ITSAC 2011

Enabling Enterprise Security Management Solution Interoperability through SCAP

November 2011

Agenda

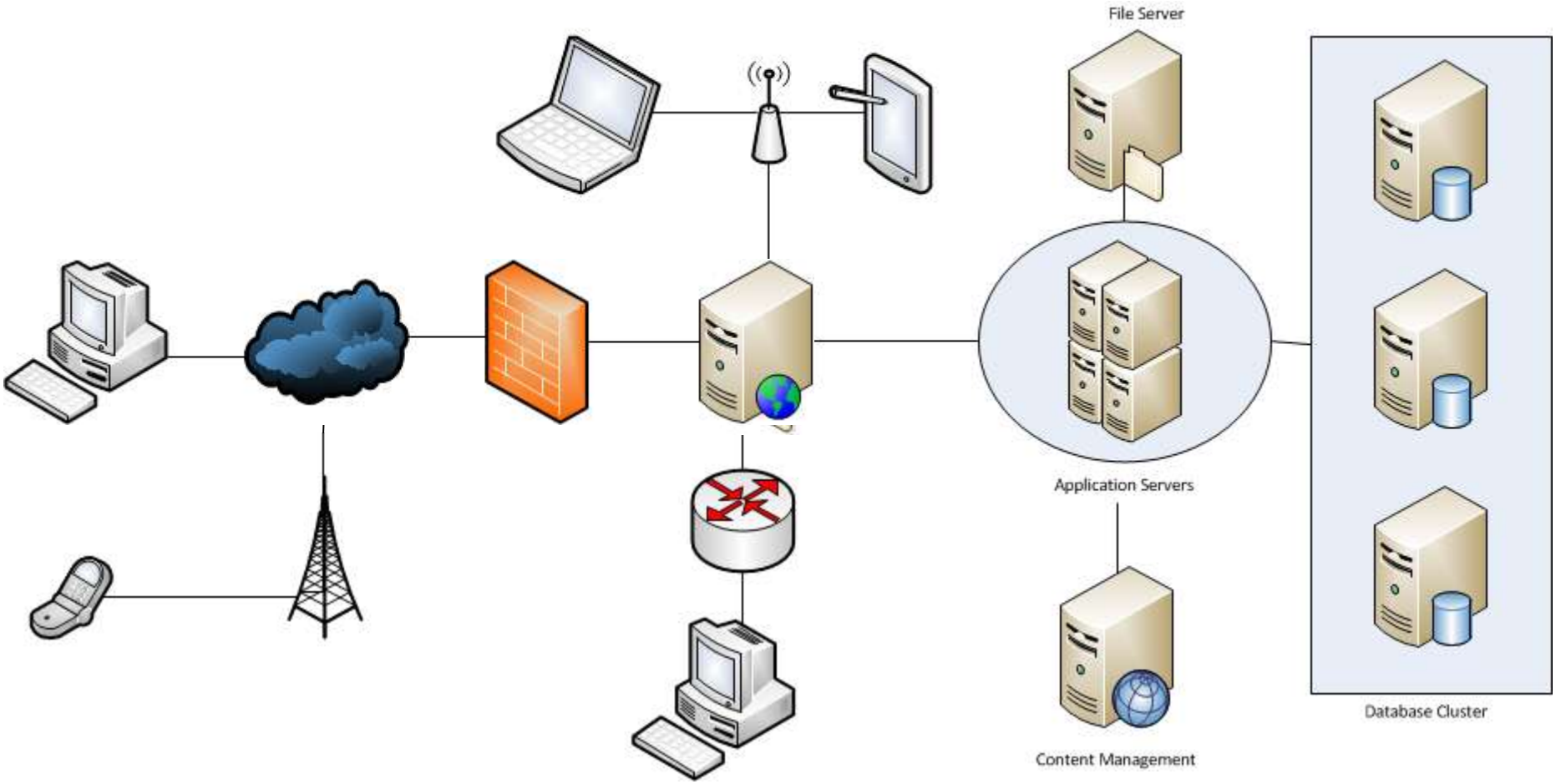
- Challenge of Today's Users
- ESM Data Flow Walkthrough
- Trusted Engineering
- How Do I Get Involved?

