

# ***Sensitive Data Management in Financial Systems***

Mike Gurevich, President & CEO  
Inventigo Corporation  
[www.inventigo.com](http://www.inventigo.com)

**INVENTIGO**

Peter Latscha, President & CEO  
uGuard Corporation  
[www.uguard.com](http://www.uguard.com)

 **uGuard**<sup>®</sup>  
Bulletproof Net Privacy™

# ***Spending Profile: Overall***

---

- Organizations spend a medium of 6% of their IT budget in security implementations.
- The worldwide market for information security services (including consulting, integration, management, and education and training) in 1998 was \$4.8 billion. This figure is expected to grow to \$16.5 billion by 2004 with security management services expected to be the fastest growing sector.

IDC's European Security Services Protecting e-business  
IDC's Plugging the holes of e-commerce

# Spending Profile: Financial Services

---

Technology spending:\*

- 2002 U.S. technology spending highest in Financial Services, at \$108.5 billion (3.1% increase from 2001)
- Banking has highest percent increase across all industries at 18.1% increase from 2001

Security budgets are ballooning:

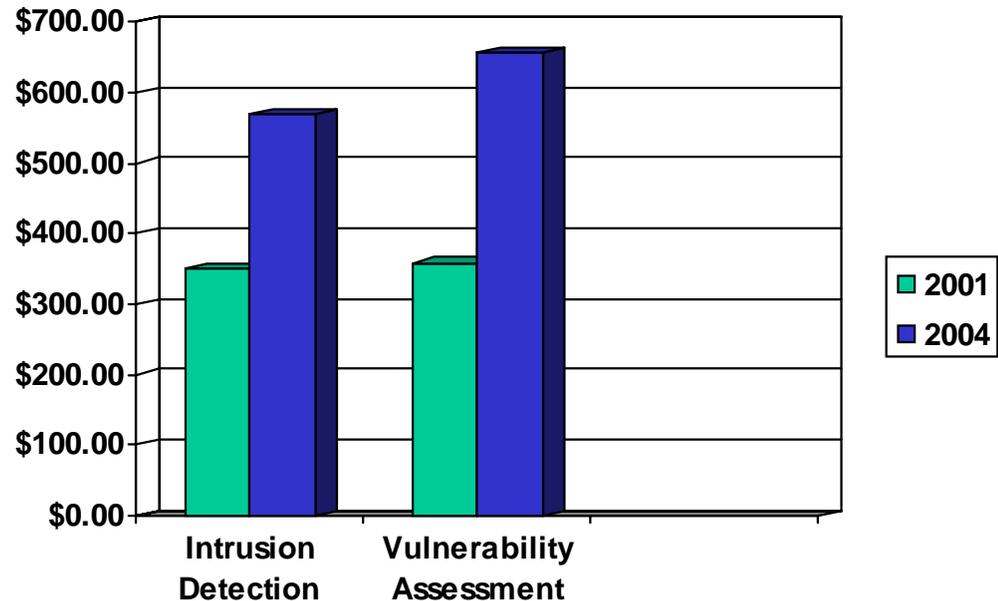
- Estimated IT security spending will grow 43% in 2002\*\*
- IDC's research indicates the financial services sector will continue to represent the single-largest source of security spending, growing from \$848 million in 2000 to >\$2 billion in 2005

