

Data Loss Prevention
by Managed Security
Services Provider

Cecil Yuen

December 14, 2007



Confusing market: DLP/CMF/CMP

Data protection	76%
Identity and access management	68%
Compliance management	58%
Threat and vulnerability mitigation	57%
Secure application architecture	54%
Secure Messaging and Collaboration	52%
Patch management	40%
Legacy platform migration	21%

CSO Summit 2007

DLP:
Data Loss Prevention/Protection
Data Leak Prevention/Protection

ILP:
Information Loss
Prevention/Protection
Information Leak
Prevention/Protection

Extrusion Prevention

CMF: Content Monitoring and
Filtering

CMP: Content Monitoring and
Protection

Vendors: Who are we talking about?

McAfee®



SafeBoot
MOBILE DATA SECURITY



VONTU



provilla

RSA™

The Security Division of EMC



CISCO

WEBSense

Raytheon

IRONPORT®

SurfControl® PORT AUTHORITY
TECHNOLOGIES
STOP INFORMATION LEAKS

OAKLEY™
NETWORKS

SECURE
COMPUTING

Lumension
SECURITY™

VERICEPT

Reconnex
INFORMATION PROTECTION. ALWAYS™

CipherTrust

SecureWave
Safeguarding Tomorrow

proofpoint®

Palisade®

VERDASYS.