Agenda

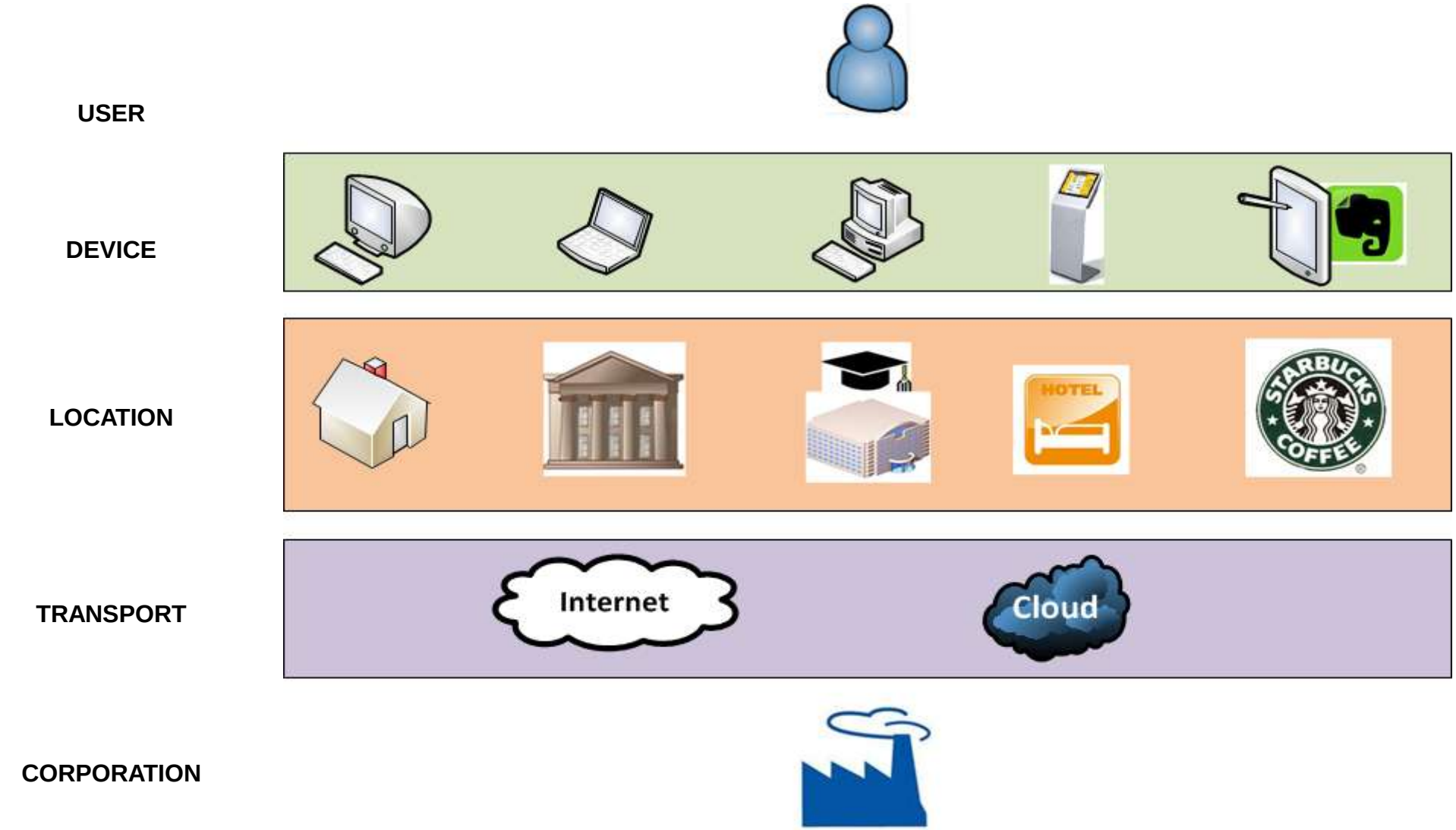
- Challenge of Today's Users
- ESM Data Flow Walkthrough
- Trusted Engineering
- How Do I Get Involved?


Continuous Compliance
Help Desk Overload
Escalating Administration Costs
Ghost User Accounts
Accumulating & Inappropriate Privileges
Auditors' Requirements
Leverage-able It Infrastructure
Negative Security-Related Publicity
"I don't want to see my organization in the news."

