ITSAC 2012

SCAP and TNC

Enabling Enterprise Security Management Solution Interoperability through Open Standards

October 2012

Agenda

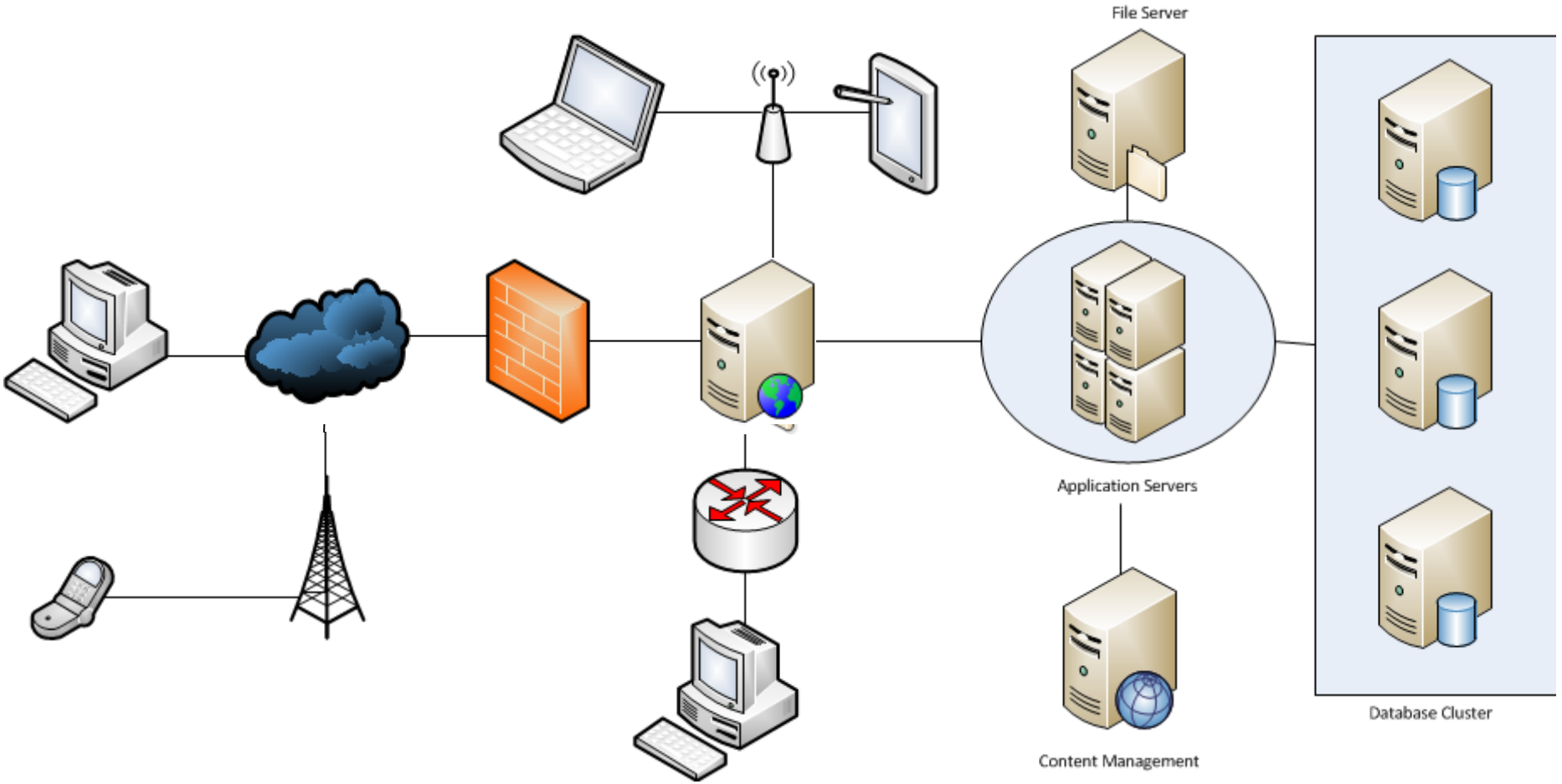
- Challenge of Today's Users
- ESM Data Flow Walkthrough
- ESM CND Architecture
- Trusted Engineering
- How Do I Get Involved?