\* Barron's Jan'02

\*\* J.P. Morgan estimate

# Is Money Well Spent?

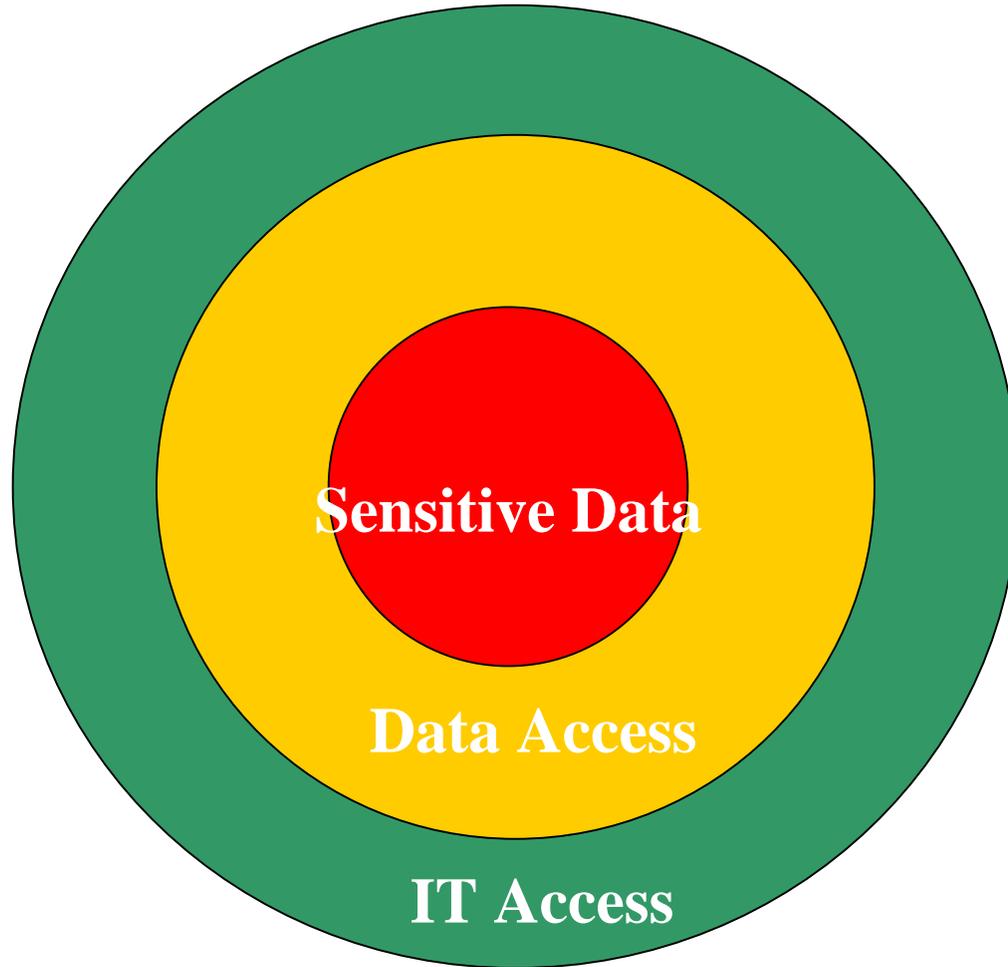
Intrusion Detection and Vulnerability Assessment (IDnA) is one of the highest growing (CAGR of 26% through 2004) segments of the fast-growing security market.



IDC's Plugging the holes of e-commerce

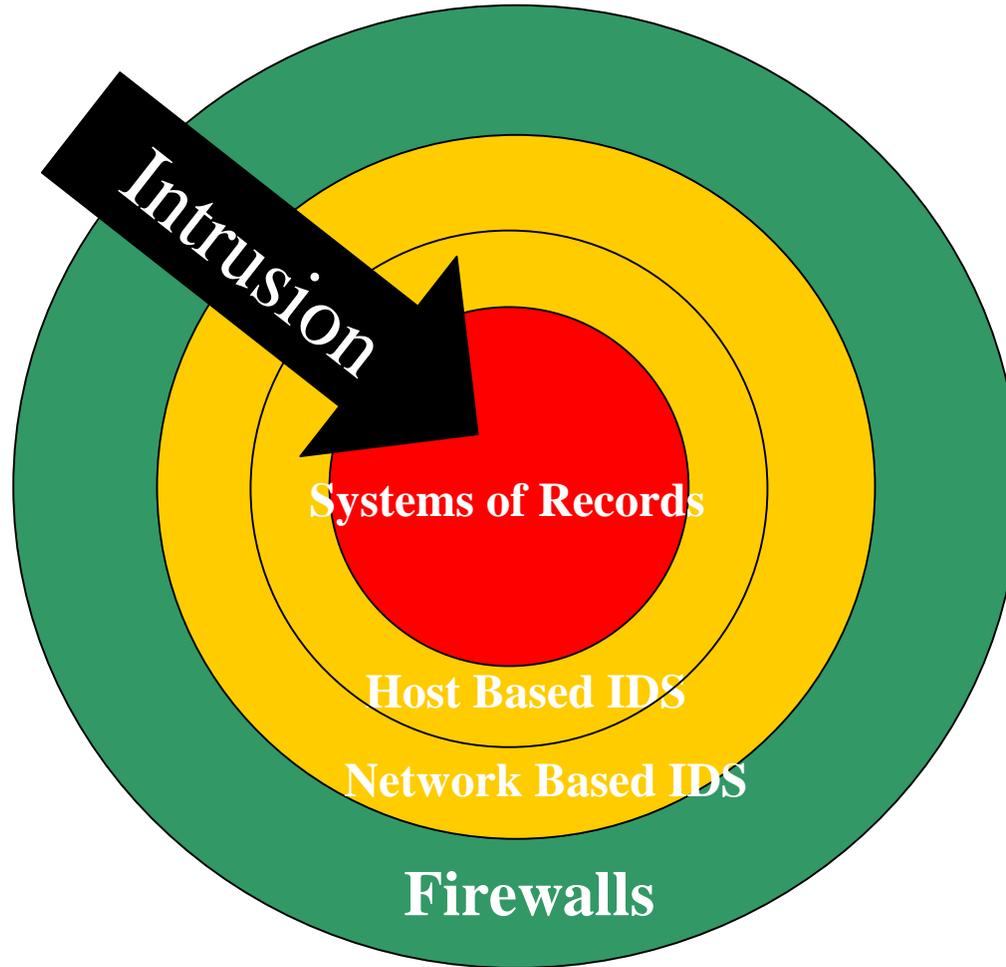
**Do Financial Institutions get the expected ROI from IDnA?**