Multiple Access Points is a security challenge



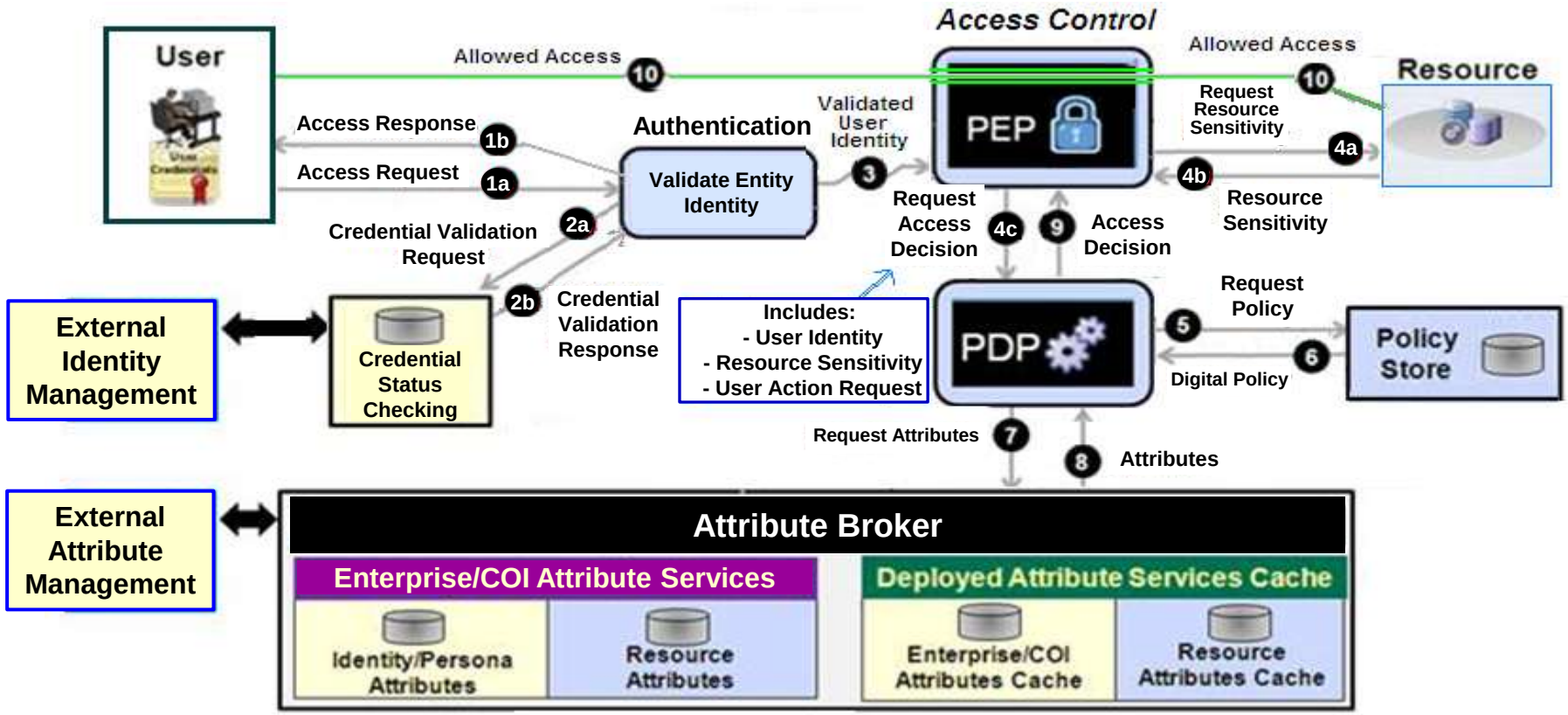
Users access information from a variety of location



Agenda

- Challenge of Today's Users
- ESM Data Flow Walkthrough
- Trusted Engineering
- How Do I Get Involved?

