

There's a Hole in the Bucket:
A Framework for Addressing Data Leakage
...Dear Liza...

Joshua Corman
Eric Hanselman, CISSP



IBM Internet Security Systems

Ahead of the threat.™

Audience Poll

- **Who has been affected by a breach/leak?**
- **Who has had a breach/leak?**
- **How many use boot passwords?**
- **How many use whole drive encryption?**
- **How many use email encryption?**
- **How many use any encryption?**



What's Your Motivation?

- **Operational Efficiency**
 - Choice to be better organized
- **Establish Trust**
 - Choice to earn Customer Confidence
- **Enable Expansion**
 - Choice to securely increase collaboration
- **Courage**
 - We've chosen to grow
- **Regulatory or Compliance**
 - The lawyers made me do it
- **Liability**
 - Loss protection made me do it
- **Catalyzing event**
 - The news/stock drop made me do it
- **Fear**
 - The devil made me do it...



The Data Leakage Problem

- **It's Big**
- **How Big?**
 - Really, really big...
- **Data is everywhere**
- **Lots of places to leak**



How Big is the Elephant?

Collaboration brings Complexity

Many Forms of data...

- Structured
- Unstructured
- Images
- Video, Voice

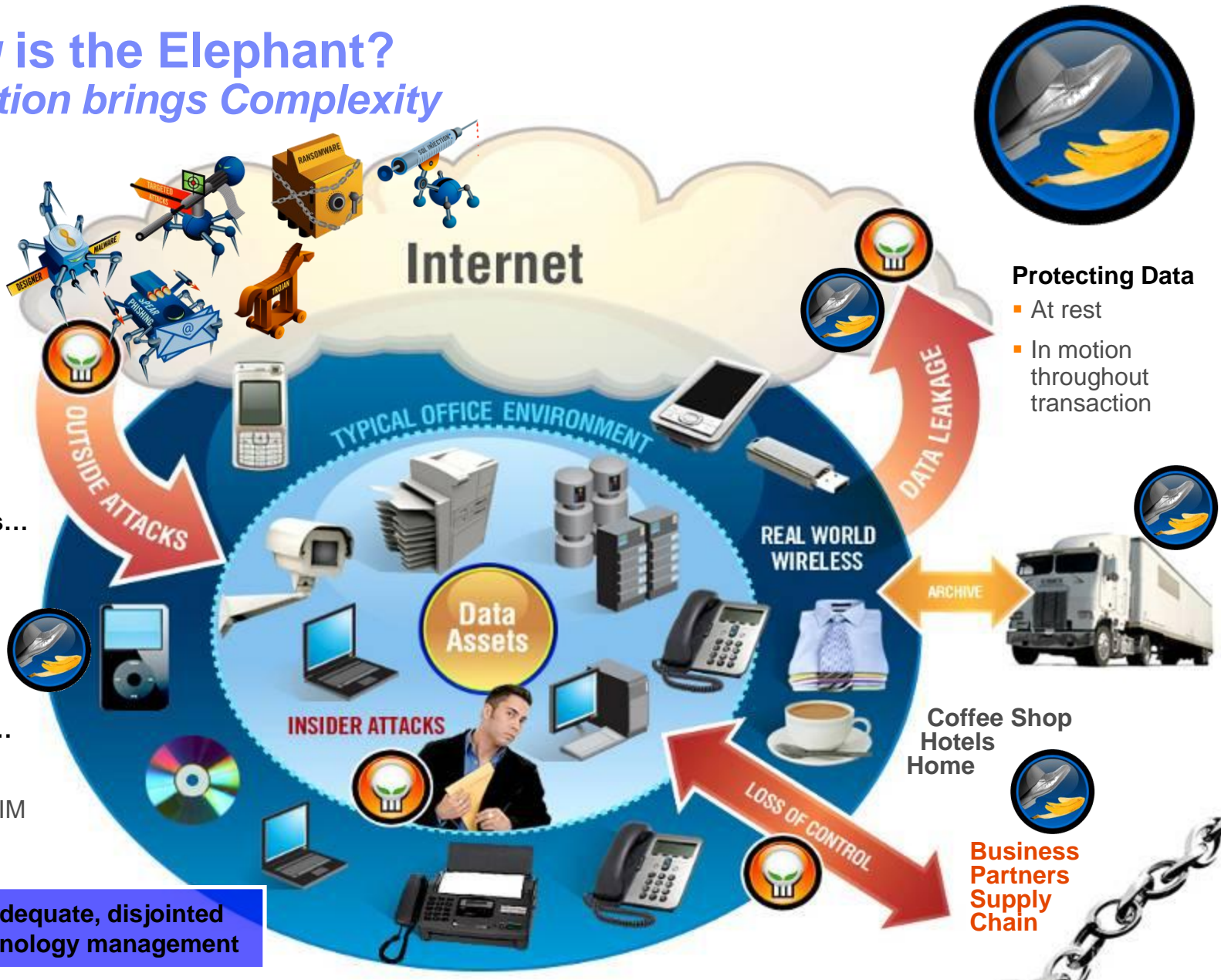
Stored in different ways on many devices...

- Cell phones
- Laptops
- PDA's, iPods
- Briefcases

With Many Forms of Travel...

