



Preventing Leakage

How to Protect and Manage the Movement of Data

Scott Shepard
Principal Consultant
GlassHouse Technologies

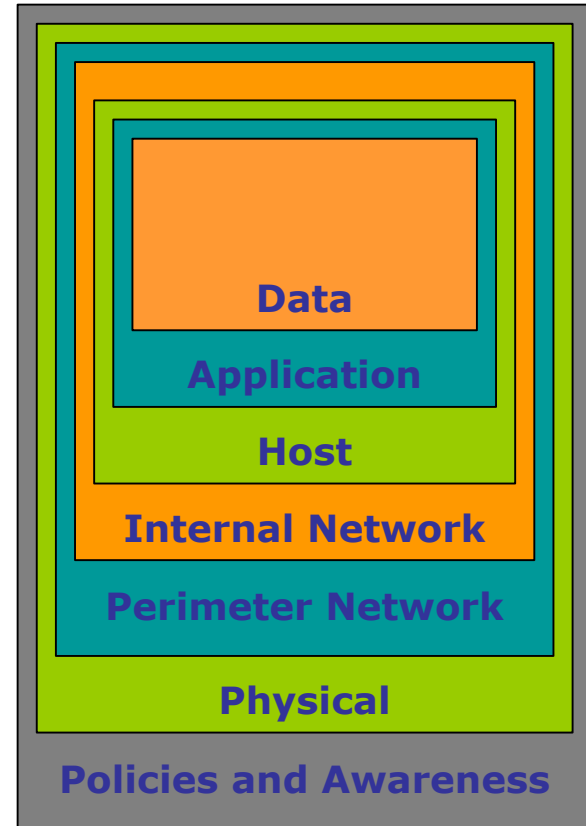
- Preventing Leakage: How to Protect and Manage the Movement of Data
 - Given the current economic climate and financial scandals, data leakage may become even more important in the coming year. Companies know how to implement systems to protect outside threats, but what about those that originate inside the company walls?
 - In this session attendees will learn how to effectively design and implement policies, frameworks and tools to protect the organization from the following:
 - Insiders sending confirmation information via e-mail
 - Accidentally spilling confidential information on the internet from using Web 2.0 technology (blog, mashup)
 - Physical/IT security – a laptop being stolen out of a hotel room or from a trade show
- <http://camconferences.com/events/2009/threat.htm>

- Objective: How to protect and manage the movement of data
- Why change security strategies?
- Security strategy methodology
- Cast Study:
 - Moving to a Data-Centric security strategy
 - Protection of Privacy Information
 - Secure Design Center

