



# Not all users are created equal

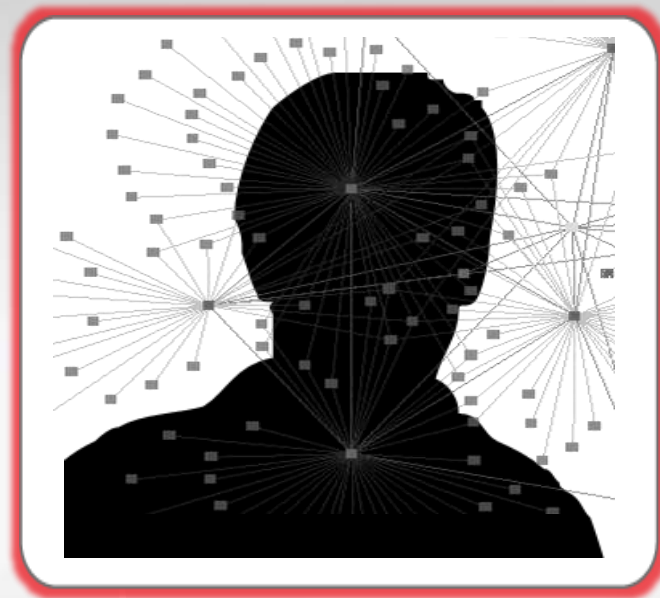
Transaction level  
policy enforcement

Vijay Sagar  
Director,  
Product Management



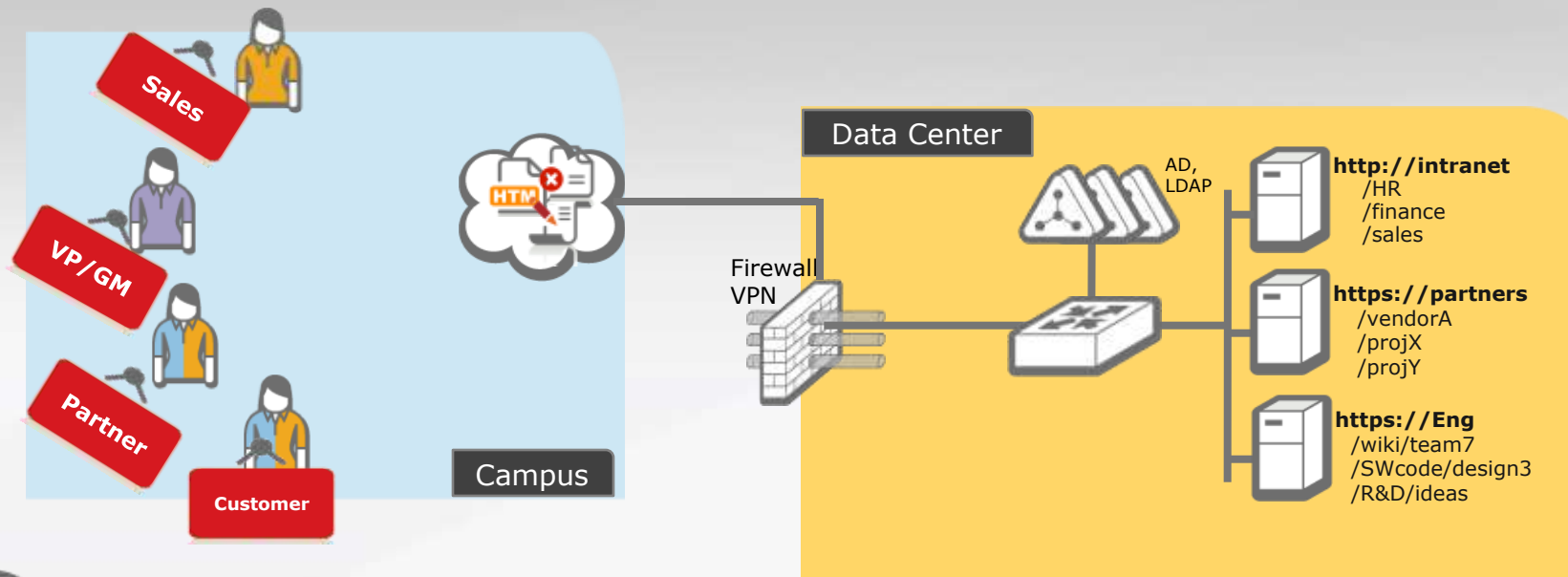
## Today's business models are changing the definition of a user

