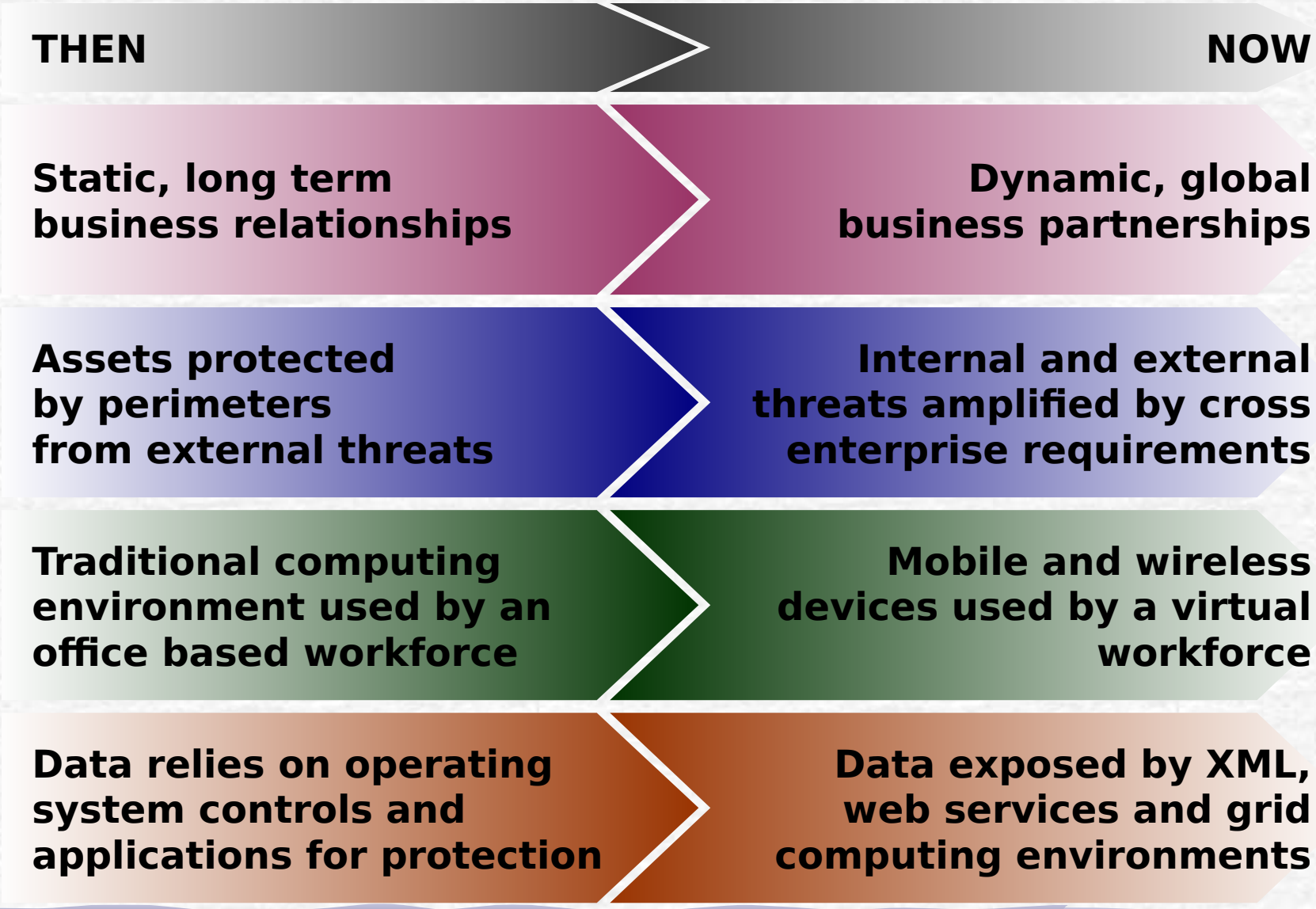
Doing the Time Warp. Again.

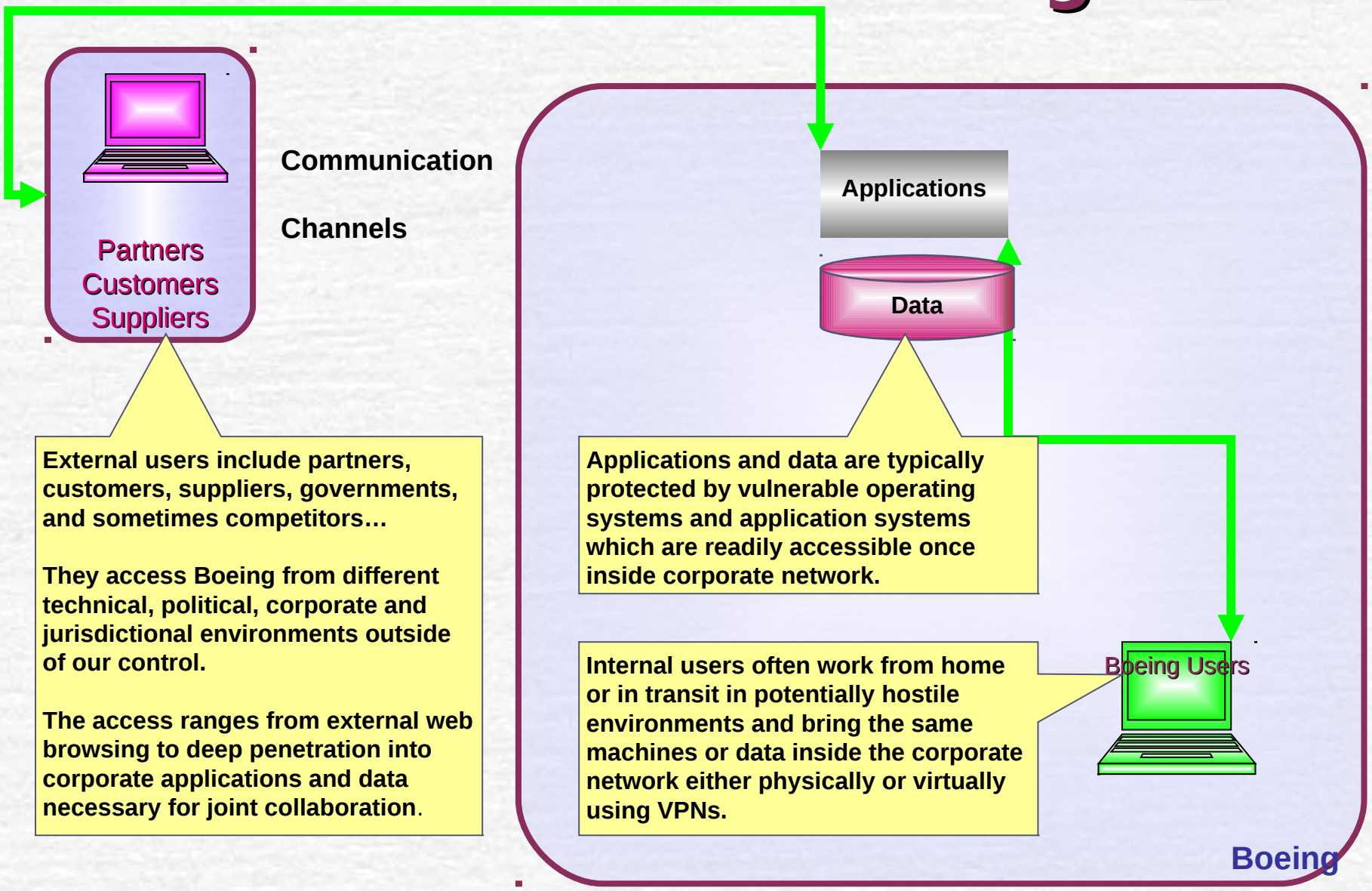
Security Directions at Boeing

Stephen T. Whitlock
IT Security Architect
stephen.whitlock@boeing.com

Security Drivers



IT Infrastructure Challenges



External users include partners, customers, suppliers, governments, and sometimes competitors…

They access Boeing from different technical, political, corporate and jurisdictional environments outside of our control.