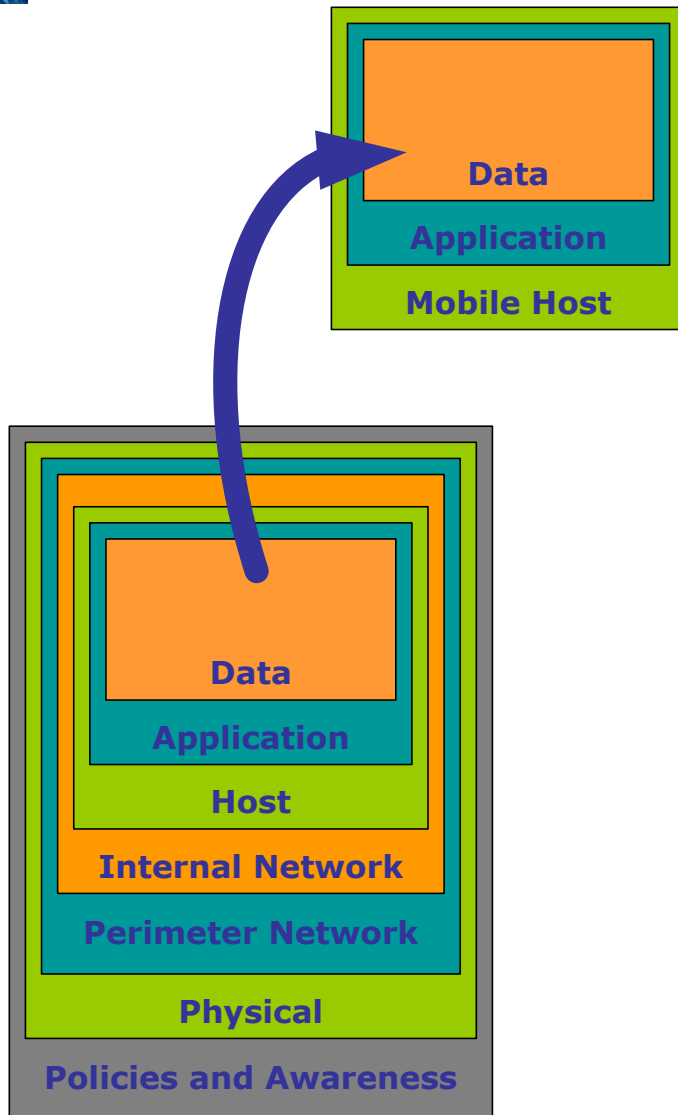


Defense-in-Depth

- “Multiple layers of defense are placed throughout an Information Technology (IT) system” –Wikipedia
- Objective:
 - Slow down the attacker
 - Allow IT to respond
 - Hopefully prevent the data from leaking.



Data-Centric



- What happens when . . .
 - Sensitive data leaves the traditional layers of protection?
 - Users abuse their privileges? (Insider Threat)
- “Data-Centric” security strategy applies defense-in-depth strategies, where possible, for a data in a mobile world

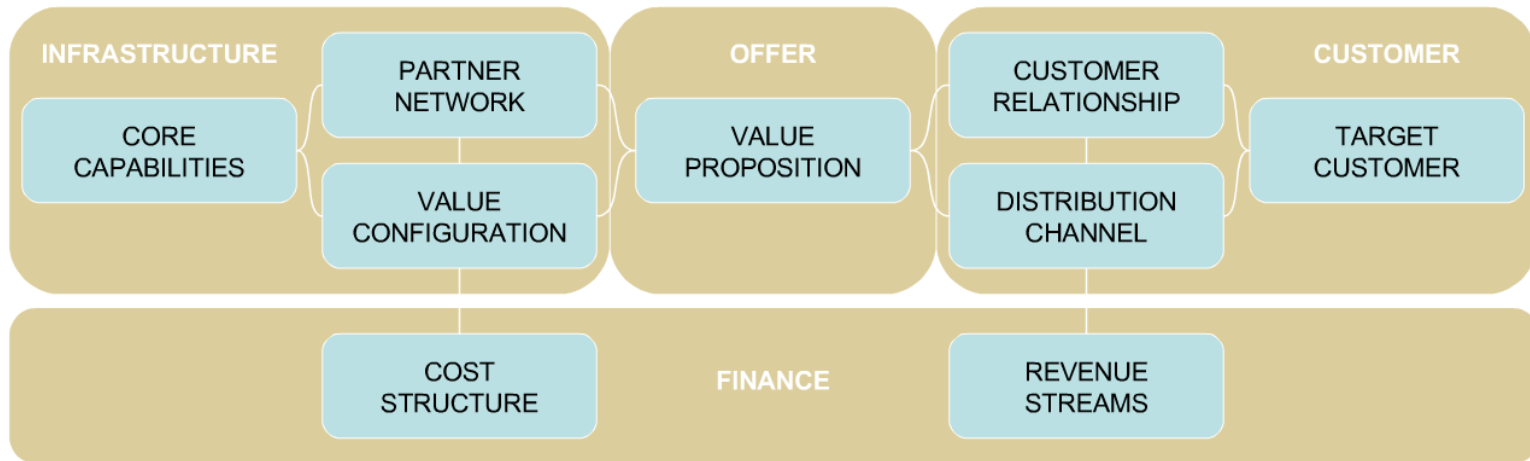


Security Strategy Methodology

- Understand the Business Drivers
- Define the Initial Policy
- Identify the Control Points
- Determine Security Measures
- Validate and Update



Understanding the Business Drivers



- Customer Relationship (Who)
 - Who are the company’s customers?
- Value Proposition (What)
 - What does the company do for customer?
- Infrastructure (How)
 - How does the company get that job done? Partners?
- Finance (How much)
 - How does the company make money?

