Welcome to the
NetSecure 11 Conference

10 Simple Rules for Implementing an Encryption Strategy

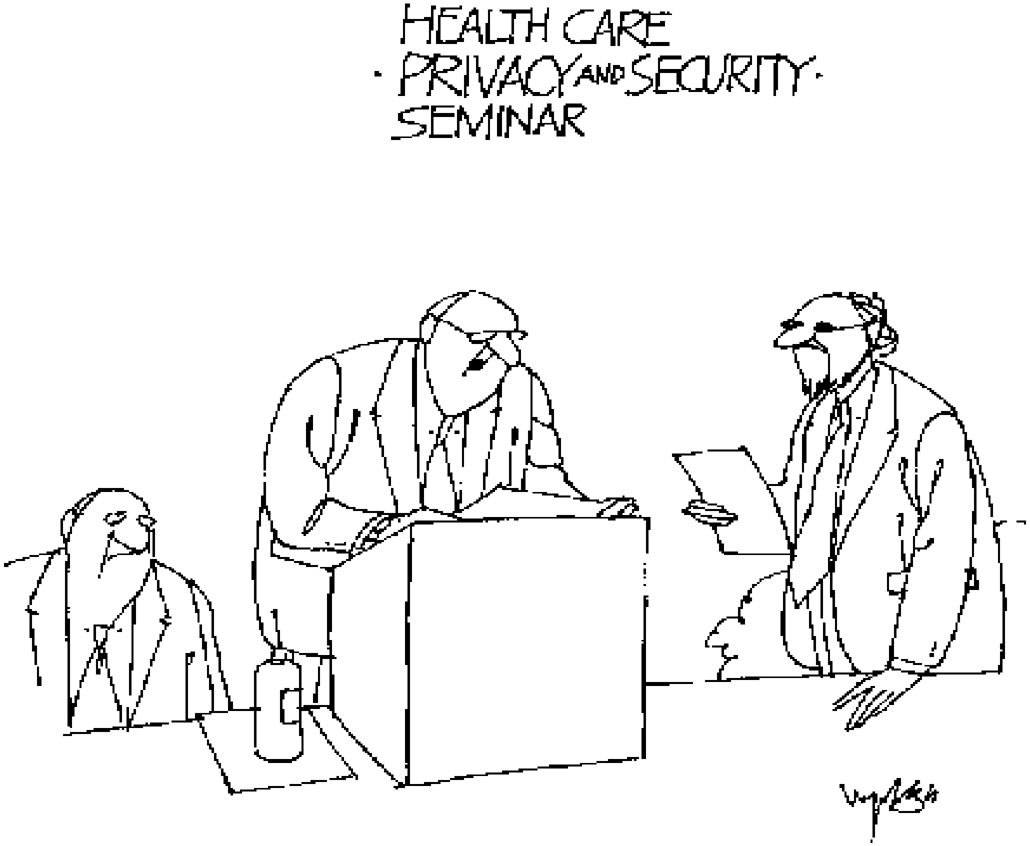
Jim Shaeffer, CEO - JCS & Associates, Inc.

The Impact of the HITECH Act on HIPAA Compliance and Data Security

https://vormetricevents.webex.com/ec0605l/eventcenter/recording/recordAction.do;jsessionid=cZBGLdTD0D8mXMvn6cyBQhpvkT2yJF7y1KV2DXnlh63PGXSb5qZG!16170486?theAction=poprecord&actname=%2Feventcenter%2Fframe%2Fg.do&apiname=lsr.php&renewticket=0&renewticket=0&actappname=ec0605l&entappname=url0107l&needFilter=false&&isurlact=true&entactname=%2FnbrRecordingURL.do&rID=1659667&rKey=7d1fdfdeb5c06895&recordID=1659667&rnd=4087497450&siteurl=vormetricevents&SP=EC&AT=pb&format=short

http://bit.ly/7yNT5u

"Our next speaker's presentation is encrypted. Those of you with laptops may log on if you have the password."



Why Encrypt?

- Common Business Drivers
  - » Compliance Objectives – PCI DSS, Internal Audit, etc.
  - » Enable new business
  - » Safe harbor from data breach disclosure (e.g. CA1386)
  - » HIPAA HITECH – emerging demand

- Obstacles to Achieving Business Objectives
  - » Data is everywhere, multiple copies, distributed architecture?
  - » Interruptions in productivity and performance? User and application resources.
  - » Can’t afford code changes to underlying, legacy applications?

Rule 1: Encryption Doesn’t Have To Be Painful

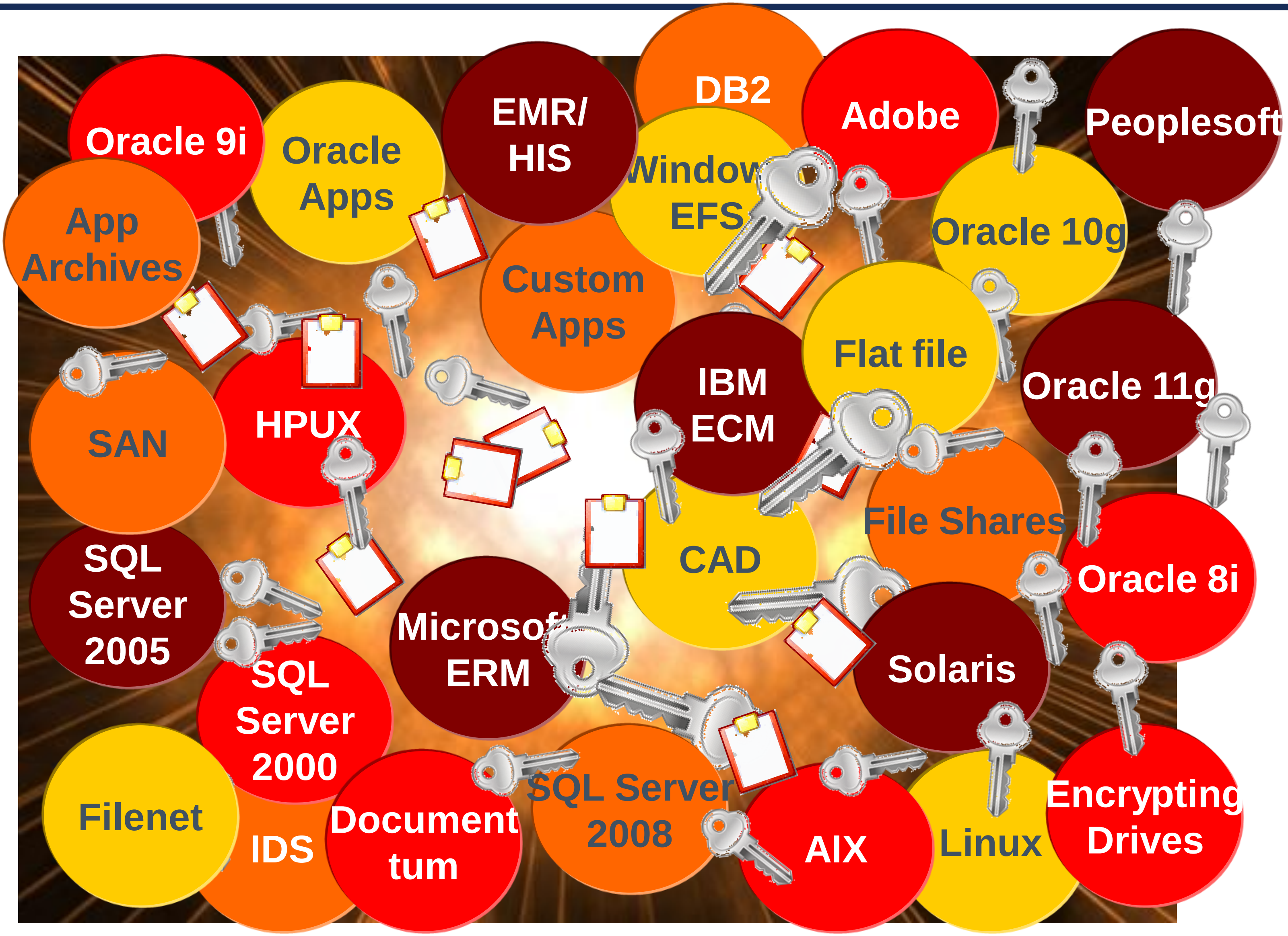
- Encryption is necessary to secure data at its source
- Encrypting data provides Safe Harbor for PCI-DSS, PIPEDA and HIPAA-HITECH
- Pain = hesitation to implement
- But, encryption technology has evolved
- Performance, application and database transparency
- New approaches to database, application and file encryption minimize the pain

Rule 2: Beware of Point Encryption Product Explosion

- System management and policy management reside in each point encryption product
- Avoid multiple point products for encryption
- Choose broad-based coverage over the largest number of systems
- This will homogenize and consolidate data security policy management

JCS &Associates, Inc.