The access ranges from external web browsing to deep penetration into corporate applications and data necessary for joint collaboration.

Applications and data are typically protected by vulnerable operating systems and application systems which are readily accessible once inside corporate network.

Internal users often work from home or in transit in potentially hostile environments and bring the same machines or data inside the corporate network either physically or virtually using VPNs.

Strategies

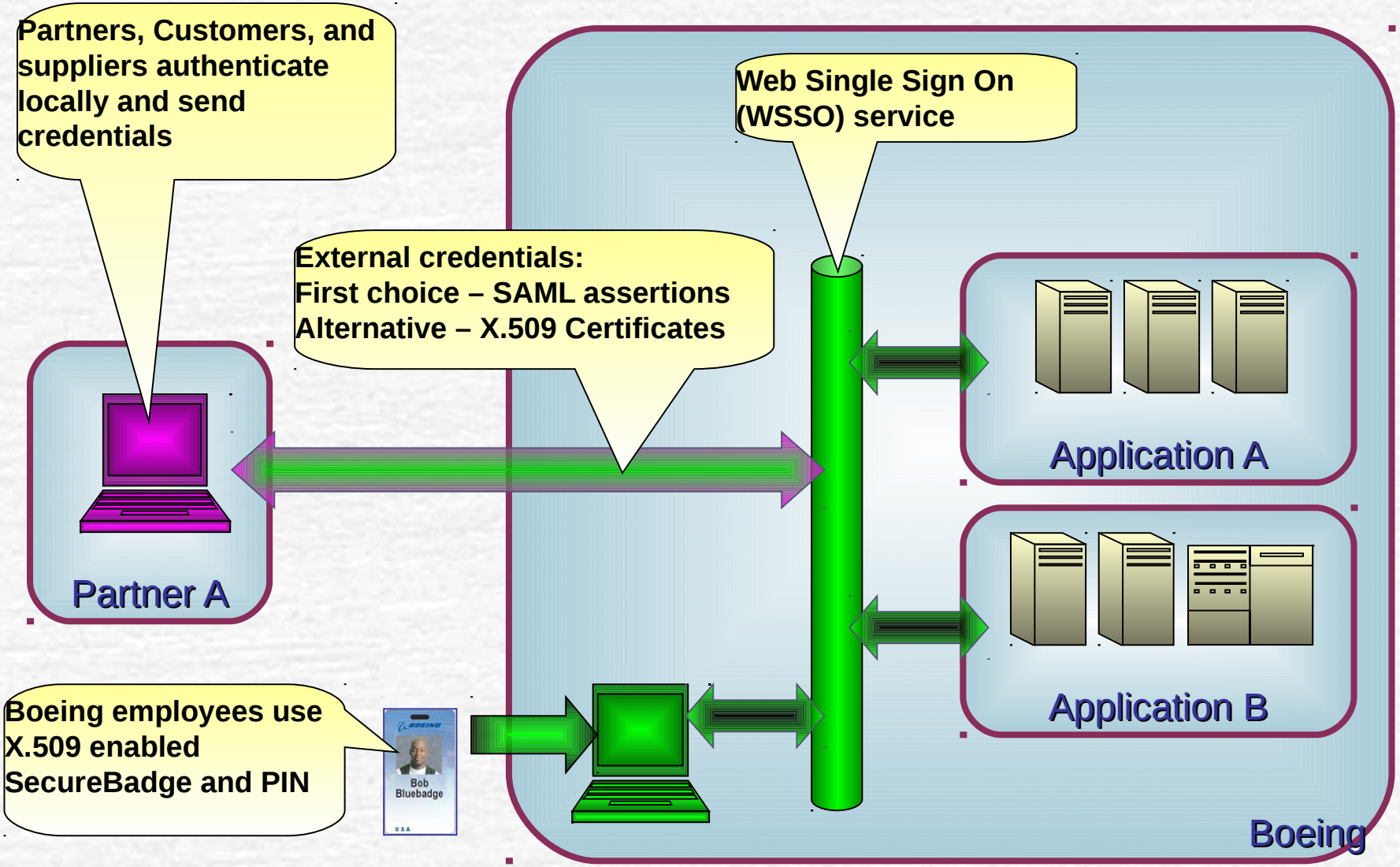
Enable extended business operations while securing enterprise information assets

1. Simplify and strengthen authentication by replacing weak passwords with SecureBadge.
2. Automate access decisions based on business information and distribute enforcement.
3. Provide the same, appropriate information and application access experience to all users inside and outside the perimeter.
4. Create virtual networks to isolate critical business components from general network traffic.
5. Protect individual users, devices, applications and networks from attack by moving access enforcement down to the end systems.

1. Simplify and strengthen authentication by replacing weak passwords with SecureBadge

- Replace password use on all authentication systems with SecureBadge.
  - Smart card containing several certificates
- SecureBadge will contain all the necessary credentials for identification, authentication and the generation of one time passwords.
  - Including Web Single Sign On (WSSO), Win2K/ActiveDirectory access, encryption and signature keys, and remote access
  - Our application developers will use WSSO where possible
- Partners/customers/suppliers will
  - Authenticate locally
  - Send credentials (SAML assertions, X.509 certificates)