- Digital
- Voice/audio
- Cut and paste, IM
- Paper, Fax

Inadequate, disjointed technology management



Who comprises this Elephant? *The Insider Threat*



Careless

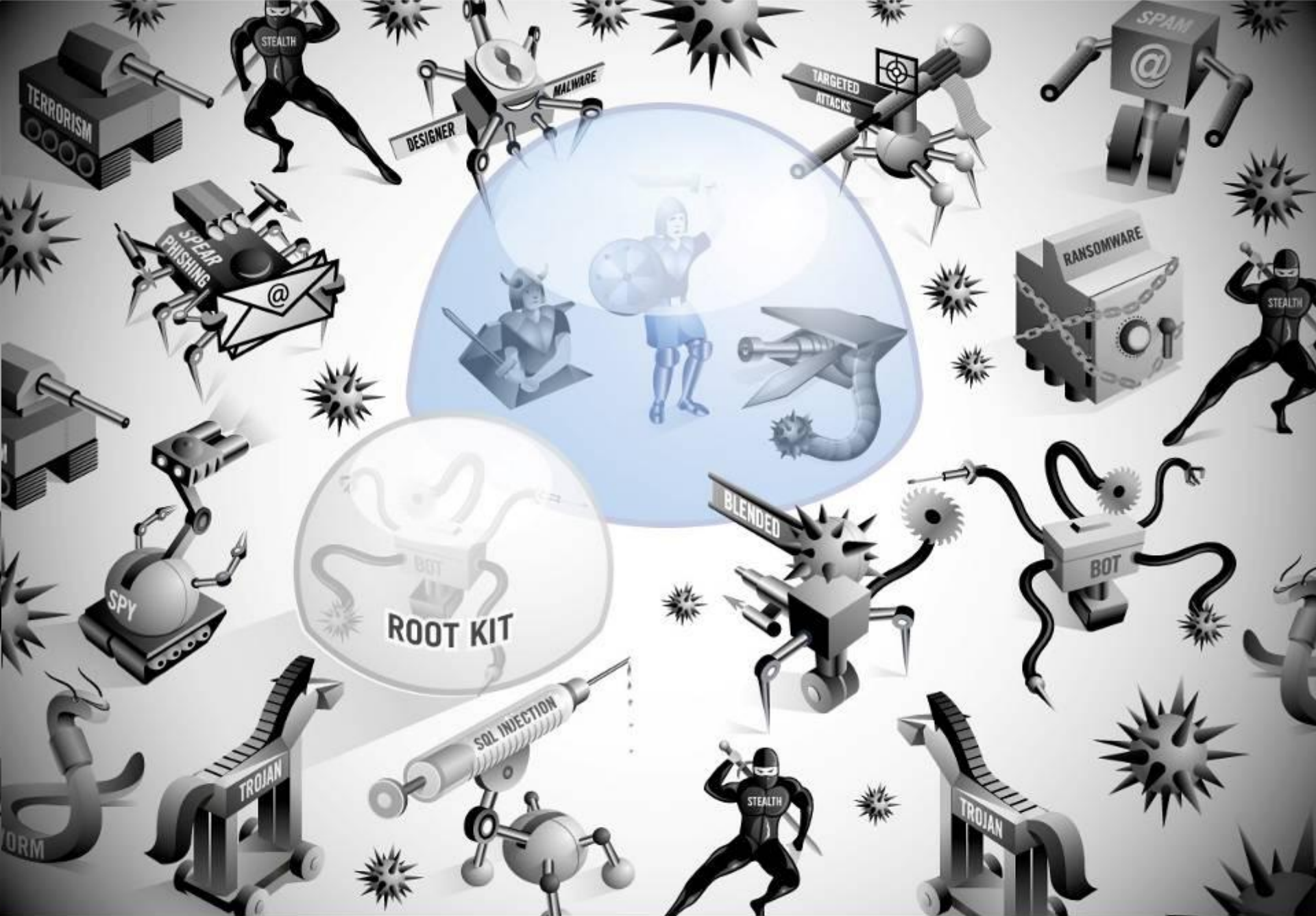


Malicious



CxO

- **Curiosity.**
 - Employee may try to hack into restricted areas to have a look around or to install spyware
- **Protest.**
 - Insiders with an agenda may use their access to company networks to blow the whistle on bad practices or take their story to the media
- **Lost productivity.**
 - Every minute workers spend watching porn or hunting for a new job on the company network costs shareholders money
- **Hostile work environment.**
 - Unseemly characters can abuse computer systems by using them to intimidate or harass their fellow employees through racism or sexual harassment
- **Revenge.**
 - Disgruntled workers may try to sabotage a corporate IT system from the inside
- **Malfeasance.**
 - Employees can use company networks to commit crimes such as identity theft or industrial espionage or to collude with vendors
- **Erroneous disclosure.**
 - Ignorance of proper procedures for handling data or technical errors may mean sensitive data is accidentally lost



The Outsider Threat – The Evolving Threat www.iss.net/evolvingthreat/

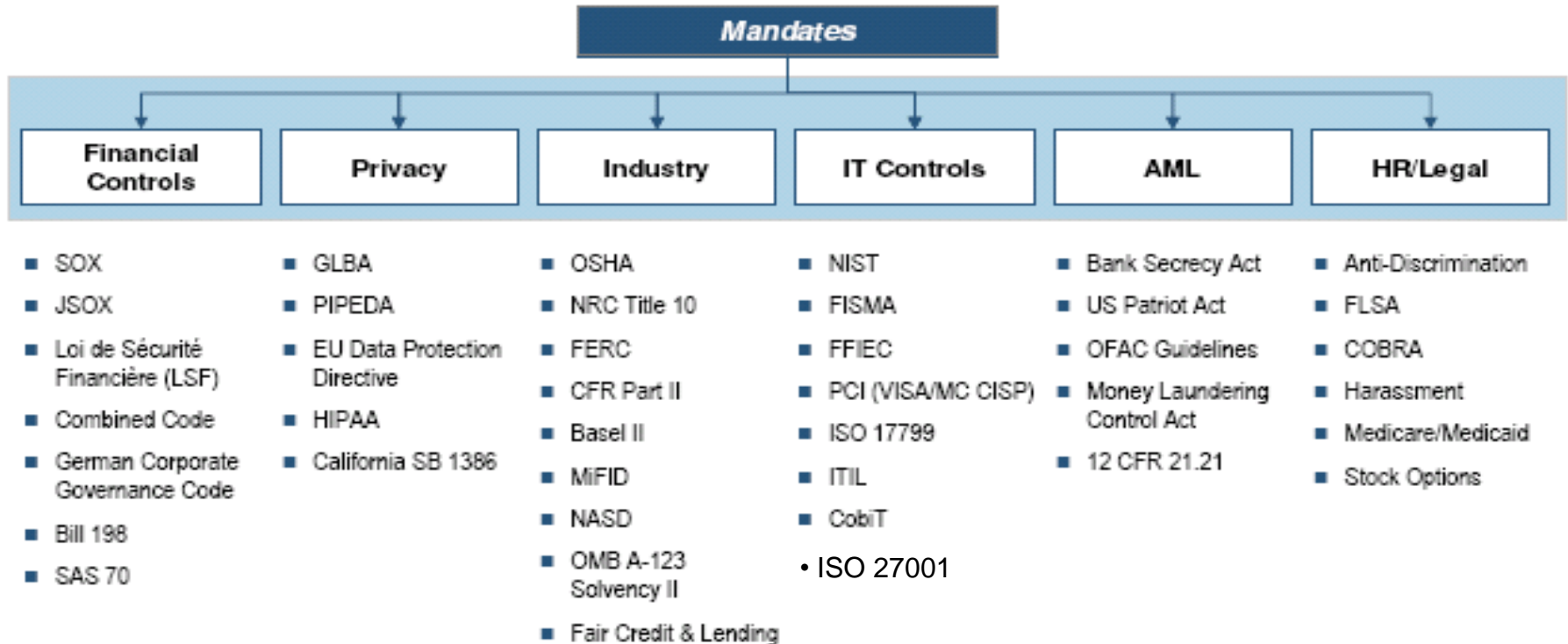
Why Should I Try to *Eat* an Elephant?

- Risks and liabilities are also large
- Larger security and process perspective
- Operational effectiveness
- Oh, and by the way....
 - Compliance!



Regulatory Mandates Are Growing Quickly

The average \$500MM corporation is subject to 35-40 major regulatory disclosure mandates



114,000 regulations introduced in US since 1981
- Forrester

And did we mention...?

Costs Associated with Data Loss are Significant

- **Direct costs** – include Internal investigation, Notification/crisis management, and Regulatory/Compliance
 - Average cost for each compromised record is \$186 *
 - The average security breach can cost a company between \$90 and \$305 per lost record**
- **Loss of future business**
 - 77% of 2,750 consumers polled said they would stop shopping at stores that suffer data breaches. ***
- **Class action lawsuits** ****

Action Against:	Potential Class Size:	Seeking Damages of: (rarely settle for full amount)	Potential Financial Exposure:
Verizon	2,000,000	\$21,000pp	\$42 B
AOL	500,000	\$ 1,000pp	\$.5B
Veterans Administration	260,000	\$ 5,000pp	\$ 1.3 B

- **Decrease in stock value**

* Average Data Breach Costs Companies \$5M, Network World – 11/02/06

** Latest Forrester Research Study

*** April 2007 report Javelin Strategy & Research

**** Tech/404® Data Loss Cost Calculator by Darwin

The Problem Might Seem Overwhelming

- Where to start?
- How to justify costs?
- Who owns this?

Have To Push Through Paralysis!