Encryption Management Exploding Complexity



Oracle 9i

Oracle Apps

EMR/ HIS

DB2

Adobe

Peoplesoft

App Archives

Windows EFS

Custom Apps

Oracle 10g

Flat file

IBM ECM

Oracle 11g

SAN

HPUX

File Shares

CAD

Oracle 8i

SQL Server 2005

Microsoft ERM

Solaris

SQL Server 2000

Filenet

IDS

Document tum

SQL Server 2008

AIX

Linux

Encrypting Drives

Rule 3: Understand the EKM Problem/Solution Area

- Primary purpose of an Enterprise Key Manager (EKM) is to provide:
  - Centralized point of key generation
  - Key Lifecycle management
  - Key backup and recovery
- EKM needs grow with the number of points for key storage
- EKMs are passive
  - Do not actively control the security of the encryption keys – that is handled by the encryption system
- A complete solution includes secure access controls
- EKM cannot provide a comprehensive strategy, as the overall key management complexities are far too great for EKM to handle alone

Rule 4: Look Carefully at Integrated Key Management

- Integrated Key Management (IKM) is the actual key management structure of an encryption system
- IKM differs from EKM in that IKM directly controls:
  - Security of keys, Storage of keys, Handling of keys
- IKM must be a critical part of the evaluation criteria for any encryption solution
- The goal should be a secure and transparent IKM system
- Reduction of overhead (cost) will be significantly reduced
- The need for EKM will grow directly with the number of encryption systems that are installed
- Selecting solutions that provide IKM for the largest number of required encryption points will reduce the EKM problem

Rule 5: Transparency is Critical

- The more transparent the encryption solution, the more easily it can be integrated and supported long term
- The need for transparency in the decision-making process cannot be emphasized enough
- Without transparency, encryption solutions can take up to a year to install, resulting in significant costs during application changes
- With transparency, encryption can be implemented within days
- Transparent encryption solutions never need to be considered as an inhibitor to implementation
- This results in optimal use of encryption within the information management solutions that are already in place

Rule 6: Look Beyond the Column

- Intuitively, column-level encryption seems like the most practical database data encryption methodology
- However, the invasiveness (all applications that use that column of data must be modified) and scalability make it inefficient
- Limitation of protection and usability can also suffer
- Column-level encryption is not transparent to databases and apps
- The lack of transparency can drastically complicate application change management and require significant customization of apps
- Performance will suffer as a result of column-level encryption
- Every time a new column is created or identified that needs protection, more coding within the application must be done
- Log files, both database and application contain PII
- Column-level encryption offers no protection for unstructured data

Rule 7: Prepare for Virtualization

- Virtualization changes the overall security model
- Virtualization is increasing exponentially through enterprises
- The Operating System (O/S), because it is now portable, can be moved from system to system
- Full disk encryption and physical security lose their effectiveness in virtualized environments
- Instead of stealing a disk, entire operating environments can be logically accessed and easily transferred
- Data and system protection mechanisms should be reviewed when considering a virtualization, in light of the new security risks
- Implement data encryption that travels with the O/S in conjunction with or instead of full disk encryption

Rule 8: Policy is Key

- Encryption is easy
- Without the right encryption approach, decryption controls for strong security can be hard
- By combining encryption with an access control-based decryption policy, the value of encryption grows as controls are placed on the data
- Defining policies, linking them to entities in the directory, and then reusing those policies will save the organization time and money
- Having a single console to enter the policies into, no matter where the data-at-rest resides, results in lowered total cost of ownership
- Successful encryption projects are defined not by scrambled bits, but by the application of security policies on the data itself during decryption of that data

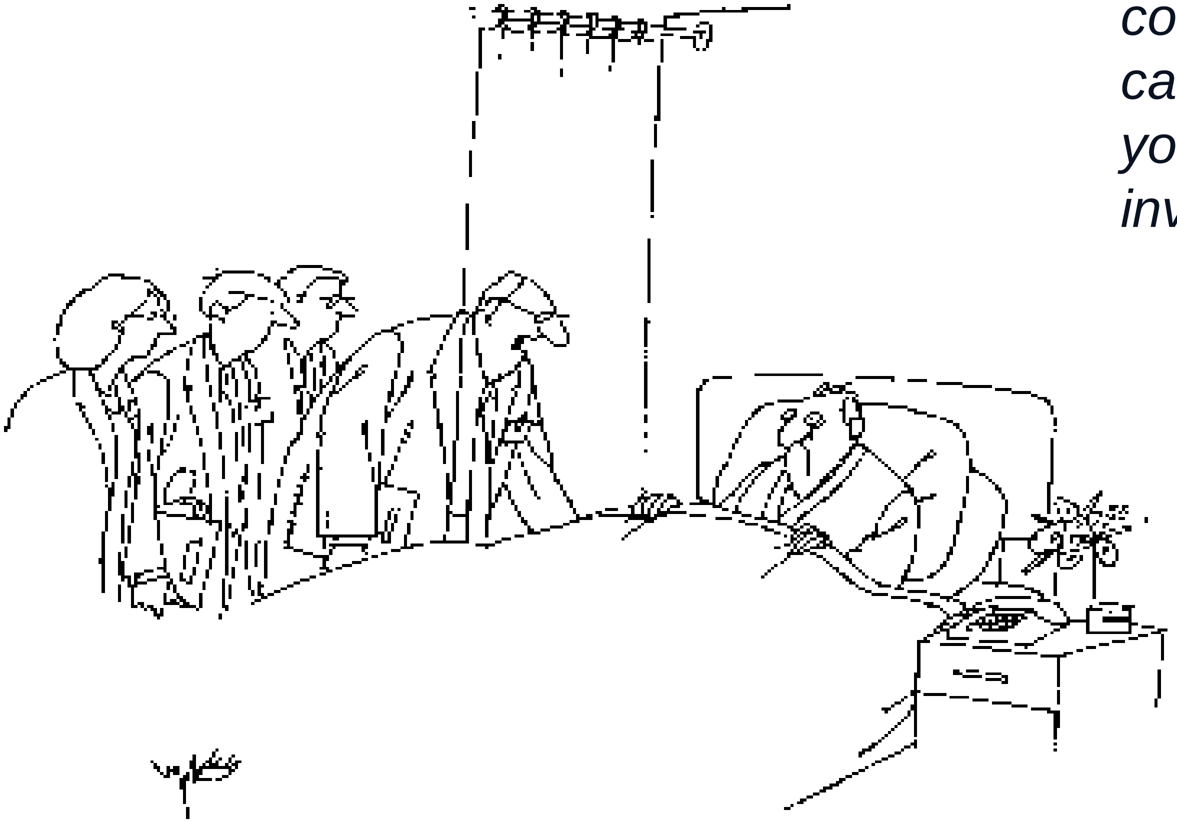
Rule 9: Consider ALL Applications and Operating Systems

- Many encryption solutions are tied to specific versions of applications and operating systems
- Numerous databases may be operating on a wide array of different operating systems
- Implementing encryption as part of the application leads to an explosion in the number of encryption solutions
- Version specific database encryption can lead to a huge hole the the overall security solution if all databases cannot be upgraded
- Training costs will increase with a wide array of point solutions that are tied to the application or the operating system
- Solutions exist that can cover all applications across multiple operating systems transparently, resulting in a reduction in key management issues and implementation and administration costs

Rule 10: Think of Encryption as an Enabler

- Encryption can help your business, enabling compliance with regulations, resulting in increased customer confidence
- State and Federal regulations require organizations to protect sensitive information, with penalties for noncompliance
- The use of encryption demonstrates proactive dedication to data protection and adherence to State and Federal regulations
- With today's technologies, encryption should no longer be feared!
- Effective, cost efficient solutions, on the endpoint, at the server level, within e-mail and FTP are available today
- A broad data security program can be deployed without changing applications or requiring administrators to deploy, update and learn multiple solutions

Changes to the HIPAA Privacy and Security Rules: Additional Limitations on the Use and Disclosure of PHI



"Normally, I'd discuss your condition with these first-year residents, but because of confidentiality restrictions, all I can really tell them is that you're a shoe-in for an invasive procedure."