Orchestria
Good Controls are Good Business

aungate

GTB
TECHNOLOGIES

CODE GREEN
NETWORKS

INTRUSION

Workshare™

FIDELIS
SECURITY SYSTEMS

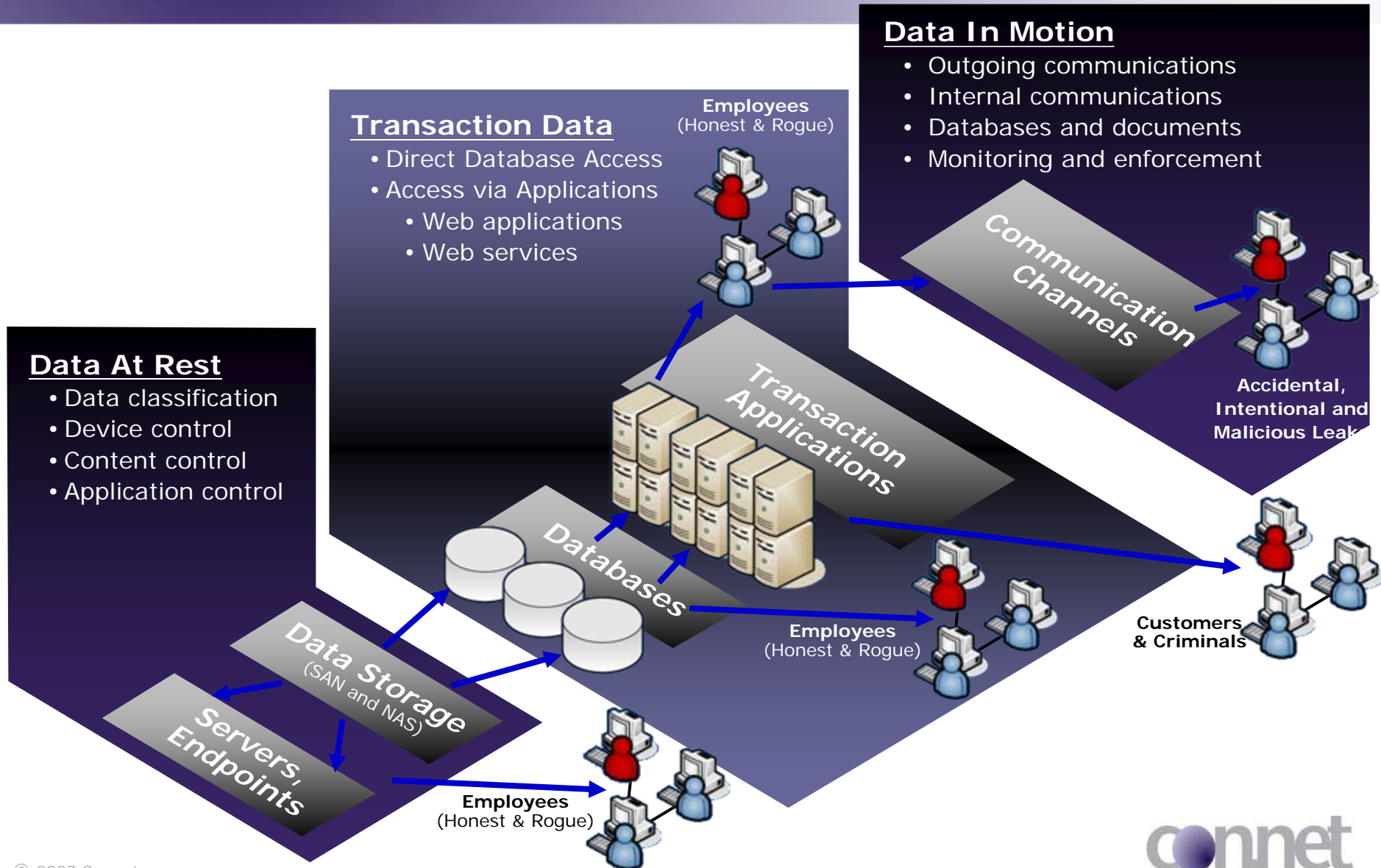
connet

Near paperless: Do you know where your data is?

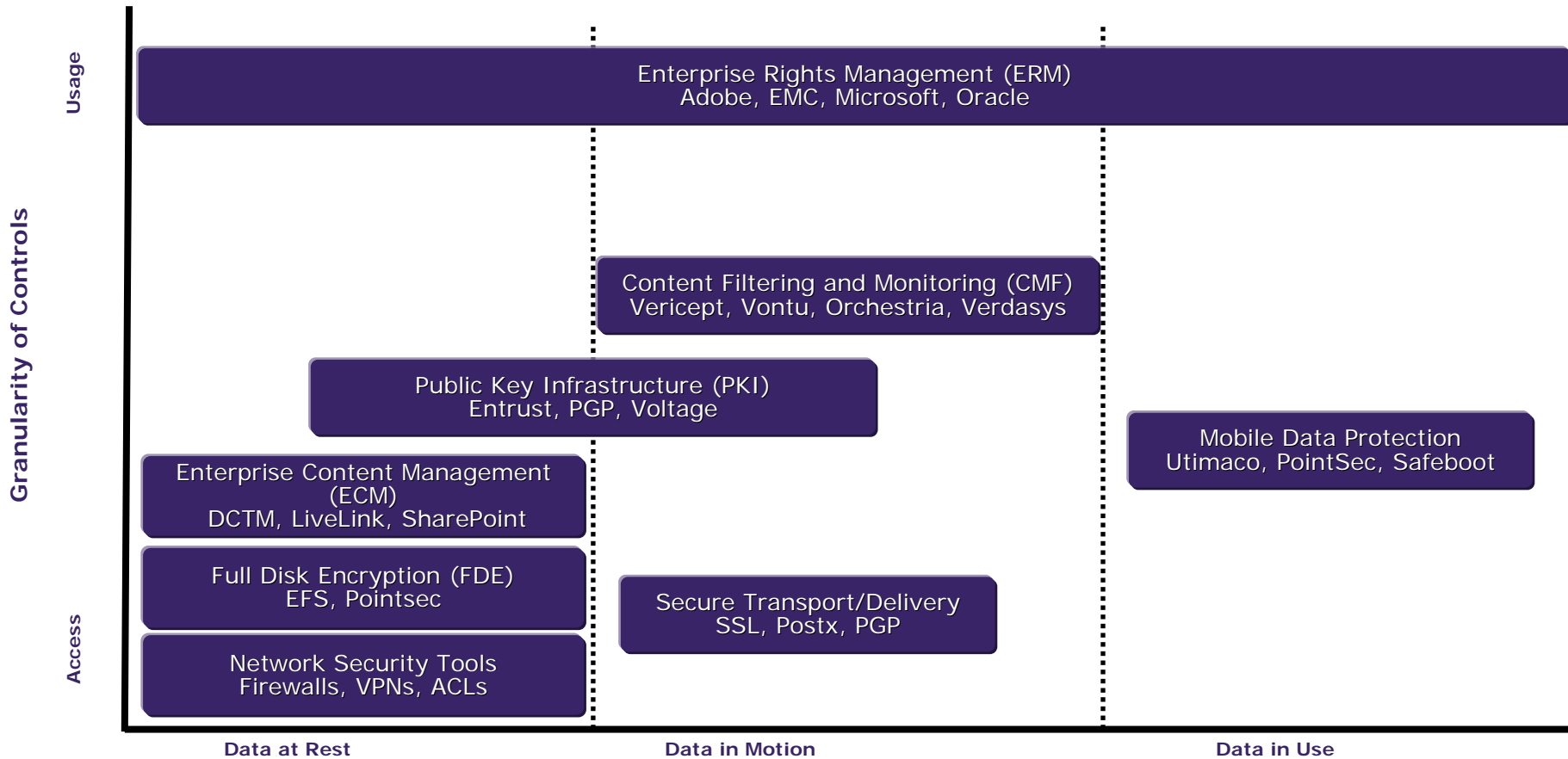
- Phase 1: email only
- FRCP (Federal Rules of Civil Procedure)
ESI (Electronic Stored Information)
- Phase 2: Data in motion (network)
IM, FTP, HTTP, TCP/IP
- Phase 3: Data at rest
(discovery/storage/endpoint)
analysis of static, stored data, integration with
document management systems / endpoint
agents
- Phase 4: Data in use (users' device/endpoint)
all channels (network interface, OS, applications)