Step 0: Data Protection *Inverts* Security Thinking

- **Traditional thinking flows inward**
 - Fear used to be about outsiders getting in
 - *From the perimeter to the host*
 - Access denial is necessary, but insufficient
- **Data protection flows from point of use**
 - Data *must* flow to add value
 - Lots of directions at host
 - Fewer paths reach network perimeter
- **Our thinking has to adapt!**
 - It will feel unnatural
 - You will regress
 - This will take discipline and focus



This solution STARTS at the End-Point!

The Reverse Flow of Traditional Network Intrusion



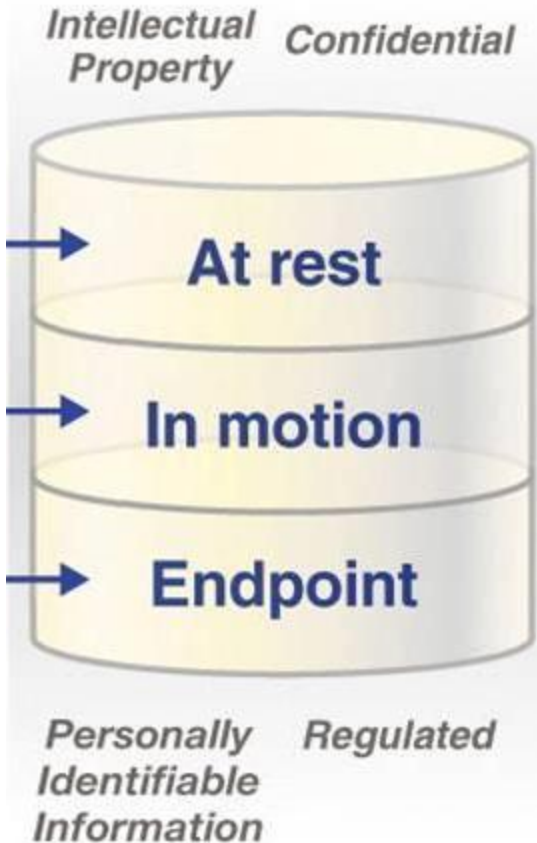
The Bank Robbery: Value Stolen

- You don't stop robberies with roadblocks 20 miles from the bank...
- And you can't reliably stop leaks at the perimeter



**ROADBLOCKS ARE SET UP AROUND
A 20-MILE PERIMETER**

Model 1: The *Locations* for Eating an Elephant



- **At rest**
 - The Servers
 - The Databases
- **In motion**
 - Data in transit
 - The well-worn points of egress
- **On the endpoint**
 - The “point of use”
 - Numerous points of egress
 - Full view of **Content** and **Context**



This model oversimplifies the problem space and encourages blind spots...

Easy is preferred – Effective is required

Model 2: The *Process* for Eating an Elephant

- **Assess:** Data At Rest

“Do I have intellectual property, confidential records, or personally-identifiable information that violates policy or government regulations and/or is on the verge of being compromised?”

- **Protect:** Data Usage at the Endpoint

*“Are there sophisticated ways to categorize my data, standardize my policies, and manage my data protection issues **at the point of use?**”*

- **Defend:** Data In Motion

*“Guarding my data had not been a problem, **but now I need manageable policies that defend while sharing critical info.** Internal threats are increasing.”*

- **Monitor:** Integrated Solutions

*“I have dozens of tools and am drowning in reporting & tracking info – **I have so much control that I am out of control.**”*

- **Control / Respond:** Data Exposure

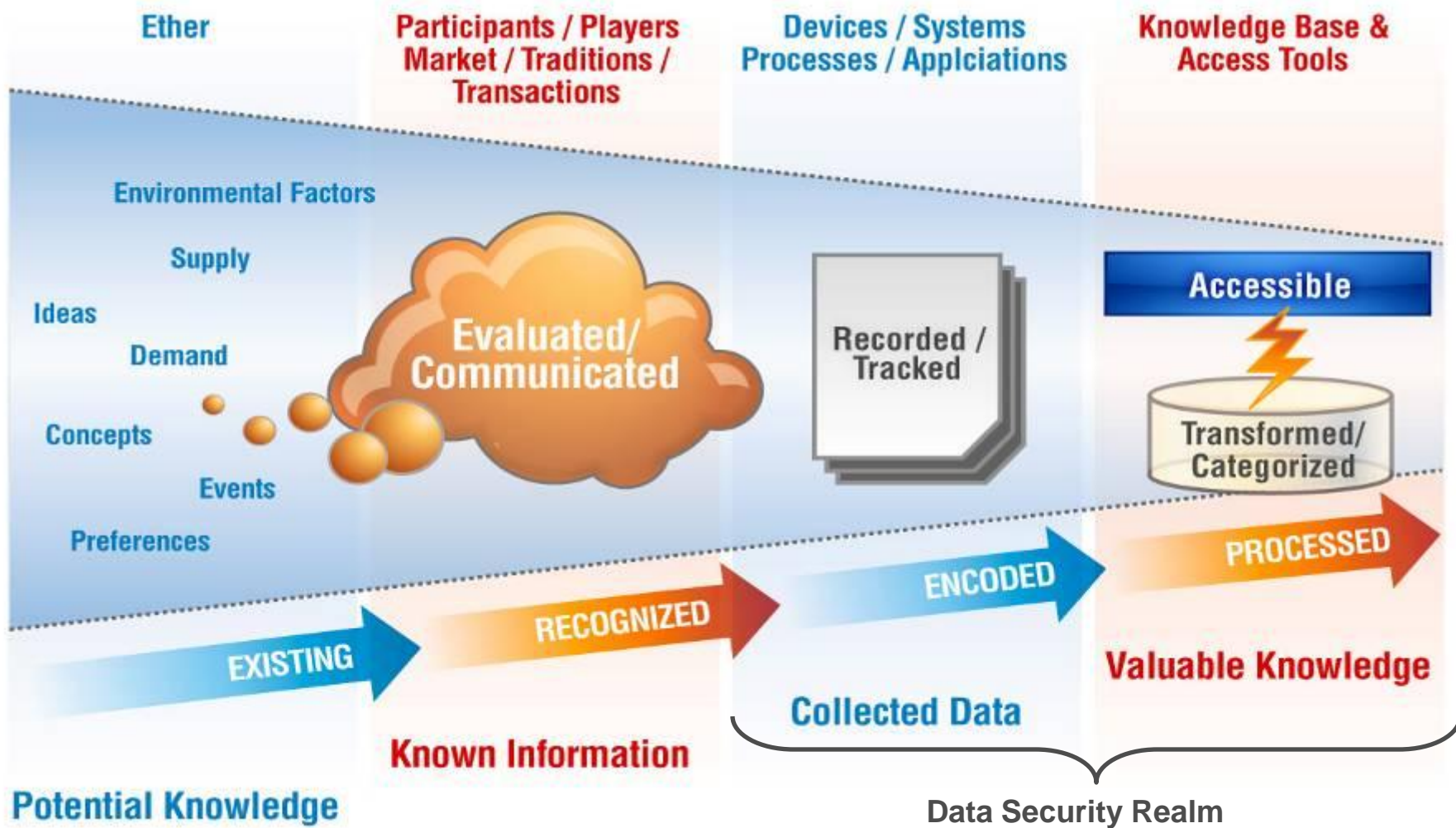
*“**The false positives are killing me.** The real violations are slipping through my fingers.”*