# ***The Access Onion***



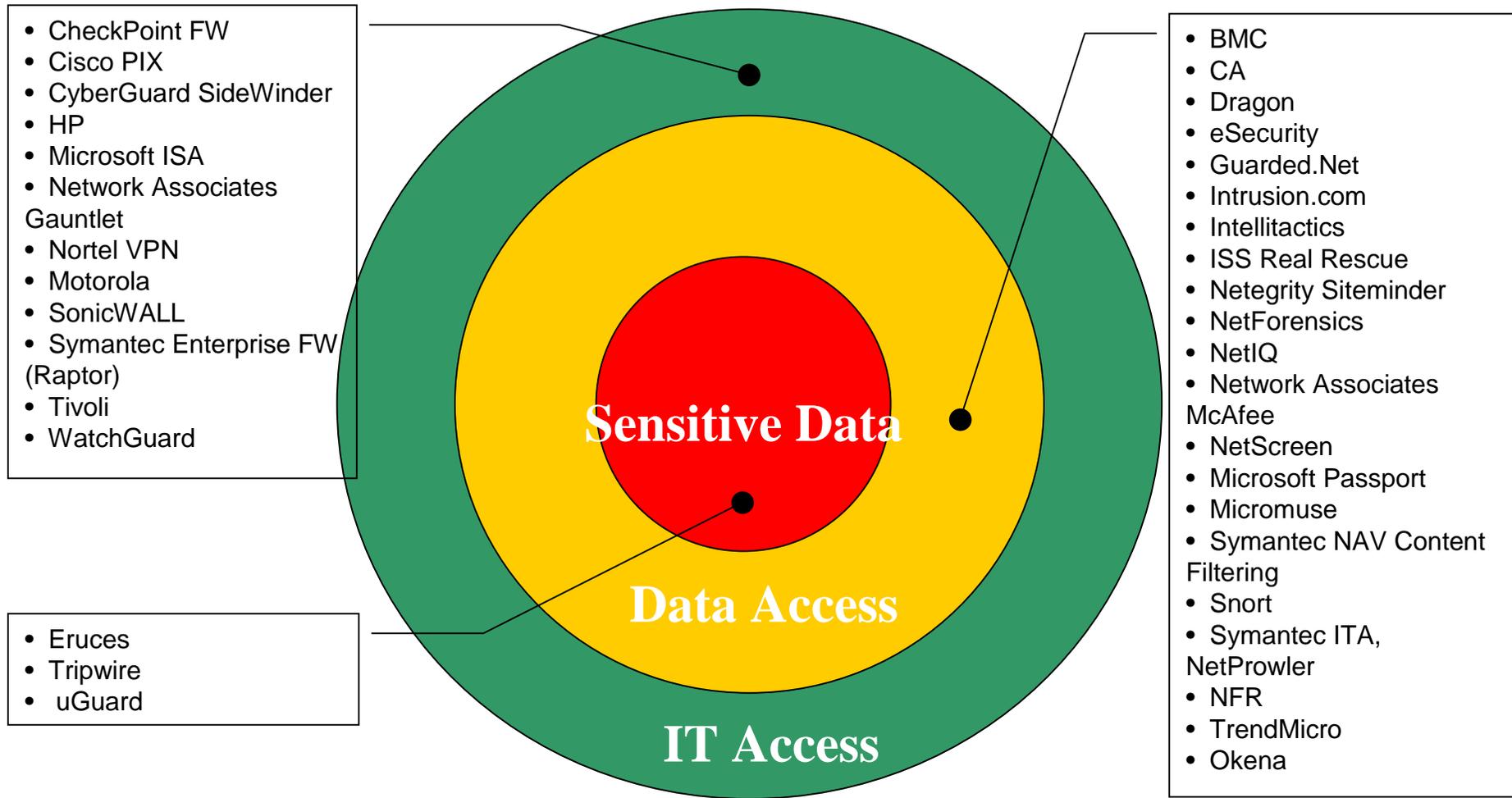
***Majority of attacks happen inside the organization***

