
protegrity

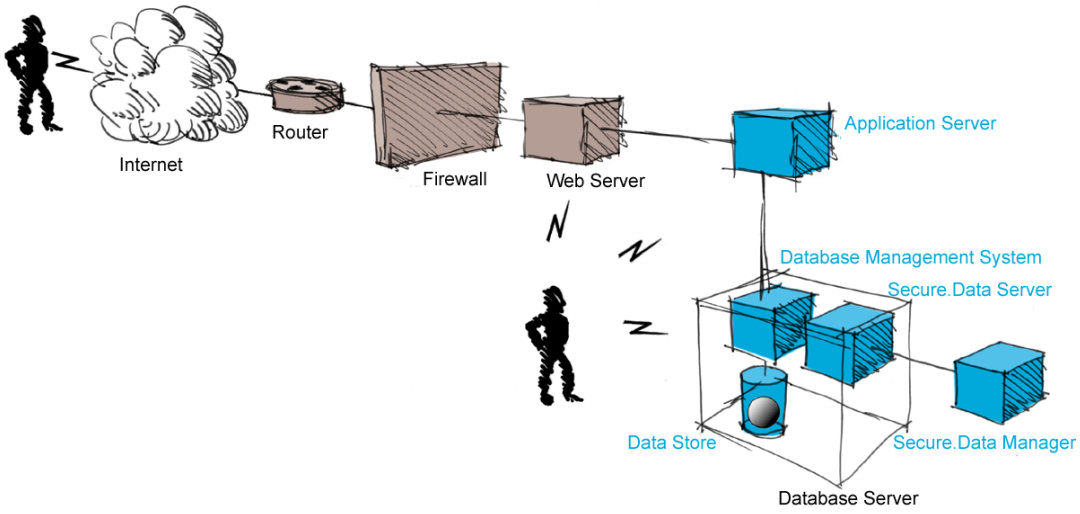
protegrity is an information-security company specializing in the encryption of databases. Protegrity's database-protection solution, **Secure.Data**™, is designed to selectively target and protect the privacy, integrity and security of our clients' most valuable and sensitive information. This unique technology is the only system of its kind to encrypt and secure information within a database itself, at the data-item level.

Protegrity's Secure.Data product suite uses role-based security parameters to enable selective encryption and access to user-specified data in various enterprise databases. Clients use our technology for a broad range of applications, including:

- Manufacturing – where sensitive bills of material need special protection;
- Finance – where analysts and investment bankers require separate access/clearance to different information resident in the same database;
- Electronic Commerce – where vendors must encrypt customer credit-card numbers gathered from Web transactions and stored in their databases;
- Healthcare – where private patient records must be protected from misuse or destruction;
- Government – where classified and highly confidential information requires the most advanced security measures.

Protegrity's products also provide unique solutions to the common security concerns shared by many businesses, such as the protection of payroll information, social security numbers, HR records or uniquely sensitive records that warrant restriction to any unauthorized personnel, including technical administrators.

Protegrity is expert in the implementation of scalable and manageable data-level security solutions that are platform independent. Through our ongoing relationships with leading hardware, software, database and security vendors, we ensure that the Protegrity solution can be integrated with existing technologies, thus protecting our clients' IT investments. The company's team of specialists represents a unique combination of technical skills in the areas of database architecture, client/server computing and public-key cryptography. Headquartered in Stamford, Connecticut, Protegrity has engineering, sales and support operations in the U.S. and internationally.



The Threat

The rise of Internet communications has fueled enormous, but largely misplaced, concerns about information security. The common misconception is that data traveling over the Internet can be intercepted by nearly anyone with a PC and a modem. In fact, these security risks are highly exaggerated. The Internet consists of a vast number of switches, routers and pathways over which data is dissected into many small packets and transmitted over multiple virtual paths. The likelihood of data being intercepted as it winds its way through various network infrastructures is remote, due both to the speed and complexity of these networks.

Sensitive data, such as credit-card information or corporate formulae, is far more likely to be attacked where it resides, i.e., the database where the information is usually stored. Industry statistics show this to be true. The vast majority of attacks target data repositories, as was the case reported for one Web electronics retailer.

Hackers were able to steal from the company's archives nearly 8,000 invoices for online credit-card orders and a 15MB inventory database.* Such attacks frequently originate internally, i.e., through an organization's own intranets. In fact, internal breaches of security are more likely, and are usually more sophisticated and dangerous, than attacks from outside an organization. In a 1998 Information Week Security Survey, respondents reported that their biggest threats are internal, with 58 percent of the surveyed firms indicating that one or more authorized users abused their systems in the past year.**

Most existing security systems consist of firewalls that are intended to protect private networks from external penetration. A firewall is the electronic equivalent of a chain-link fence that isolates an internal network from the outside world, i.e., the Internet. However, once the firewalls are compromised and the network is penetrated, the database itself is completely vulnerable. And while there are a growing number of products positioned as "all-in-one" enterprise-security solutions, a single enterprise security solution does not exist.