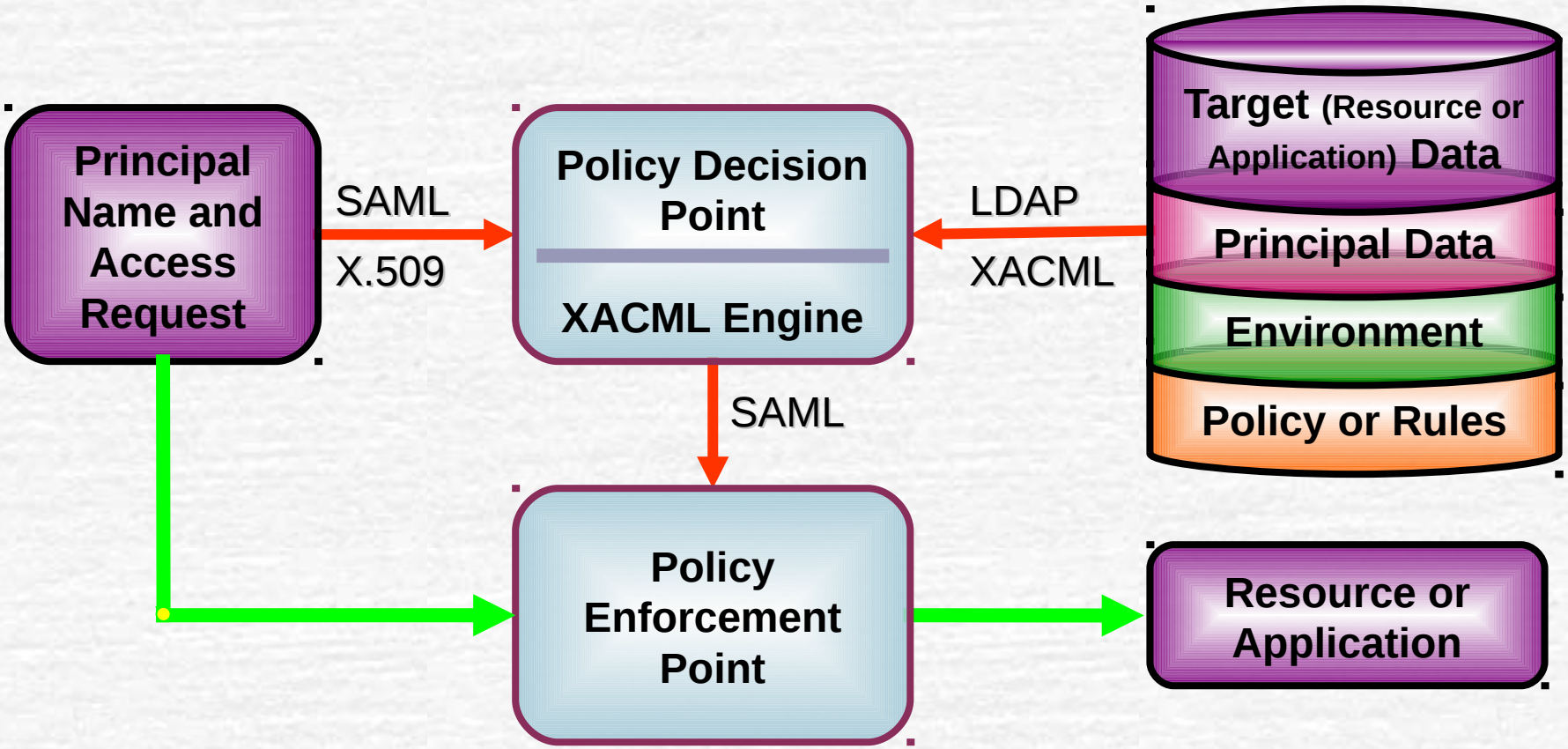
Authentication Flow



Automate access decisions based on business information and distribute enforcement

- Information will drive decisions about people, devices and relationships
  - Access Assignment – Privileges, encapsulated in roles, are automatically assigned based on a principal's attributes.
  - Decision Enforcement – Target application and data attributes, principal roles, and general access rules will contribute to access decisions that will drive discrete access controls.
    - Policy decisions will be made using XACML (eXtended Access Control Markup Language) and recorded in LDAP accessible directories.
    - Policy decisions will be communicated to enforcement mechanisms using SAML assertions.
  - Administration Delegation – Access decisions will be delegated to information owners via management tools and SAML assertions.

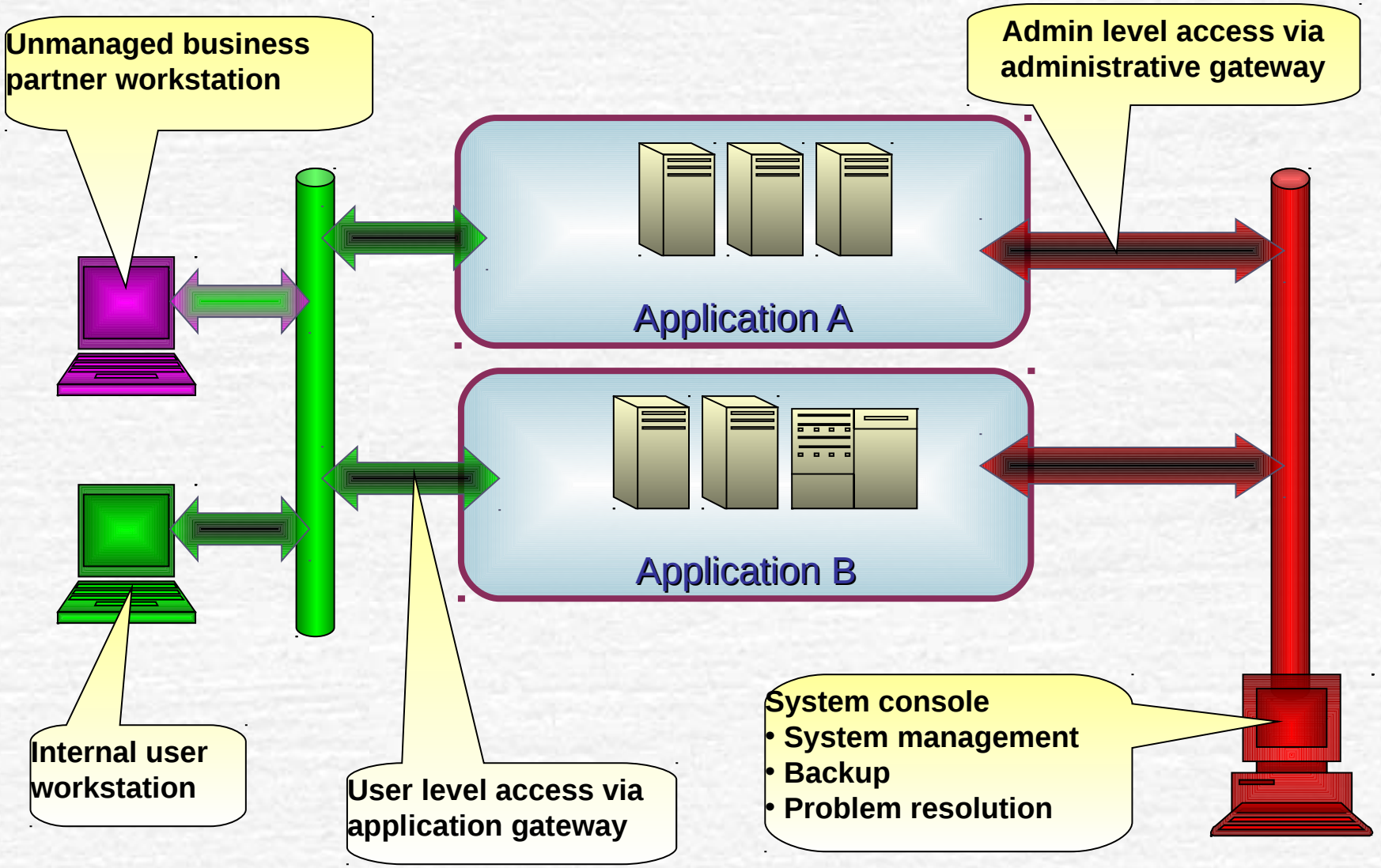
Authorization Flow



3. Provide the same, appropriate information and application access experience to all users inside and outside the perimeter

- Provide a common access method independent of location
- Distinct access level, dependent on role
  - Application gateways for user access
    - Preferred access method
    - Targeted for partners, customers, suppliers and most internal users
    - Built using web portals, terminal servers, etc.
  - VPNs for administrative access
    - Targeted for administrators, problem management, etc
    - Secure full network access

