eCommerce the SAFE and EASY way

Request a Call Back

CHAT ONLINE

Home Company Helpful Advice Products Support Pricing Partners Buy SSL Sign Up Login Contact Us

eWAY Home » Company » eWAY Technology » Ingrian

About eWAY
eWAY Explained
PCI DSS Compliance
Media Room
eWAY Success Stories
eWAY Technology
Ingrian
Verisign
Data Centre
Data Recovery
Diagrams
SSL Partners
GPayments

Ingrian

As a payment processor, **eWAY** must ensure that all credit card and transaction data is not accessible to outside parties.
We achieve this through Ingrian, the world's leading data security provider.

Many organizations have had their brands severely tarnished and lost millions because sensitive customer data held in databases was exposed. Further, a range of security and privacy policies are dictating that just about any large organization will need to encrypt sensitive data held in databases.

INGRIAN™ NETWORKS Relax. Your Data is Compliant.

Visa, MasterCard, American Express and other card issuers are mandating that organizations must encrypt credit card data stored in databases, thus ensuring they are PCI compliant.

Ingrian encryption solutions are based on an integrated security architecture that provides customers with standards-based cryptography, a proven key management strategy, easy deployment and support, and solutions interoperability—giving organizations all the components required to harness encryption and ensure complete data privacy.

"eWAY is a great example of how payment processors can differentiate themselves and help customers by deploying the right security technology," said Michael Howard, CEO at Ingrian. "Centralized key management is an important component to a merchant's encryption strategy and as more consumers purchase online, payment gateway providers will need to provide smaller merchants with a scalable yet powerful encryption technology solution that is interoperable with their own security systems. With its smaller footprint and easy integration, Ingrian EdgeSecure is an excellent choice."

Securing customers' sensitive data has never been more vital, yet in spite of the many billions spent each year on IT security, data theft remains a common problem. While traditional network security mechanisms such as firewalls, IDSs, and other products remain vital, they're not 100% foolproof, and they do not address many of the threats that confront organizations today.

To ensure that sensitive data remains secure, both from internal and external threats, many organizations such as **eWAY** are taking a more proactive approach to ensure data privacy. Ingrian DataSecure Platforms deliver sophisticated capabilities for achieving database encryption. These products feature granular encryption, seamless integration, and centralized security management, enabling organizations to eliminate an array of critical security threats with unprecedented ease and cost effectiveness.

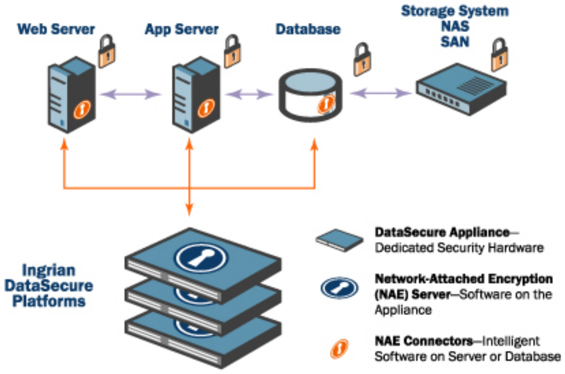
Advantages of the DataSecure platform include:

- **Robust security** - Addresses a broad range of threats with capabilities for granular database 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.

Platform Components

The Ingrian DataSecure Platform is comprised of three components:

- The DataSecure appliance, a dedicated hardware product,
- 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.


Web Server
App Server
Database
Storage System
NAS
SAN
Ingrian
DataSecure
Platforms
DataSecure Appliance—
Dedicated Security Hardware
Network-Attached Encryption
(NAE) Server—Software on the
Appliance
NAE Connectors—Intelligent
Software on Server or Database

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.