# *The Security Onion*



***Perimeter defenses miss majority of attacks***

# The Security Onion: Problem of choice



**Too many players to choose from in IT and Data Access**

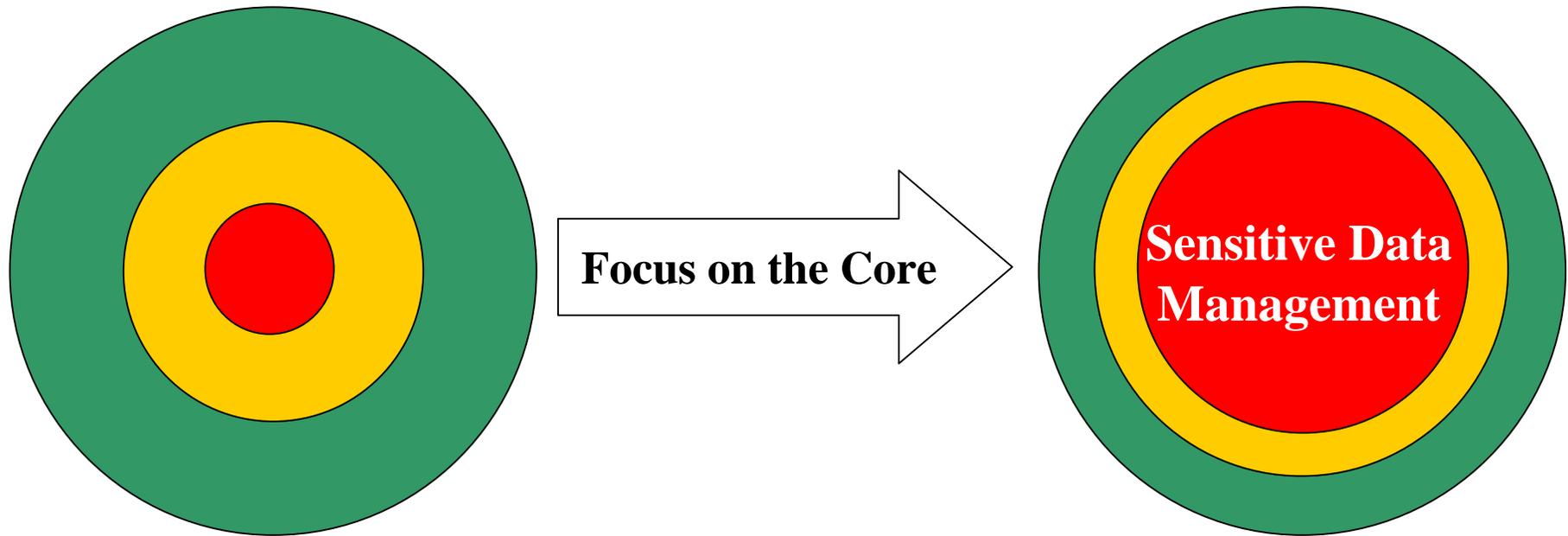
# *The Security Onion: Problem of choice cont'd*

Very crowded market...