Model 3: The *Value* within the Information Lifecycle

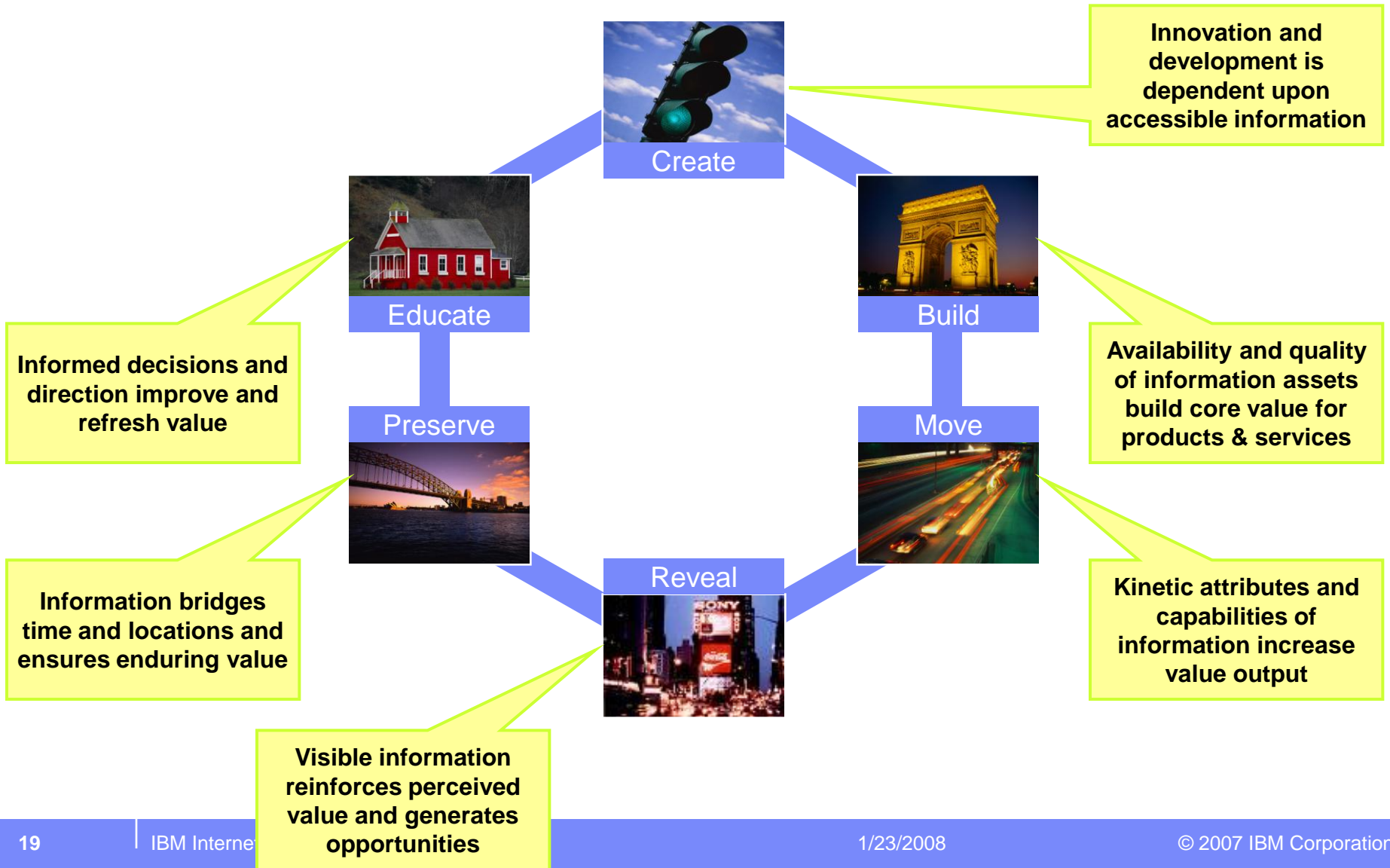
- **Our Data Leakage prevention strategy does not begin with protection.**
- **On the contrary**
 - the purpose of information is to *add value* through access and use ...
 - to *enable* collaboration
- **Our Data Security strategy begins with the design of Information Access.**

Data Leakage is Prevented Primarily at its Origins – the Points of Access and Use

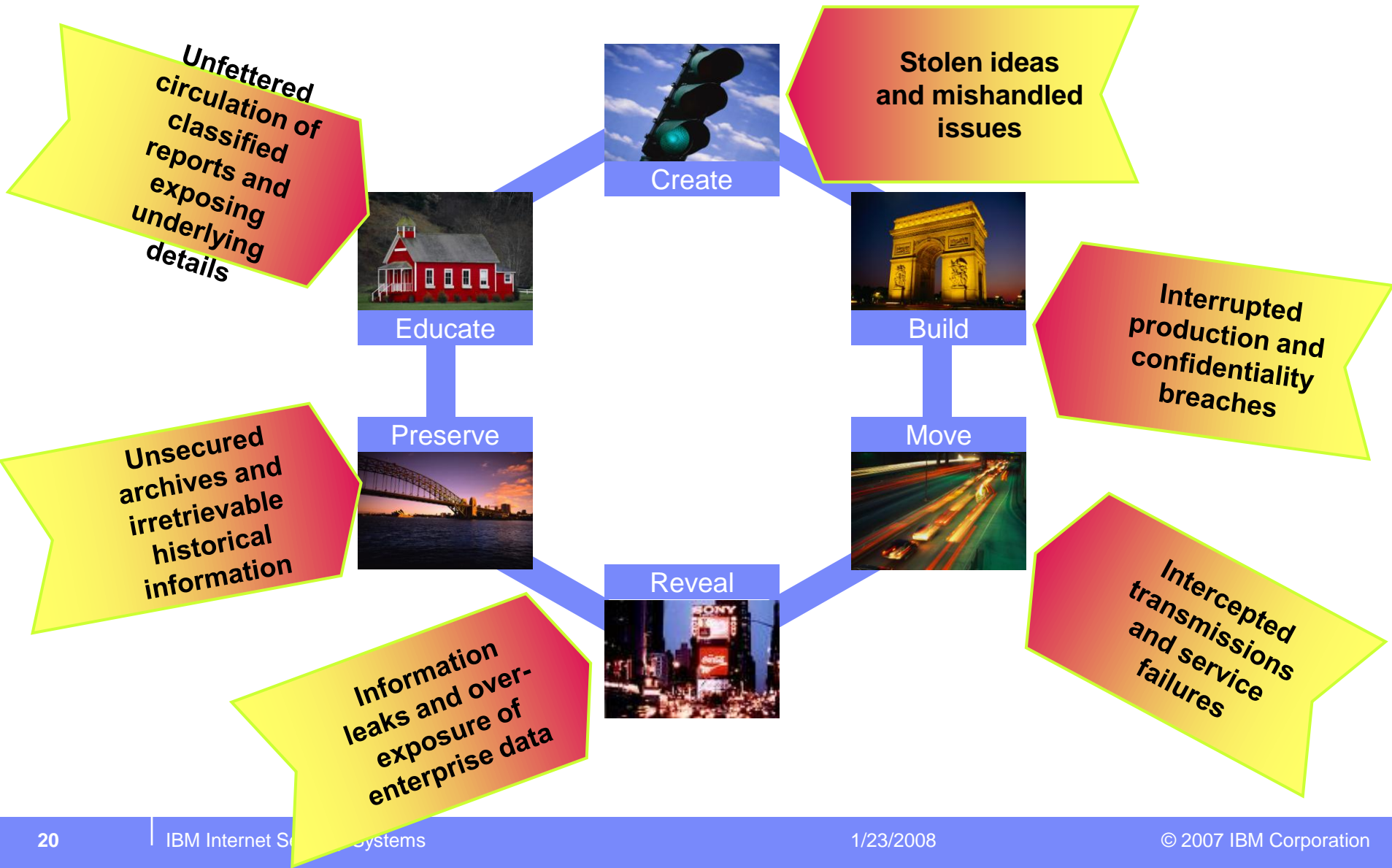
Organizations Transform the *Value* of Information by Passing it Through a “Knowledge Funnel”