- **Business collaboration** exposes resources to partners, customers and even competitors
- **Outsourcing** of HR, manufacturing and other business functions
- **Regulatory Mandates** demand segregation of duties (SoD)



**Who is on my network? What are they doing? How can I control and monitor them?**

## Who is on my Network... and what are they doing?



- Accessing financial data?
- Checking project status?
- Deleting or copying intellectual property?
- Accessing sensitive HR applications?

For consideration when **planning** Access and Entitlement controls



For consideration when **architecting** and **deploying** Access and Entitlement controls



## Today's options for providing transaction level controls

Option		Challenges
Modify applications to include explicit authorization controls	➔	<ul style="list-style-type: none"><li>• Numerous applications</li><li>• Inconsistent coding standards</li><li>• Costly and time-consuming</li></ul>
Server and client side agents	➔	<ul style="list-style-type: none"><li>• Deploying agents doesn't scale</li><li>• Expensive to deploy across broad range of applications</li></ul>

# A Network-based approach addresses requirements for enterprise wide Policy enforcement

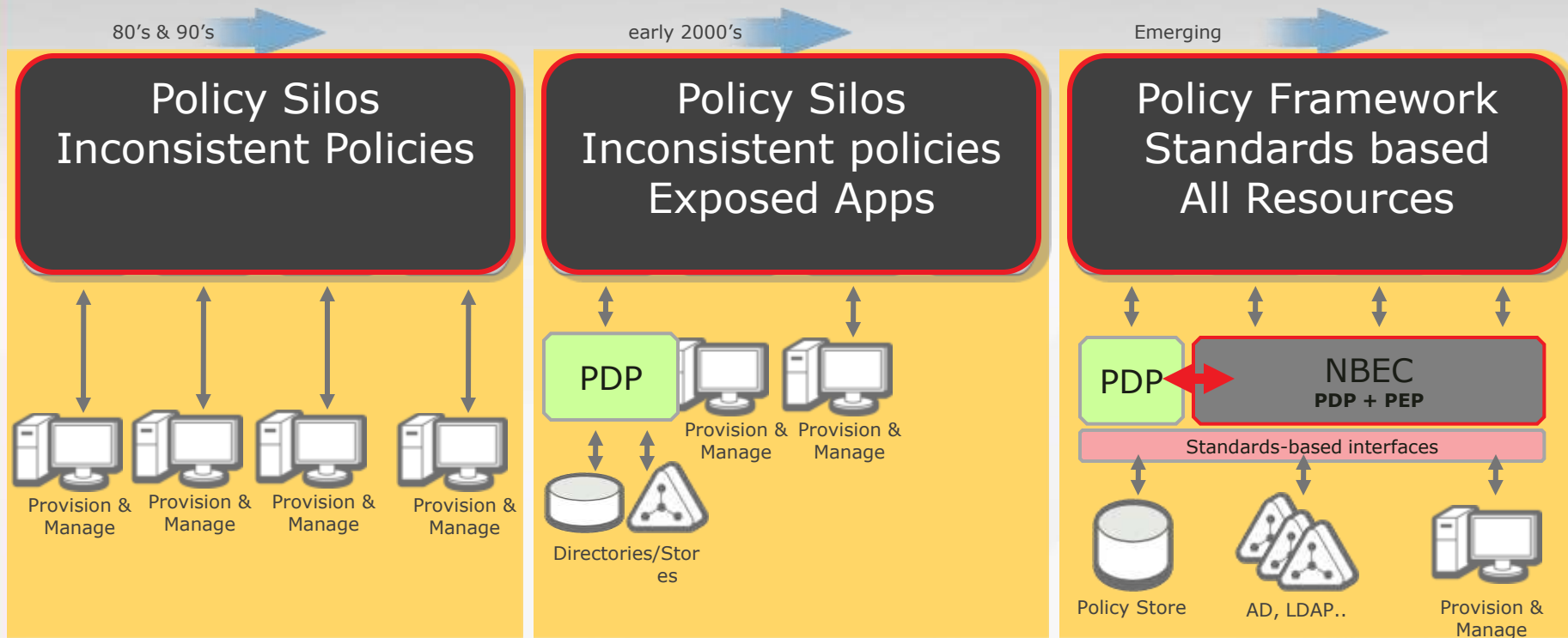
NBEC delivers transaction level policy enforcement to secure data center resources