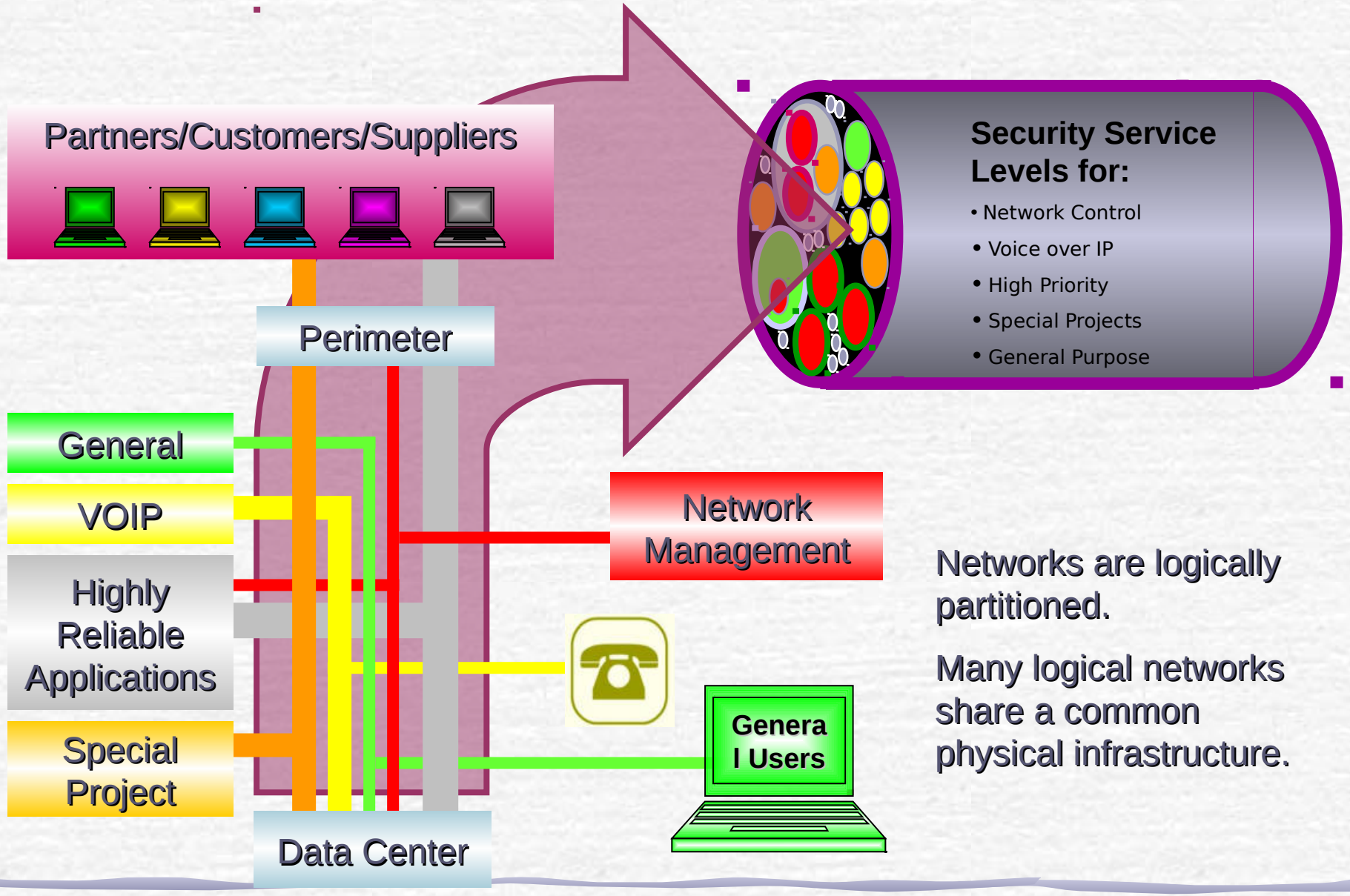
Application Access



4. Create virtual networks to isolate critical business components from general network traffic

- Partition the network by service type and criticality to prevent attacks on weak devices from taking down entire infrastructure.
  - Secure enforceable rate control for specific services and protocols.
- Partition the network by organization, project or geography to protect different user communities from each other.
  - Multiple internal network partitions focused on task based boundaries.

Network Partitioning by Service



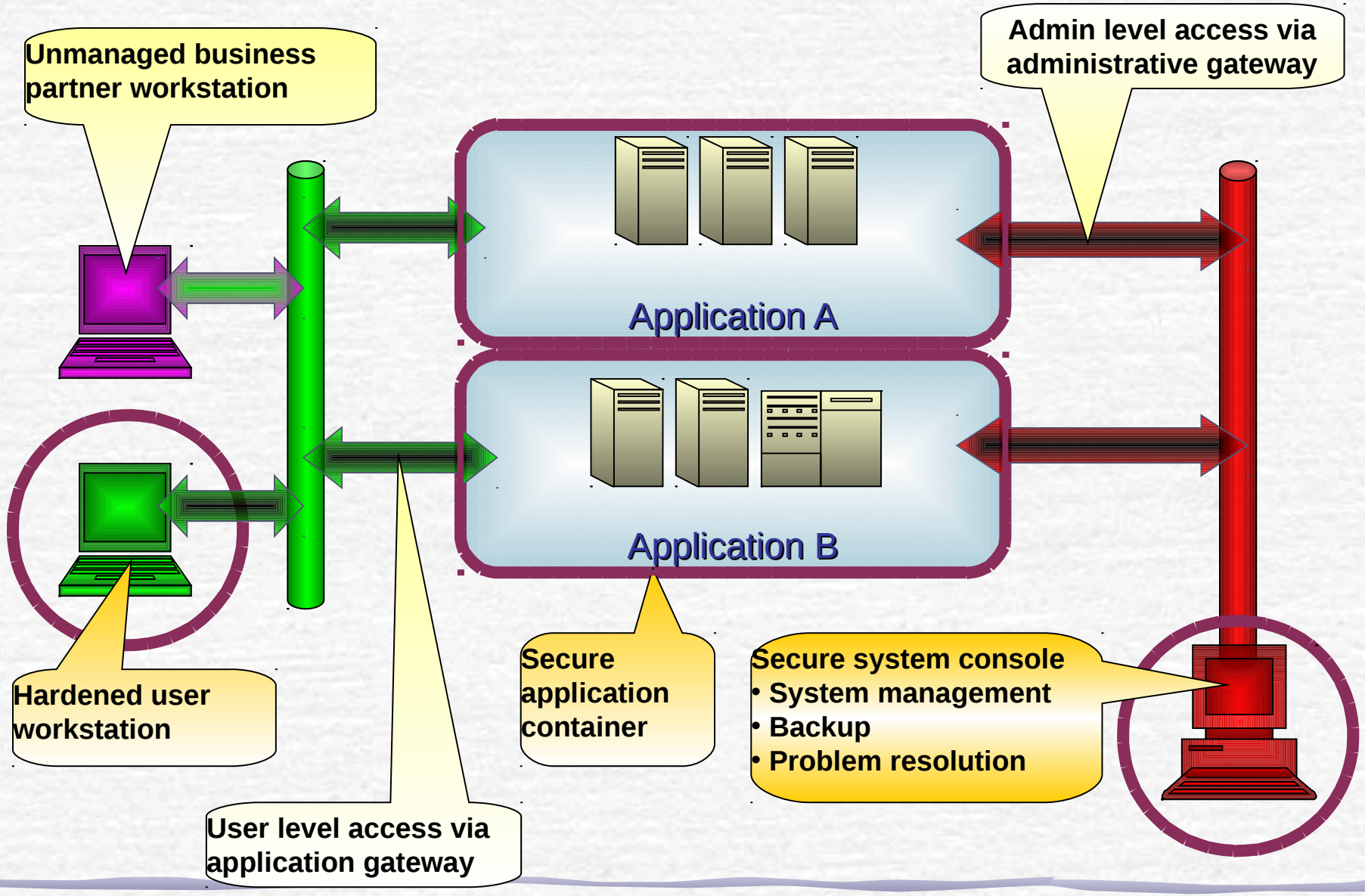
Networks are logically partitioned.

Many logical networks share a common physical infrastructure.

