Content – The Next Generation of Incident Response

Gib Sorebo, JD, CISSP

June 2009

SAIC
From Science to Solutions

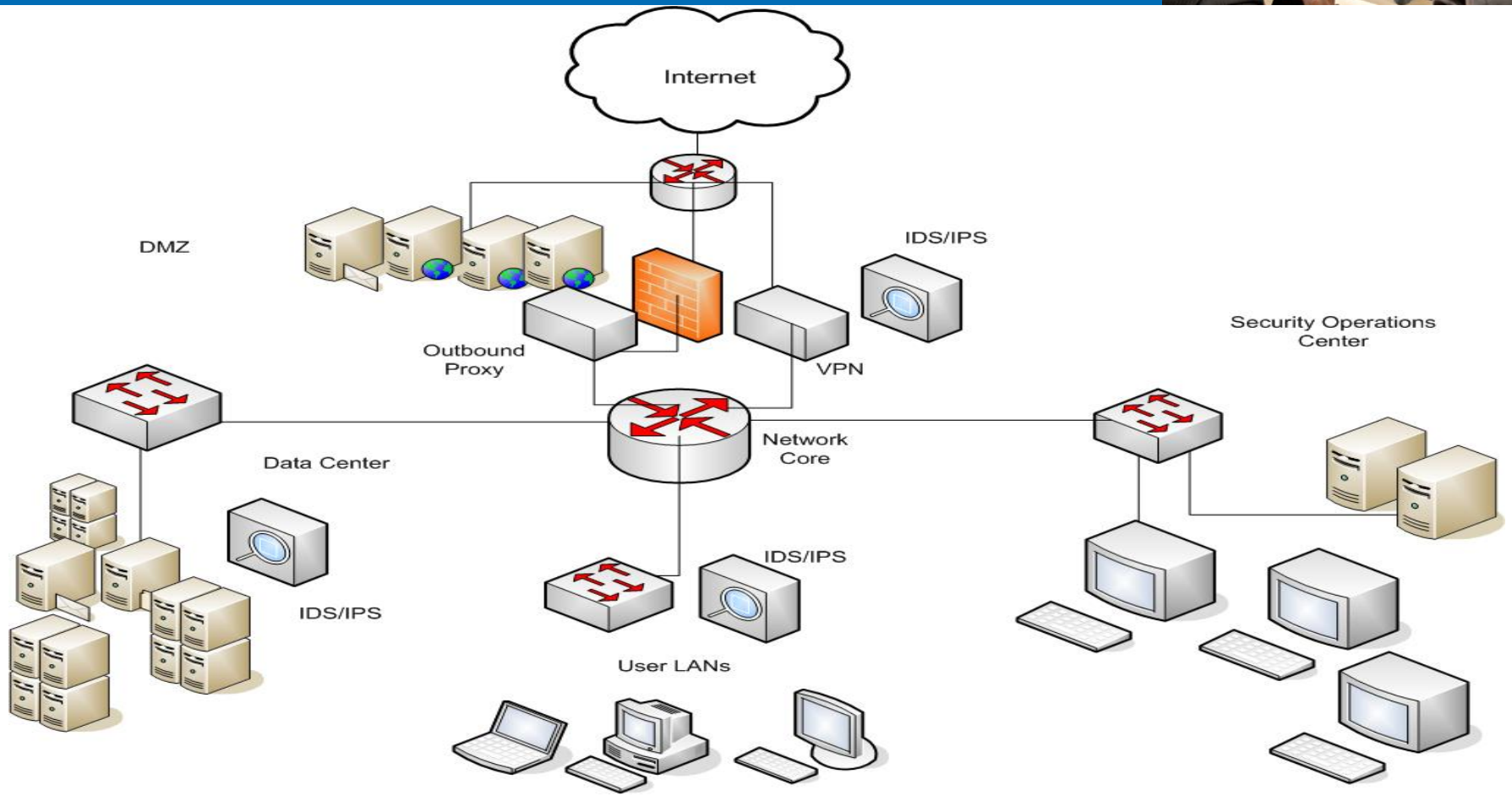
Overview

- Threat and regulatory environment
- Current state of security monitoring and incident response
- Future states and solution approaches