JCS Data Protection Solution Set

- Vormetric
  - Data-at-rest Encryption for Database, Application and File Servers Running on Windows, Linux and Unix
- Safend’s Protector and Encryptor
  - All-in-one endpoint security agent and Data Loss Prevention at the endpoint
- PKWARE
  - Compression/Encryption on all Platforms
- Pano Logic
  - Zero Client Desktop Virtualization

Integrating Best of Breed Security Solutions

Data Security Resource Planning Process

(closed loop, framework approach)

> Safeguards & Controls <

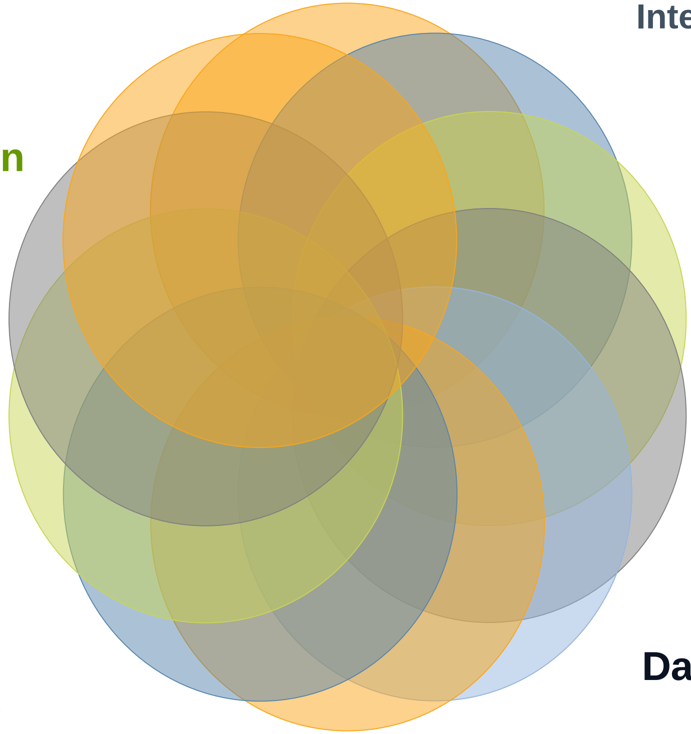
Data Backup and Retention
Vormetric

Data Leakage & Protection
Network - PacketSure
Endpoint - Safend
E-mail - PacketSure

Database Security
Servers – Vormetric
Network – PacketSure

Data Encryption
Servers - Vormetric
Endpoint - Safend

Audit & Compliance Review



Access Controls
Servers - Vormetric
Endpoint – Safend
Internet – PacketSure

Risk Assessment
Internal and External Auditors

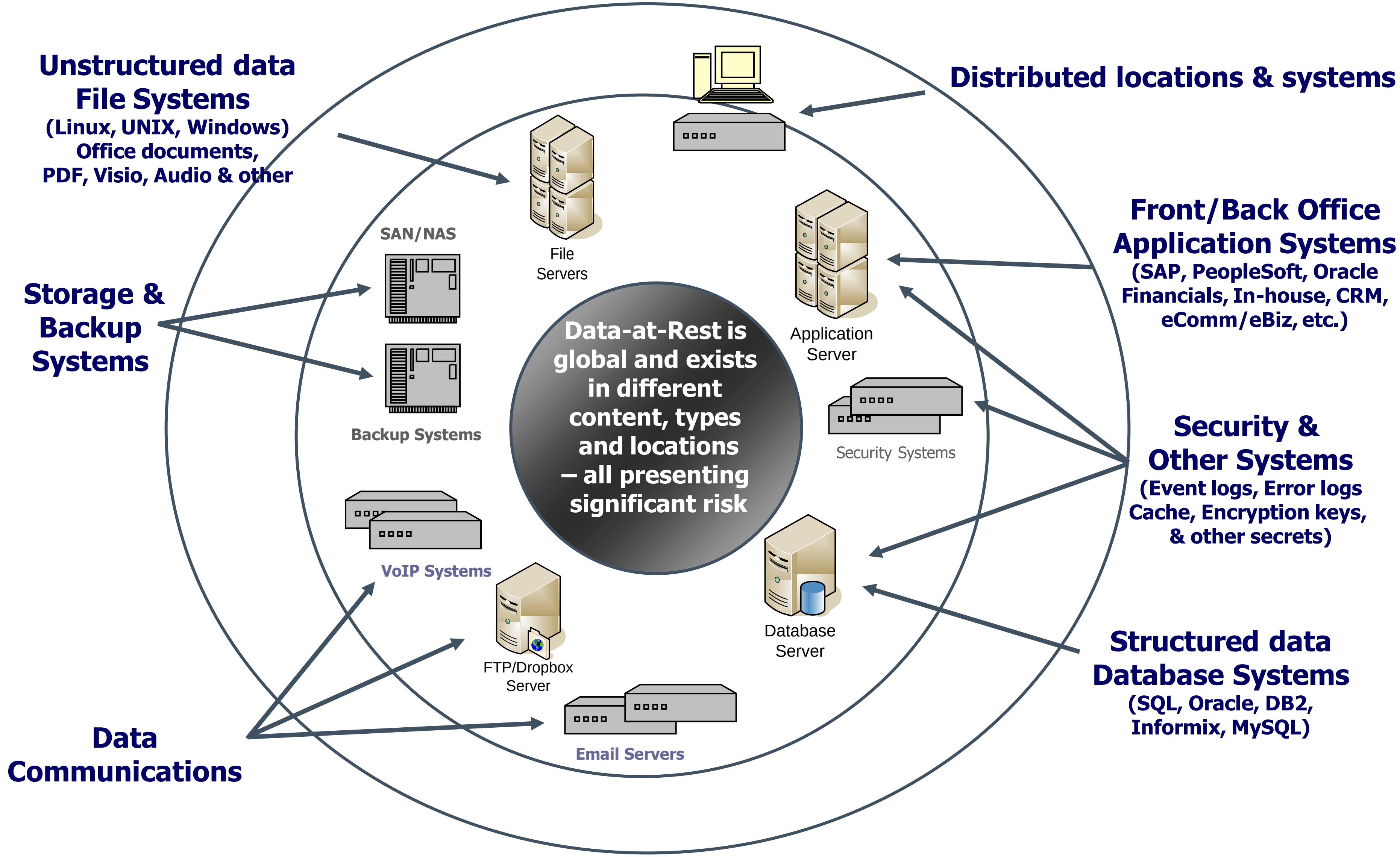
Data Classification
Retention Requirements

Data Discovery/Mapping
Data flow, including HL7 Trans.
Data exposure points
Cloud storage of data

Data Protection Gap Assessment
Internal and External Auditors

> Process & Policy <

Data-at-Rest Server-level Environment



Data-at-Rest is global and exists in different content, types and locations – all presenting significant risk

Unstructured data File Systems
(Linux, UNIX, Windows) Office documents, PDF, Visio, Audio & other

Distributed locations & systems

Front/Back Office Application Systems
(SAP, PeopleSoft, Oracle Financials, In-house, CRM, eComm/eBiz, etc.)

Storage & Backup Systems

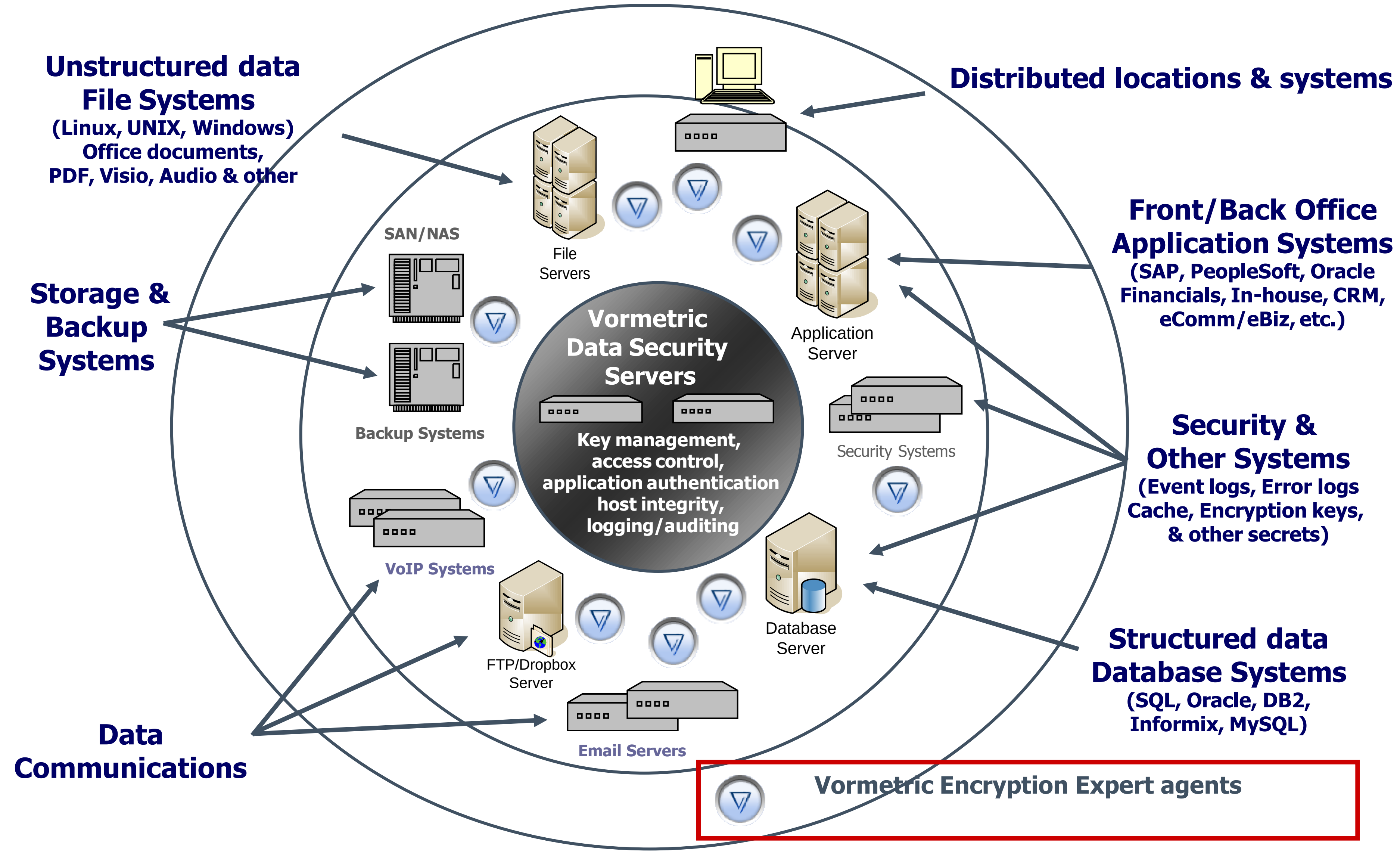
Security & Other Systems
(Event logs, Error logs Cache, Encryption keys, & other secrets)