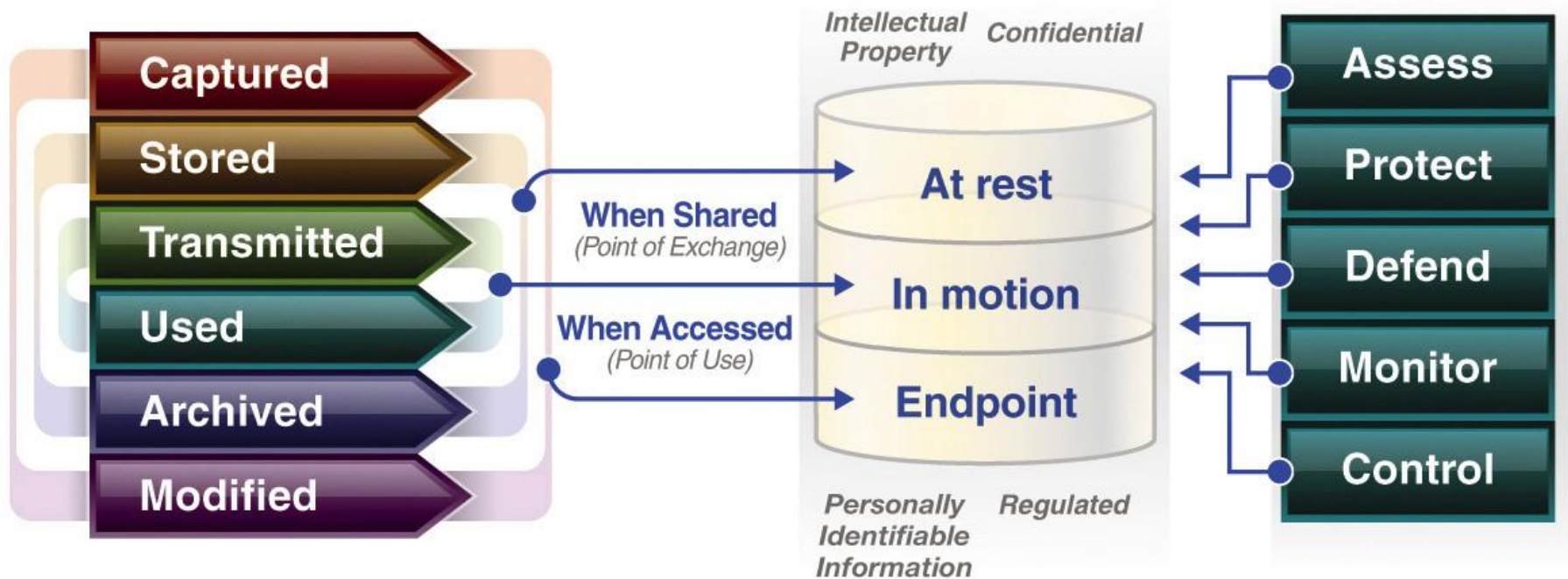
Information Access Creates Value...



...but Data Leakage Puts *Value* at Risk

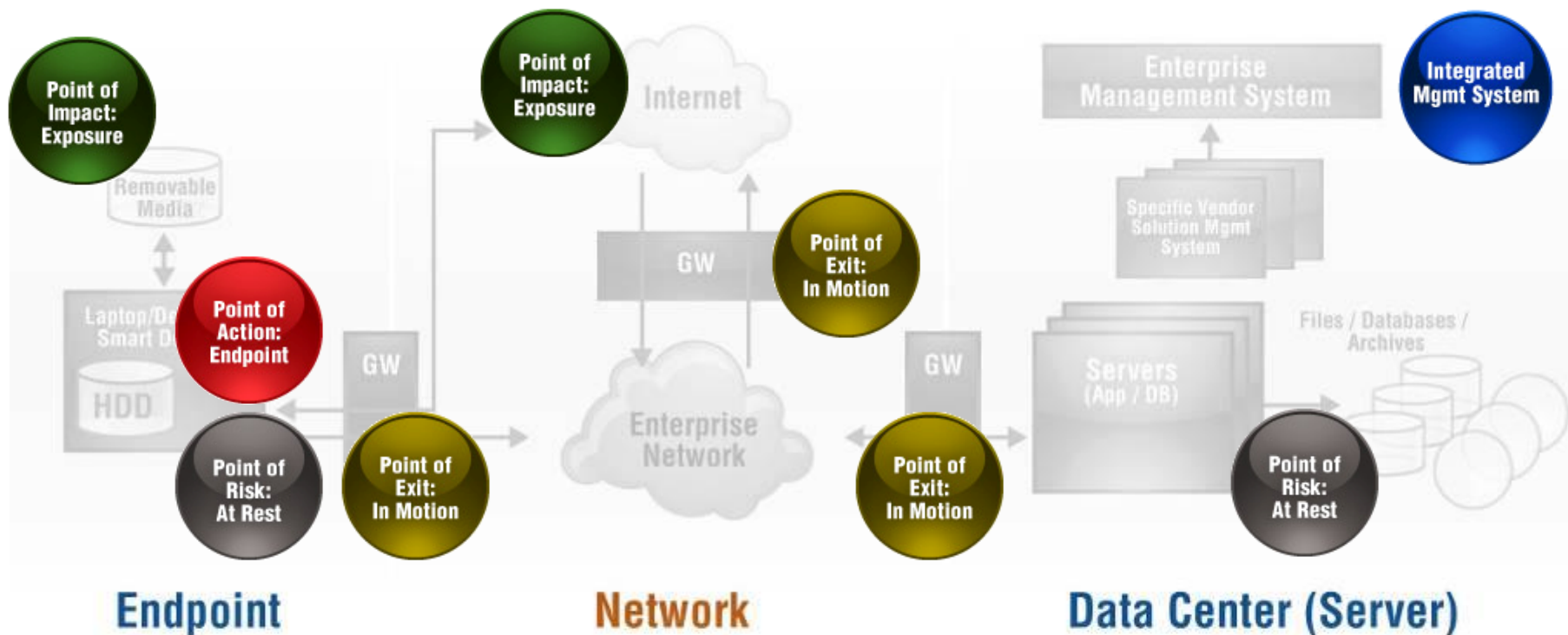


The Traditional Data Model isn't Enough



We use these models alternately, since they overlap and yet offer insights: coverage checklist, product alignment