*Based on “Business Model Ontology” by Alexander OSTERWALDER, UNIVERSITE DE LAUSANNE

Define the Initial Policy



- Align the security policy to the business drivers
 - Protection of Intellectual Property
 - Service Availability
- Determine the applicable laws and regulations the company



Control Points

- Identify the Control Points
 - Where in the flow and storage of data can security control points be inserted to protect confidentiality, integrity, and availability
- Control Points
 - Applied at traditional layers:
 - User, network, system, application, data
 - Targeting
 - Access (entry and exit), authorization, use, trust relationships, management, configuration, storage, and transport



Apply Security Measures

- Determine Security Measures (Processes and Technologies)
 - For each control point identified, consider protective, detective, and response security measure
- Identify when to layer process and technology while maximizing the security benefit
 - Consider tradeoffs between best in breed and a broad range of coverage
 - Don't layer DRM on Full Disk Encryption

- Validate and Update
 - Periodic security assessments
 - Adjust to address gaps in control points
 - Adjust to address gaps in process and technology
- Expect the Policy, Control Points, Processes, and Technologies to change
 - Don't under estimate the business willingness to take risk

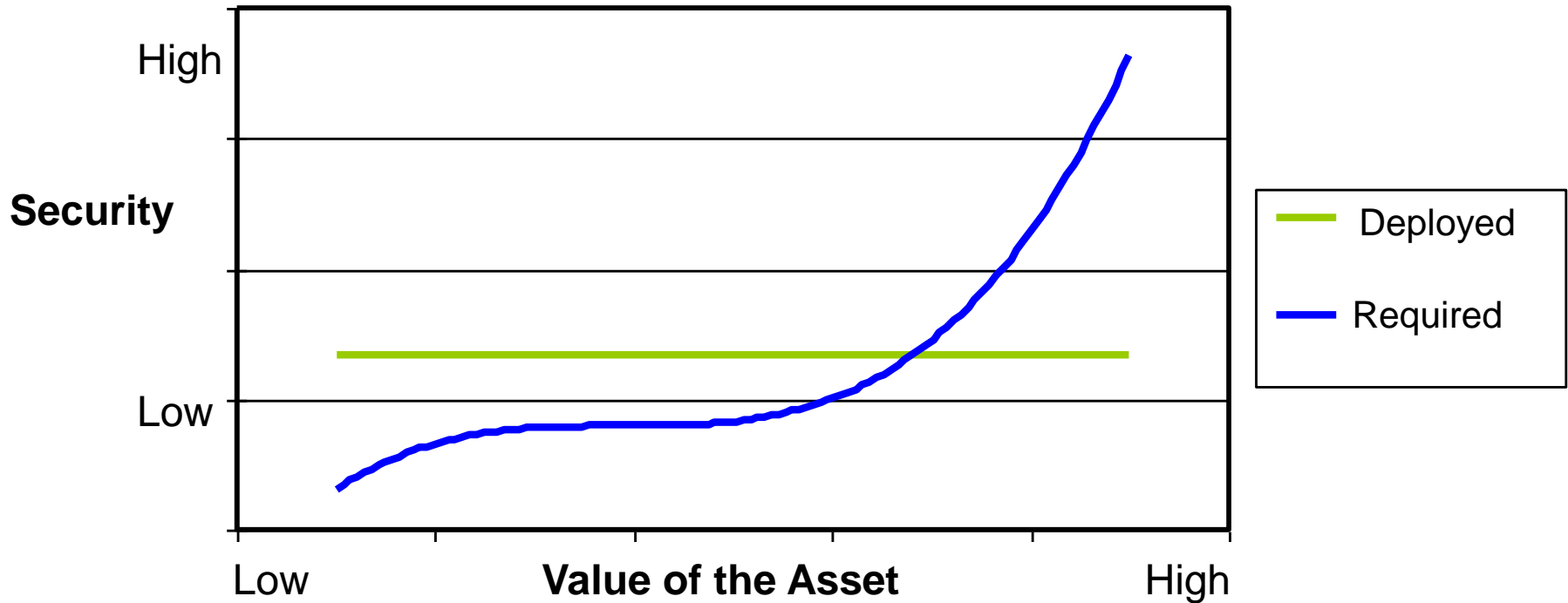


Case Study

- Company
 - Large product manufacturing company
 - 90,000 users (35% contractors)
 - 100,000+ systems
- Business Drivers
 - “Getting to your data anywhere”: the movement of data through the interaction of mobile devices on Enterprise network and Internet
- Security Drivers
 - Defining a “data-centric” security architecture to protect data regardless of where it resides.