Structured data Database Systems
(SQL, Oracle, DB2, Informix, MySQL)

Data Communications

Integrating Best of Breed Security Solutions

Data-at-Rest
Server-level Environment



Vormetric Safe Harbor for Compliance

FIPS Certified Encryption	✓
Secure Key Management	✓
Meets NIST 800-111	✓
Proven Performance	✓
Encryption + Access Control	✓
Audit	✓
Separation of Duties	✓
Low TCO	✓
Rapidly Deployable	✓

"Vormetric encrypts in a way to minimize performance overhead. It also offers separation of duties, centralized key management and policy management"

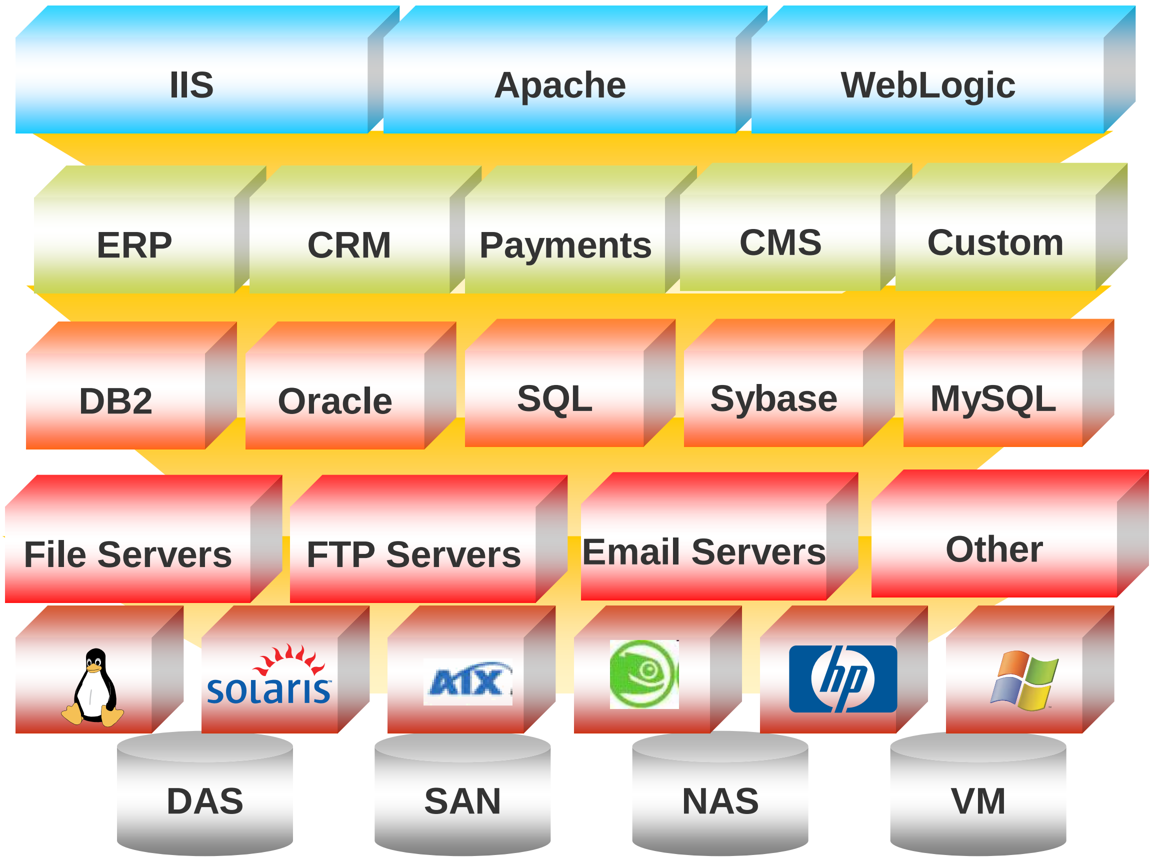
Noel Yuhanna
Forrester Research

Vormetric's Extensible Solution

•Log Files
•Password files
•Configuration files
•Archive

•Data files
•Transactions (HL7)
•Exports
•Backup

•File shares
•Archive
•Content repositories
•Multi-media
•Log Files



IIS | Apache | WebLogic

ERP | CRM | Payments | CMS | Custom

DB2 | Oracle | SQL | Sybase | MySQL

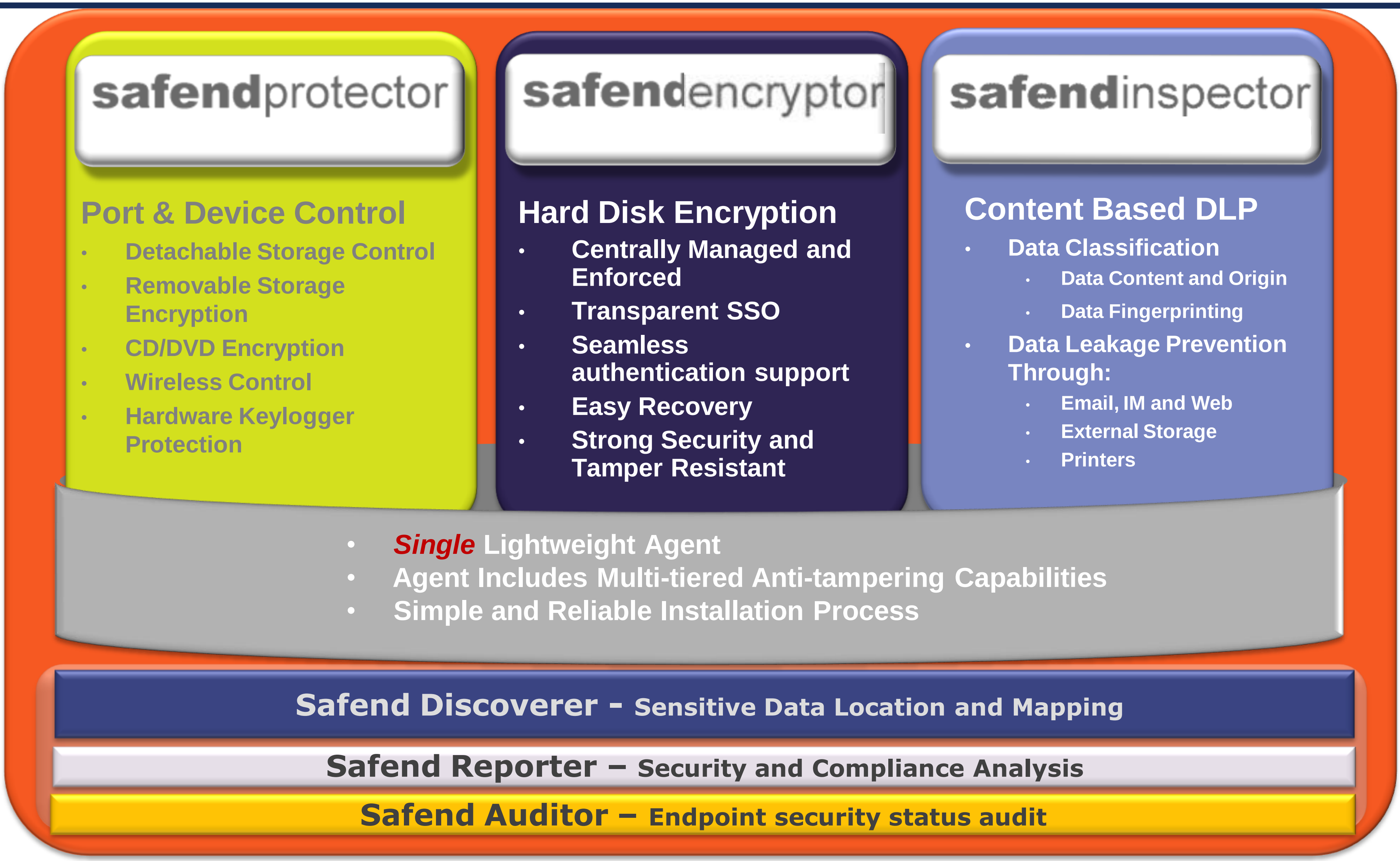
File Servers | FTP Servers | Email Servers | Other

DAS | SAN | NAS | VM

> *"Future scalability to apply this solution where additional needs may arise was a significant consideration"*
>
> **Thomas Doughty, CISO, Prudential**