- Arcot Systems
- iLumin
- Covalent
- Entegritty
- GeoTrust
- NTRU
- Digital Media On Demand
- DocuTouch
- Lockstart
- Shym Technology
- CyberSafe
- enCommerce
- ValiCert
- NetScreen
- OneSecure
- Spearhead Technologies
- iPass
- OpenReach
- Arula Systems
- Ecutel
- Exario
- IP Dynamics
- Aliga Networks
- Aventtail
- GeoVideo
- Imperito Networks
- Indus River Networks
- IPNet Solutions
- Network Alchemy
- RedCreek Comm
- Ethentica
- Courion
- Interlink Networks
- Authen Tec
- Authentor Systems
- Bionetrix
- eTrue
- Verdicom
- WildCard Systems
- Innoventry
- Interlink Networks
- @Stake
- Riptech
- Telenisus
- Counterpane
- Guardent
- Totally
- SecureWorks
- Foundstone
- TrueSecure
- METASeS
- NETSEC
- Para-Protect
- SiteSmith
- AlterEgo
- Zantaz.com
- Digital Paper
- ecVision
- MicroVault
- eCash Technologies
- NET delivery
- Sigaba
- Intralinks
- iWitness
- PentaSafe
- ProactiveNet
- Recourse Technologies
- ClickNet Software
- NetBotz
- Qiave Technologies
- Quatys
- Netwhistle.com
- Okena
- Sanctum
- Shwoo
- Tripwire Security Systems
- Zone Labs
- Securant Technologies
- Disappearing Inc.
- Finjan Software
- Internet Dynamics
- Vyou.com

Note: some companies are acquired

# ***Trend: Transformation of Security Focus***



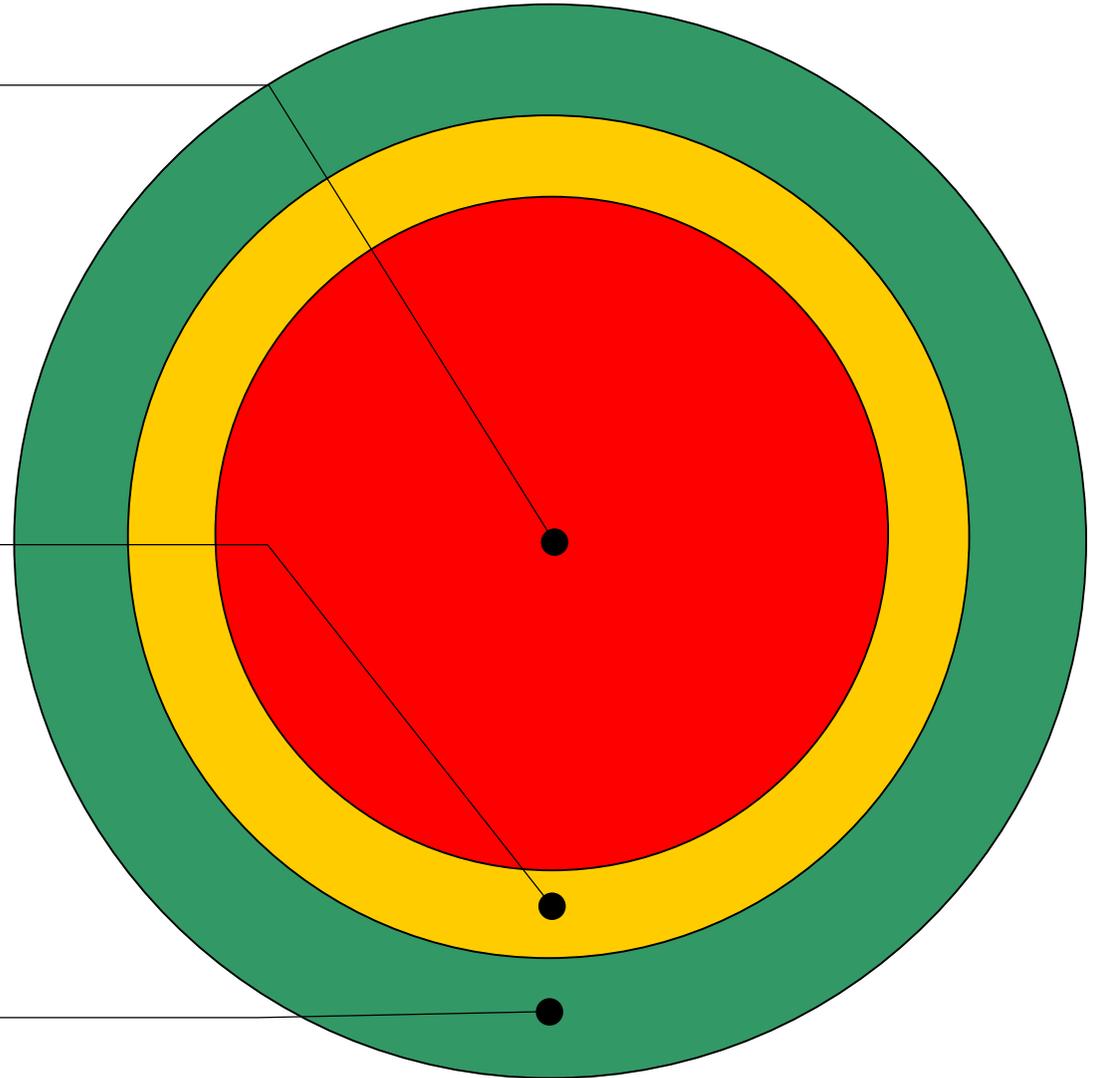
***Emerging Market for Sensitive Data Management***