**Introducing:  
Network-Based  
Entitlement Control  
(NBEC)**

***New!***

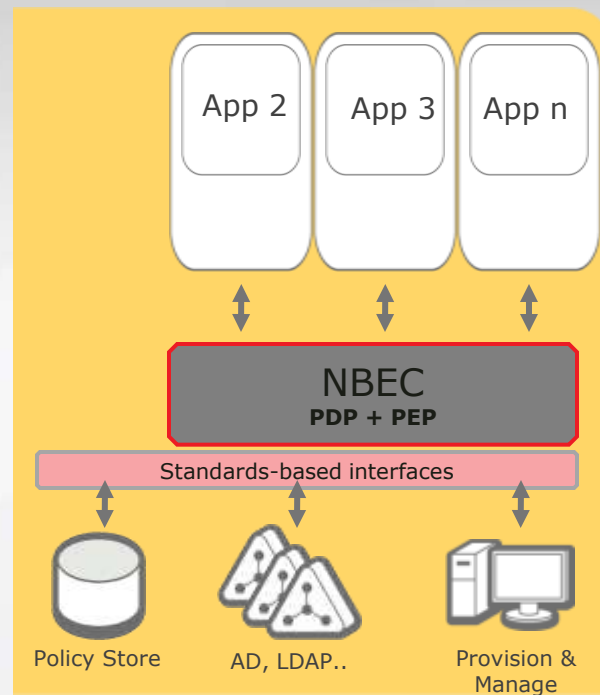
**No Touch to Applications  
No Touch to Clients  
Rapid Deployment**

