Secure The Data, Not Just The Underlying Infrastructure

摘譯自 -- May 11, 2006, Forrester Research

EXECUTIVE SUMMARY

New business pressures mean that organizations need to share data across ever-widening organizational and geographical areas. However, at the same time, they are increasingly accountable for ensuring that data is properly protected, even when it resides on infrastructure over which they have little or no control. This has led organizations to look at ways to secure the data itself, rather than just the infrastructure that holds and transports it. What do they find? The technology to help them is still embryonic with only a few vendors offering solutions. Mainstream migration to a datacentric security model will take five years to evolve, but today, companies need to define a strategy for atacentric security starting with information classification and data encryption.

新的市場壓力使得企業必須在跨組織與跨地區間分享資料，這也增加了確保資料安全的責任，尤其是在很少被控管的基礎設施上，這使得企業必需去尋找以保護資料爲主的方案，而不再僅僅是著墨於基礎設施而已。他們找到什麼了 ？目前能夠幫助他們的技術都還在萌芽期，只有少數的廠商能提供解決方案。這種以資料爲中心(Datacentric)的安全方案將需要五年時間的演進才會成爲主流，但今天，企業必須開始去設立一個以資料爲中心的安全策略，可以從資訊分類與資料加密開始著手。

NEW BUSINESS DEMANDS RENDER OLD SECURITY MODELS OBSOLETE

- Increased data accountability.
- More intellectual property fluidity.
- Highly distributed work environments.

Past Security Approaches Have Concentrated On Infrastructure Rather Than Data

- Leave data alone, and have the underlying infrastructure to secure it.
- Use blocking and tackling to enforce policy.
- Rely heavily on contracts and processes.

THE FUTURE OF SECURITY IS DATACENTRIC

- Infrastructure-centric measures: Firewall, VPN…

- Datacentric measures. Datacentric measures, on the other hand, protect the information directly, independently of the infrastructure components that store, transmit, or process it. One example is an encryption solution, which provides the means to encrypt a piece of data; and wherever that data travels, it remains encrypted. Only when an authorized user obtains the keys to decrypt the data does it become usable. Datacentric security measures have been less common in the past, but will be a central part of most organizations' security strategies in the future.

Datacentric Security Will Become The Primary Mode Of Infrastructure Protection . . .

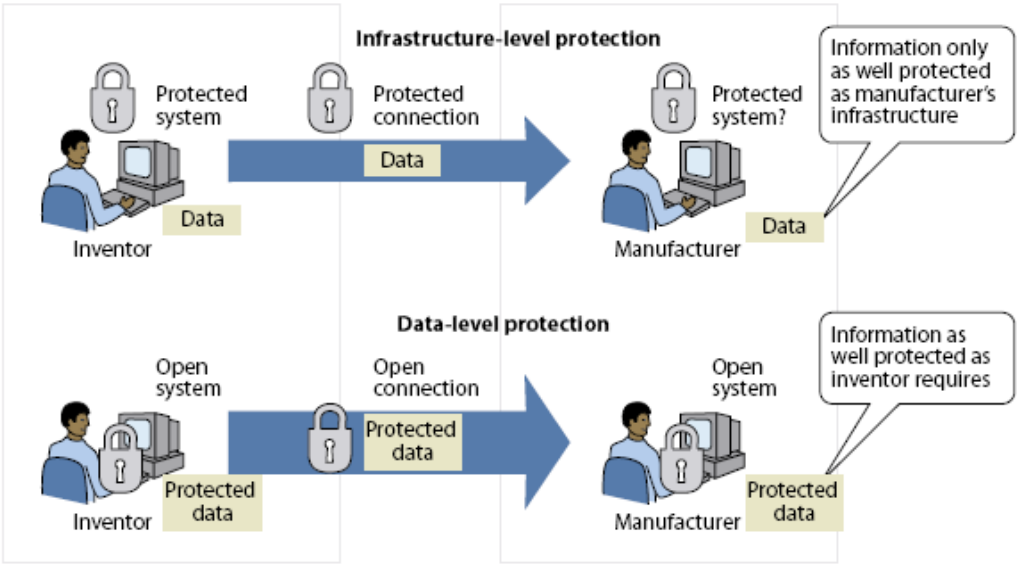
place a greater emphasis on securing the data itself, and use the infrastructure as a secondary layer of protection rather than as a primary layer

以 Datacentric 爲最優先, Infrastrature 做第二層保護

- Make security attributes travel with the data itself.
- Enforce security policy at every stage in the information life cycle.
- Build security into the infrastructure from the ground up.

. . . And Organizations Need To Focus On Secure Design And Information Protection

Figure 1 Data-Level Protection In An Inventor-Manufacturer Relationship



394438 Source: Forrester Research, Inc.

Figure 2 Infrastructure Security Gets Complemented By Data Security

Old security model	New security model
Defensive, threat-protection-oriented	Securely designed from the ground up
Manual, audit-based policy enforcement	Automated policy enforcement
Focused on securing infrastructure	Focused on securing the data

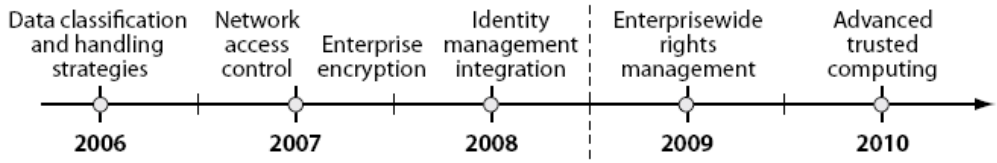
39438 Source: Forrester Research, Inc.

- Deploy more identity-driven security at the infrastructure level.
- Concentrate threat protection measures on critical systems.
- Adopt an enterprisewide approach to encryption.

A Datacentric Security Model Will Evolve Over The Next Five Years

- 2006–2008: Encryption, identity management, and network access control dominate.
- 2009–2010: Rights management and trusted computing enable true datacentric security.

Figure 3 Datacentric Security Timeline For Mainstream Organizations



39438 Source: Forrester Research, Inc.

A DATACENTRIC SECURITY MODEL IS A HARD TASK — BUT HELP IS APPEARING

Interoperability, Maturity, And Governance Are Barriers To Greater Adoption

- **Datacentric technology is immature.**

- **Existing solutions are not interoperable.**
- **Organizational slowness hinders wholesale changes.**

Vendor Community Rises To The Data Security Challenge

- **Encryption vendors focus on solutions that span platforms.**
- **Entrust addresses information classification and handling.**
- **Trusted computing consortia address hardware-level security.**
- **Adobe and IBM look to secure the collaborative design process.**

R E C O M M E N D A T I O N S

- **Start with information classification.**
- **Then, move onto roles.**
- **And get a handle on your encryption strategy — start with homegrown applications.**

W H A T I T M E A N S

Greater control over information will allow data owners to share it with the parties they trust, safe in the knowledge that they won't accidentally or maliciously share it with anyone else.

- **Overcoming the privacy pandemic will spur online commerce.**
- **Security audit budgets will get slashed and burned.**