5. Protect individual users, devices, applications and networks from attack by moving access enforcement down to the end systems

- Devices are highly mobile and must be able to protect themselves. This requires:
  - Hardening the security of end user devices and infrastructure components
    - Improved device firewalls, file/disk encryption
  - Improved software solutions and new hardware platform designs
    - TCA/NGSCB – Next Generation Secure Computing Base
- Application and infrastructure servers require additional protection and isolation.
    - Virtual machine or NSA NetTop type application architecture
    - Application specific (e.g. web services) firewalls
    - Policy driven encryption

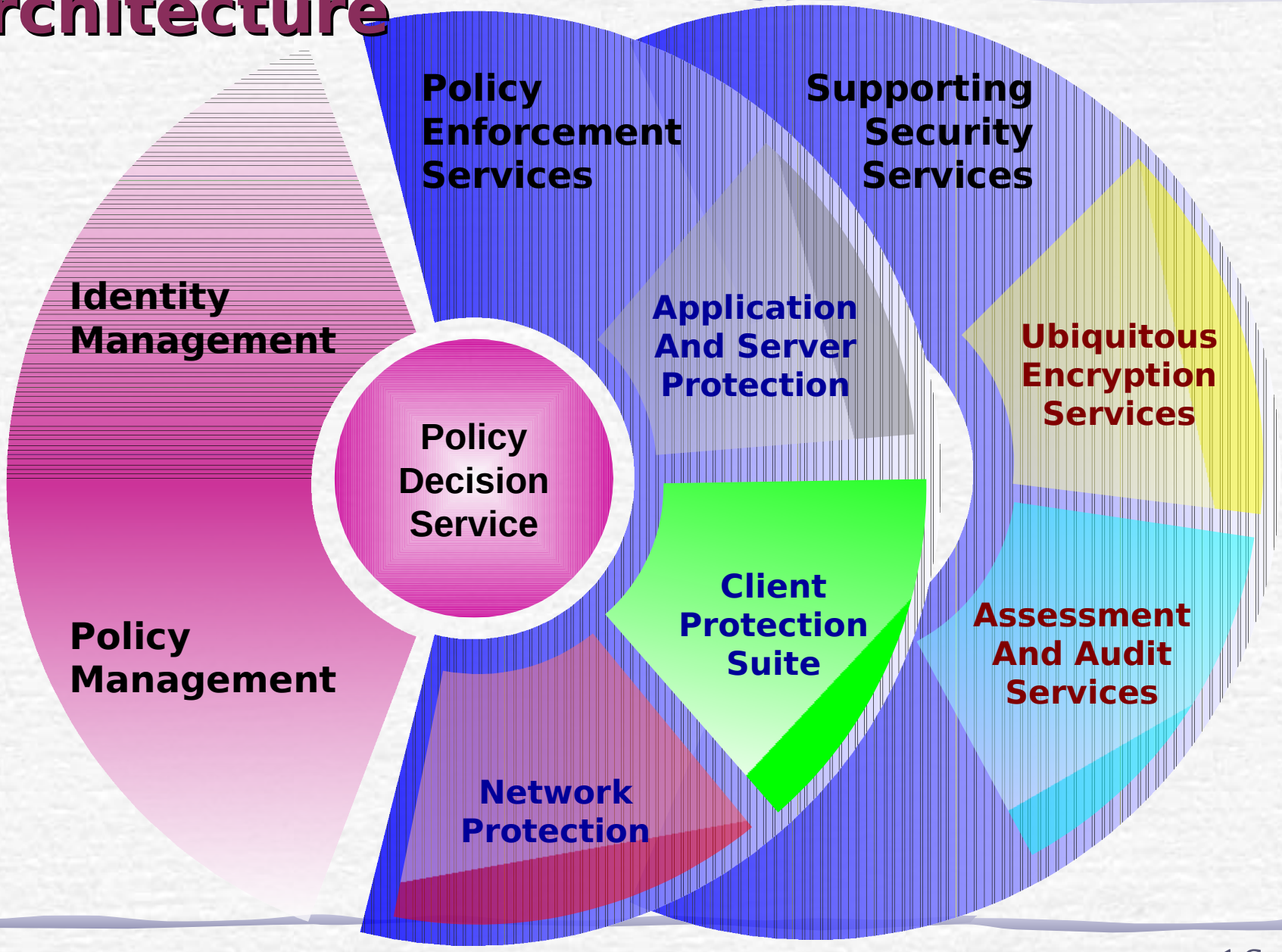
Application Access & Hardening



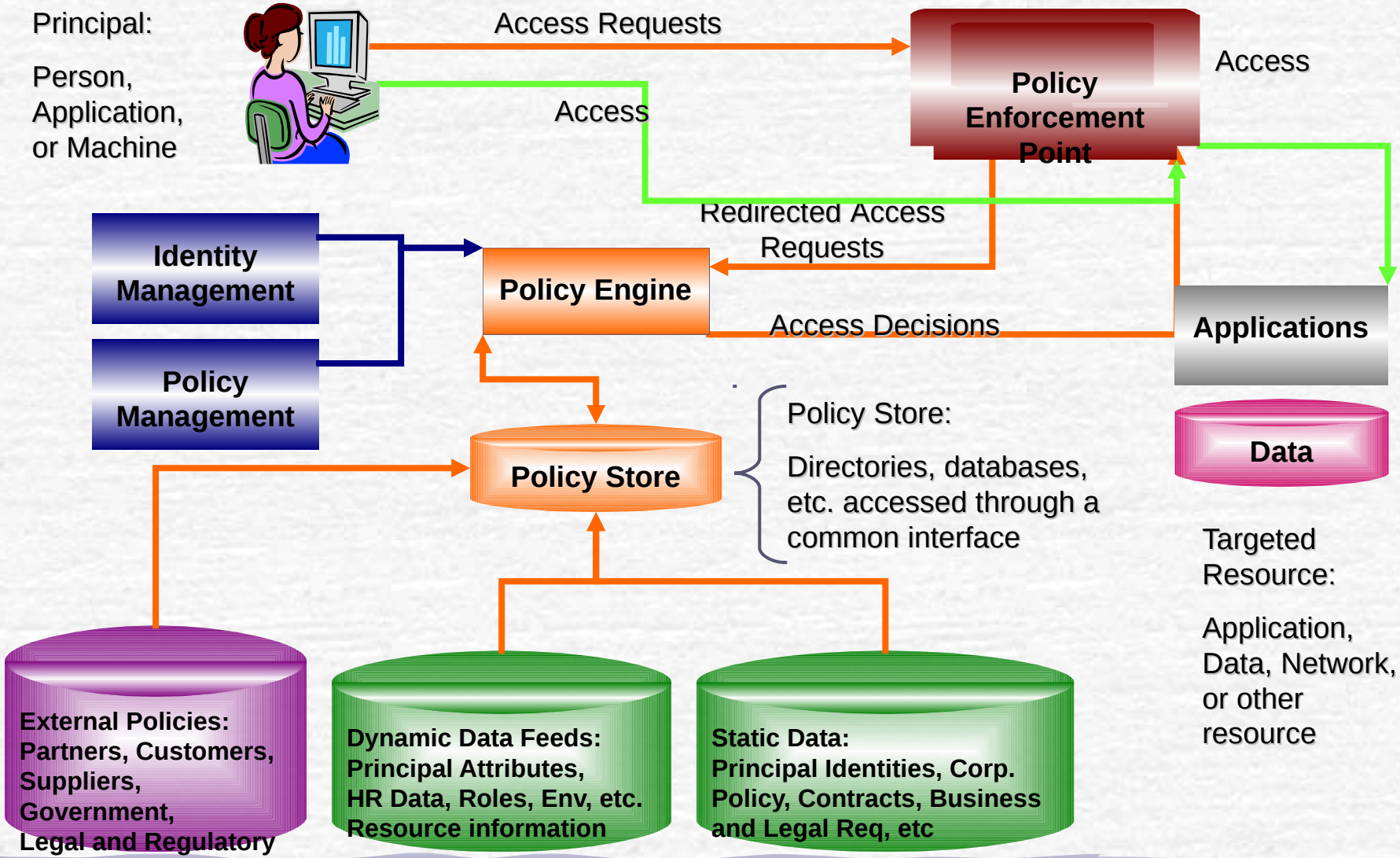
Challenges

- Reliance on SecureBadge will impact user if badge is lost or damaged.
- Acceptance of partner/supplier/customer credentials increases threat exposure.
- Network partitioning will add complexity and may shut down applications which expect full access to all IP based services.
- End to end encryption challenges some current policies and designs which inspect and block content.
- Protecting end devices may hamper central device management and operational support.
- Automating and distributing access decisions will cause additional work for application and information owners.