# NBEC delivers a flexible policy framework across a broad range of applications and extends existing investments

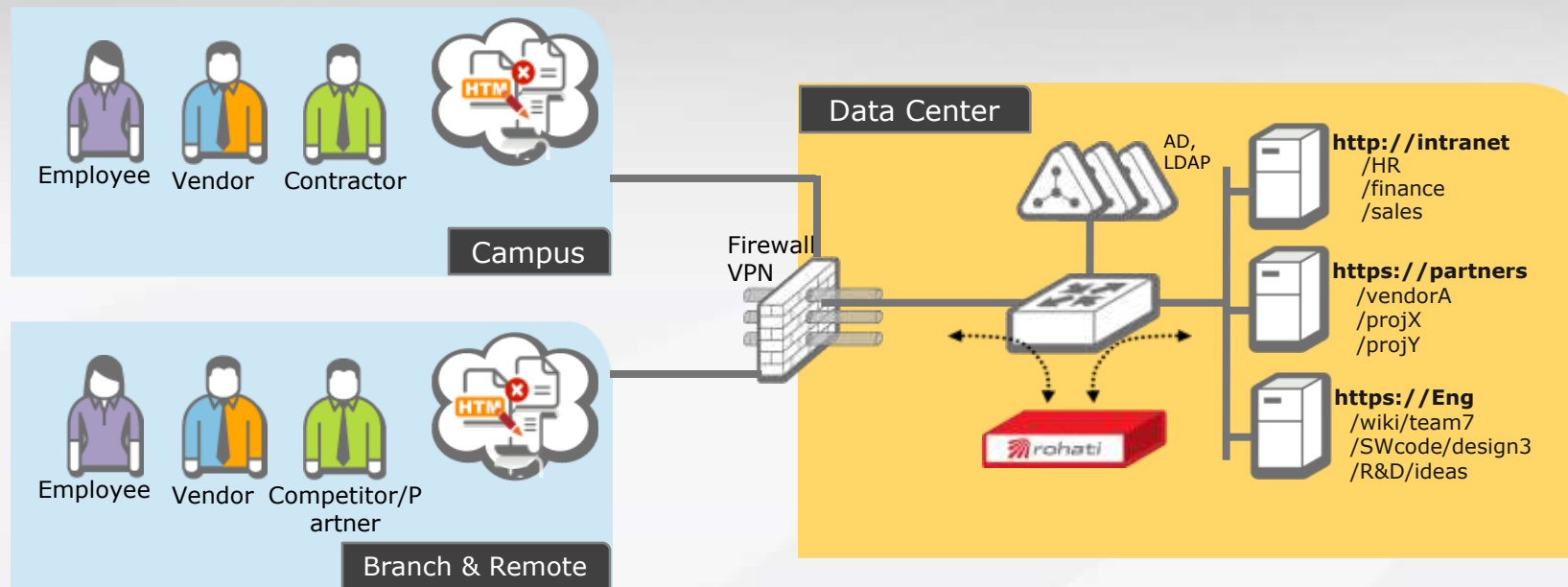


## Advantages of a network-based approach

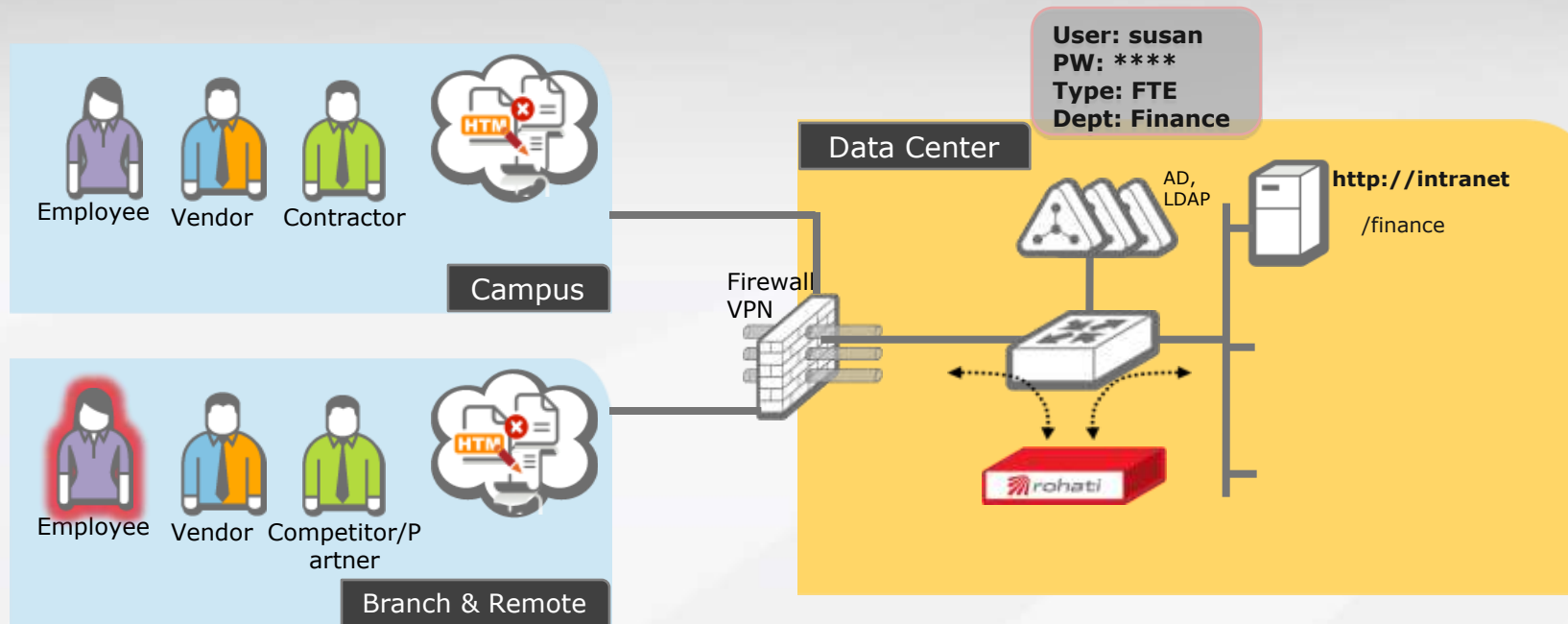
- No server or client-side agents
- Hardware-based enforcement
- Common *authentication* scheme across applications
- Per transaction *authorization*
- Resources are 'invisible' to those who don't 'need to know'
- Rapid deployment across broad range of applications
- Centralized logging and reporting