Integrating Best of Breed Security Solutions

Safend Data Protection Suite



safendprotector

Port & Device Control

- Detachable Storage Control
- Removable Storage Encryption
- CD/DVD Encryption
- Wireless Control
- Hardware Keylogger Protection

safendencryptor

Hard Disk Encryption

- Centrally Managed and Enforced
- Transparent SSO
- Seamless authentication support
- Easy Recovery
- Strong Security and Tamper Resistant

safendinspector

Content Based DLP

- Data Classification
  - Data Content and Origin
  - Data Fingerprinting
- Data Leakage Prevention Through:
  - Email, IM and Web
  - External Storage
  - Printers

- *Single* Lightweight Agent
- Agent Includes Multi-tiered Anti-tampering Capabilities
- Simple and Reliable Installation Process

Safend Discoverer – Sensitive Data Location and Mapping

Safend Reporter – Security and Compliance Analysis

Safend Auditor – Endpoint security status audit

For more information, go to http://www.jcsinc.com,call 800-968-9527 or e-mail info@jcsinc.com

Regaining Control of Your Endpoints

Visibility Safend Auditor & Discoverer

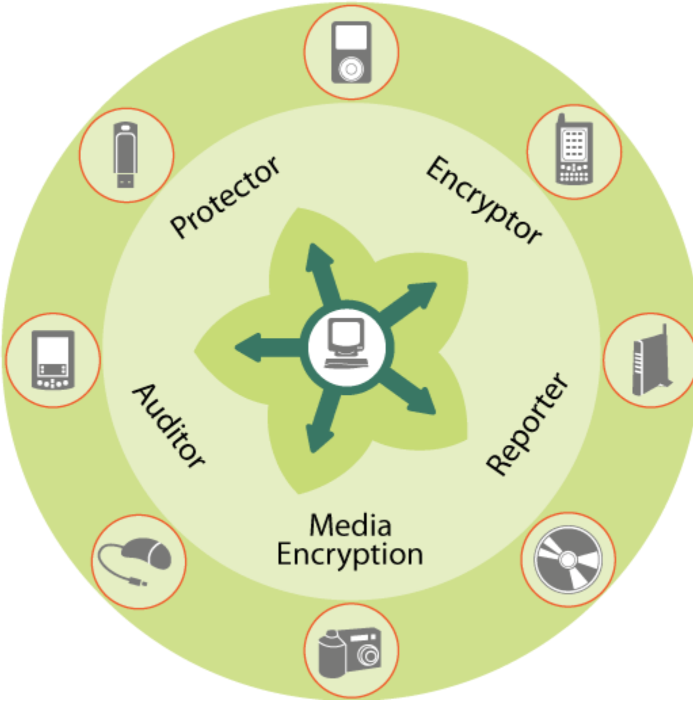
- Shows who’s connecting which devices and wireless networks to every enterprise endpoint

Control Safend Protector

- Controls the use of wireless ports and removable devices by file/device type
- Encrypts removable media and optical media

Protection Safend Encryptor

- Enforces hard disk encryption of all data stored on laptops and PCs
- Easy recovery of machine and files



Inspection Safend Inspector

- Prevents sensitive data leakage through e-mail, web, removable storage, and additional data transfer channels

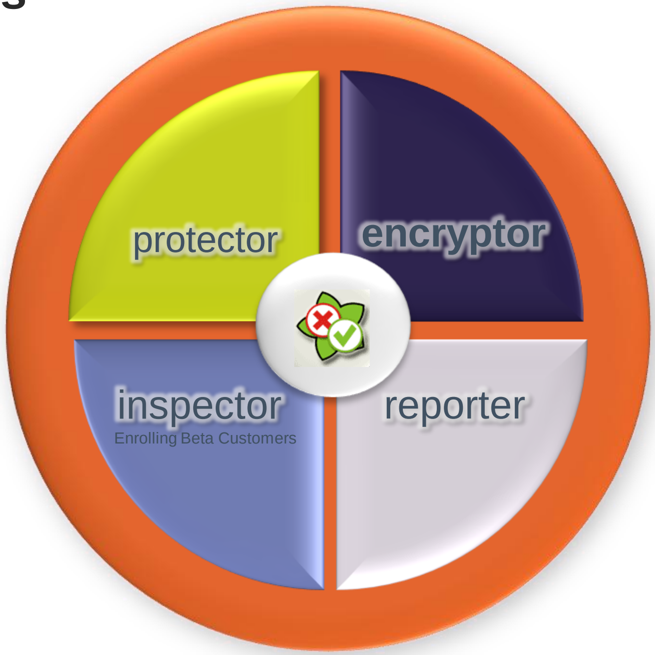
Analysis Safend Reporter

- Provides graphical security reports and analysis of your Safend protected environment

For more information, go to http://www.jcsinc.com,call 800-968-9527 or e-mail info@jcsinc.com

Safend Data Protection Suite

- **Safend Data Protection Suite features and benefits**
  - Transparent Internal Hard Disk Encryption
  - External storage encryption for removable storage devices, optical and external hard drives
  - Robust port and device control
  - Wireless control
  - Hardware keylogger protection
  - Tamper resistant
  - Enterprise grade management, providing full visibility and control over organization security status



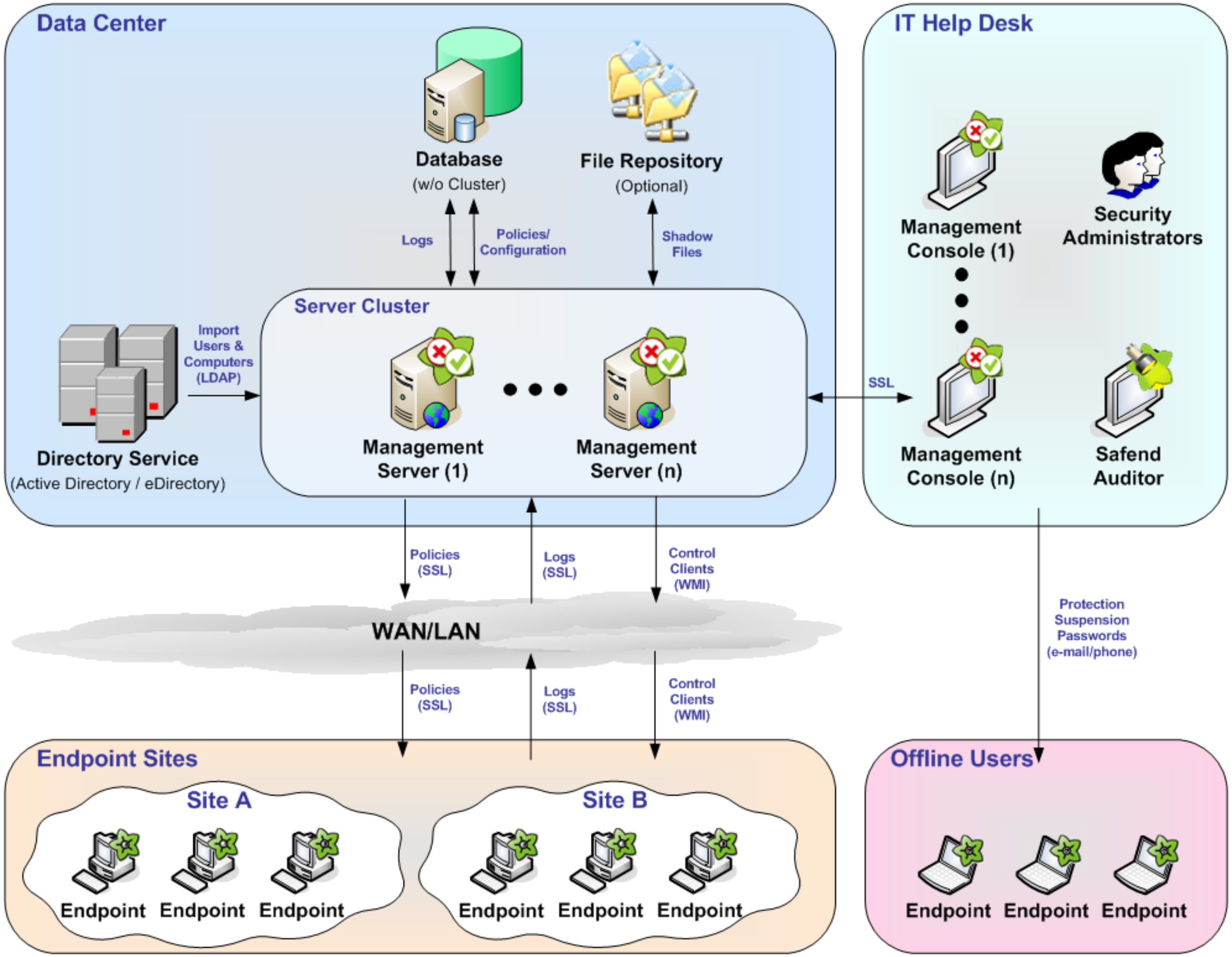
- **All functionality is provided by a single management server, single management console and a single, lightweight agent**