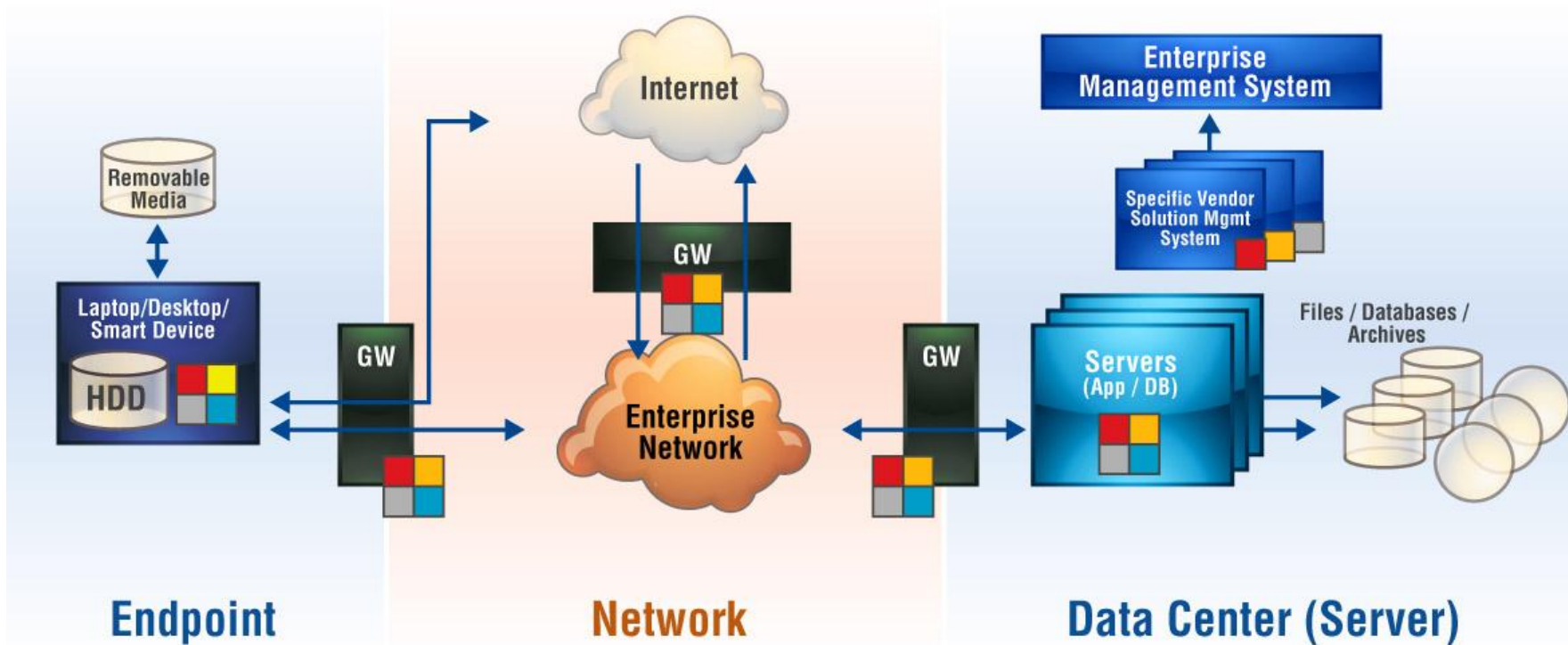
DLP solution components are dispersed across segments of the enterprise: Endpoint, Network, and Data Center Server



Data Security Components in control points

- Endpoint: Activity Monitoring
- At Rest = Discovery
- In Motion = Content / Context Inspection
- Exposure = Crawling, Encryption, LoJack
- Management = Unified Policies, Reporting, Forensics, Correlation

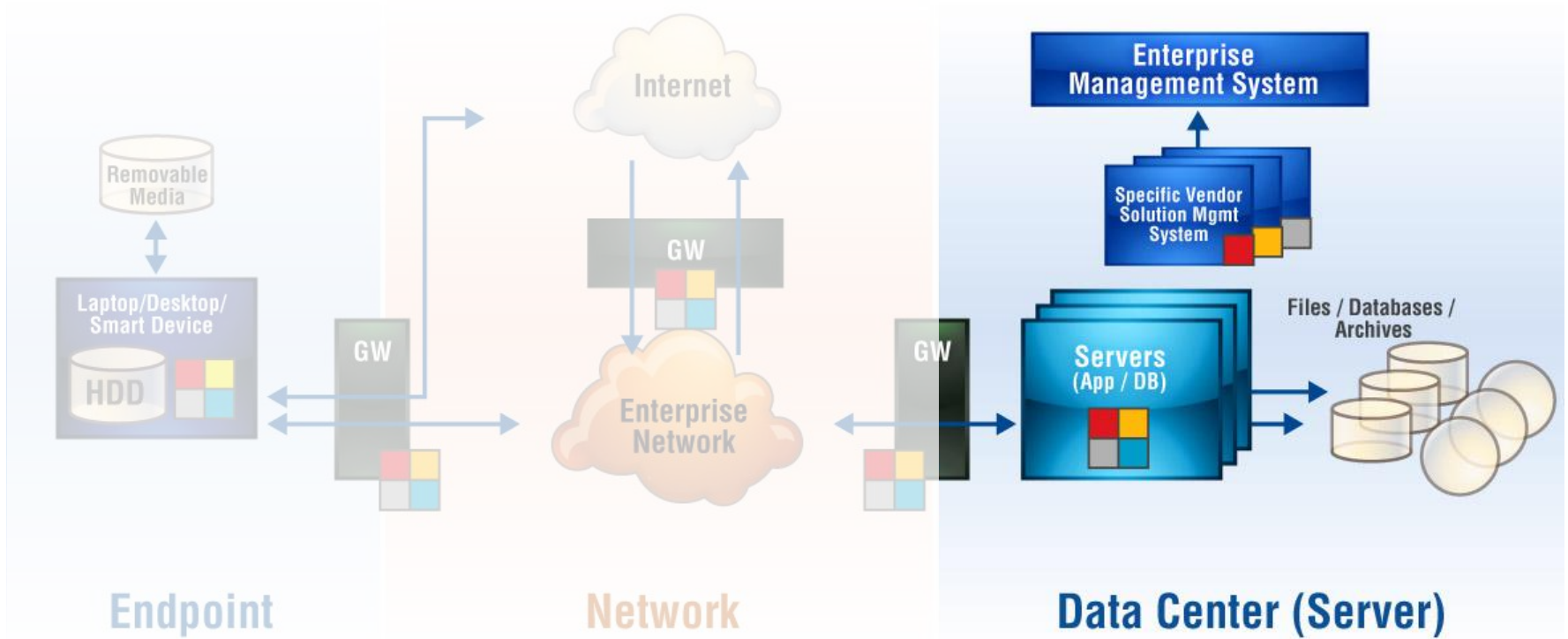
Data Security Model – Solution Components are dispersed across 3 control points in the enterprise (Endpoint, Network, Data Host)



Data Security Components in control points

- Encryption
- Content Inspection
- Privilege User Monitoring
- Management

Data Security Model – Data Center (Server)



Data Security Components in control points

- Encryption
- Content Inspection
- Privilege User Monitoring
- Management

Data Center (Server)