Threat and Regulatory Environment

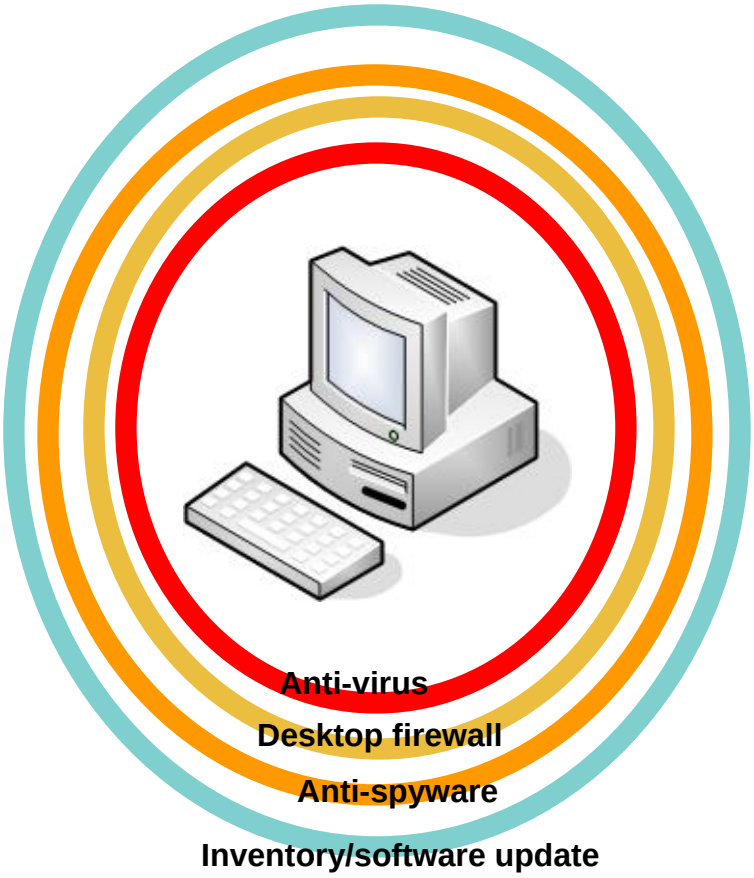
- Content is becoming the weak link
  - 2008 Verizon Breach Report
    - Sixty-six percent of breaches involved data the victim did not know was on the system
    - Only 4 percent of breaches were detected by event monitoring or log analysis
    - Seventy percent of breaches first discovered by third party (e.g., customers)
  - Ponemon Institute
    - Average business loss is $202 per customer record
  - Recent breaches
    - Recent government breach involved a test server containing personally identifiable information; officials acknowledged that they weren't aware the data was still on the server
    - More attacks are targeting data to be sold or used to make money illegally (for example, identity theft) making breaches less detectable
- Legal/regulatory landscape
  - Office of Management and Budget (OMB) Memorandums 06-16 and 07-16 specifically target personally identifiable information (PII) and other sensitive agency information
  - Growing awareness of the importance of protecting PII and taking actions to mitigate the dangers from inadvertent disclosures
  - State breach laws increasingly are targeting both the disclosure of breaches and mandating minimal controls to protect PII