Agenda

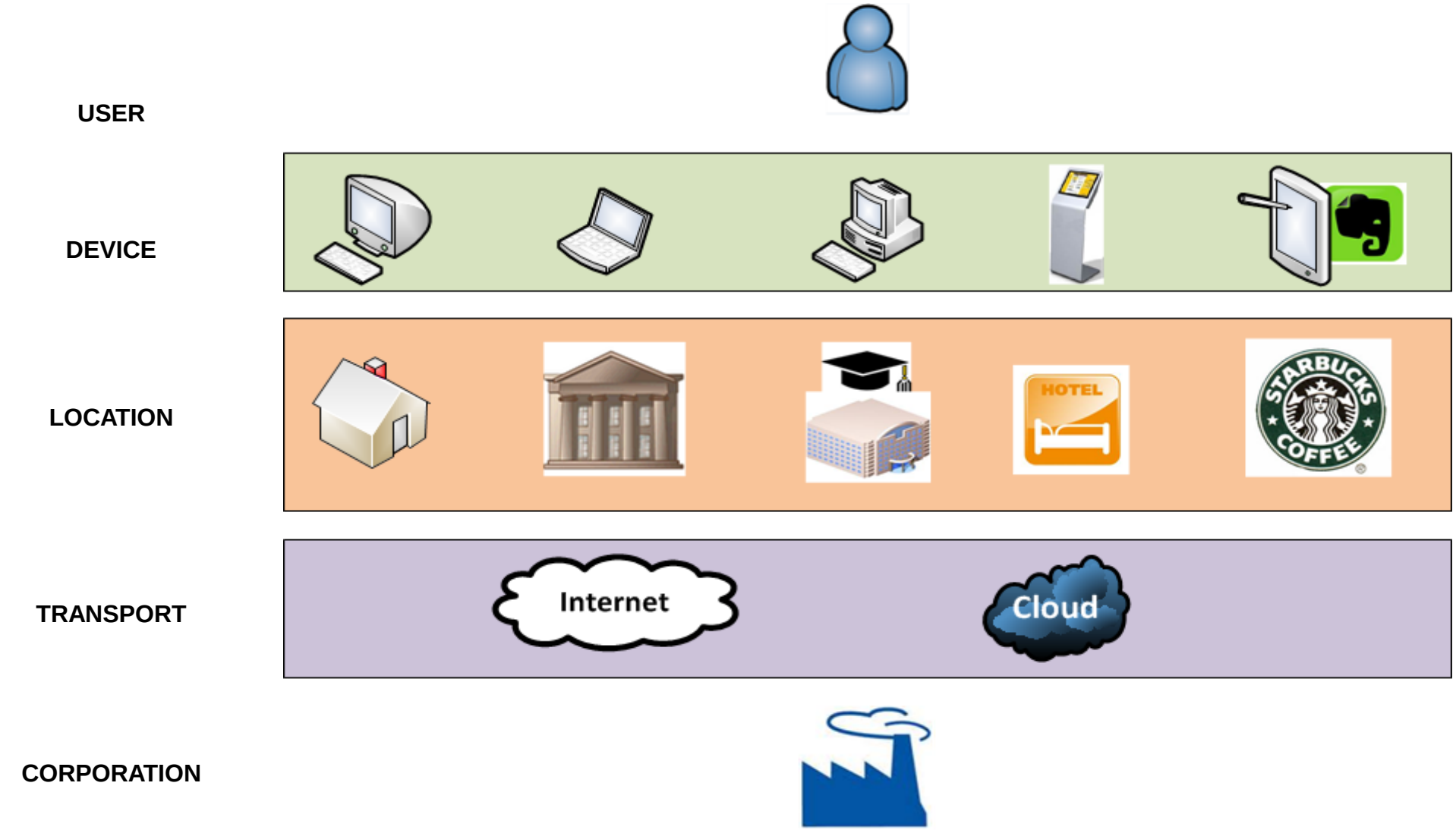
- Challenge of Today's Users
- ESM Data Flow Walkthrough
- ESM CND Architecture
- Trusted Engineering
- How Do I Get Involved?