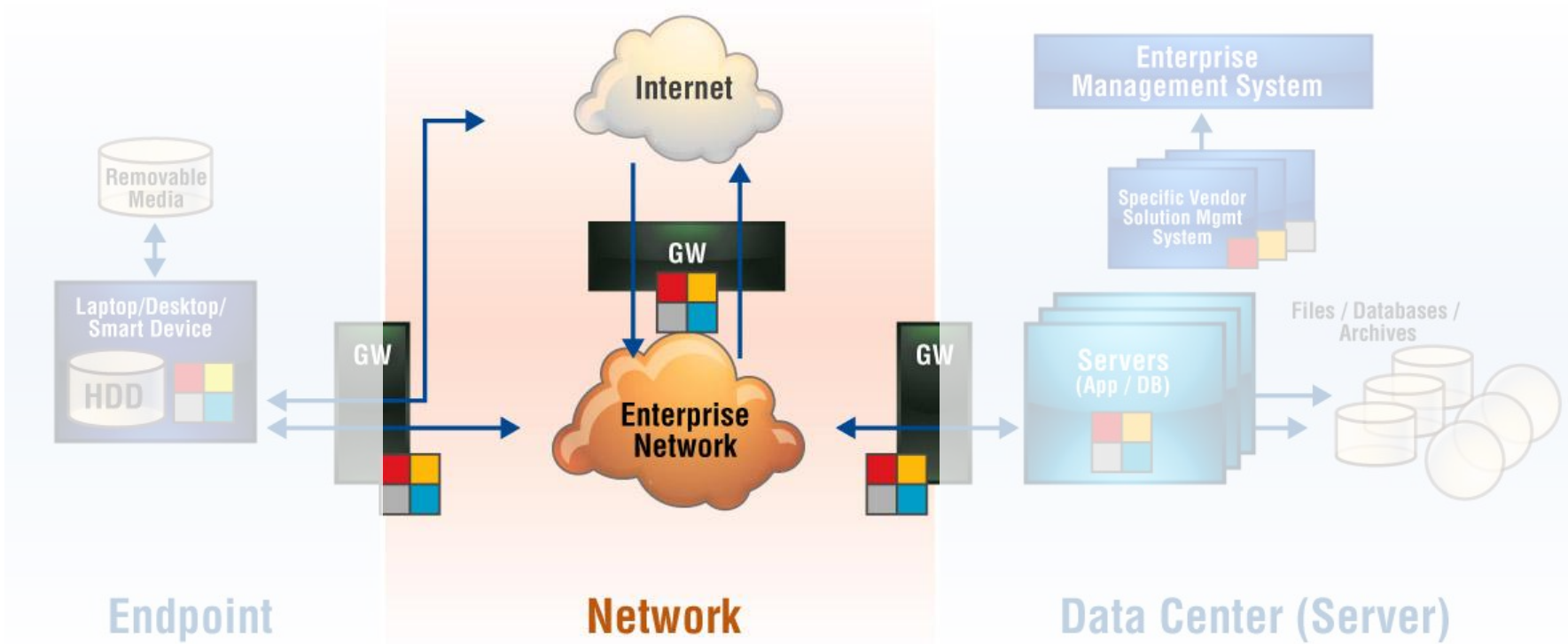
- **Privileged Users**
 - DBAs
 - Direct Access to Db - right past applications
 - They hold the *Keys to the Kingdom*
- **Activity**
 - Compliance
 - Monitoring
 - Enforcement
- **Discovery and Protection**
 - Structured Data
 - Data Masking

Not Data Leaks...

...Data FLOODS!



Data Security Model – Network



Data Security Components in control points

- Encryption
- Content Inspection
- Privilege User Monitoring
- Management

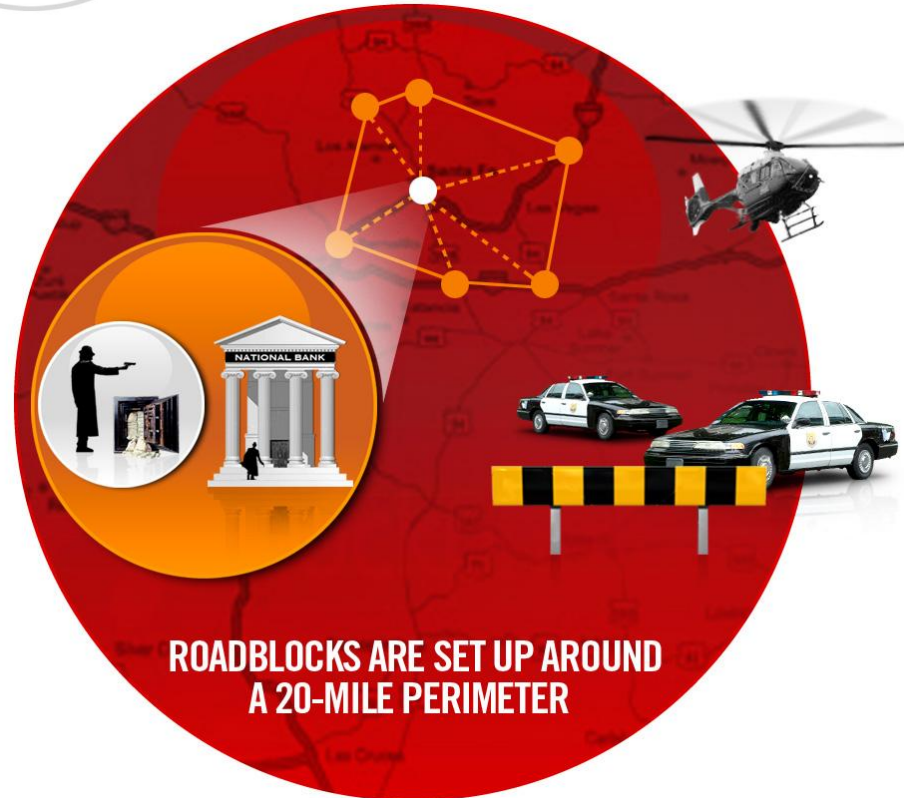
Network Protections

■ Pros

- Ease of deployment
- Visibility
 - Catches all network transfer

■ Cons

- Visibility
 - Encryption
 - Application data
 - Non-network transfers

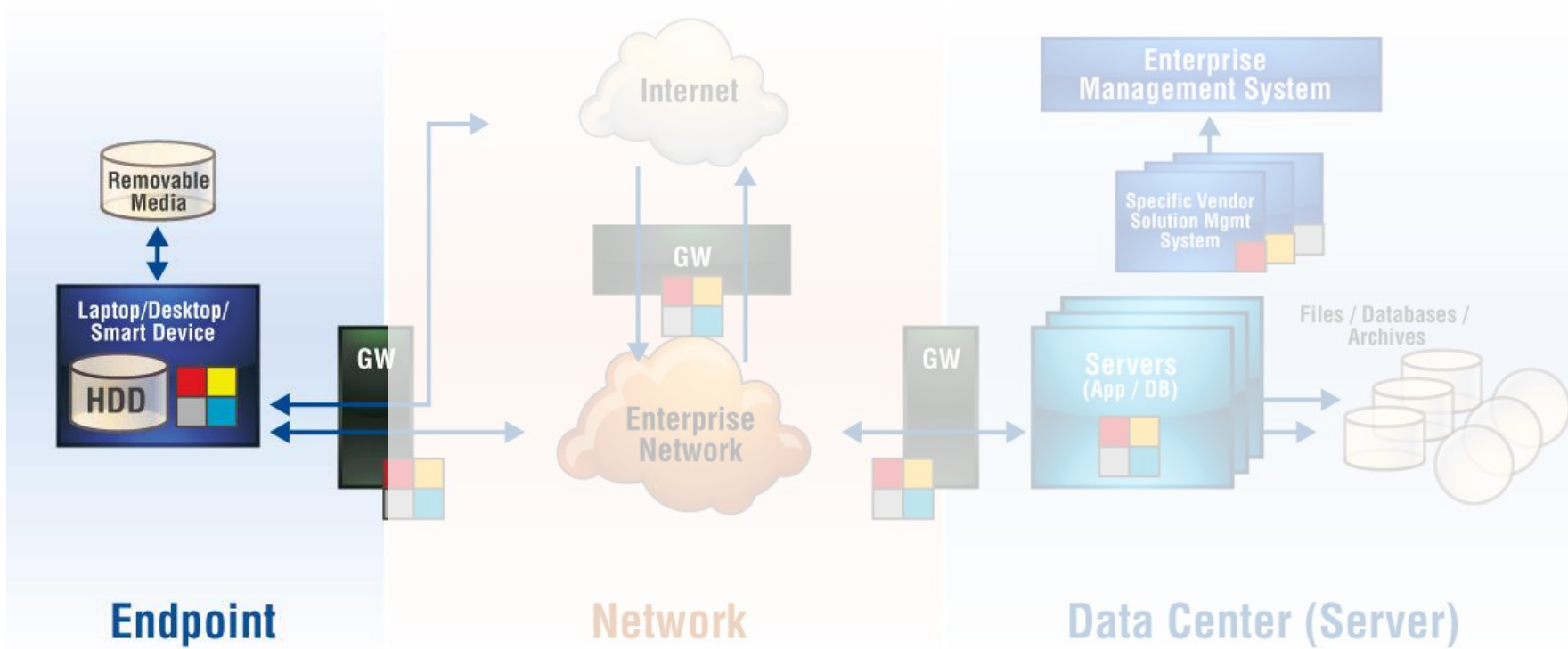


Network Suitability

- **Monitoring data movement**
- **Catching network transfer**
 - Where host tools can't go
- **Alerting on attacks and attempts**