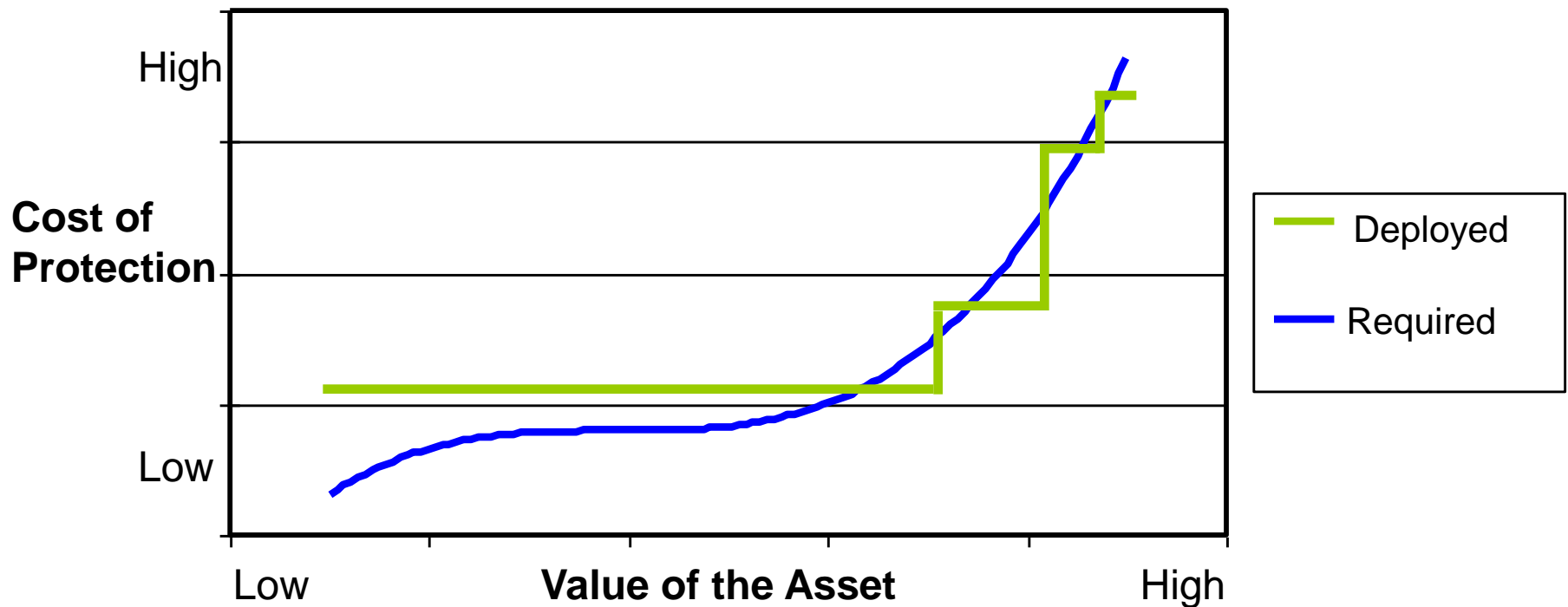
Traditional Security Strategy



- Traditional security strategy protects everything equally.
 - Over spending in protection of low value assets
 - Under spending in protection of high value assets