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



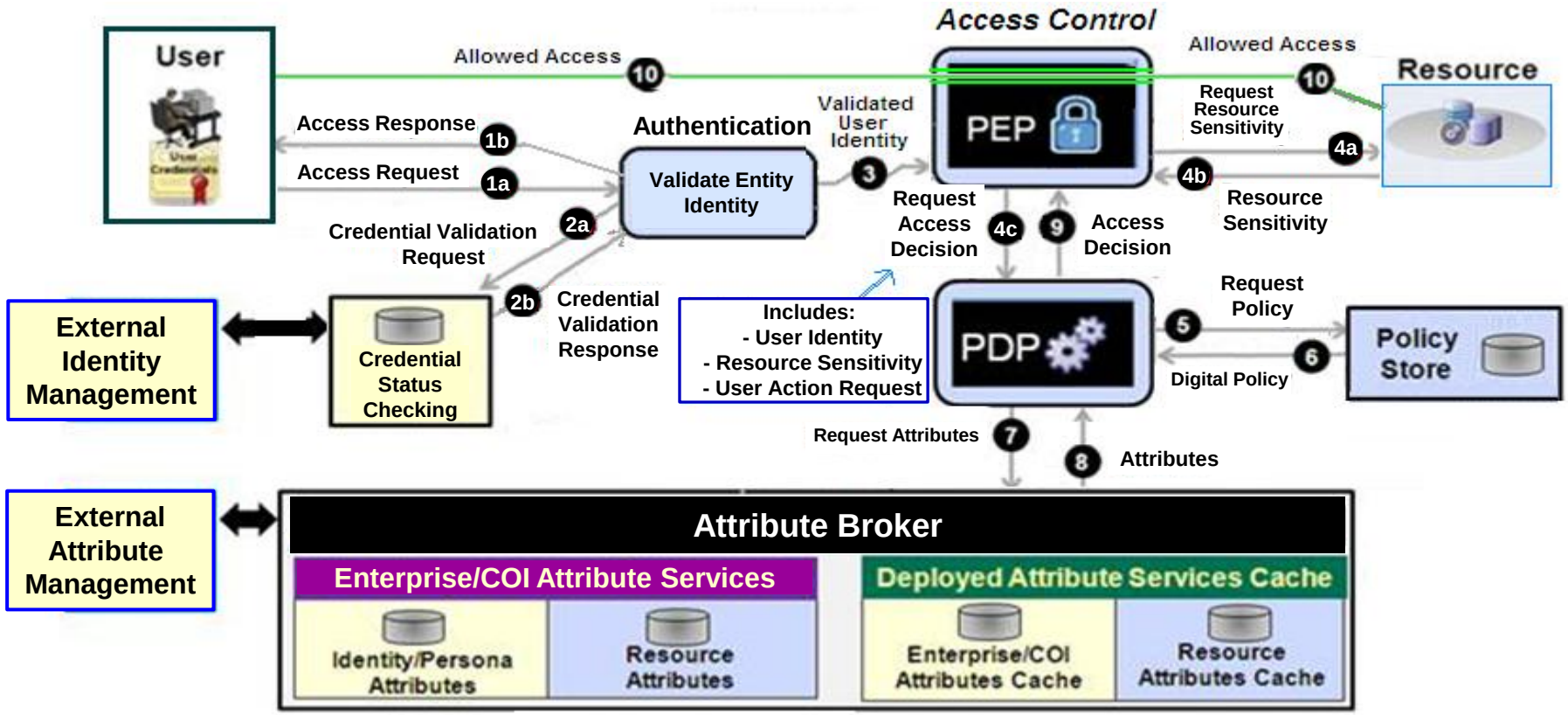
Users access information from a variety of location



Agenda

- Challenge of Today's Users
- ESM Data Flow Walkthrough
- ESM CND Architecture
- 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)

APT is single largest problem facing anyone on the Internet today

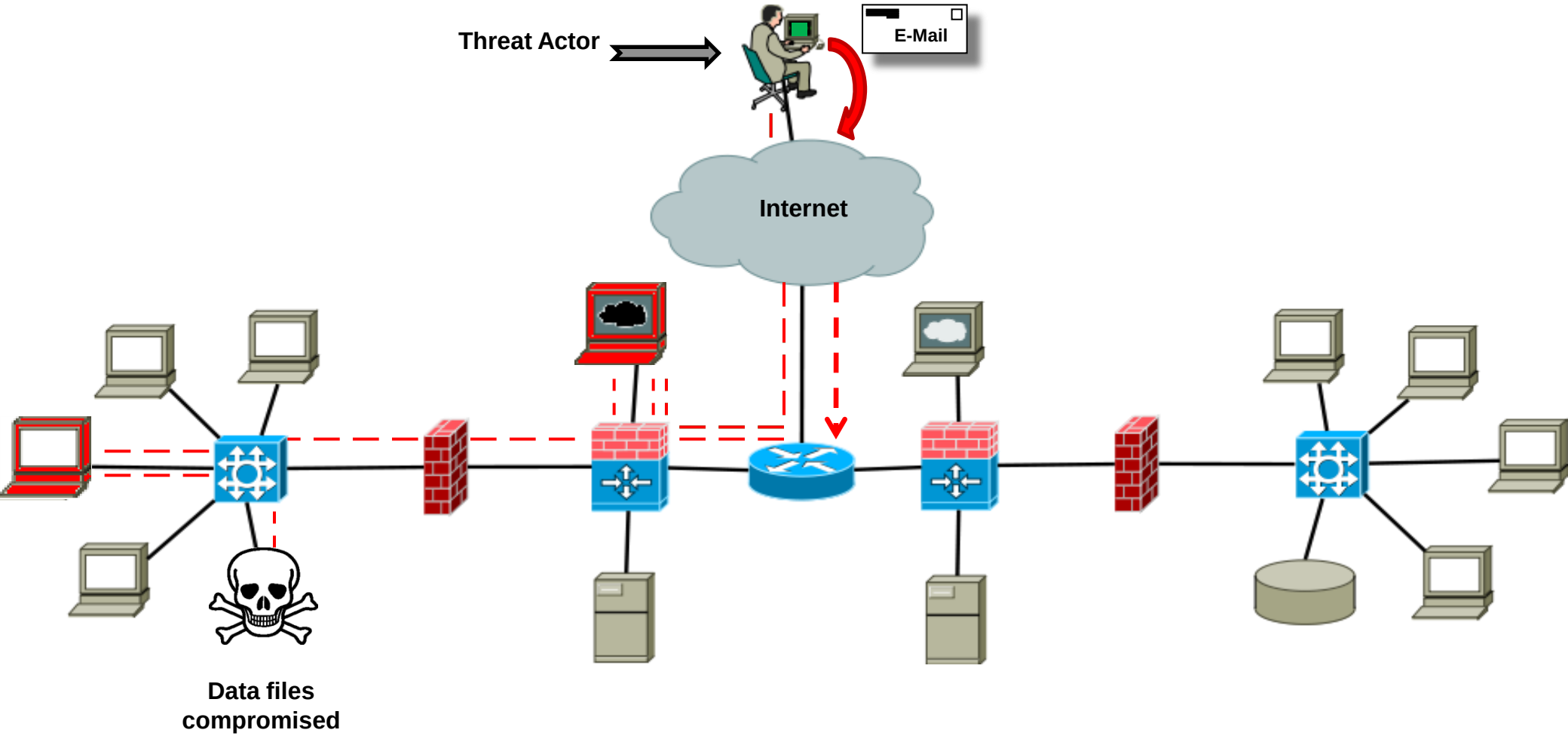
- "…Malware attacks against end users continue to rise, leading to increases in financial damage, intellectual property theft…"[1]
- By 2018 on average 1.6% of all corporate revenue will be lost due to data exfiltration
- Cost of Cyber Crime Study by Ponemon[2]
  - $5.9 Million is median total cost per compromise
  - 47% of participating U.S. organizations indicated they had experienced APT attacks or infections in the past two years.
  - More than 75% of all advanced malware goes undetected by *signature-based* security solutions
- In the last year Verizon RISK team responded to 855 incidents [4]
  - 58% of all data theft was tied to activist groups
  - 69% incorporated malware (+20% from 2011 report)
  - 96% of attacks were not highly difficult
  - 85% of breaches took weeks or more to discover