- **Certifications**
  - Common Criteria EAL2 certified
  - FIPS 140-2 Validated

Safend Protector
Common Criteria
EAL-2 Certified

FIPS VALIDATED 140-2

Safend Data Protection Suite - Architecture



Integrating Best of Breed Security Solutions

VORMETRIC

PKWARE®

safend
Securing Your Endpoints

PKWARE Introduction

Two Significant IT Challenges

30%
70%
110%

Explosive
Data Growth

The Security
of That Data

PKWARE Solutions

Data Reduction

Data Security

PKWARE Benefits

1 **Reduce Costs** Related to Data

2 Improve Data Center **Performance Metrics**

3 Manage Issues Related to **Governance, Risk and Compliance**

What is a .zip? It's a Portable Container

A Few Things About Portability

WITHOUT PKWARE, PORTABILITY OF DATA IS LIMITED BY:

•Size of the data

•Sensitivity of the data

•Interoperability of the data

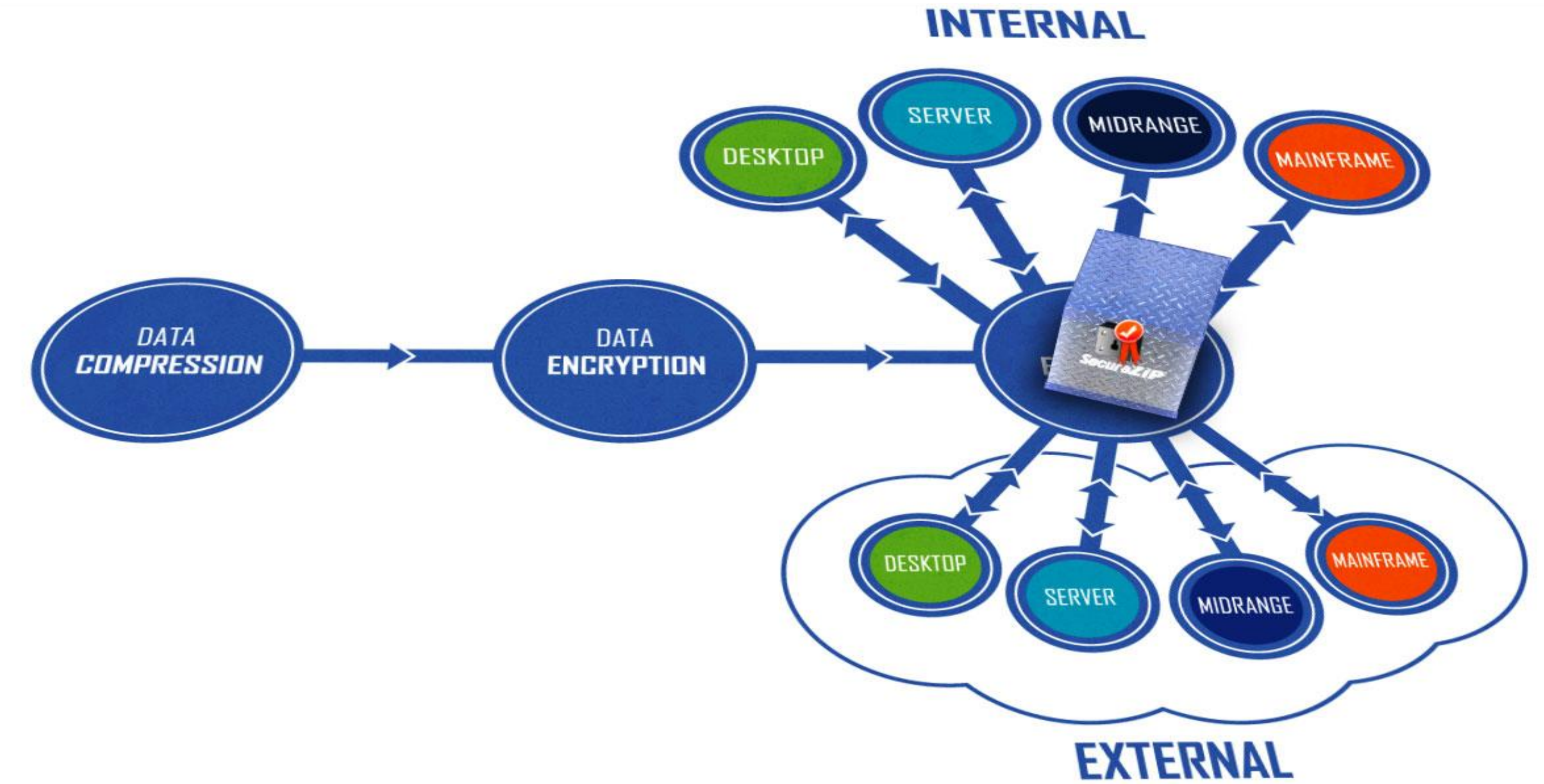
To the Cloud!

7(B) EMC MAKES NO WARRANTY THAT THE SERVICE WILL BE AVAILABLE ON AN UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE BASIS

14 WE DO NOT PROMISE THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE.

7.2 SECURITY. WE STRIVE TO KEEP YOUR CONTENT SECURE, BUT CANNOT GUARANTEE THAT WE WILL BE SUCCESSFUL AT DOING SO, GIVEN THE NATURE OF THE INTERNET.

What PKWARE Does



PKWARE Solutions

SecureZIP PartnerLink

Benefits

- Secure data exchange with business partners based on a single solution
- Increase business efficiency
- Integrate seamlessly with existing IT infrastructures

SecureZIP

Benefits

- Secure data everywhere at all times
- Maintain control of data for audit and recovery purposes
- Flexible security depending on organization infrastructure
- Conserve storage space and reduce processing costs and file transfer time
- Minimize deployment and management costs

PKZIP®

Benefits

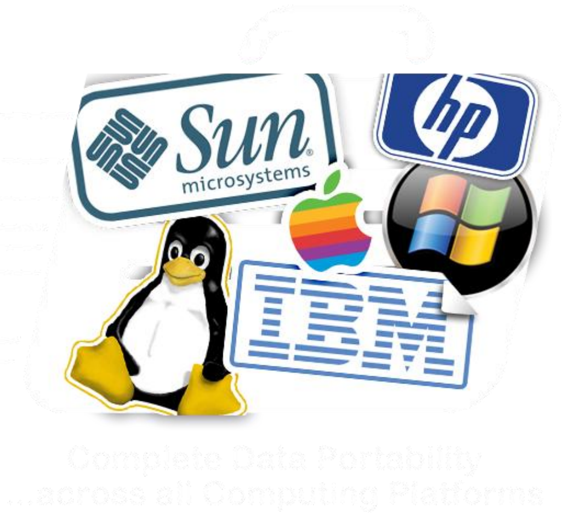
- High ROI and improved end user productivity with reduction in storage, network bandwidth, and processing hardware costs
- Ease of use enabling high rates of user adoption
- Simplified management through centralized policy controls
- Secure corporate data quickly through easy upgrade to SecureZIP

For more information, go to http://www.jcsinc.com,call 800-968-9527 or e-mail info@jcsinc.com

Metrics

	Storage Requirement on Send Side	Elapsed Time (seconds)	CPU Seconds Consumed	Storage Requirement on Receive Side	Is the Data Secure?
RAW File	**500 MB**	104	N/A	**500 MB**	**NO**
Competition	160 MB	**141**	90	160 MB	**YES**
PKWARE	160 MB	**64**	12	160 MB	**YES**

Only Total Integrated Single Solution



Only vendor to place unstructured data in portable containers

Move container **across every platform** in your enterprise, internally & externally