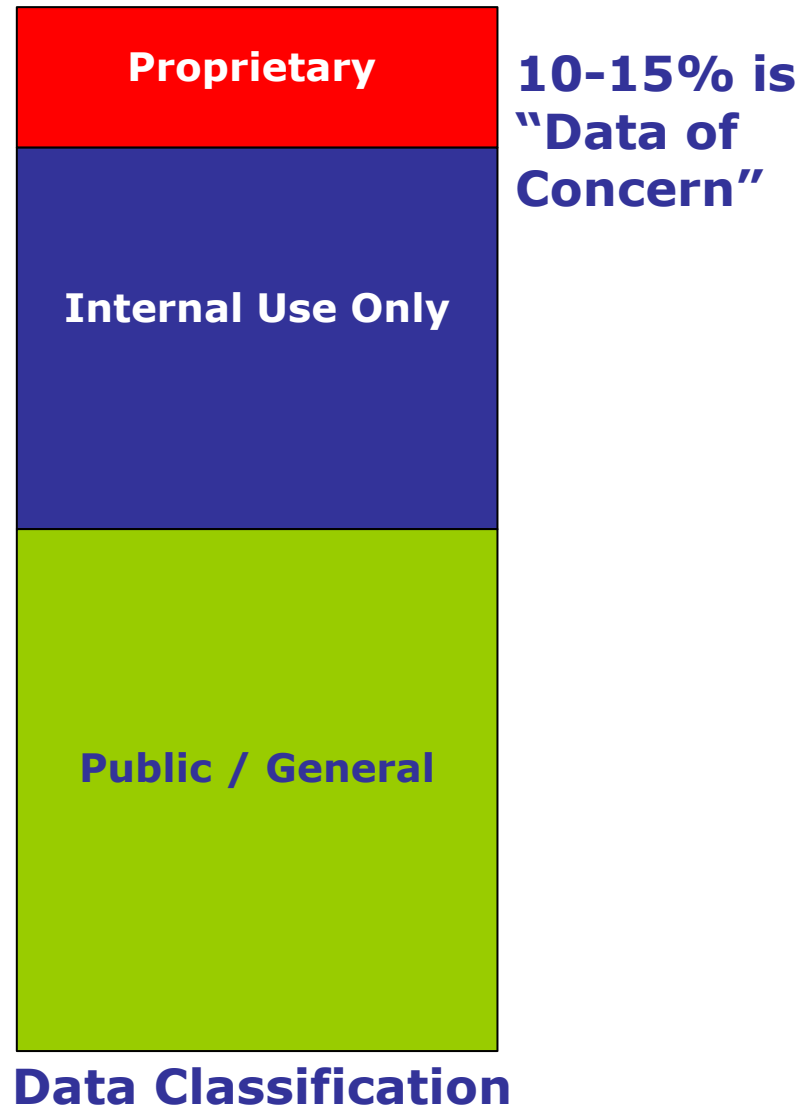
Data-Centric Security Strategy



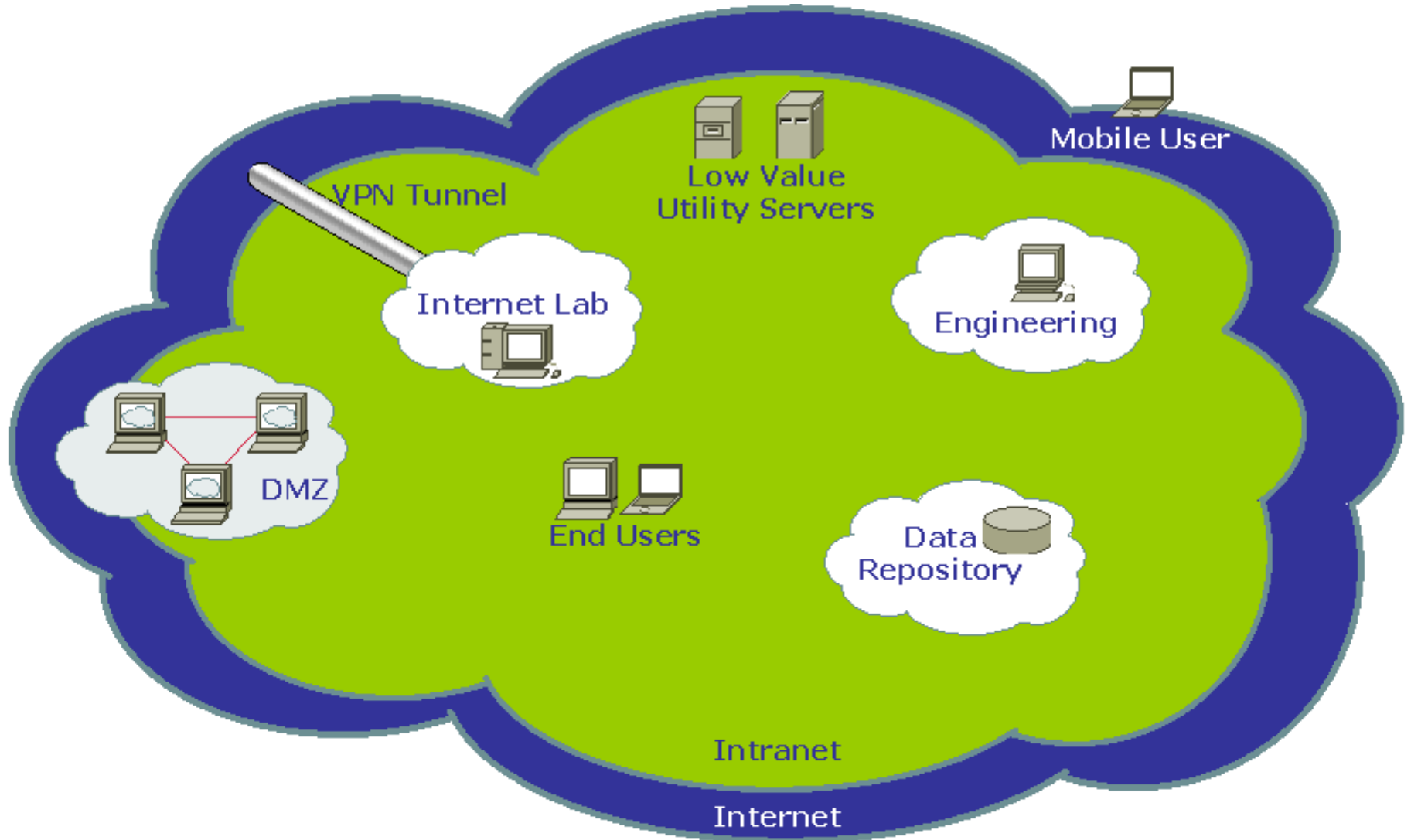
- Add Enhanced Protection for high value assets
- Each Step is an identified security control (policy or technology) for protection of critical assets.

Data-Centric Security Policy

- Data Protection Policy
 - Policy focuses efforts on protecting “data of concern”
 - Policy drives data classification
- Data of concern
 - The small percentage of data where protection is required by Law or regulation, or determined proprietary by company policy
- Fundamental security for all data
- Tiers of security for data of higher value.



Identify Control Points



- Network Control Points



Identify Control Points

- System Control Points
 - Configuration and system management
 - Patch management
 - System and application level access
- Data Control Points
 - Authorization and access
 - In use, at rest, or in transit
- User Control Points
 - Authorization
 - Accountability and Responsibility



Enhanced Security

- Security Awareness Training
 - Control Point: Accountability and Responsibility
 - Rewards/Consequences to protecting information
 - Security Drivers license
 - Technology can assist, but not the focus
- Internal Network Segmentation (Zones)
 - Control Point: Network Segmentation
 - Risk assessment process
 - Zone migration process
 - Access control process
 - Firewall / Network Isolation Technology



Enhanced Security

- Network Data Leakage Prevention
 - Control Point: Monitoring networks for data leakage
 - Intellectual Property Definition process
 - Response and investigation process
 - Network-based DLP Technology deployed to monitor web and email traffic

- End Point Data Leakage Prevention
 - Control Point: Monitor end points for data leakage
 - Intellectual Property Definition process
 - Response and investigation process
 - Host based DLP technology



Enhanced Security

- Full Disk Encryption
 - Control point: Protecting data at rest
 - Key management & recovery process
 - Full disk encryption technology
- Enhanced security logging for critical systems
 - Control point: Protection and monitoring of critical systems
 - Access Verification Process
 - System and access logs
 - Log management technology