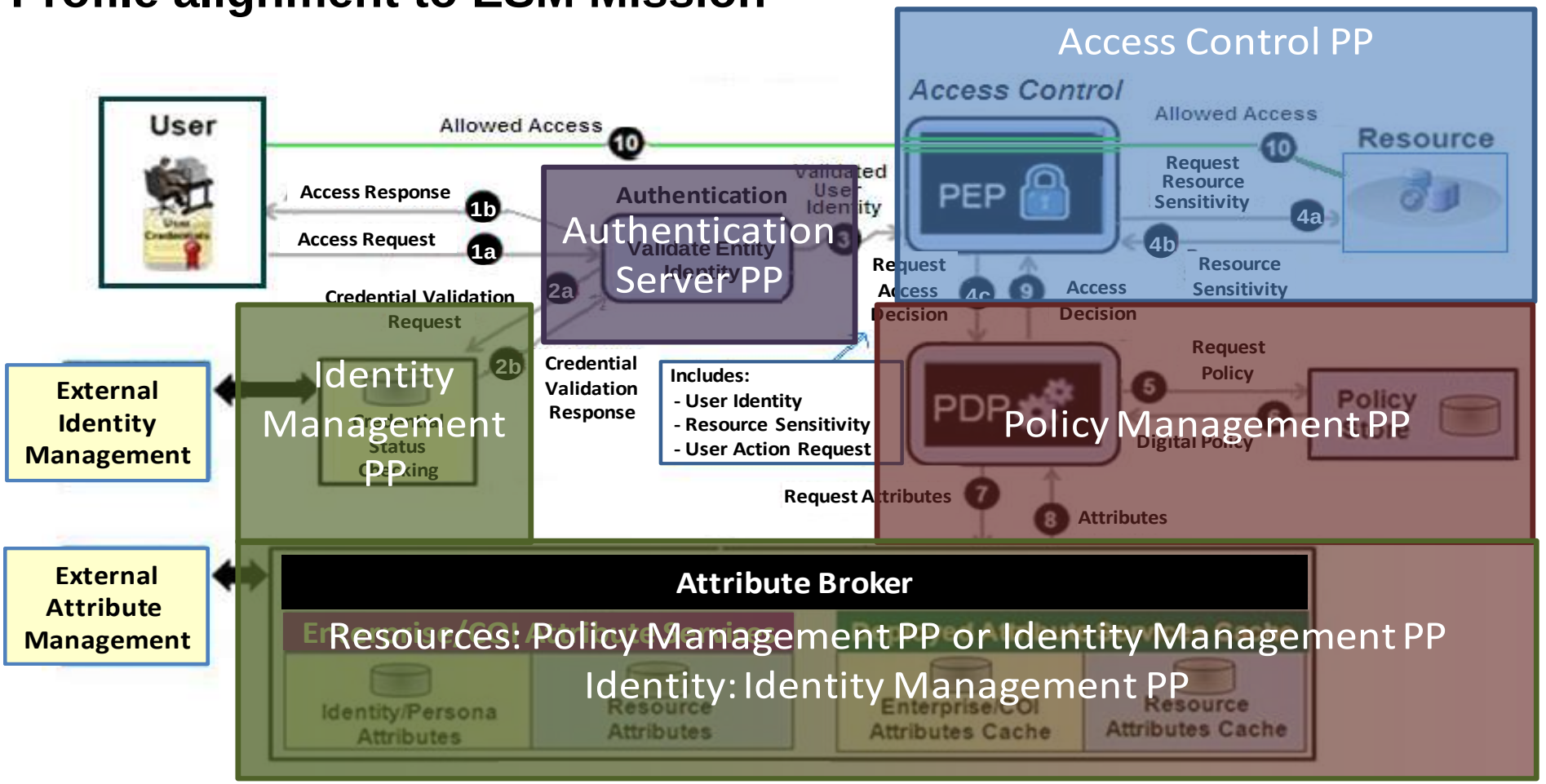
Enterprise Security Management
Access Control Use Case



Types of Access Control Solutions

Type	Object	Operation
Host Based	Processes	Execute | Delete | Terminate
		Change Permissions
	Files	Create | Read | Modify | Delete
		Change Permissions
	Host Configuration	Read | Modify | Delete
	Authentication Function	Login
Web-Based	URLs	Access via HTTP operation
	Files	Open | Download
	Executable Scripts	Execute
		Enable | Disable
	Forms	HTTP GET | HTTP POST
Application -Based	Application Configuration	Create | Modify | View | Delete
	User Interface Elements	View | Modify
	Commands	Execute
	Managed Resources	Create | Modify | View | Delete
DLP	Print Spool	Submit (transfer outside security domain)
	Application Layer Protocol	Transmit (transfer outside security domain)
	File	View | Move | Copy (to another security domain)
	Clipboard	Copy | Paste (to another security domain)
	Removable Drive	Write To (transfer outside security domain)