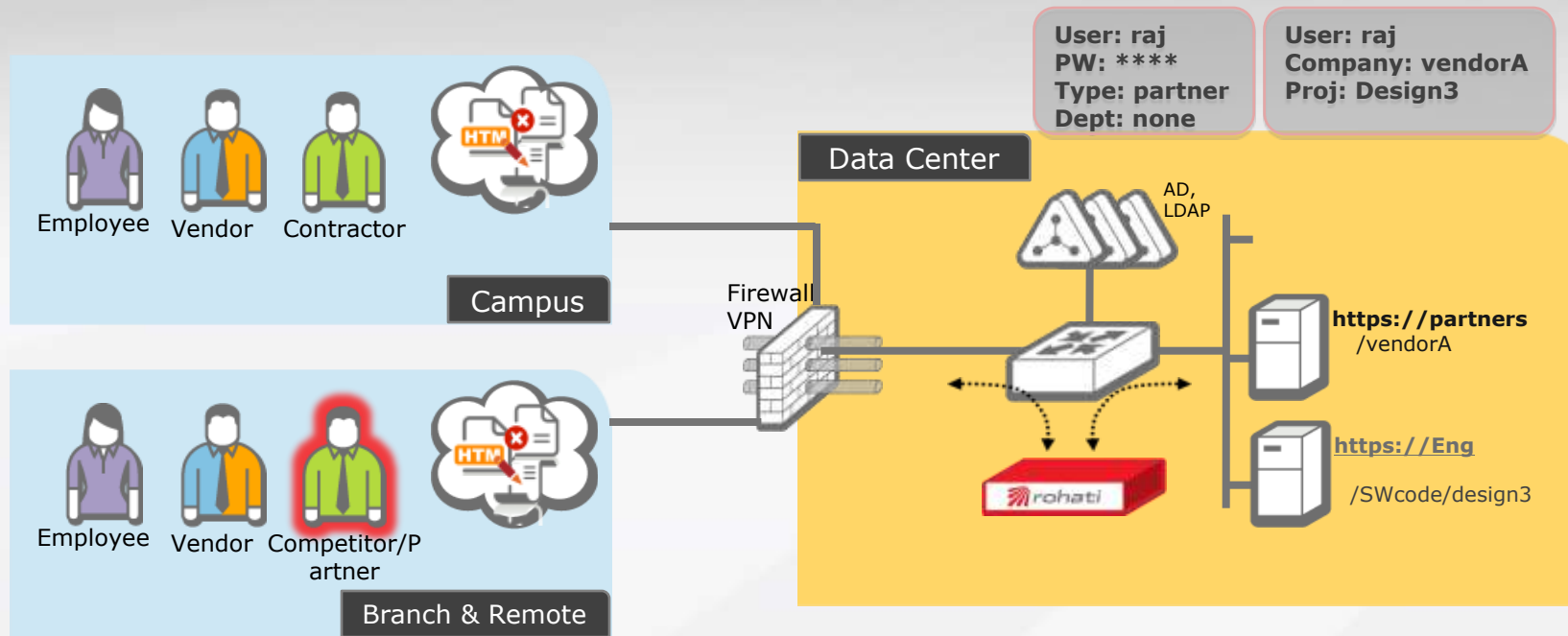
# Authenticate every user and authorize every transaction