Current State of Security Monitoring

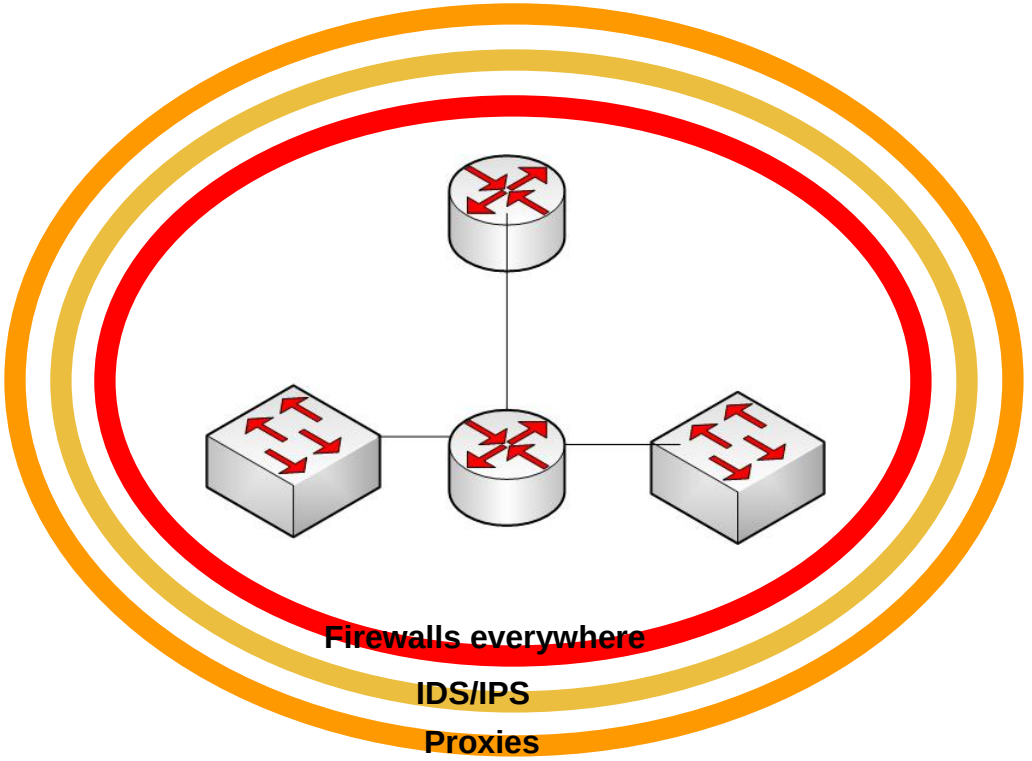


DMZ = demilitarized zone IDS/IPS = Intrusion Detection System/Intrusion Prevention System
VPN = virtual private network LANs = local area networks

What's the Problem?



Agent Overload?