# *The Need for Transformation*

**Sensitive Data Management**

**Data Access Management**

**IT Access Management**



## *The Need for Transformation in IT Access Management*

- **Majority of attacks happen inside the organization**
- **Perimeter defenses miss majority of attacks**
- **Too many players to choose from**
- **Growing complexity of IT environments diminishes ROI**

# ***Unsolved IT Security Issues Drive Transformation***

## **Where is sensitive data located and how securely is it managed?**

- Common practice: secure IT environment but not the data
- Intrusion by insiders
- Vulnerability compounded with universal data repositories or 'wallets'

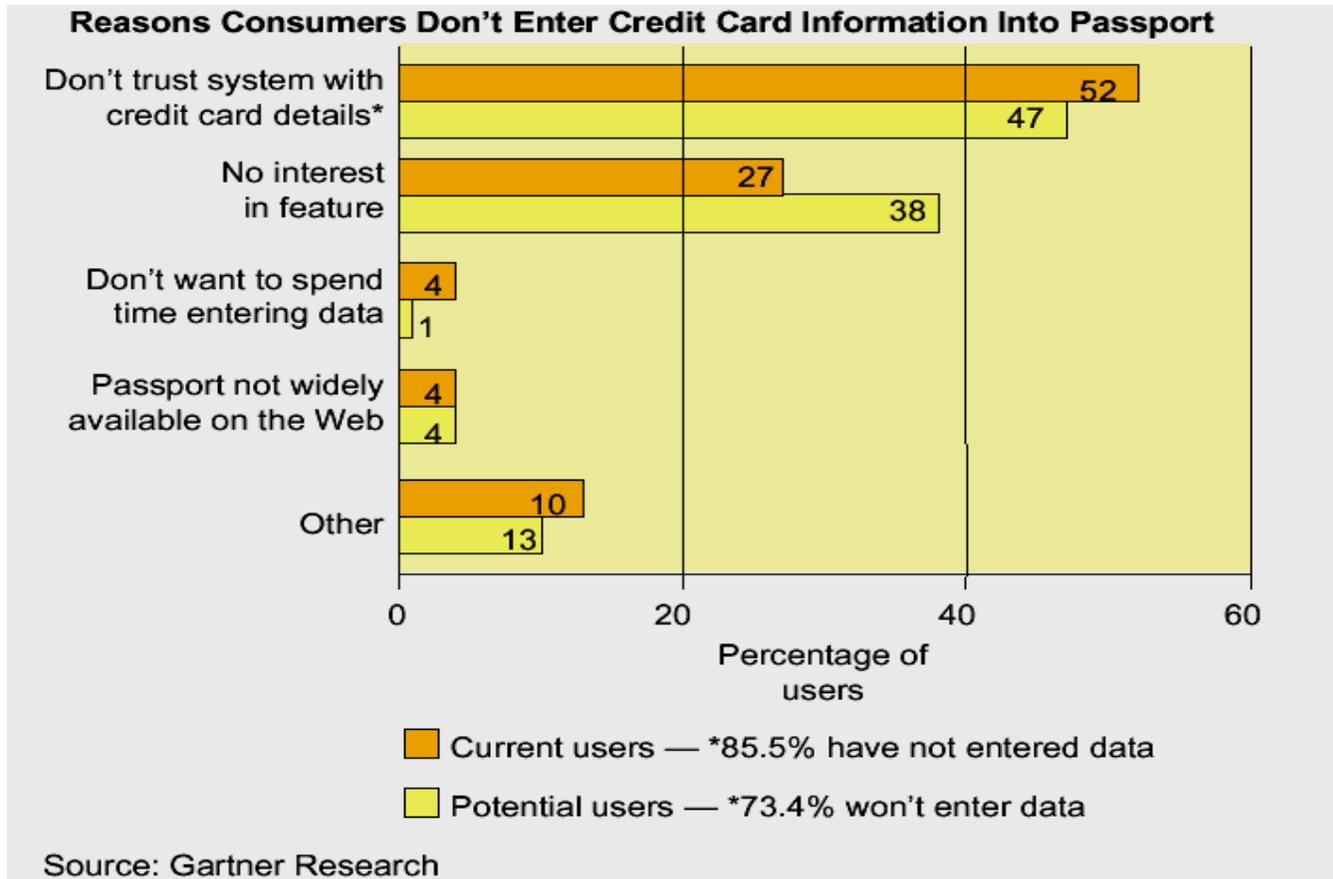
## **How secure is data in transit?**

- Often not encrypted
- Many solutions rely on SSL (Secure Socket Layer) to provide data privacy
  - SECURITY ISSUE: SSL does not provide end-to-end security: data in the clear at intermediary systems