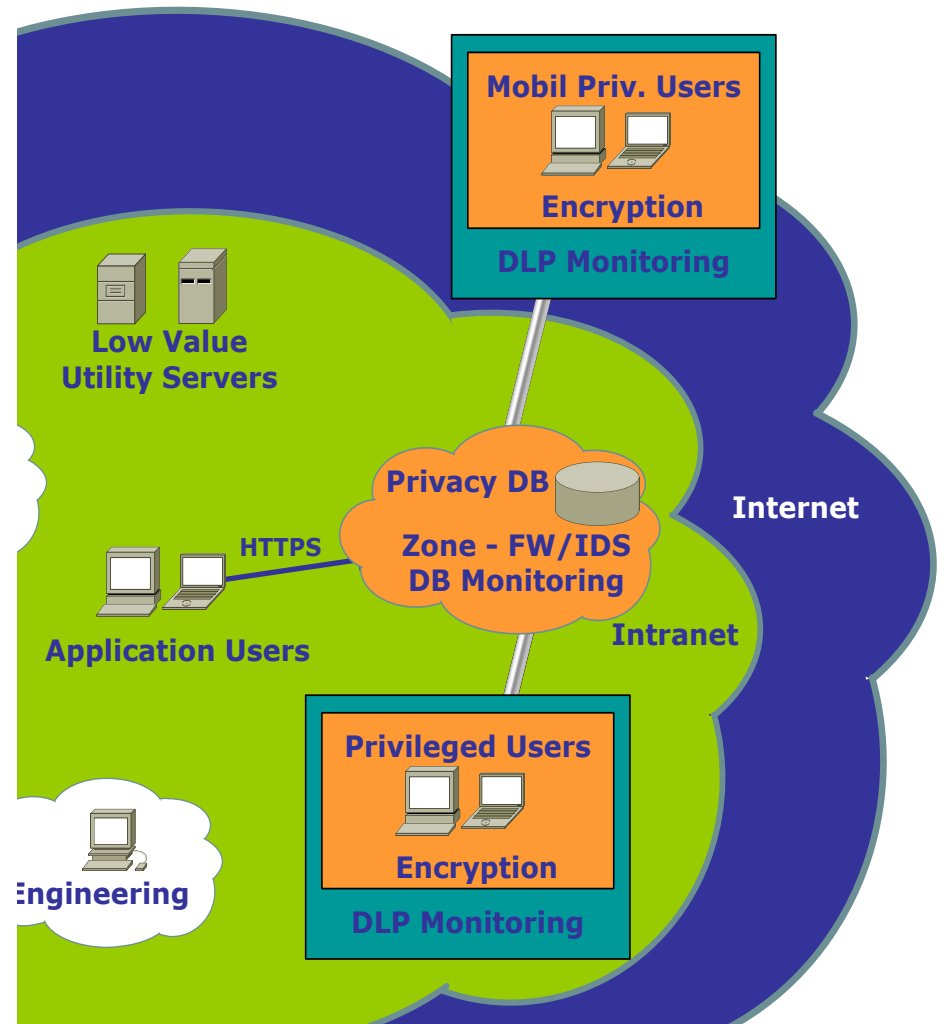


Enhanced Security

- Enterprise Digital Rights Management
 - Control Point: Protection and monitoring of sensitive information in databases
 - Key management process
 - Access and rights management process
 - E-DRM technology
- Enhanced data repository security
 - Control Point: Protection and monitoring of sensitive information in data repositories
 - Intellectual Property Definition process
 - System and Application logging technology
 - Log management technology for correlation