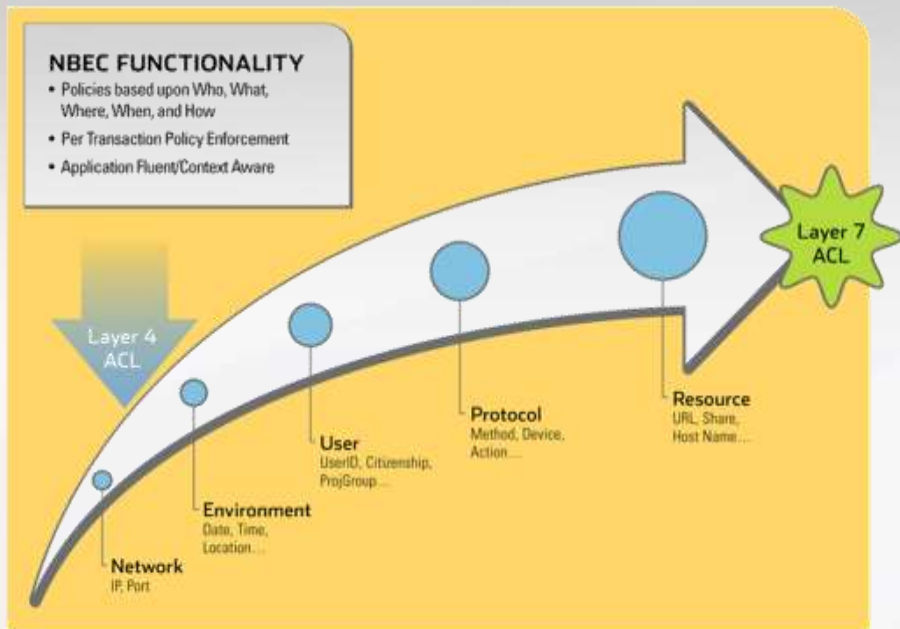
## Resources are invisible to those who aren't explicitly authorized



# Authorizations based upon any combination of user, resource, network and environmental attributes



## Layer 7 ACL's Enable Per Transaction Controls



	L4 ACL		L7 ACL
<b>Unit of Operation</b>	Packets and flows	➔	Transaction
<b>Resource definition</b>	IP address	➔	URL or URI
<b>User identification</b>	IP address	➔	User ID
<b>Policies based on</b>	"5-tuple"	➔	Business attributes

## Policies need to directly reflect business intent

### Policy Protect\_Finance\_web\_app

target resource Finance\_web\_app

rule-combine permit-overrides

rule Permit\_Finance

rule Permit\_Contractor



### rule Permit\_Finance

effect permit

condition 0 attribute usertype equal\_to

Employee

condition 1 attribute Department equal\_to

Finance

### rule Permit\_Auditor

effect permit

condition 0 attribute usertype equal\_to

contractor

condition 1 attribute vendor equal\_to

AcmeAudit

## Benefits:

- Human readable
- Policies based upon business in addition to network attributes
- Resource centric
- Easier to manage and audit
- Flexible logging