Sources:
[1]Gartner Report Mar 2012
***[2]Klogix* report "The Real Cost of Data Loss"**
[3]Ponemon Institute, 2012 U.S. Cost of a Data Breach Study
[4] 2012 Data Breach Investigations Report (DBIR)

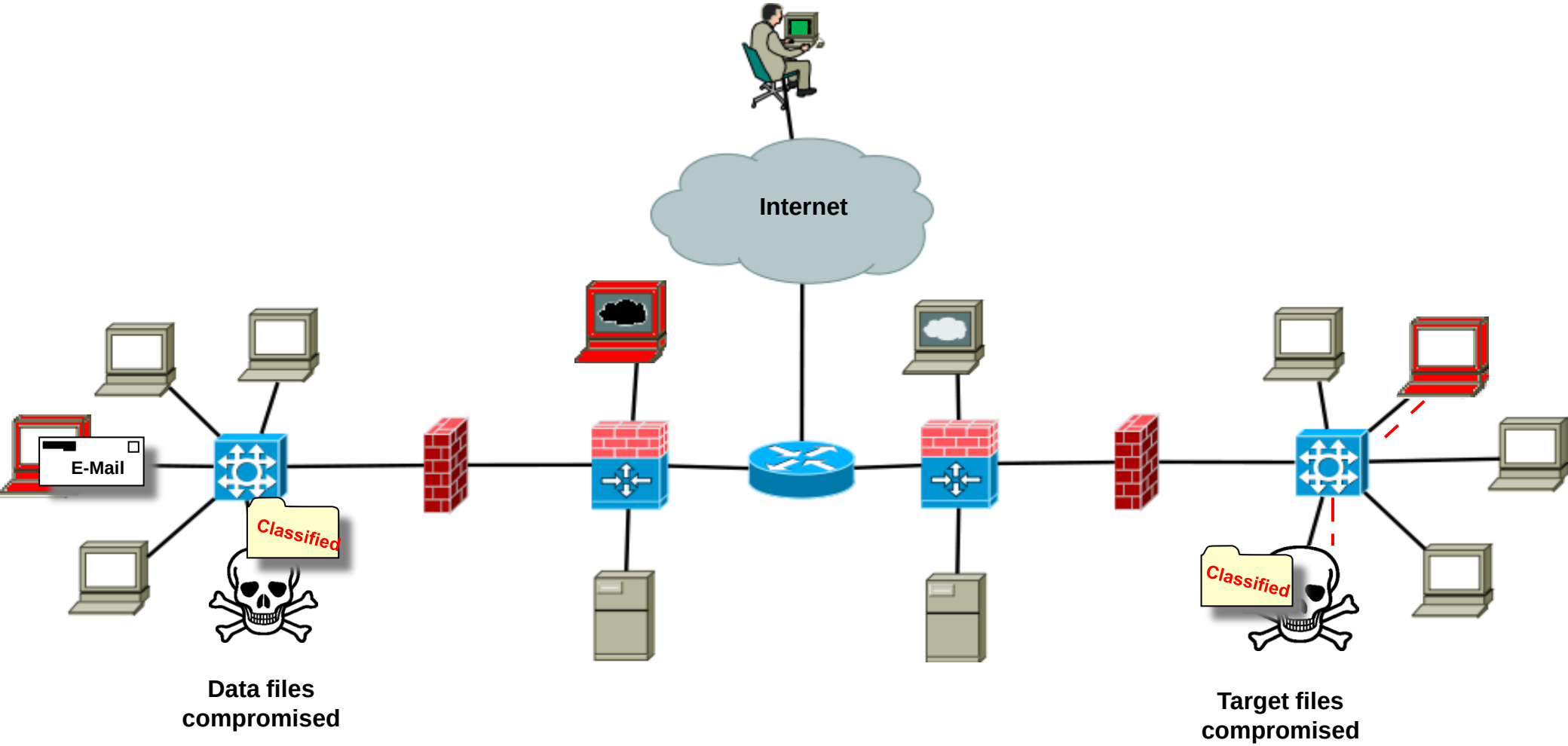
Agenda

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

Current Action: At[illegible]