Data Security Model – Endpoint



Data Security Components in control points

- Encryption
- Content Inspection
- Privilege User Monitoring
- Management

Endpoint Protections



- **Pros**
 - Coverage
- **Cons**
 - Deployment
- **Access to full *Content* and *Context***
- **The Deterrent Effect**
 - Visible Monitoring
 - Just-in-time Education
 - Forensics



Protecting the System AND the Data

System Protection

- Network Firewall
- NIDS/NIPS
- Web Content Filter
- Network encryption/VPN
- Vulnerability Scanning
- AV & AS, VPS
- IDS/IPS
- Pers. Firewall/VPN
- Security Hygiene (patch levels, security config)
- Sec Patch Management
- System lockdown
- Access control
 - SSO
 - Strong Authentication
 - NAC

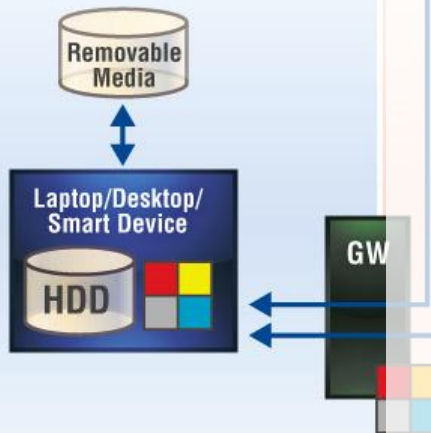
Data Protection

- Data content Monitoring/Filtering
- Activity Monitor/Enforce
- Secure Messaging (email/IM)
- Data Backup/Restore
- Full disk encryption
- File encryption
- Removable media device control and data encryption

Coexistence
(compatibility/bundling)

Integration
(Modularity)

Endpoint



Endpoint

Data Security Components in control p...

Encryption

Maybe its Time to Roll Out Full Disk Encryption...

A Chronology of Data Breaches - Microsoft Internet Explorer

Address: <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen backup tape	5,000 - 6,000
Sept. 22, 2005	City University of New York	Exposed online	350
Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Sept. 29, 2005	Univ. of Georgia	Hacking	At least 1,600
Oct. 12, 2005	Ohio State Univ. Medical Center	Exposed online. Appointment information including SSN, DOB, address, phone no., medical no., appointment reason, physician.	2,800
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Nov. 4, 2005	Keck School of Medicine, USC	Stolen computer	50,000
Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 8, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves. Total affected now reaches 163,000 (see Feb. 15 & Sept. 16)	[Total later revised to 163,000 -- see 2/15/05 above]
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Georgia Tech Ofc. of Enrollment Services	Stolen computer, Theft 10/16/05	13,000
Nov. 11, 2005	Scotttrade Troy Group	Hacking	Unknown
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank	161,000



Headlines – Endpoint Data Exposures in the News

- Ernest & Young laptop losses exposes information on Sun Microsystems, Cisco, IBM employees and 243 Hotel.com customers. (June 2006)
- Health insurer Aetna on said a laptop computer containing personal information on about 38,000 of its members was stolen from an employee's car (April 2006).
- Fidelity laptop loss exposes personal information about 196,000 HP employees (March 2006)
- ING laptop loss exposes social security numbers and other personal information on 13,000 employees and retirees (June 2006)
- Los Alamos Nuclear Weapons data found on 3 USB flash drives during drug raid (Oct 2006)
- 478 IRS laptops lost or stolen over 4 year period; 112 held sensitive taxpayer data, including social security numbers (Nov 2006)
- North Carolina Department of Revenue report stolen laptop with sensitive tax payer information and SSNs (13 January 2007)
- University of Idaho Advancement Services Office report 3 laptops stolen, PII exposed for 330,000 employees (11 January 2007)

- Lost/Stolen Laptops: **673,000** in US in 2005 (11,300 left in Cabs in 6 month period)
- Lost/Stolen Desktops PC: 520,000 in US in 2005 in 6 months
- Lost/Stolen PDAs: 714,000 in US in 2005 (31,400 left in cabs in 6 month period)

Source: PriceWaterhouseCoopers/CNN/FBI (CSI/FBI Computer Crime and Security Survey 2005)

Data Diapers

- **How do I stop leaks?**
 - It “depends”



Data Leakage Requires a Comprehensive Solution Set

Comprehensive Models

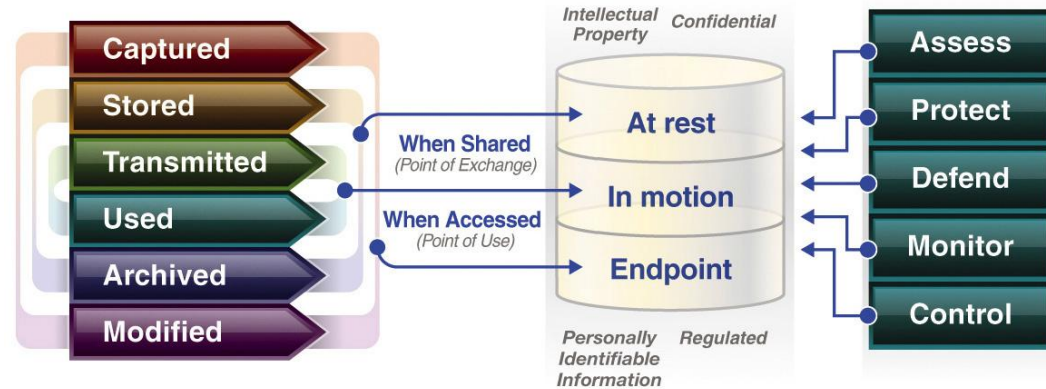
- Understand the problem space
- Address the *Complexity* with *Confidence*

Comprehensive Services & Products

- Assessment / Discovery / Baseline
- Data Compliance Workshop
- Education
- Content Policy / Rule Creation
- Policy Management
- Ongoing Content Monitoring
- E-mail / Secure Communications
- Management Console / Portal
- Supporting Products & Assets
- Incident Response Management

In an Organized, Unified, and Integrated System

- We cannot secure Data with piecemeal or patchwork
- We cannot use band-aids to pass Compliance audits
- We require *solid, integrated tools* that *interoperate*
- REMEMBER – This solution must hold water



...and the *Discipline* to invert your thinking

Internal Proprietary and Confidential



IBM Global Services

Now let's get to Work!

Thank You!

Joshua Corman
Eric Hanselman, CISSP



IBM Internet Security Systems

Ahead of the threat.™

1/23/2008

© 2007 IBM Corporation