## Context based logs provide “Who, What, Where, and When”

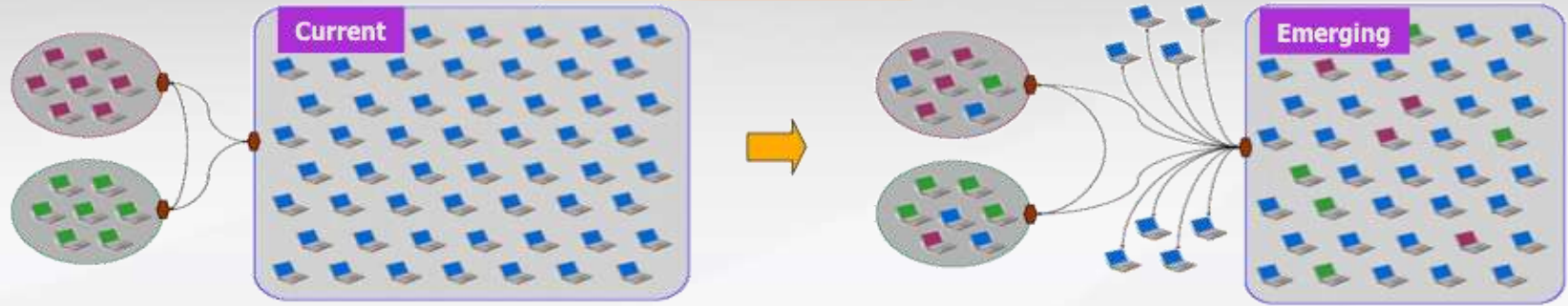
usr▼	uri▼	dc▼	Vendor▼	Department▼	Rule▼	Client IP▼
jdoe@rohati.com	/finance/mywebapp.htm	Permit		Finance	Permit_Finance	10.10.0.56
aroy@rohati.com	/finance/mywebapp.htm	Permit	AcmeAudit	Finance	Permit_Auditor	10.10.0.2
rogue@rohati.com	/finance/mywebapp.htm	Deny		Sales	Permit_finance	192.168.1.5
jboss@acmeaudit.com	/finance/mywebapp.htm	Permit	AcmeAudit		Permit_Auditor	10.10.0.7

- Business context is implicit in the logs
- Aggregates attributes and users from multiple directories
- Provides rule which resulted in the log entry

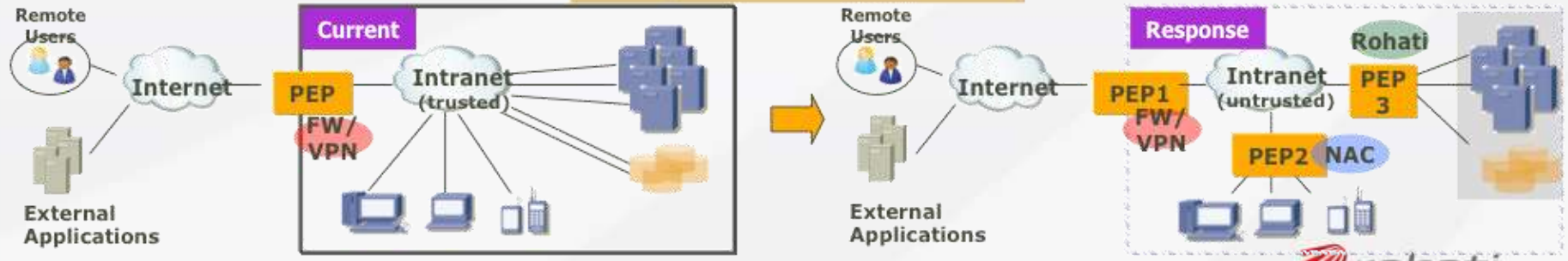
# Defense in depth approach compliments existing PEP investments

- Aerospace example

## User Communities



## Policy Enforcement Point



© Copyright 2008 Rohati Systems Confidential, Inc. All Rights Reserved.



PEP: Policy Enforcement Point

## Transaction level Policy enforcement and logging supports business needs and compliance mandates

Business  
Responsiveness

Compliance and  
Security

Operational  
Simplicity

- ⑩ Quickly and Cost-Effectively secure all data center resources inc web
- ⑩ No touch to applications, users or network
- ⑩ Based on the 'Layer 7 ACL' to deliver transaction-level enforcement
- ⑩ Centralized deployment and management ensure operational simplicity
- ⑩ Per-transaction logging and reporting drives down cost of Audit

### Technology Foundation

Layer 7 ACL's, Zero Click HA, Virtual Directory, Wire speed...



Thank you

