TECH CHOICES

August 8, 2005

Database Encryption Solutions Scorecard Summary: nCipher SecureDB

Key Findings From "The Forrester Wave™: Database Encryption Solutions, Q3 2005"

by Noel Yuhanna
with Randy Heffner, Kimberly Q. Dowling, and Lindsey Hogan

EXECUTIVE SUMMARY

nCipher did well overall in our evaluation, capturing a spot in our leader category largely because of its good balance of features, functionality, and vision. nCipher is strong in its centralized administration, pluggable-crypto support, and the type of algorithms supported but lacks support for primary and foreign keys and can be expensive with an average price of $70,000. Customers looking for an easy-to-use end-to-end encryption solution will find nCipher to be a good fit. Forrester finds that nCipher has a good vision and continues to extend its cryptographic solutions at all layers.

nCIPHER IS BEST SUITED FOR MULTIPLE MEDIUM-SIZED DEPLOYMENTS

nCipher is a public company with a sole focus on cryptographic security, and has been marketing encryption products as its primary source of revenue for the past eight years. nCipher has a number of patents focused on encryption-based security. With more than 400 customers worldwide using various products, nCipher reports annual revenues of $28 million for fiscal year 2004 on $0.78 million profit. nCipher's SecureDB product provides column-level database encryption for Oracle, DB2, and SQL Server on multiple platforms. However, it has limited separation of security roles and therefore, nCipher users rely mainly on DBMS' roles.

nCipher solutions go beyond database encryption. It offers a solution to secure private keys on Web servers, secure public key infrastructure (PKI), authentication, and communications and applications. nCipher offers the option to protect keys using Federal Information Processing Standards (FIPS) 140-2 Level 3 certified hardware security modules (HSMs). Enterprises can use nCipher to secure data across servers and applications, with centralized management. Forrester evaluated nCipher's current offering and strategy for database encryption solutions against approximately 100 criteria (see Figure 1). Overall, the product has strong support for integration with HSMs, many encryption algorithms, pluggable crypto, role separation, centralized administration, but lacks support for primary and foreign keys, international character sets, comprehensive encryption modes, and can be expensive. This means that the product is an especially good fit for buyers who:

- **Want data-at-rest encryption rolled out on multiple databases.** When supporting an environment that requires several databases to be encrypted, nCipher is a good fit because it offers simple, centralized administration from a single interface.

- **Want to encrypt data at all layers.** nCipher's solution integrates with HSMs, and no additional development or coding is required for such integration. nCipher also supports pluggable crypto to customize encryption algorithms. Customers will find that the nCipher cryptographic solution is not only simple to use, but it can also encrypt at network and application layers, besides databases.

To see how nCipher stacks up against six other competitors, see the Forrester Wave™ evaluation of the database encryption solutions market.[1]

Figure 1 nCipher SecureDB Evaluation Overview

CURRENT OFFERING

Levels of encryption	nCipher supports column-level database encryption, with support for various column sizes. However it does not support encryption of primary and foreign keys. Also, it does not support table-level, or database-code-level protection. However, through integration with nCipher HSMs and encryption APIs using nCipher's CipherTools tool kit, the entire file containing the table can be encrypted.
Encryption options	nCipher supports leading encryption algorithms and offers the flexibility to support additional algorithms and pluggable crypto. The initial set-up is done using a wizard-based GUI; multiple databases can be configured from the central management console. nCipher offers security policies that can be used to customize the environment. It offers the ability for separation of roles, and access to encrypted columns is controlled by setting access policies.
Encryption keys management	nCipher allows the master key to be stored in a table, file, or HSM. It only supports automated encryption key generation (no manual support). Optionally, it allows keys protection using FIPS 140-2 Level 3 certified HSMs. SecureDB currently only supports CBC encryption mode.
Integration	nCipher supports UNIX, Windows, and Linux platforms and offers integration with hardware acceleration modules. It also supports integration with LDAP and other directory solutions. nCipher offers integration with DBMS schema, creating additional objects in the database, such as tables, stored procedures, etc. nCipher also supports Oracle, SQL Server, and DB2 DBMS. In most cases, nCipher does not require any changes to the application. It also provides a solution that enables encryption at any point in the application stack or network architecture. nCipher provides a cryptographic tool kit that allows customized approaches to cryptographic security to be deployed.
Usability	nCipher offers centralized administration and keys management. Space requirement would depend on the algorithm used and number of columns encrypted. SecureDB includes real-time auditing capability, which can be monitored from the SecureDB Management Console. nCipher offers equality search, but range scans are achieved by decrypting all of the data before performing the range scans. Equi-joins on encrypted data are supported, as long as the data is encrypted using the same keys on both the columns involved in the join criteria. SecureDB also supports bulk encryption to improve performance when dealing with large amounts of data.