Current Action: Send m

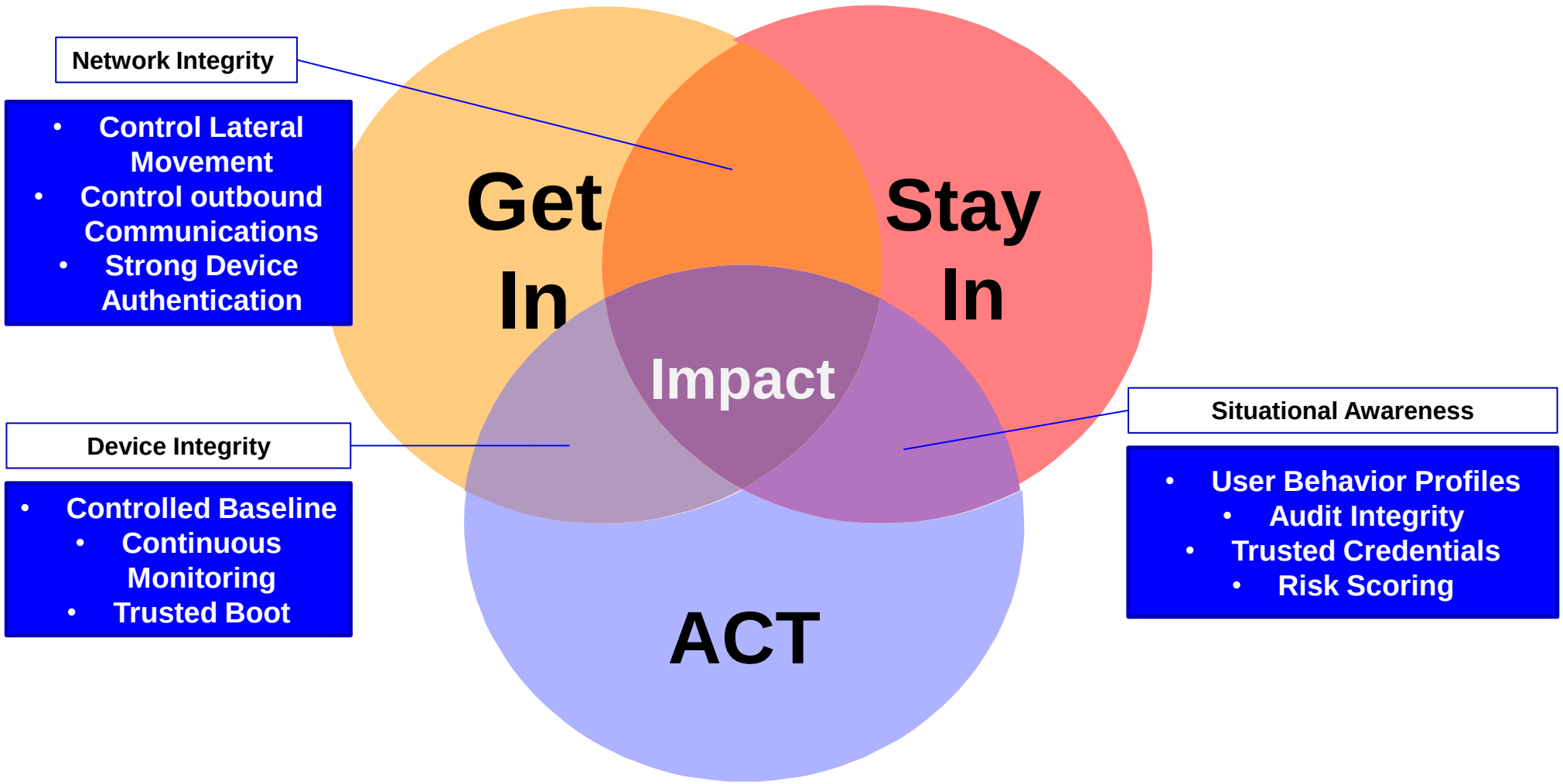


Data files compromised

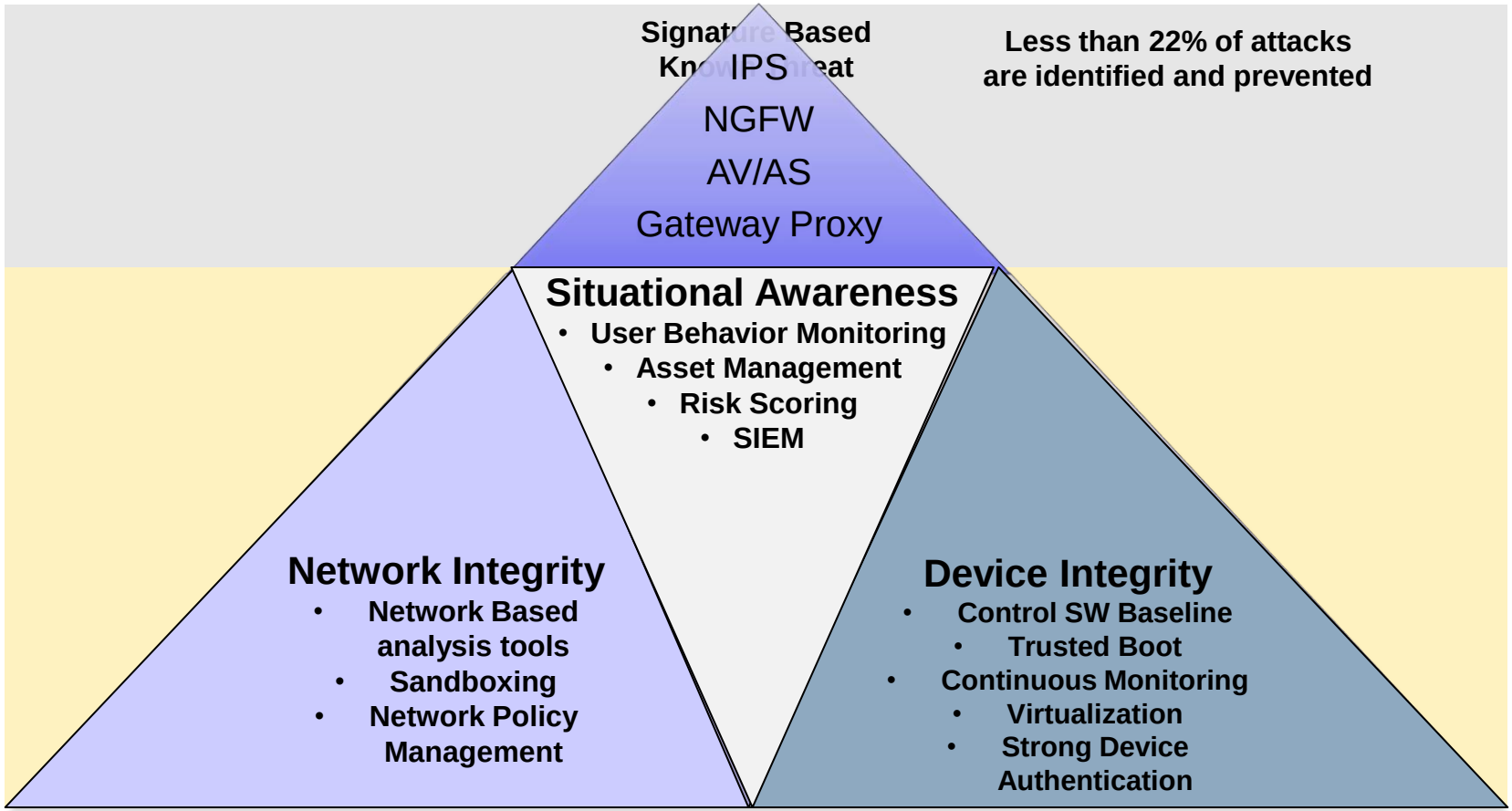