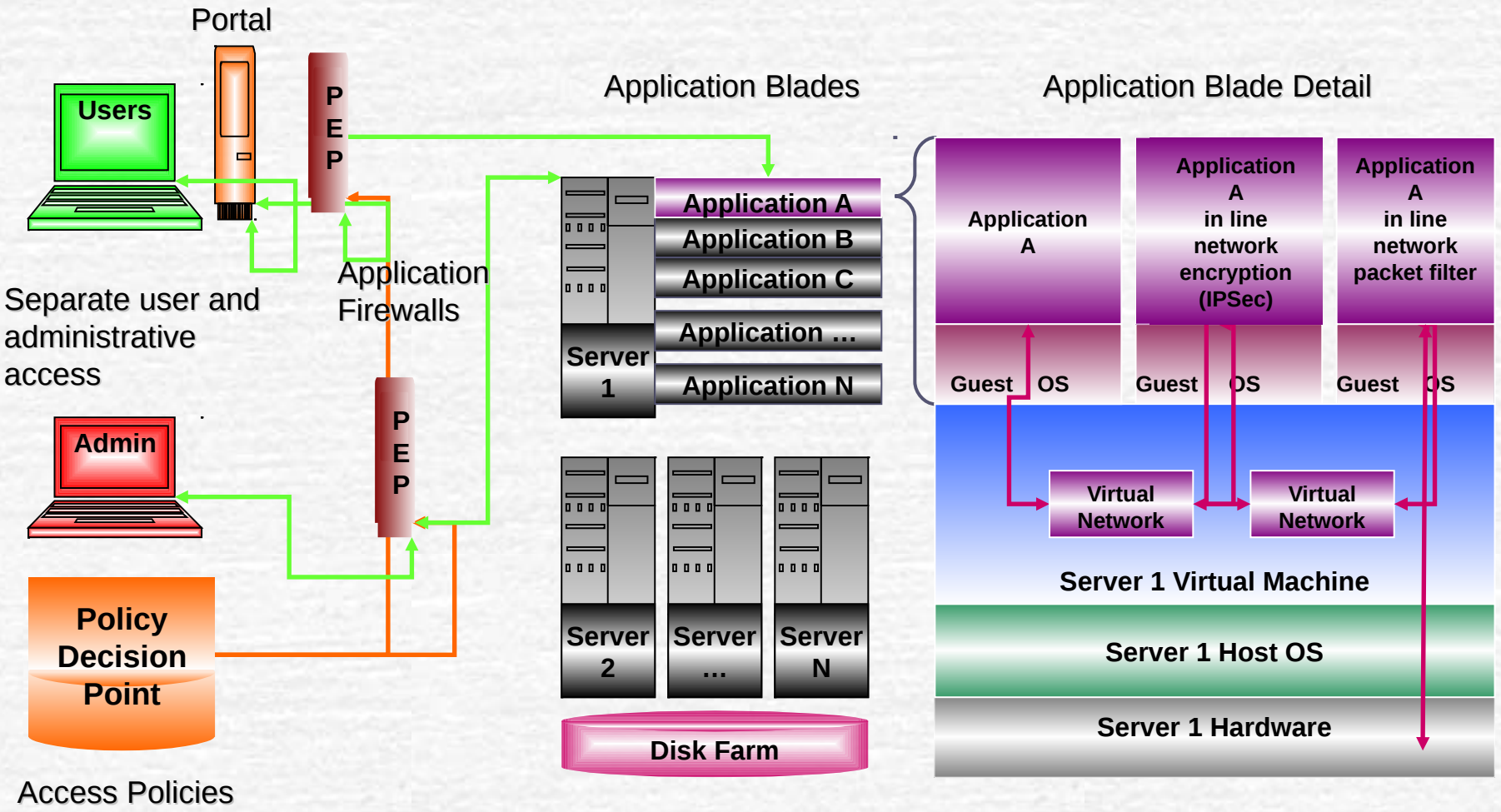
Policy Driven Security Service Architecture