“Wrap” portable data containers **with strong security**

Integrating Best of Breed Security Solutions

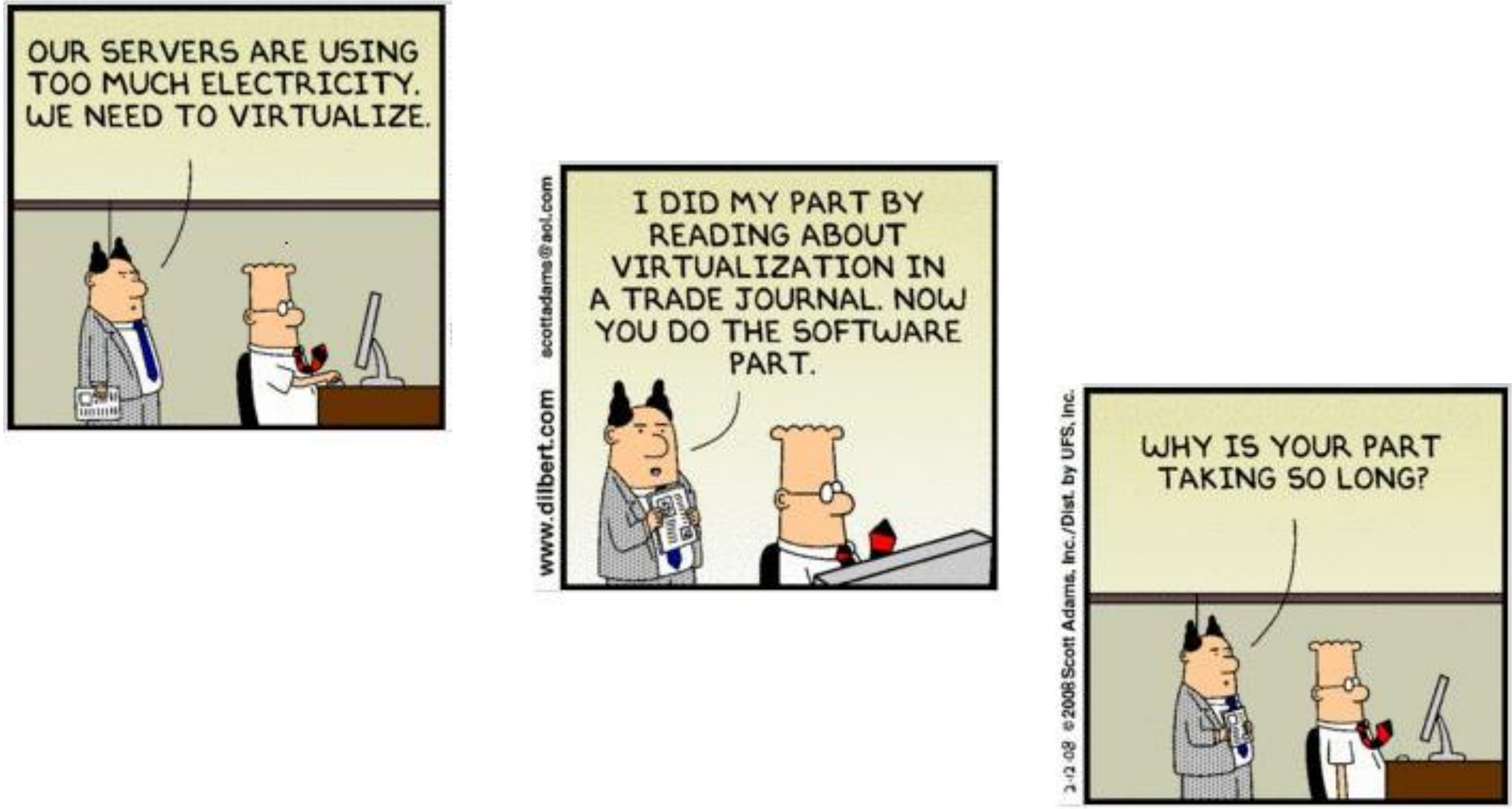
VORMETRIC

PKWARE®

safend
Securing Your Endpoints

pano
LOGIC

Dilbert’s World of Virtualization


OUR SERVERS ARE USING TOO MUCH ELECTRICITY. WE NEED TO VIRTUALIZE.
I DID MY PART BY READING ABOUT VIRTUALIZATION IN A TRADE JOURNAL. NOW YOU DO THE SOFTWARE PART.
WHY IS YOUR PART TAKING SO LONG?
www.dilbert.com scottadams@aol.com
3-12-08 ©2008 Scott Adams, Inc./Dist. by UFS, Inc.

Traditional Desktop Management

Excessive Costs Capex & Opex

- 3-5 Year Refresh Cycles
- Hidden Costs from Gap Filling Technologies
- High Operating Expenses
- Exorbitant Energy Costs

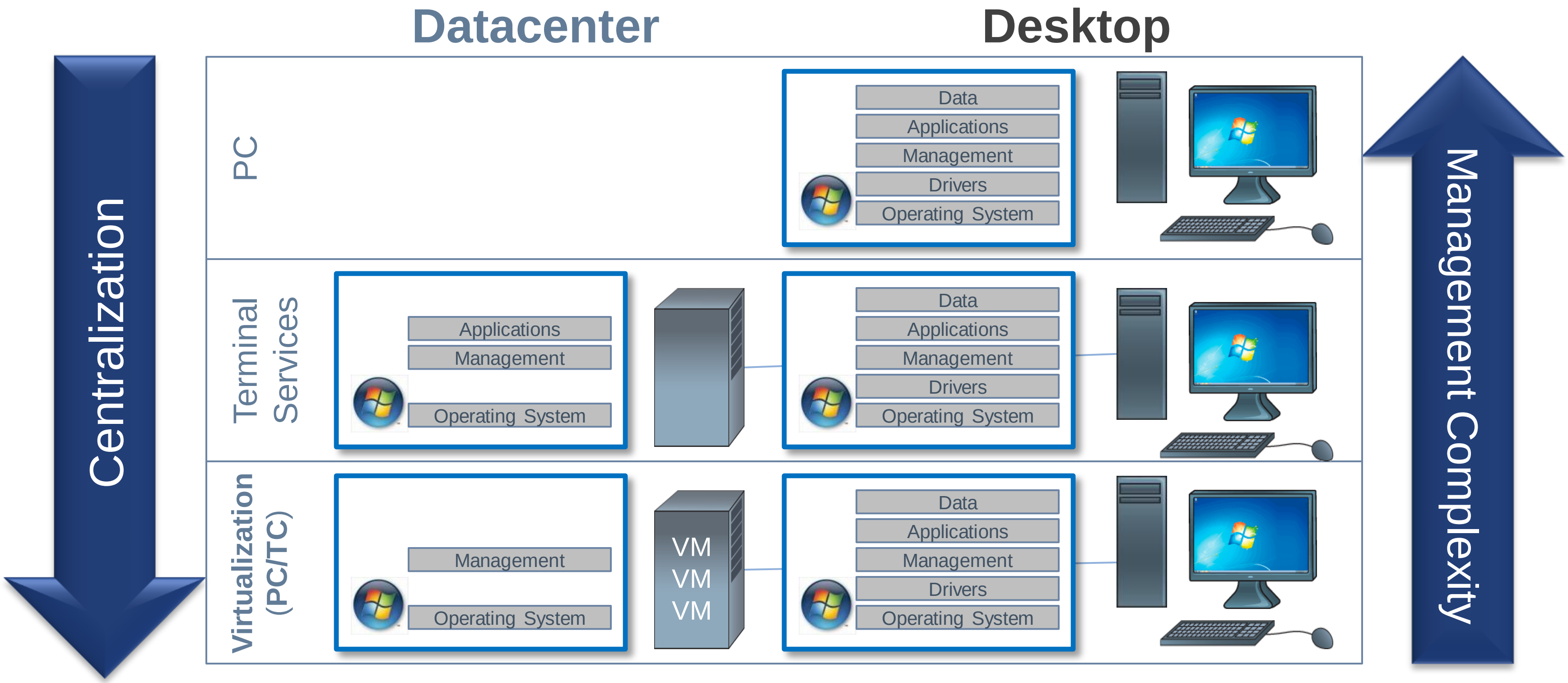
Overburdened Management

- Multiple Vendors
- Multiple Products
- User Customizations with Different Systems, Users, Images, Applications
- Distributed PC Architecture

Security and Compliance Risk

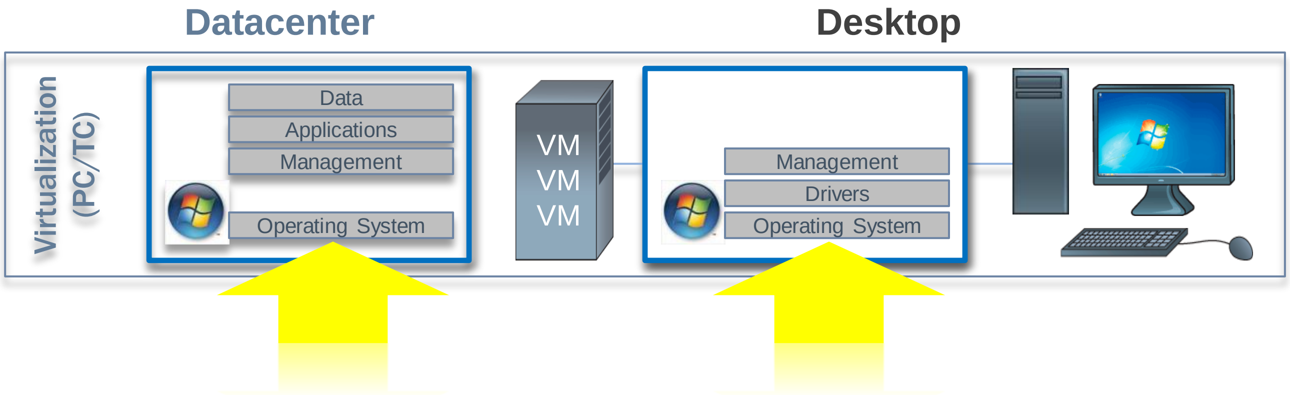
- Endpoint Breaches
- Regulatory Compliance: HIPAA, SEC, Grahm Leach-Bliley, PCI-DSS
- Intellectual Assets at Risk
- Unpredictable user activity

Desktop Virtualization Today



For more information, go to http://www.jcsinc.com,call 800-968-9527 or e-mail info@jcsinc.com