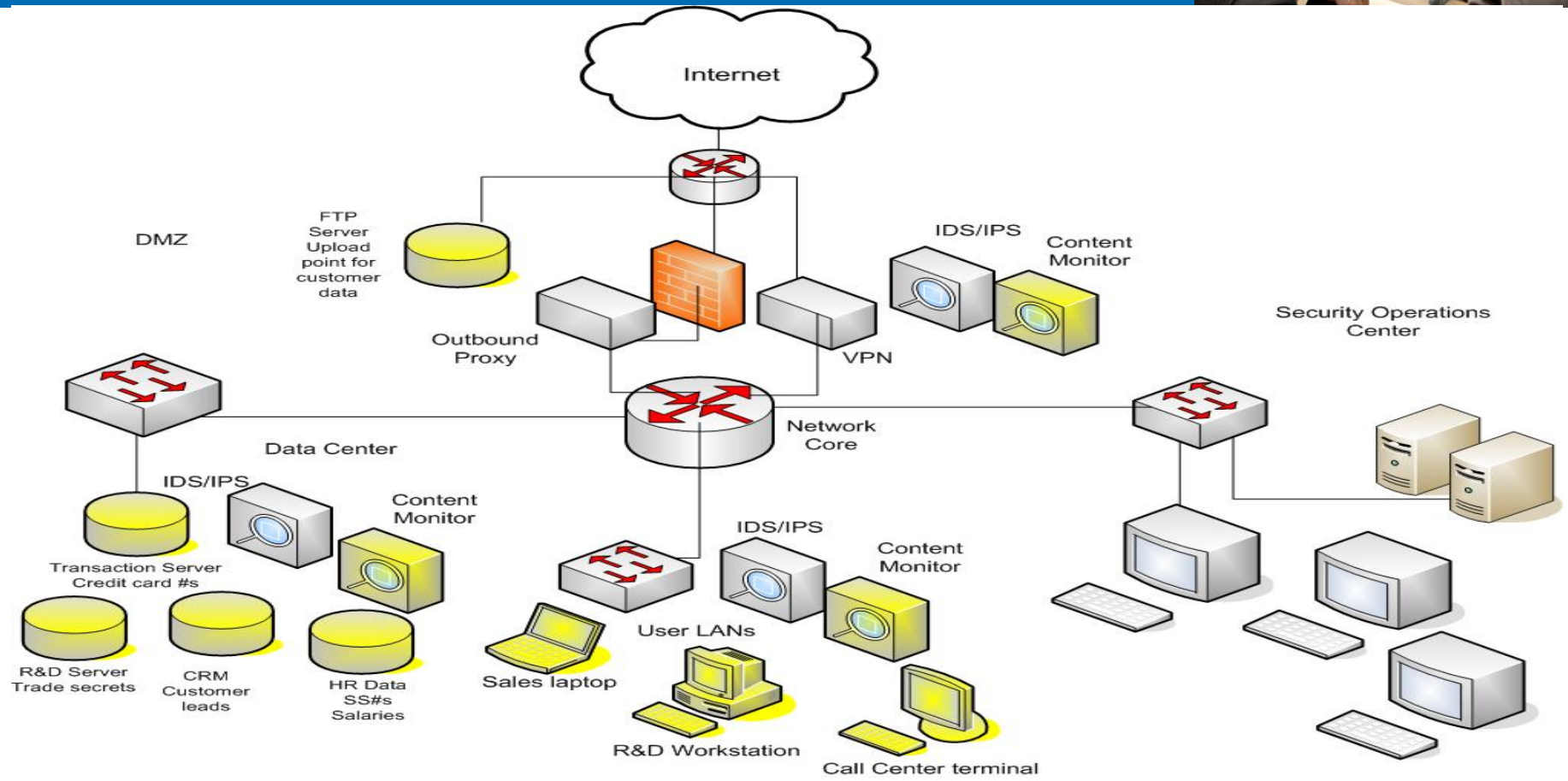


So many devices to help us see and protect, and yet, we're still blind

IDS/IPS = Intrusion Detection System/Intrusion Prevention System

SAIC From Science to Solutions

What If We Add Content and Context?



DMZ = demilitarized zone FTP = File Transfer Protocol IDS/IPS = Intrusion Detection System/Intrusion Prevention System
VPN = virtual private network LANs = local area networks CRM = customer relationship management

That Might Mean…

- Security operations could know about
  - The trade secret data being transmitted to an unknown party at 2 a.m.
  - A call center employee downloading 100 credit card numbers at once
  - A departing sales employee sending customer lists to his personal e-mail account
- Management could be made aware of
  - Unusual employee activities after hours
  - Sensitive data on development servers
  - Data mismatches (e.g., human resources data on R&D servers)
  - The kinds of data affected by a server's breach
  - Sensitive data stored on vulnerable devices (i.e., laptops, mobile media)
  - Data retained long after needed