***DATA AT REST AND DATA IN TRANSIT IS AT RISK***

# The Need for Transformation in Data Access Management

Web services primed to be the next big development for Internet-based applications and transactions but adoption is hindered because of unsolved security issues:



# ***The Need for Transformation in Data Access Management***

**Currently 165M registered Microsoft Passport accounts worldwide**

- **Only 25M will actively use Passport for single sign on by 2003\***
- **Only 2M entered credit card info into Passport**

## **Liberty Alliance**

- **Focus on security issues**
  - **Companies control their data**
  - **Data exchange via open standards; no single central authorization**
  - **Authentication via different devices**

\* - Gartner Research, October 2001

# ***Unsolved Net Privacy Issues Drive Transformation***

**Subscribers of all Web based services want their identity and data guarded when online**

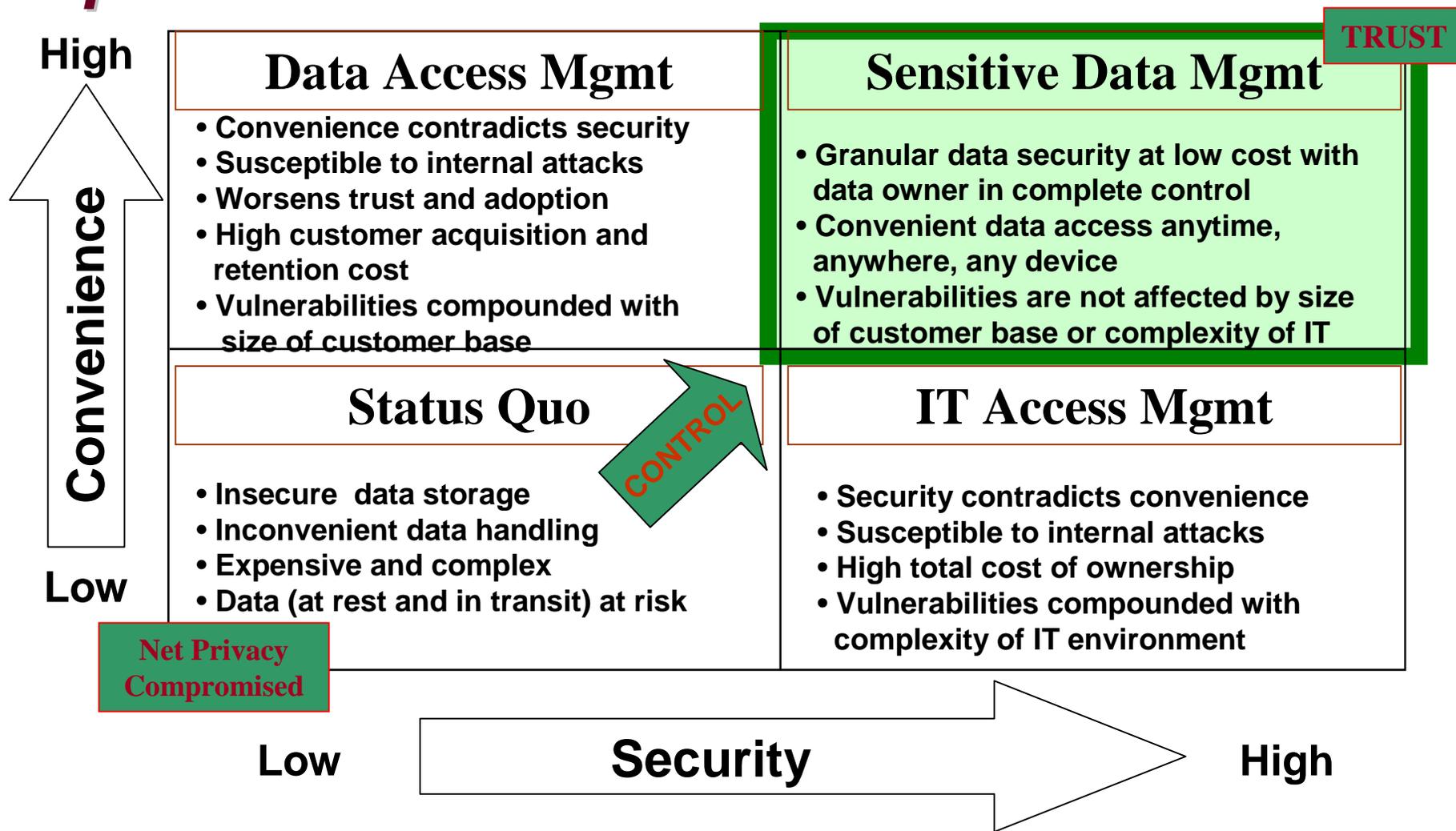
- Anytime, anywhere, on any Internet enabled device
- Financial services particularly affected