The Solution

Protegrity's solution protects mission-critical information from inadvertent, malicious and premeditated unauthorized access. In today's networked world where multi-tiered architectures serve as the vehicles for distributing information, organizations no longer know for certain where their data may eventually come to rest, in whose hands, and in what state. The only way to be certain that information is accessed by designated, authorized parties, and is not altered or obtained without approval, is by individually targeting specific data items and wrapping them with a strong layer of security.

Protegrity's Secure.Data product suite provides organizations with a flexible means of protecting corporate information, without having to change the way they work. Our unique approach allows companies, for the first time, to apply their existing security policies to the information at risk. A problem common to most companies is the lack of available solutions that enable them to directly apply and enforce their security policies to the data they deem sensitive. Most security policies are built around data that auditors have assigned a risk level, along with a level of financial loss. It is for this reason that we believe the majority of security solutions can be divided into one of two categories; those that implicitly secure data as infrastructure solutions, and those that directly secure data. Because security policies are built around data and not infrastructures, we believe that our Secure.Data represents a true asset in the way companies rely on their data.

Secure.Data is differentiated by its granular data-protection technology, which is designed to encrypt individual data elements within a database. Protegrity's solution assumes that network defenses can be compromised. It is not intended to supersede other security technologies such as network layer firewalls and operating-system protection, but represents the core element of a complete enterprise information security solution.

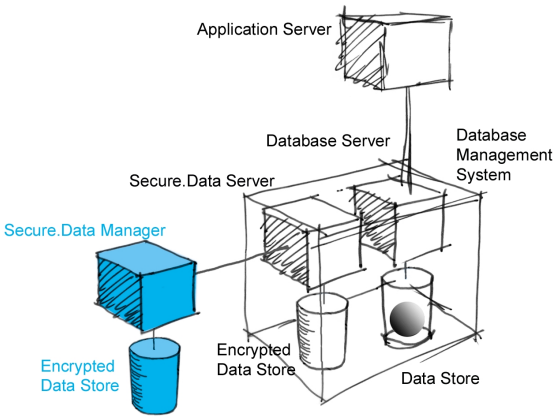
Secure.Data Product Suite

Secure.Data actively secures enterprise databases with selective encryption of sensitive data at the column level, combined with a unique process of access control based on user roles and workgroups. The Protegrity system also provides a centralized console for control, administration and management of data security policies and procedures. Secure.Data operates in a distributed environment across various platforms and databases, including Web and Internet-enabled database applications.

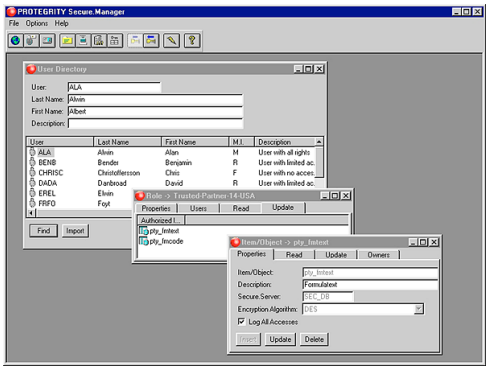
The Secure.Data product suite includes the **Secure.Data Manager**™ and **Secure.Data Server**™ modules.

Secure.Data Manager

Secure.Data Manager is the central point of control for administration and management of an organization's security policies and procedures. This component of the Secure.Data product suite is where the security official defines user settings; assigns roles, workgroups and data-access privileges; specifies the data to be encrypted; and selects algorithms, keys and other security parameters. Once defined in Secure.Data Manager, the security policy or updates to the policy are communicated in a secure way to Protegrity's Secure.Data Server environment for enforcement at the database level.



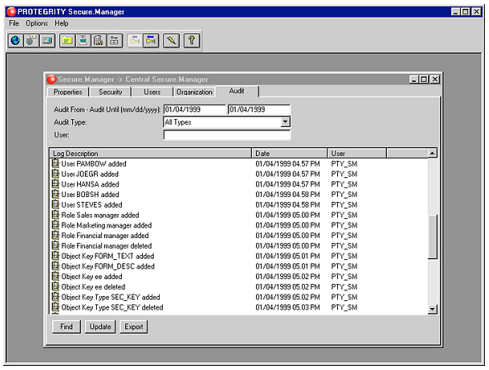
Secure.Data Manager Advantages



Protection Secure.Data Manager operates in its own self-secure encrypted environment, protected by strong authentication that ensures the confidentiality and integrity of all Secure.Data security parameters. Secure.Data Manager runs on a workstation separate from both application and database servers.