Source: Forrester Research, Inc.

Figure 2 nCipher SecureDB Evaluation Overview (cont.)

STRATEGY

Product strategy	nCipher is focused on delivering application, network, and database encryption solutions. nCipher has partnerships with several vendors and ISVs, such as Oracle, Microsoft, and IBM. SecureDB is a good technology, and offers some flexibility in integration with other security solutions, including storing keys outside of the database.
Corporate strategy	nCipher is a public company that has focused on cryptographic security for the past eight years. nCipher has a number of patents focused on encryption-based security and has strong senior management commitment. nCipher is a profitable company with cash in excess of $70 million.
Cost	SecureDB's average price is $70,000 and lowest price is $13,000. The maintenance is 20% for gold support and 25% for platinum support.

MARKET PRESENCE

Installed base	SecureDB product, which was launched less than a year ago, has less than 10 customers, but has more than 400 customers in various verticals for all products.
Revenue	nCipher reports earnings in pounds sterling. These numbers have been converted using a rate of 1.97. nCipher's fiscal year 2004 operating profit was approximately $0.78 million and its revenue was approximately $28 million.
Revenue growth	nCipher claimed that in 2004 it achieved continuous sequential growth in sales revenue during all four quarters. Total revenues for the year amounted to approximately $28 million (using 1.97 conversion), an increase of 10% compared with 2003 total revenues.
Systems integrator	nCipher does not have integrators.
Services	nCipher has a services staff of more than 15 employees worldwide who help in SecureDB implementation. It does offer on-site and classroom training.
Employees	nCipher has more than 25 development and QA engineers, with a total employee base of 120. It has sales force in various locations worldwide.
Technology partners	nCipher claims that there are no companies that bundle SecureDB, but has more than 20 reseller partners.
International presence	nCipher has offices located in the UK, US, and India, with 58% of revenue represented outside of the US.

Source: Forrester Research, Inc.

The Forrester Wave™
Smart data for smart decisions

Go online to download additional in-depth data and scores for this vendor and other vendors included in this Forrester Wave evaluation.

SUPPLEMENTAL MATERIAL

Online Resource

The underlying spreadsheet for Figure 1 is available online. The spreadsheet includes more detailed data and scores for this vendor.

This detailed data and scores for this vendor are also available online through an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we narrow our final list to those presented here. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of questionnaires, demos, and discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in this document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weighting to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

ENDNOTES

[1] In the past two years, the need for database-level encryption has grown significantly, mainly because of regulatory requirements, and enterprises taking stronger measures to protect data as more intrusions occur across the globe. To assess the state of the database encryption market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top database encryption vendors across approximately 100 criteria. The result: Protegrity and Ingrian provide the strongest options in the third-party vendor category, and Oracle leads the DBMS vendors pack. Included in this report is an interactive vendor comparison tool that provides detailed product evaluations and customizable rankings. See the August 8, 2005, Tech Choices "The Forrester Wave™: Database Encryption Solutions, Q3 2005."