**Subscribers demand secure authentication and secure access to their personalized services**

- Currently experience insecure storage and inconvenient handling of their sensitive data

***Internet users justifiably fear their Net privacy is compromised***

# Expected Outcome from the Transformation



**Emerging Market for Sensitive Data Management**

# ***Crossing the chasm***

---

What is needed

## **Granular Data Security**

- Resilience to internal and offline attacks
- Security for data at rest
  - “Client-present” cryptography
- Security for data in transit
  - Secure Dynamic Data Routing

## **Interoperability**

- Interoperable Key Reference

## **Verified Domain Specific Usage Profiles**

# ***Crossing the chasm: OMG in the lead***

---

## Approach

### **FDTF (other domains)**

- **Profile Definitions**
  - **Passport**
  - **Secure DDR**
  - **Secure log**
  - **etc**
- **Deployment and validation**

### **Sec SIG**

- **Core Components**
  - **Interoperable Key Reference (IKR)**
  - **Cypher Data Type (CDT)**
- **Profile Convenience Interfaces**
- **Endorsement**

# *Crossing the chasm: Profile example*

---

## Profile for Secure Dynamic Data Routing

### **Originator:**

- **Data Elements:** produces the Data Element(s) in clear text. Sufficient for DDR level of granularity.
- **Keys:** generates individual Key(s) for each Data Element.
- **IKRs:** acquires IKR(s). Preferably generates IKR(s) locally.
- **Key Store:** stores Key(s) in a Key Store referencable by IKR(s). The Key Store should resolve IKR collisions for locally generated IKRs.
- **Encryption Keys:** Preferably generates Encryption Key(s) locally involving the Key(s).
- **Cypher Elements:** individually encrypts the Data Element(s) using the Encryption Key(s).
- **Message:** contains Cypher Element(s) together with (or means for obtaining) the IKR(s).

# *Crossing the chasm: Profile example cont'd*

---

## Secure Dynamic Data Routing

### **Terminator:**

- **Message:** receives the Cypher Element(s). Receives/obtains the IKR(s).
- **Key Store:** Retrieves Key(s) from the Key Store via the IKR(s).
- **Decryption Keys:** Preferably generates Decryption Key(s) locally using the retrieved Key(s) from the Key Store.
- **Data Elements:** Decrypts the Data Element(s) using the Decryption Key(s).

# ***Crossing the chasm: OMG in the lead***

---

## Next Steps

### **RFP “Sensitive Data Management for Financial Systems”**

- Core Components
- Profile Definitions

### **First to Focus**

- Core Components: Interoperable Key Reference



**Thank You**

*mikeg@inventigo.com*  
*www.inventigo.com*

*platscha@uguard.com*  
*www.uguard.com*