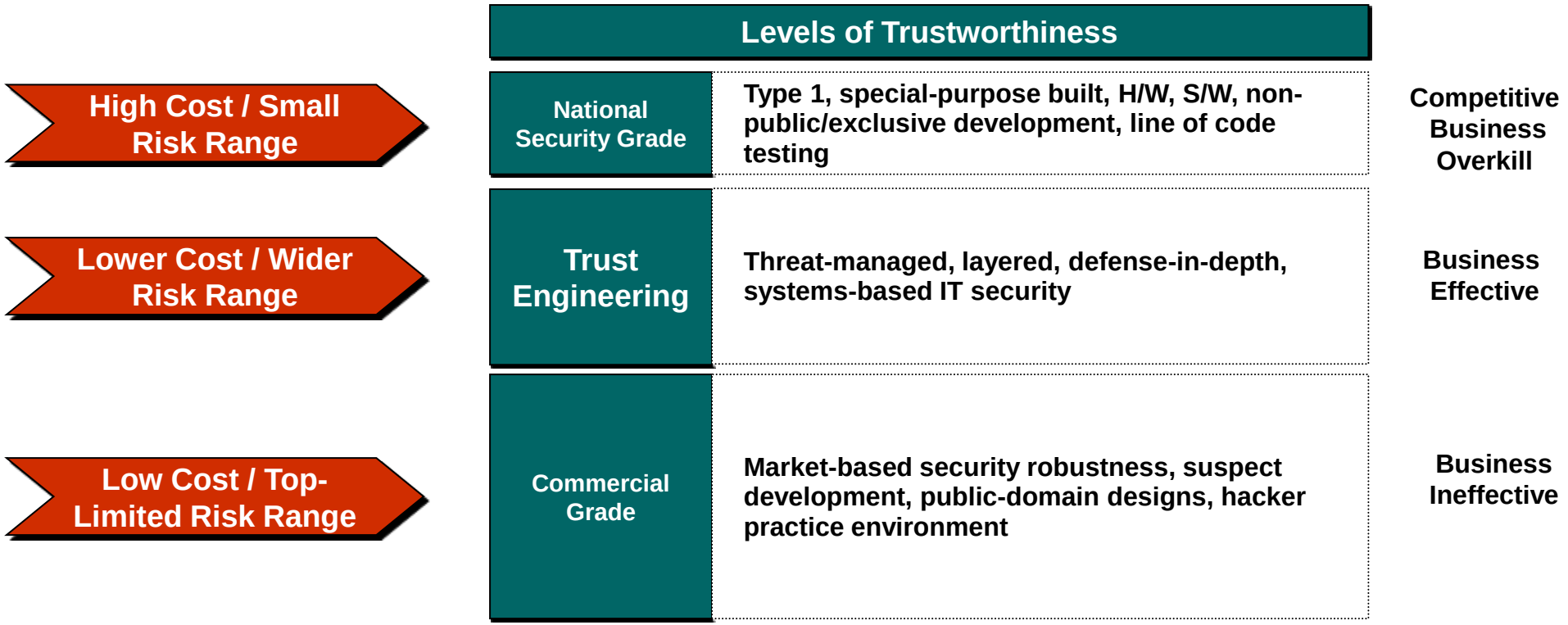
Profile alignment to ESM Mission



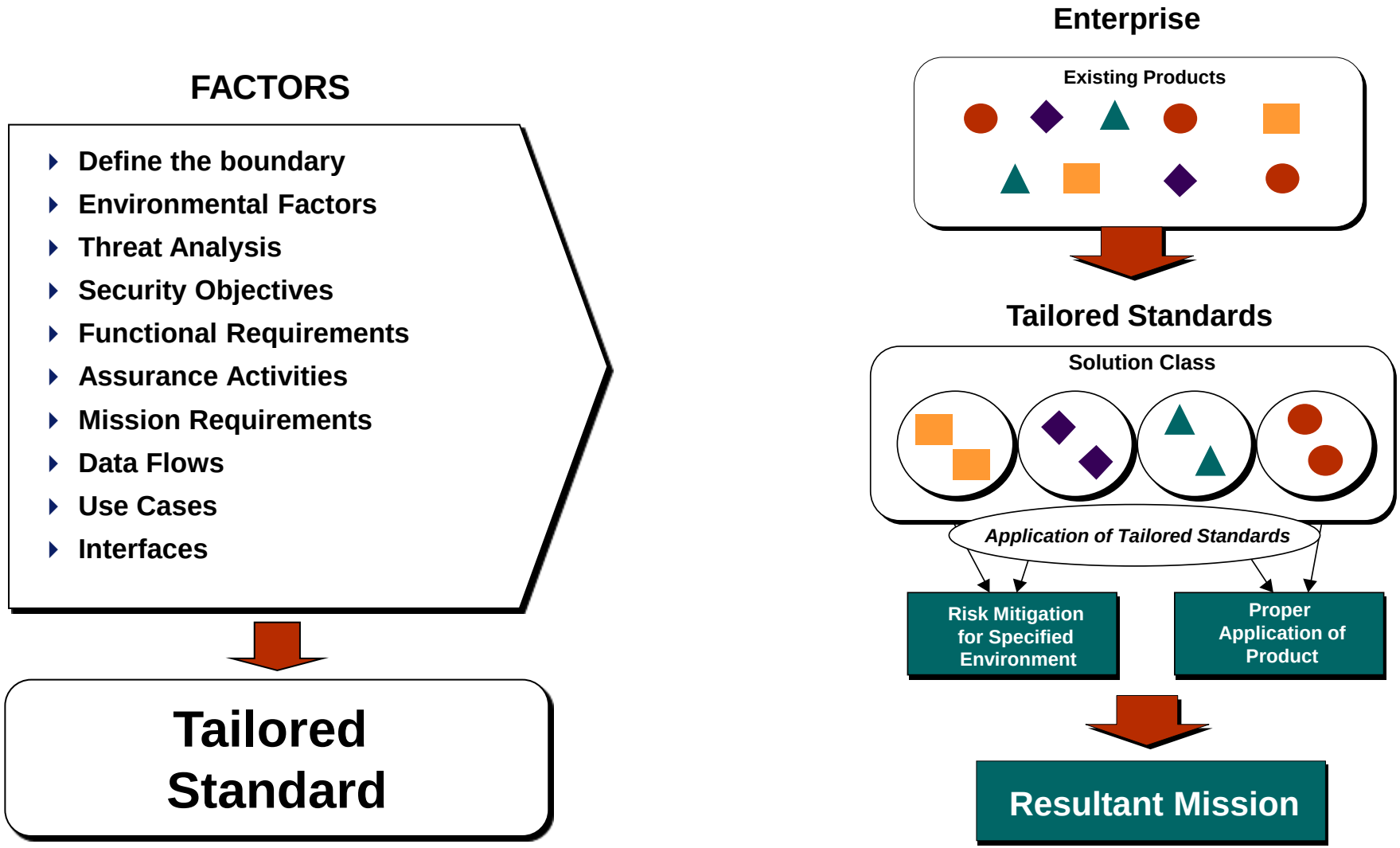
Agenda

- Challenge of Today's Users
- ESM Data Flow Walkthrough
- Trusted Engineering
- How Do I Get Involved?

Trust Engineering Layers available and relatively un-trusted components/applications to compose system solutions that enhance security posture while enabling business processes.



Enterprise requires development of standards to support the ESM solution class



Agenda

- Challenge of Today's Users
- ESM Data Flow Walkthrough
- Trusted Engineering
- How Do I Get Involved?

The team, so far (growing!)

We are always looking for more participants!

ca technologies

Booz | Allen | Hamilton

IBM

Microsoft

EMC²

ORACLE

EWA Enabling a More Secure Future

CSC

NIAP

cisco

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

Common Criteria Evaluation and Validation Scheme — NIAP CCEVS Validation Body

SAP

THALES

Australasian Information Security Evaluation Program (AISEP)

Common Criteria Consulting LLC

McAfee

RIM

symantec.

APEXASSURANCE GROUP

Questions

- Join us at:
  - http://groups.google.com/group/enterprise-security-management

Eric Winterton

CCTL Director, Booz Allen Hamilton

- winterton_eric@bah.com
- 410-684-6691