Current Content Monitoring Capabilities

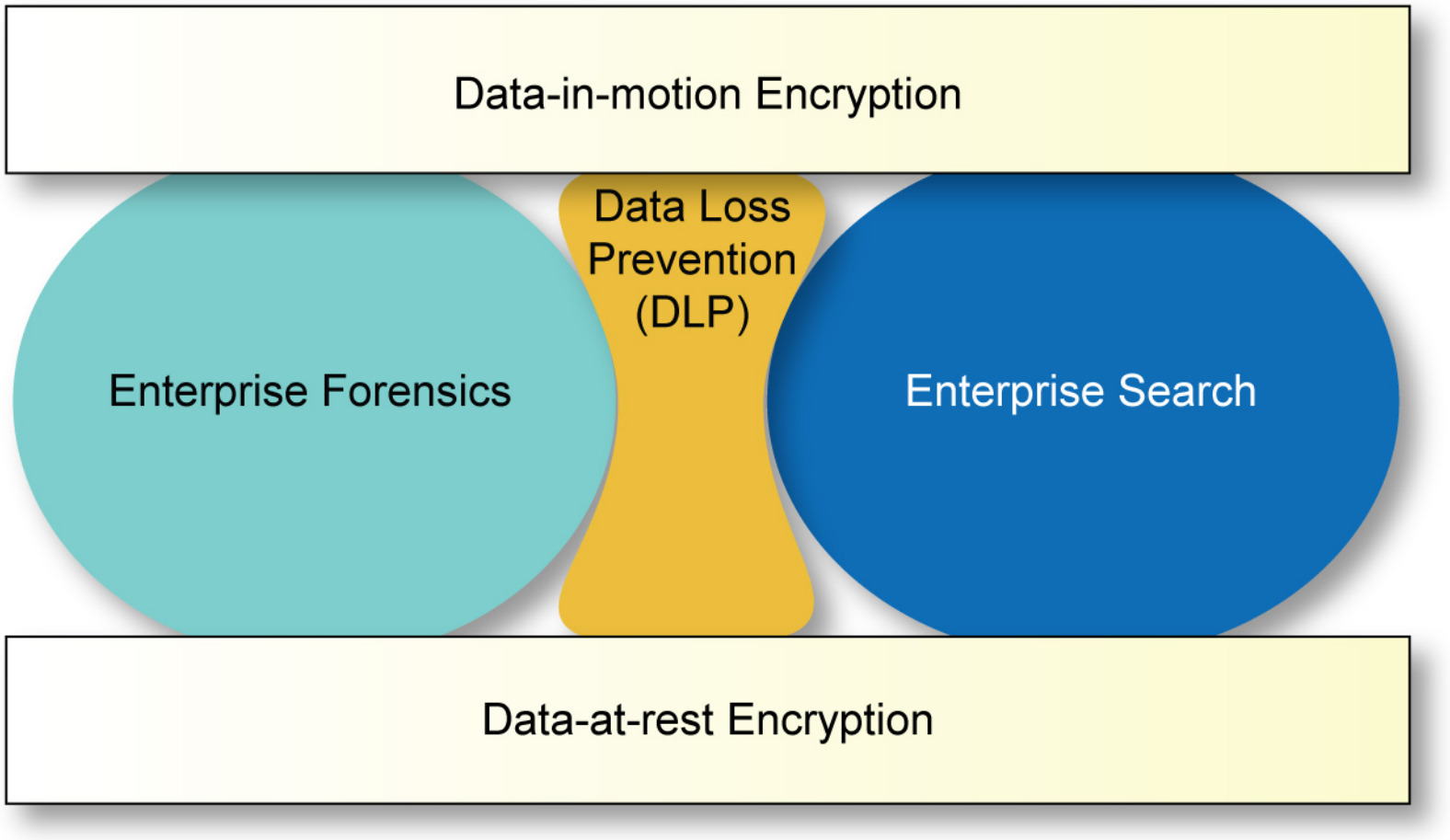
- Only partial solutions currently available
  - Extensive customizations required for complete solutions
  - Products currently lack the intelligence to effectively manage large quantities of documents containing personally identifiable information
    - Group data (i.e., data based on project, category, subject matter, etc.)
    - Current products utilize date/time file stamp (90-day clock); don't address "data use no longer required"
- Market is in its infancy
  - Multiple approaches from different perspectives (e.g., computer forensics/e-discovery, data leak prevention, digital rights management)
  - Most are targeting the detection and prevention of data leaving the organization at the perimeter