Target files compromised

Goals of APT

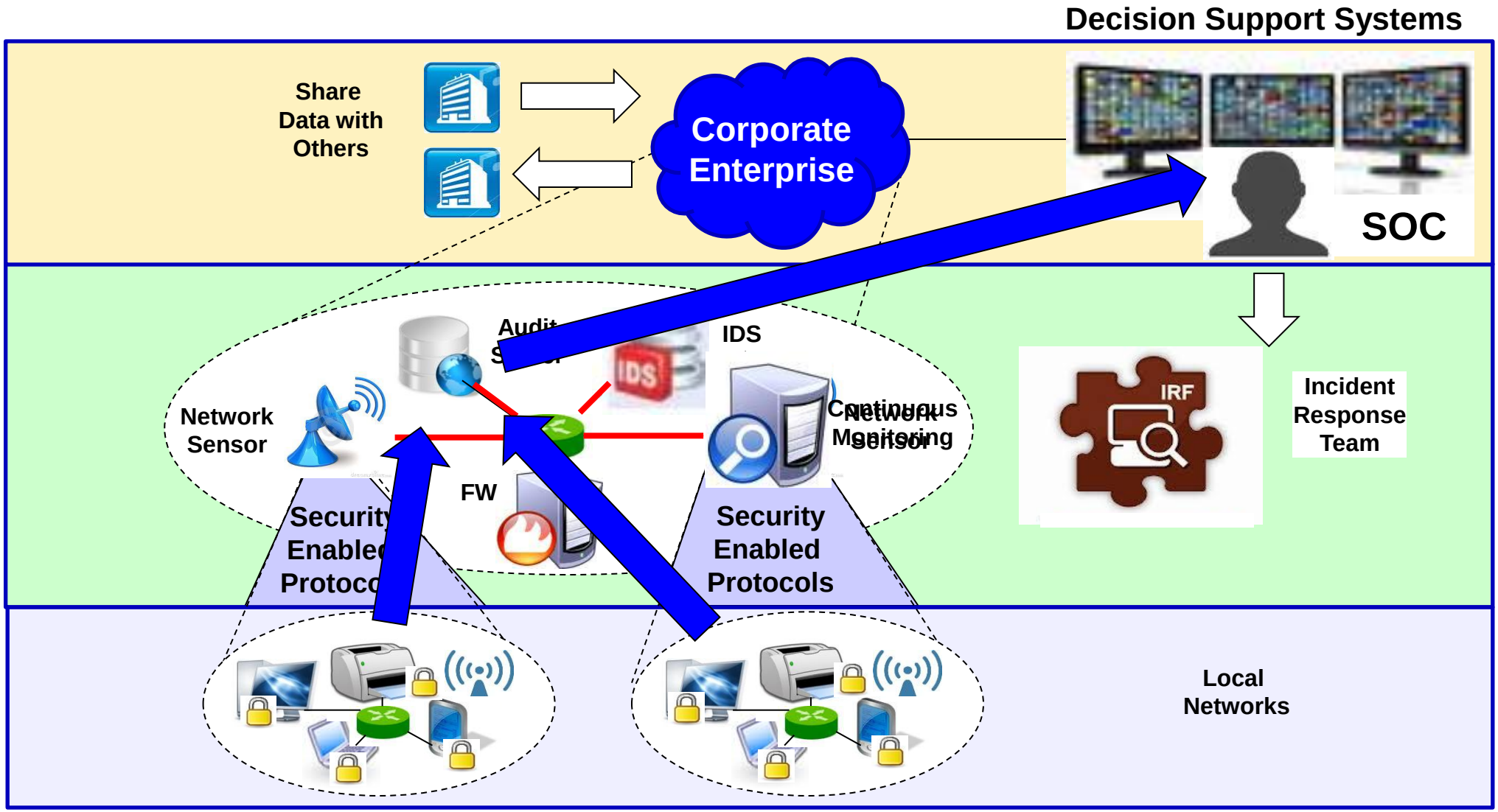
Security Controls to Defend Your Enterprise