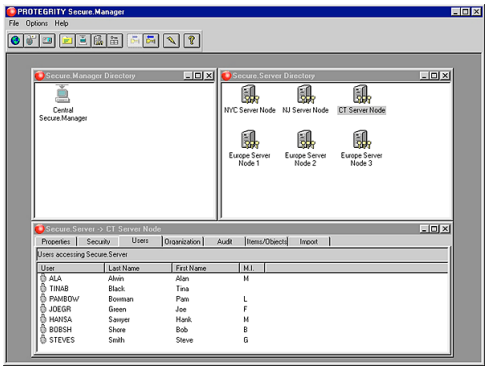
Simple User Interface Secure.Data Manager's graphical user interface incorporates the latest Windows techniques, such as "drag and drop" and "browse and pick." The easy-to-use GUI greatly simplifies implementation and management procedures, such as assigning access privileges and choosing data-protection methods.

Audit and Reporting Encrypted logs are produced to track both the Secure.Data Manager administrator's activities and Secure.Data Server activities around protected data, such as records of changes to the security policy and unauthorized access attempts. Real-time auditing ensures non-repudiation of transactions on sensitive information and is independent of the DBMS audit mechanism. Secure.Data Manager also includes a report generator with various templates that can be tailored by the security operator and exported for use.



High Granularity By using role-based access control and multilevel security, Secure.Data Manager allows operators to define user roles, workgroups, access rights and encryption requirements down to the data-item level.

Single Point of Control Unlike other security systems, Secure.Data does not require security operators to update security parameters for various servers individually. Secure.Data Manager's centralized administration allows operators to maintain the integrity of all Secure.Data policies and configurations from a single location.



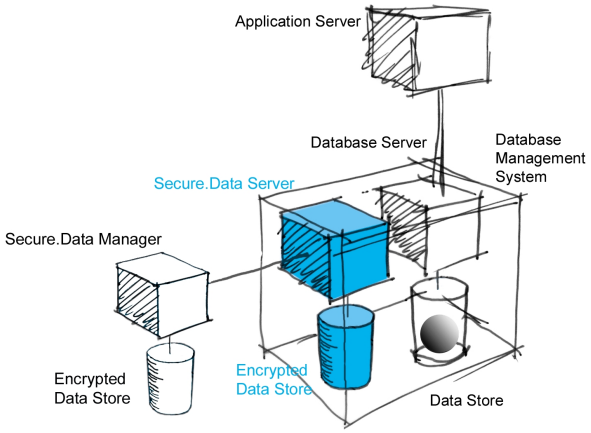
Secure.Data Server

Protegrity's Secure.Data Server is the active component of the Secure.Data suite of security software and performs real-time security processing for our clients' sensitive information. Secure.Data Server plugs into the database as a security middleware component. As the run-time portion of the security system, Secure.Data Server enforces the security procedures and policies that have been defined in Secure.Data Manager.

Working within the Database Security Environment

Protegrity's Secure.Data system enhances the security architecture of enterprise databases by adding role-based access control and selective column encryption to protect specified data within the database. This layer of security also extends across a distributed database environment. As a plug-in to the DBMS, Secure.Data Server is application blind.

Secure.Data Server Advantages



Encryption Options Applies column-level encryption using the same or separate keys per column and standards-based encryption algorithms.

Granularity Enforces role-based access control and multi-level security down to the column, row and data-item level. Each item or object of sensitive information is effectively wrapped in a chosen level of security.

Compatibility Protegrity is committed to maintaining Secure.Data Server's compatibility with future versions of leading databases. New applications can also take full advantage of the security policies defined in the Protegrity system.

Transparency Secure.Data Server enforces the security policies defined in Secure.Data Manager without modifying the database structure, thus allowing legacy applications to access the database as they always have.

Ease of Implementation Seamless integration with the database environment through the use of standardized interfaces that add programmability and extensibility at the database tier.

High Performance Secure.Data Server protects only sensitive organizational data, introducing a minimum of performance overhead, while providing maximum security.

Secure.Data Server Minimum Requirements

20 MB available hard-disk space

225 MB available memory

Oracle, Informix, Microsoft SQL Server, IBM DB2, Sybase

Operating system: IBM AIX, SUN Solaris, HP-UX, Windows NT, Windows 2000

Secure.Data Manager Minimum Requirements

20 MB available hard-disk space

32 MB available memory

Operating system: Microsoft Windows NT 4, Windows 2000

For more information, please contact:

protegrity
info@iq-net-works.com