs. Important configuration information is replicated in real-time to other Ingrian products. Other information can be securely copied to any number of other platforms and locations via an encrypted file. Ingrian also functions as an accelerator. The platform handles as much as 50 times more cryptographic operations than a typical Web or application server, processing over 2,000 encryption transactions per second.
- Highly available—Down time costs money. Ensuring uptime of your data protection service is an important concern. Ingrian’s data privacy products are built to provide a solution that is always available. The DataSecure platform has complete failover and load balancing support. In addition, redundant hardware components are offered on the platform.

Consolidating your cryptographic services to Ingrian also leads to a more secure infrastructure. Ingrian delivers products with key management technologies that are Federal Information Processing Standard (FIPS) 140-2 Level 3 compliant. DataSecure extends protection of sensitive data to storage in the database. This level of security means lower risk.

About Ingrian Networks

Ingrian Networks brings complete data privacy to the enterprise. Ingrian DataSecure Platforms ensure that sensitive information is impervious to attacks, whether data is at rest, in transit, or in use. Ingrian DataSecure Platforms offer intelligent, granular control over what data is protected, they adhere to open standards and are cost effective to deploy, and they deliver comprehensive security capabilities. For all these reasons, Ingrian is the smart choice for addressing one of today’s most critical security threats: data left unprotected within the enterprise. Ingrian is a privately held company backed by such investors as American Express (NYSE:AXP), Globespan Capital Partners (formerly JAFCO Ventures), HighBAR Ventures, Partech International, and Prism Venture Partners. For more information, visit www.ingrian.com.