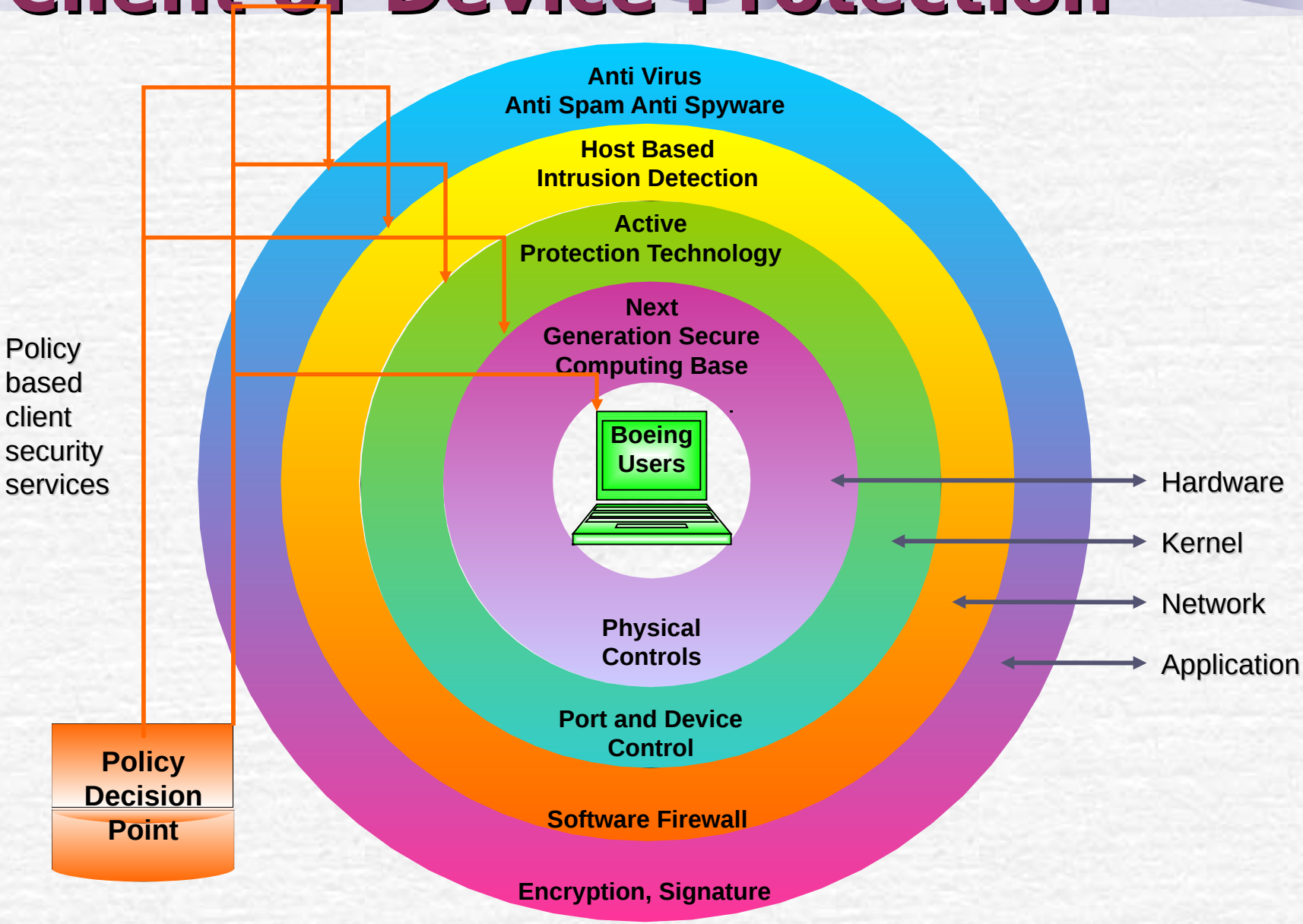
Policy Decision and Enforcement



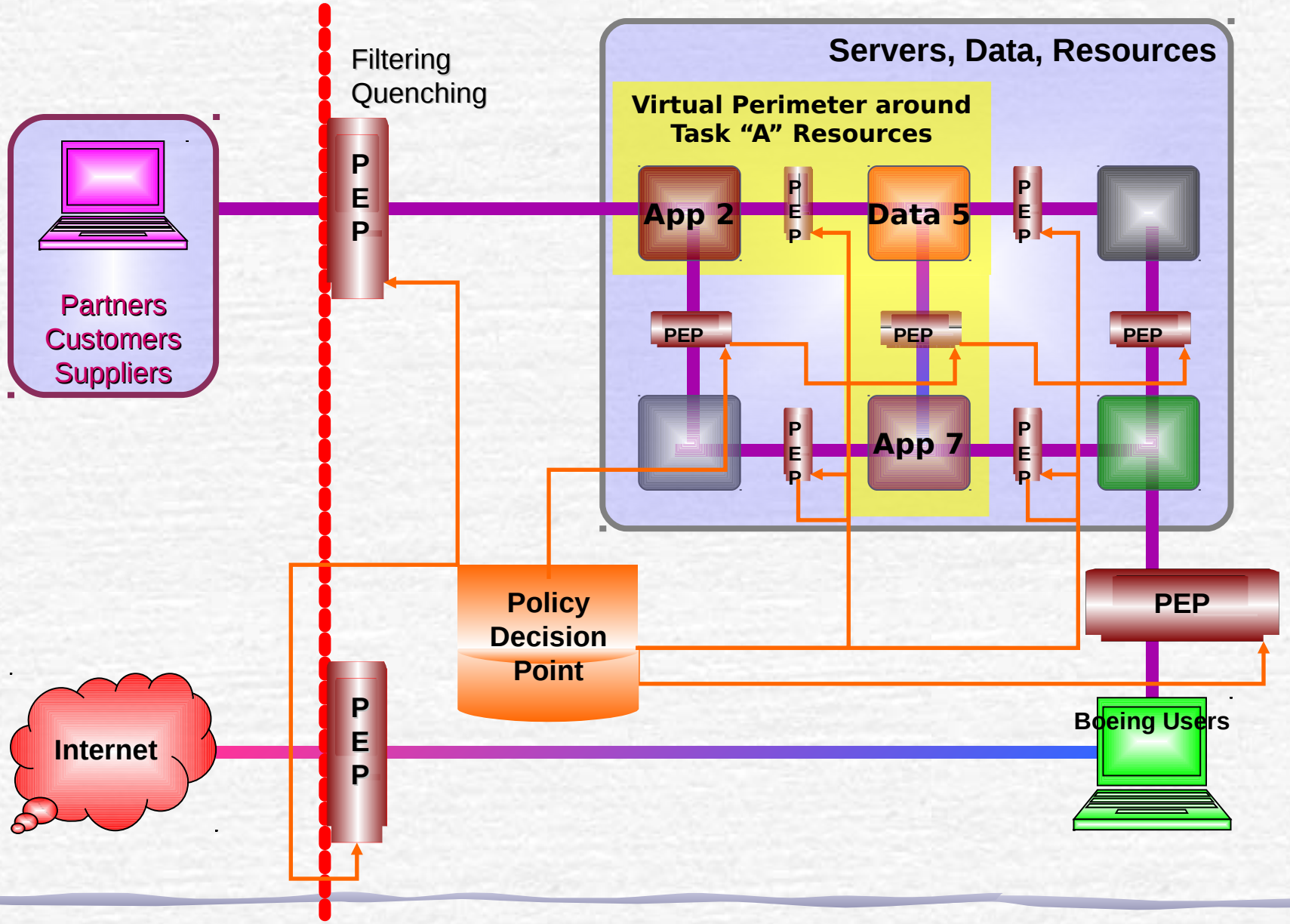
Application or Server Protection



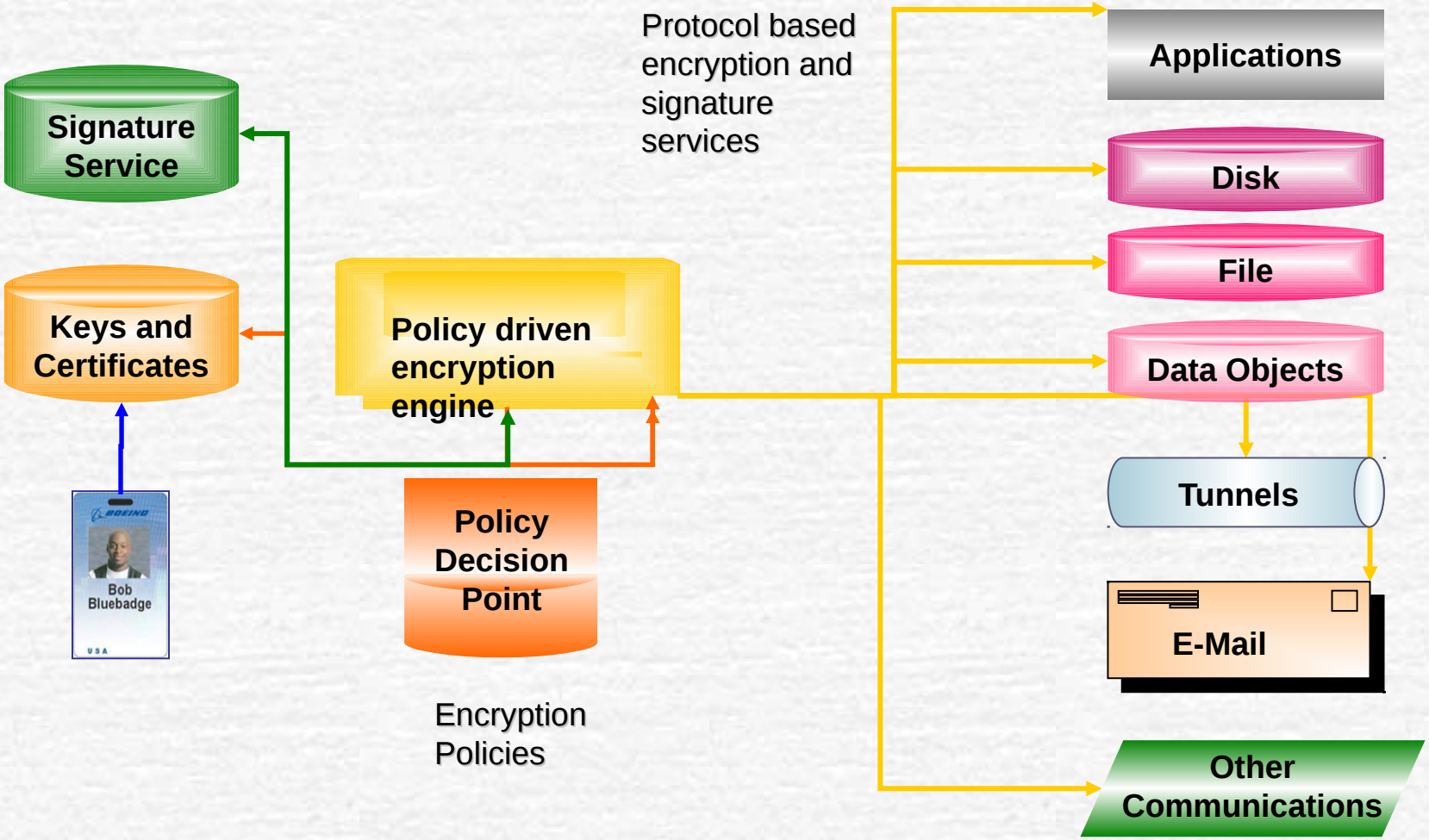
Client or Device Protection



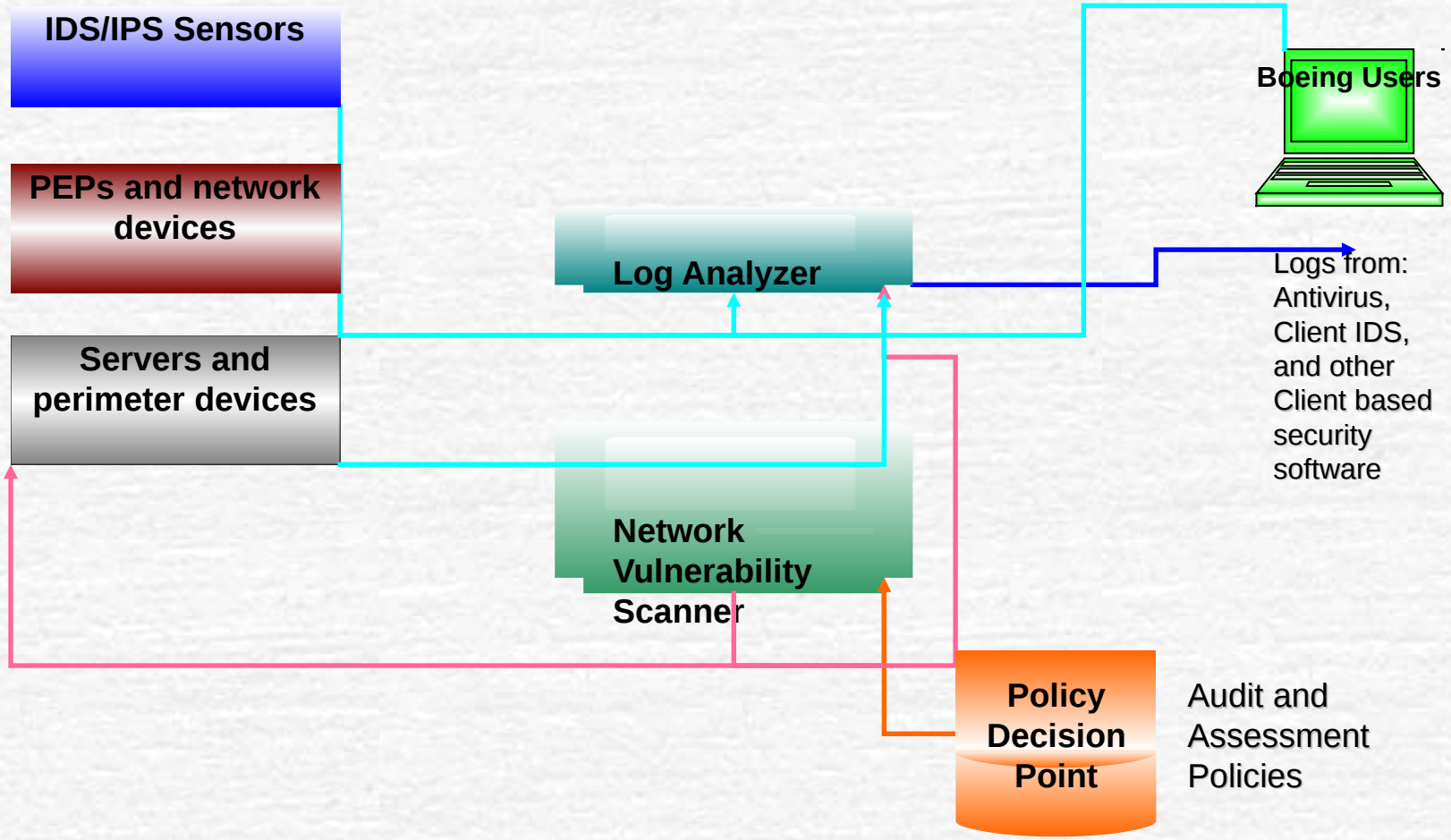