Content Monitoring and Protection – Product Categories

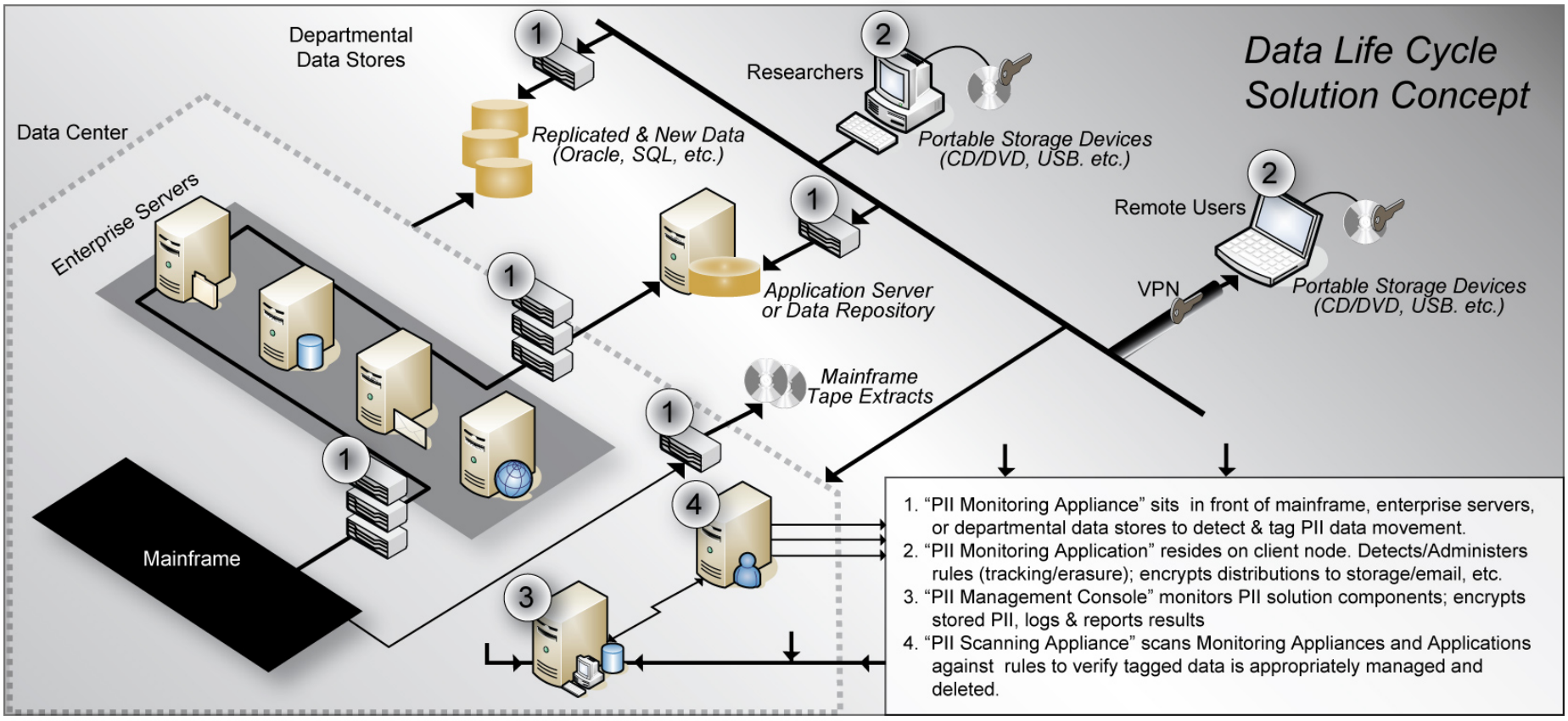
Product Category	E-Discovery/ Computer Forensics/ Inventory	Digital Rights Management (DRM)	Traditional Security Monitoring/ Intrusion Detection System/ Incident Response	Data Leak Prevention (DLP)	Log Analysis/ Security Information Management	Database Monitoring/ Analysis	Encryption
Vendors*	• Guidance Software® • Paraben® • Proventsure™ • Technology Pathways • AccessData®	• Liquid Machines® • Microsoft® • Adobe®	• iWitness™ • Enterasys® • 3Com® • Cisco™ • SourceFire®	• Vontu® • Vericept® • Reconnex® • WebSense™ • Fidelis® • Verdasys®	• LogLogic® • ArcSight® • netForensics®	• Vormetric® • AppSec	• Guardian Edge® • PointSec • PGP®
Product Character	• Focused on locating data in the enterprise • Some categorization and keywords and generally used	• Generally requires a good degree of application integration and developer assistance	• Identifies security events; generally content neutral; triggers based on known exploits and traffic anomalies	• Content-based discovery and prevention capabilities	• Analysis of log information from various sources; not quite real-time response	• Ability to natively analyze databases and identify critical information; perhaps a subset of the e-discovery category	• Ability to encrypt data, sometimes based on triggers initiated by data loss prevention and other category products

*Trademark attributions and other vendor name references are provided on slide 16

Are Data Loss Prevention Solutions Getting Squeezed Out?