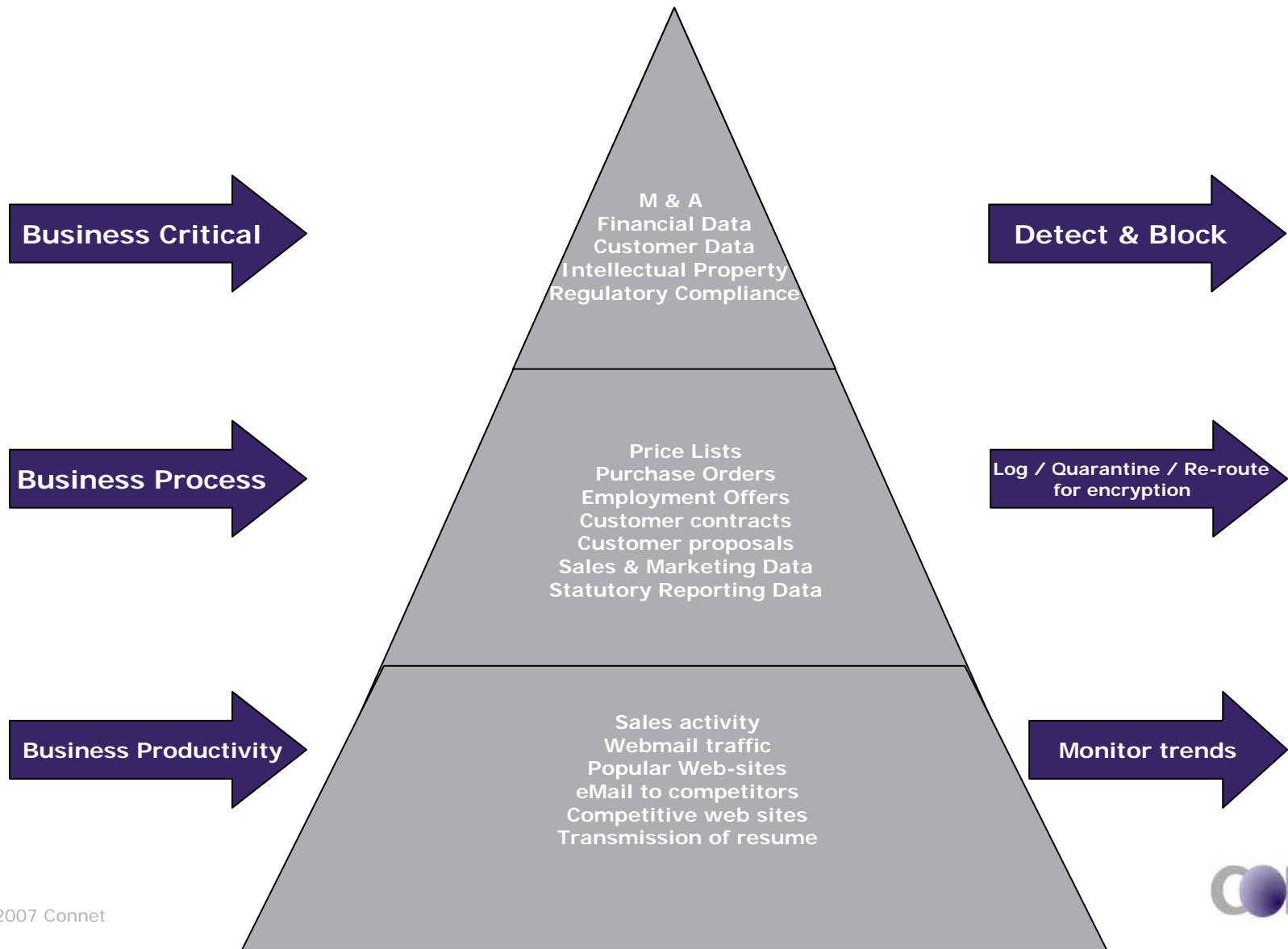
DLP landscape



DLP category



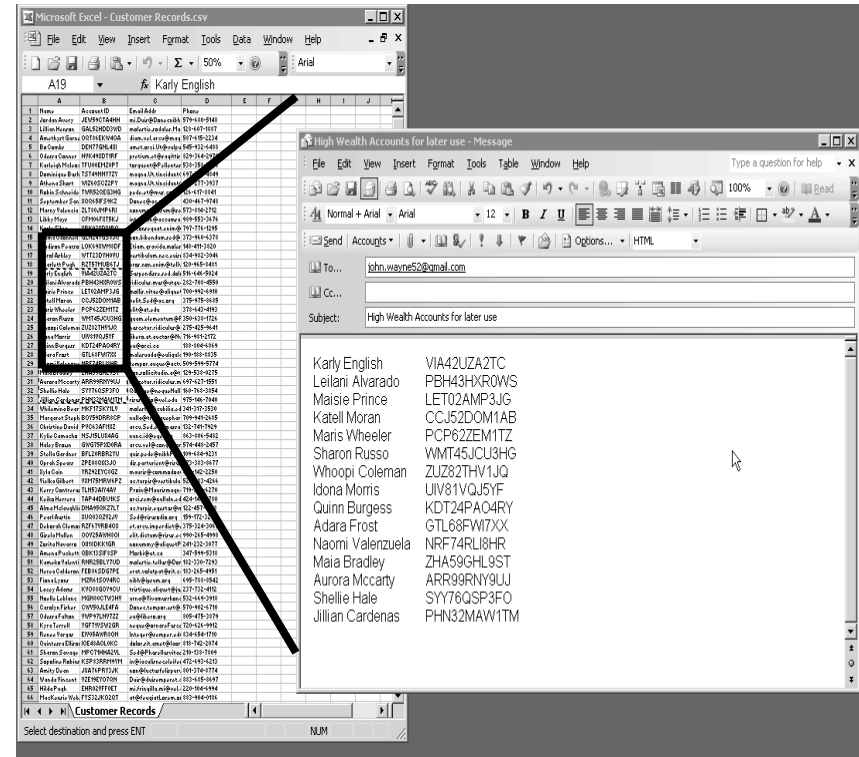
DLP hierarchy



Typical policy

- Derogatory comments to public blog
- Review 30 days external communications prior to departure of key employee
- Chat earnings 3 hours before public release
- by "score", basically the # of private terms in messages, e.g. Patient Name + X-ray
- transaction anomaly detection (TAD)
Geo-location, suspicious access patterns
- "Protect any credit card numbers" vs
"Protect all 1 million credit card numbers"
- Customer database elements:
 - Name
 - Date_of_birth
 - Social_security_number
 - Credit_card_number
 - Account_number

"If (SMTP or HTTP or FTP) contains more than 4 occurrences of name and (Social_security_number or Credit_card_number or Account_number) then log the incident, block the transmission and retain a copy of the message."



Case Management

ID	time	policy	channel	severity	User	action	Status
638	1324	PII	HTTP	1	192.168.0 .3	None	Closed
639	1432	HIPAA	IM	2	Apatel	Notified	Assigned
640	1502	R&D	USB	4	Hjordan	Notified	Assigned
641	1512	Financial	Storage	4	Msmith	Encrypt	Escalated
642	1630	Source code	Cut/paste	12	mlui	Confirm	Open