Network Protection



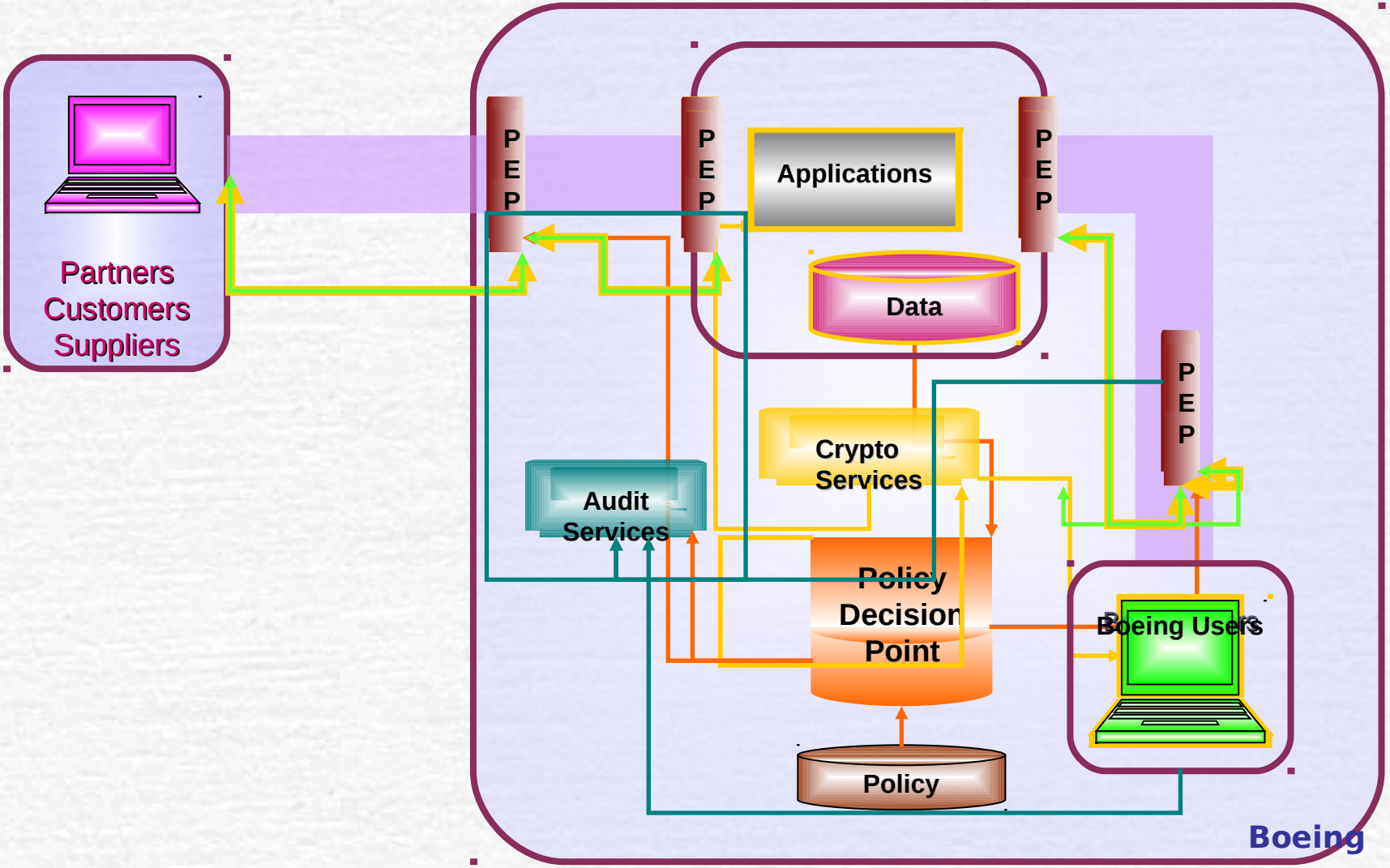
Cryptographic Services



Audit and Assessment Services



τελος


Partners
Customers
Suppliers
PEP
PEP
Applications
PEP
Data
PEP
Crypto Services
Audit Services
Policy Decision Point
Boeing Users
Policy
Boeing