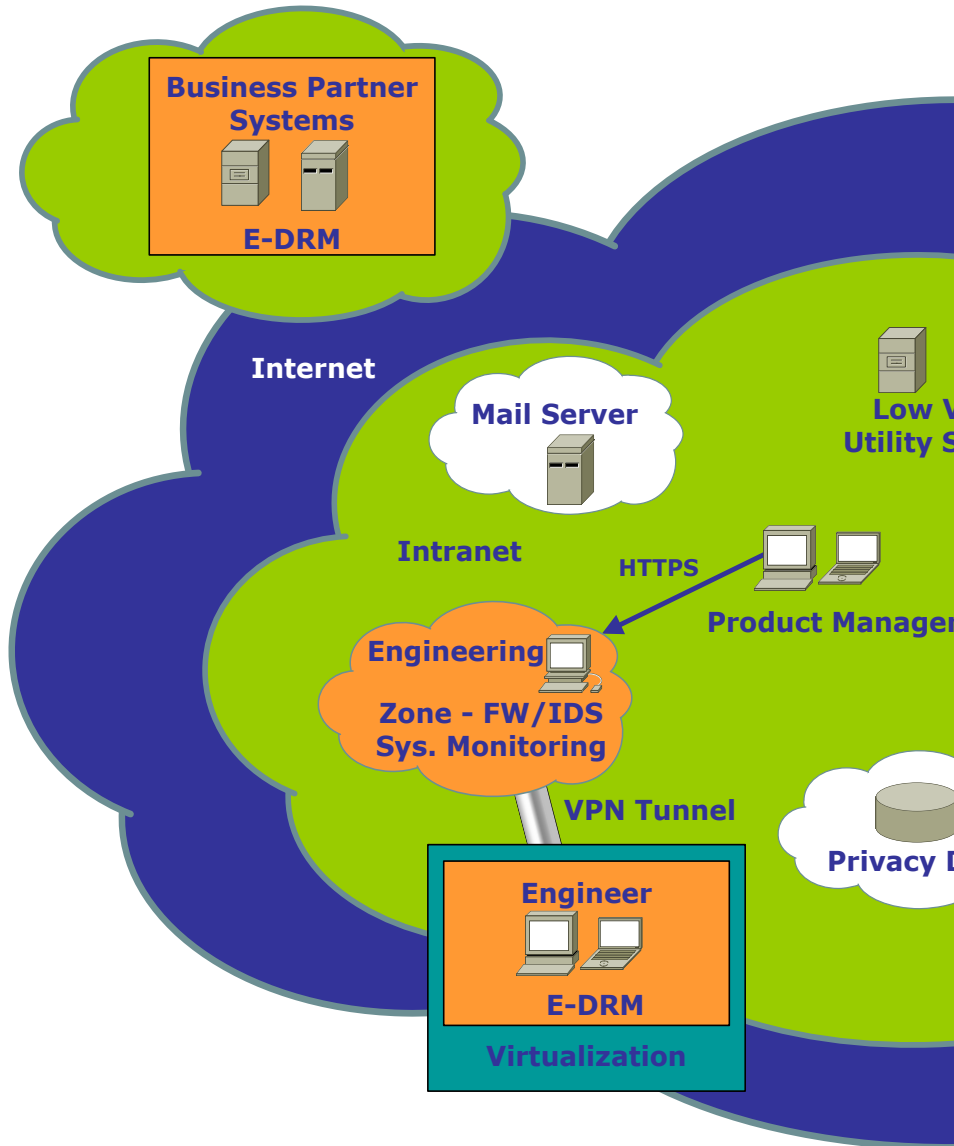
Enhanced Security for Protection of Privacy Information

- User Awareness
- Zone Privacy database
 - Limit standard user access
 - DLP Monitoring of user requests
 - VPN for Privileged Users
 - Verify encryption
- Database Protection
- Database access and log monitoring
- End Point Protections
 - Encryption
 - DLP monitoring





Enhanced Security for Secure Design Center



- User Awareness
- Zones
- Engineering System Protection and Monitoring
- End Point Security
 - Virtual Image with encryption
 - Accessed restricted to Development zone
- Enterprise Digital Rights Management
 - Sharing design



Conclusion

- Understand the business drivers
- Determine a strategy and policy aligned with business
 - Data-Centric (Research & Development, IP creation)
 - Availability (service based)
 - Defense-in-Depth (financial, government, military)
- Utilize the security strategy methodology
 - Determine the control points
 - Identify process and technology to meet the required control points.
 - Continual Validation and Verification to adjust policy, control points, process, and technologies