New Protection Profiles will Assist SOC Analyst to Defend Against APT



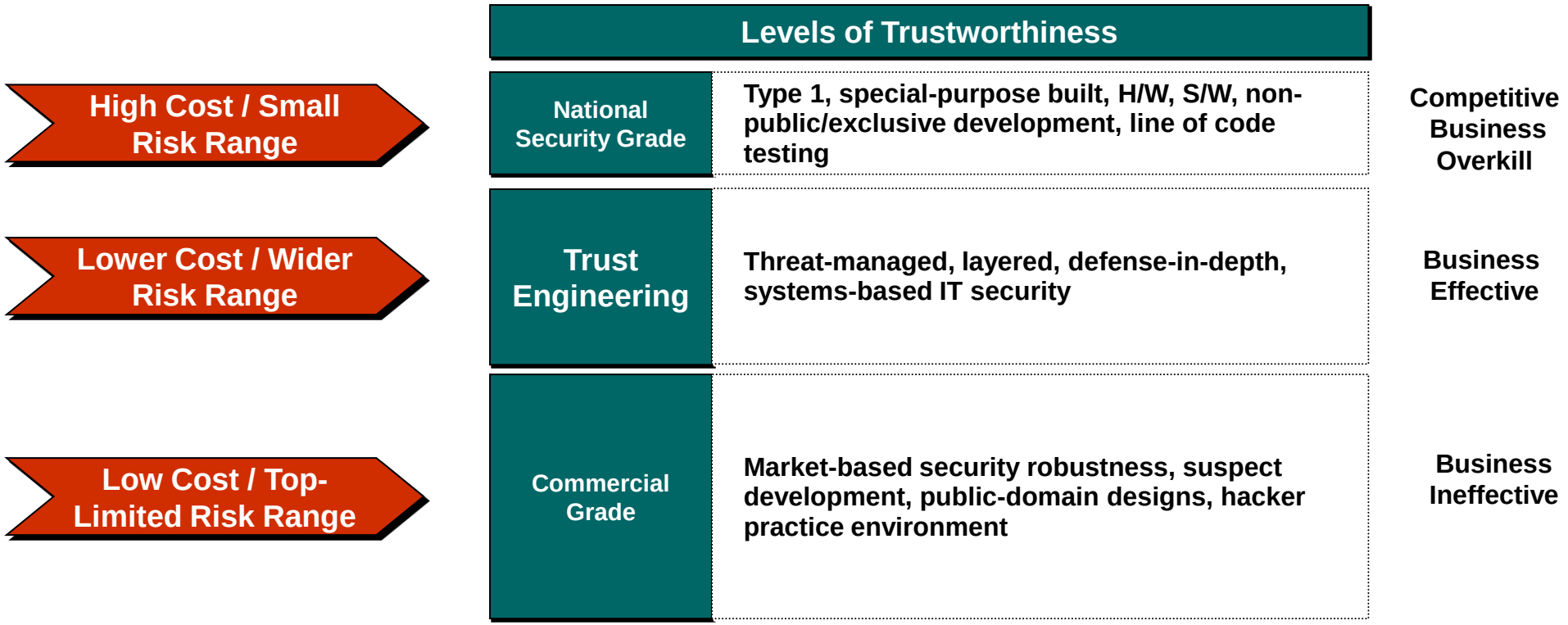
Three tier CND architecture



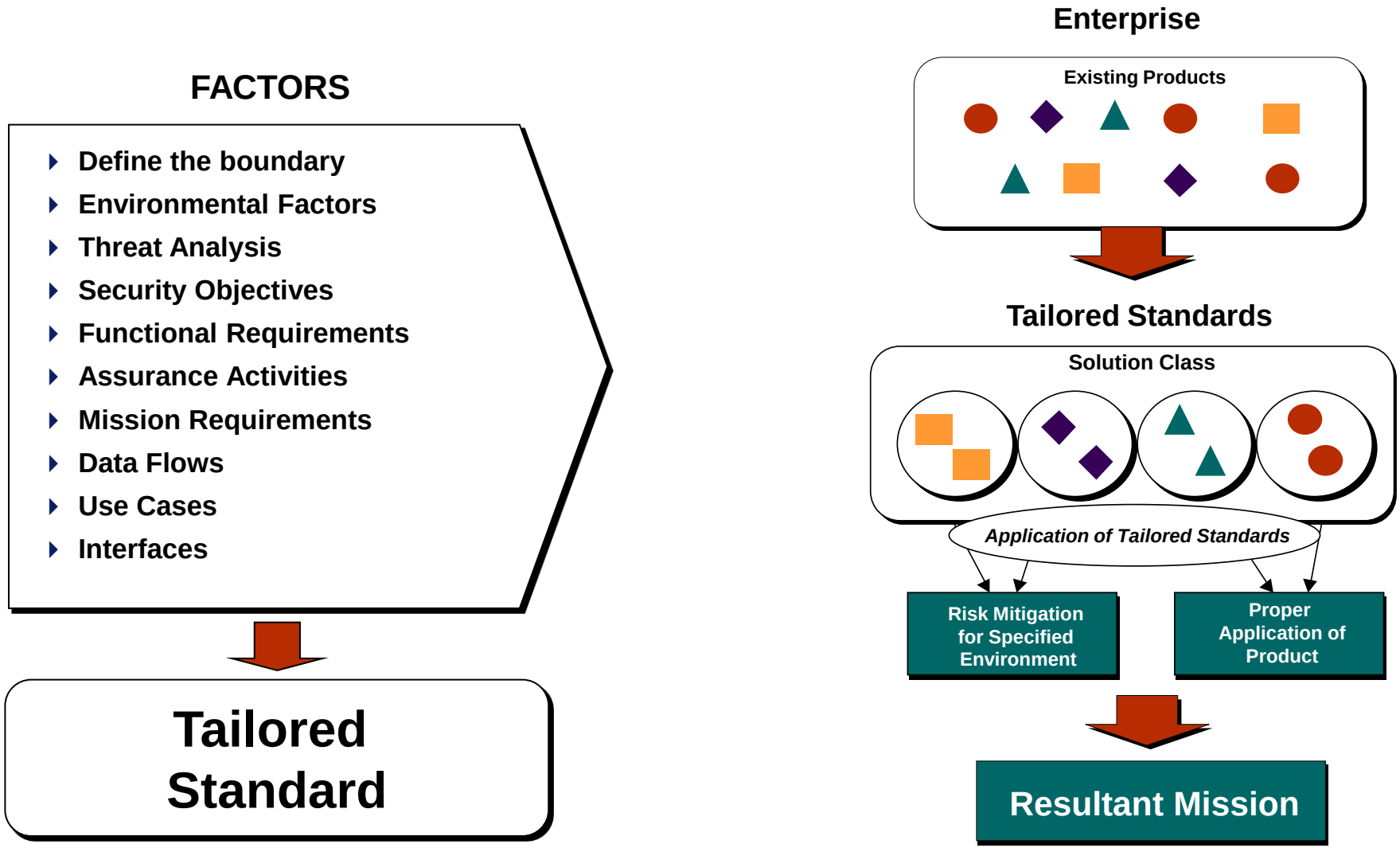
Agenda

- Challenge of Today's Users
- ESM Data Flow Walkthrough
- ESM CND Architecture
- 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
- ESM CND Architecture
- 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)

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