Desktop Virtualization Benefits Not Realized



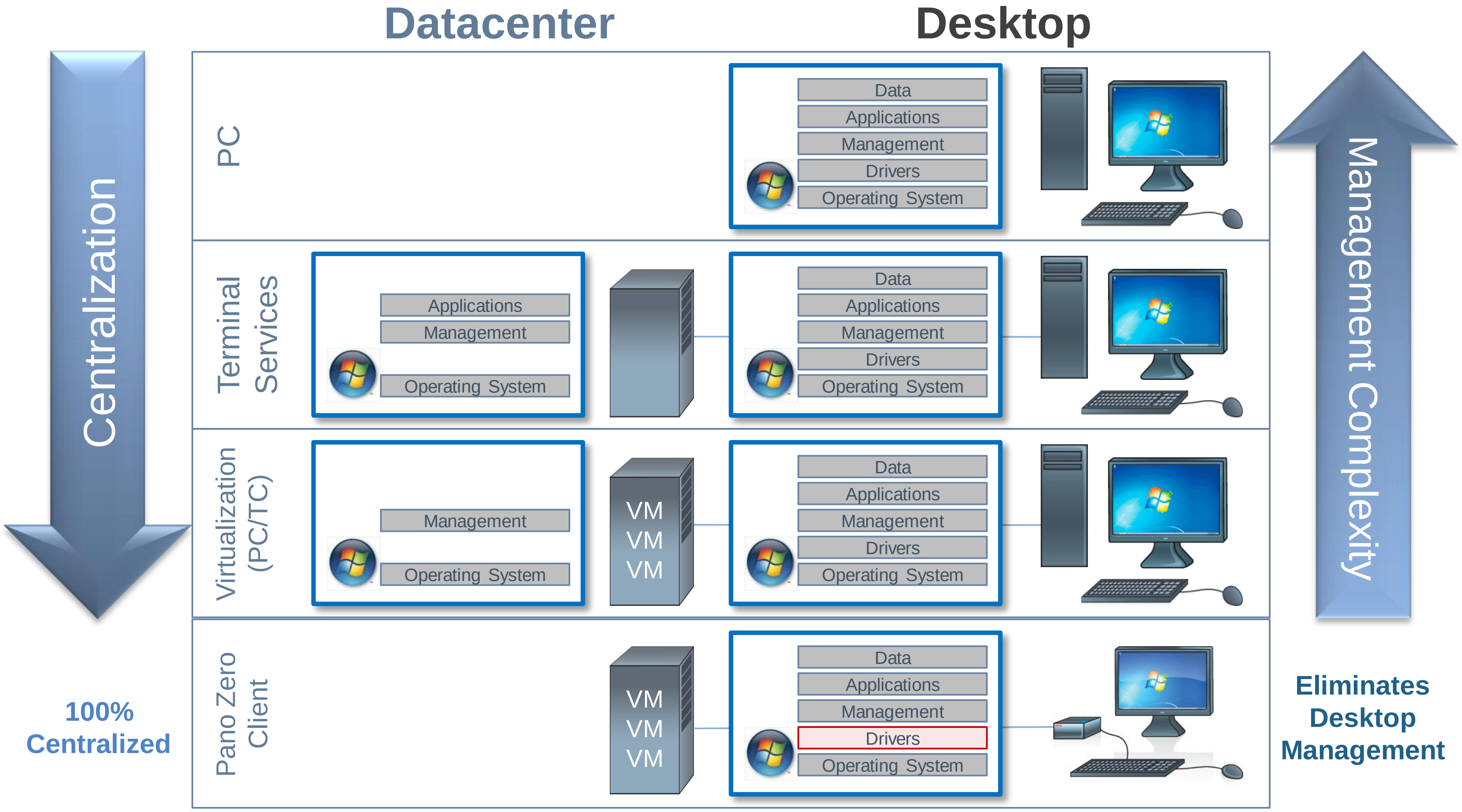
Server Virtualization

- Lower TCO
- Increased Utilization
- Standardization
- Centralized Control

Desktop Virtualization

- Costly
- Overly Complex
- Lack of Security Controls
- Management Drain

Radical Centralization



	Datacenter	Desktop
PC		Data Applications Management Drivers Operating System
Terminal Services	Applications Management Operating System	Data Applications Management Drivers Operating System
Virtualization (PC/TC)	Management Operating System VM VM VM	Data Applications Management Drivers Operating System
Pano Zero Client	VM VM VM	Data Applications Management Drivers Operating System

100% Centralized

Eliminates Desktop Management

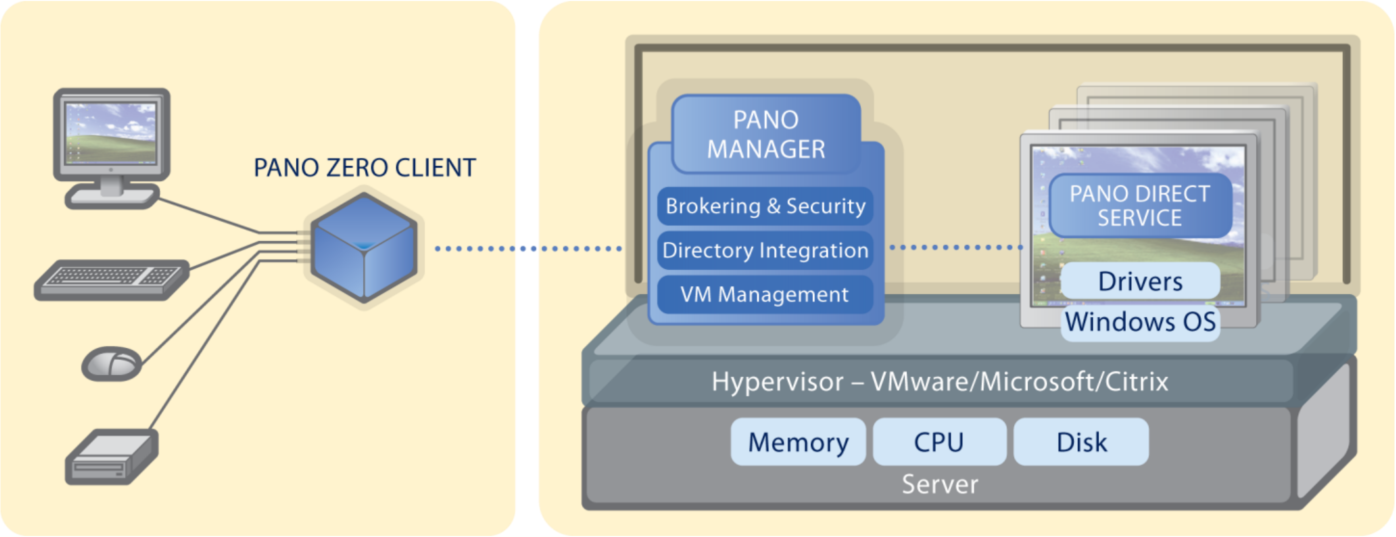
Virtual Desktop Integration

Zero Client Computing

Radical Centralization. Purpose-Built for Virtualization.

Easy to Buy, Easy to Use

- Complete Zero Client virtual desktop platform in one solution
- Installs in an hour, provisions new users in just minutes
- No need to buy add-ons or protocol extensions



For more information, go to http://www.jcsinc.com,call 800-968-9527 or e-mail info@jcsinc.com

Choice of Hypervisor Platforms

- First zero-client hyper-visor independent platform for virtual desktops
- Choice of Hyper-V, VMware or Citrix platforms
- All three platforms included with the purchase – select platform during installation

	Hyper-V Platform	VMware Platform	Citrix Platform
Connection Broker	pano LOGIC Pano Manager	pano LOGIC Pano Manager VMware View Manager (optional)	pano LOGIC Pano Manager Citrix XenDesktop 4
DVM Provisioning	Pano Manager Connector for SCVMM System Center Virtual Machine Manager	vmware vCenter Server View Composer (optional)	CITRIX XenDesktop 4 NetScaler
Hypervisor	Windows Server 2008 R2 with Hyper-V Hyper-V Server 2008 R2	vmware vSphere ESX / ESXi	CITRIX XenServer

For more information, go to http://www.jcsinc.com,call 800-968-9527 or e-mail info@jcsinc.com

Pano Logic's Vision

- Centralize Everything
  - Move all of the software and processing into the datacenter to maximize the benefits of centralization
- Make it Simple, Make it Complete
  - Deliver everything needed, in one easy-to-buy, easy-to-deploy system, that can be installed in 1 hour without requiring a systems integrator
- Be only as Disruptive as You Have to Be
  - Provide as close to a native Windows desktop experience as possible, including native driver support, to minimize user retraining and deployment disruptions

Pano Logic Value Proposition

- Best CAPEX and OPEX Choice
  - Drive IT efficiency
  - Customize resource allocation
  - Green I/T – energy savings ($80 to $100 per desktop per Year!)
- Centralized Management
  - Faster Provisioning – as little as minutes per desktop
  - Eliminate desktop break/fix
  - Dynamically scaleable
- Safer and More Secure
  - Reduced IP or virus threat at the desktop
  - Control data in the central environment

Integrating Best of Breed Security Solutions

safend
Securing Your Endpoints

Questions?

THANKS FOR ATTENDING OUR PRESENTATION

For more information, contact:

JCS & Associates, Inc.
Phone **800-968-9527**
E-Mail: **info@jcsinc.com**
Web Site: **http://www.jcsinc.com**