Where and What Should We Be Monitoring?



PII = personally identifiable information VPN = virtual private network

Oracle is a registered trademark of Oracle International Corporation in the United States and/or other countries.

How Should the Roles of Security Operations and Incident Response Change?

Current State	Future State
Analysts are alerted to a known attack signature	Analysts are alerted when sensitive data is accessed from an unknown source
Incident responders are immediately called to respond to an attack anywhere in the network	Incident response is prioritized based on the nature of the data affected and the source of the attack
Virus infections and worms need to be responded to immediately at their source	Location of infections can be quarantined remotely at the switch and router level and smart filters can be instantly deployed to block ex-filtration of targeted sensitive data

International Considerations

- Language
  - Traditional monitoring is largely language-independent
  - Content elevates importance of language
  - Language structure and usage is critical to an effective enterprise search
- Culture
  - Traditionally, an attack was an attack
  - With context, culture can dictate what is suspicious
- Legal regimes
  - Significant privacy implications to monitoring content
  - Retention requirements and obligation to law enforcement

How Do We Get There?

- **Phase 1 – Policies, inventory, network-based detection, and education**
  - Go for “low hanging fruit” such as policy changes and simple application changes that keep sensitive data from being stored on workstations and laptops in the first place
  - Deploy network-based detection and discovery tools to identify sensitive data flowing over the network and locate it later on user workstations
  - Educate security operations on data types and where they’re located
- **Phase 2 – Agent-based discovery and detection**
  - Installing agents on workstations improves the speed of discovery and detection of actions such as writing sensitive data to removable storage
  - Requires significant organizational business process change
- **Phase 3 – Application integration, digital rights management, and correlation**
  - Requires extensive application overhauls likely taking several years to complete
  - Sophisticated software to centrally correlate content, incorporate feedback from business representatives, and prioritize responses

Questions

- **For more information, contact**

  Gib Sorebo, JD, CISSP
  sorebog@saic.com
  703.676.2605

Trademark Attributions and Vendor Name References

In the United States and/or other countries

- AccessData is a registered trademark of AccessData Corporation
- Guidance Software is a registered trademark of Guidance Software, Inc.
- Paraben is a registered trademark of Paraben Corporation
- Proventsure is a trademark of Proventsure, LLC
- Liquid Machines is a registered trademark of Liquid Machines, Inc.
- Microsoft is a registered trademark of Microsoft Corporation
- Adobe is a registered trademark of Adobe Systems Incorporated
- iWitness is a trademark of AeroVironment Inc.
- Enterasys is a registered trademark of Enterasys Networks, Inc.
- 3Com is a registered trademark of 3Com Corporation
- Cisco is a trademark of Cisco Technology, Inc.
- SourceFire is a registered trademark of SourceFire, Inc.
- Vontu is a registered trademark of Vontu, Inc.
- Vericept is a registered trademark of Vericept Corporation
- Reconnex is a registered trademark of ReconNex Corporation
- WebSense is a trademark of WebSense, Inc.
- Fidelis is a registered trademark of Fidelis Solutions LLC
- Verdasys is a registered trademark of Verdasys, Inc.
- LogLogic is a registered trademark of LogLogic, Inc.
- ArcSight is a registered trademark of ArcSight, Inc.
- netForensics is a registered trademark of netForensics, Inc.
- Vormetric is a registered trademark of Vormetric, Inc.
- GuardianEdge is a registered trademark of GuardianEdge Technologies, Inc.
- PGP is a registered trademark of PGP Corporation

Additional vendor name references

- Technology Pathways is the name given for Technology Pathways, LLC.
- AppSec is the name given for AppSec Consulting, Inc.
- PointSec is the name given for PointSec Mobile Technologies, part of Check Point Software Technologies Ltd.