

enterprise security management  
protection profiles:  
global threat analysis and protection  
profile selection

**Joshua Brickman, CA Technologies**  
September 2010

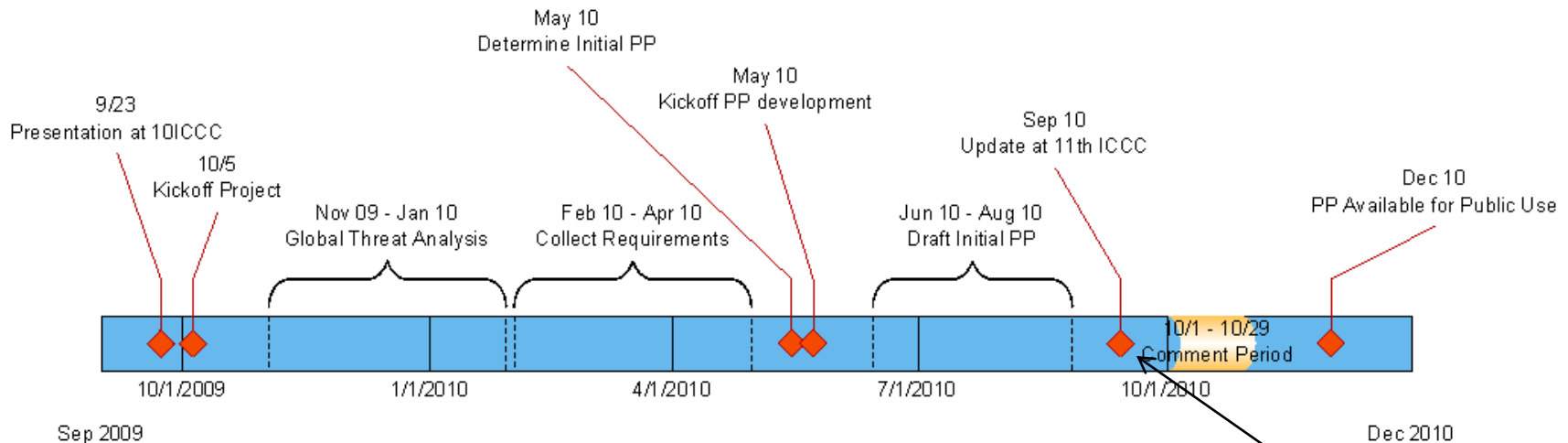


# agenda

- Review
- Enterprise Security Management— a review...what are these products?
- Some PP stats
- Schedule
- Survey instrument and demographics
- Results
- How can you get involved (participants)

# schedule

- Sept 2008 proposal
  - received well at 9<sup>th</sup> ICCC--interest by multiple vendors, NIAP, consultants and other schemes
- May 2009: NIAP pledges support for creation of the ESM PP's.
- May-Aug 2009: concurrence of ESM product categories among Microsoft, IBM, EMC, Oracle Symantec, and CA Inc solidified
- Sept 2009 implementation plan presented at 10<sup>th</sup> ICCC
- Fall 2009 global threat analysis
- Winter 2010: global threat survey
- May 2010: PP development



Today

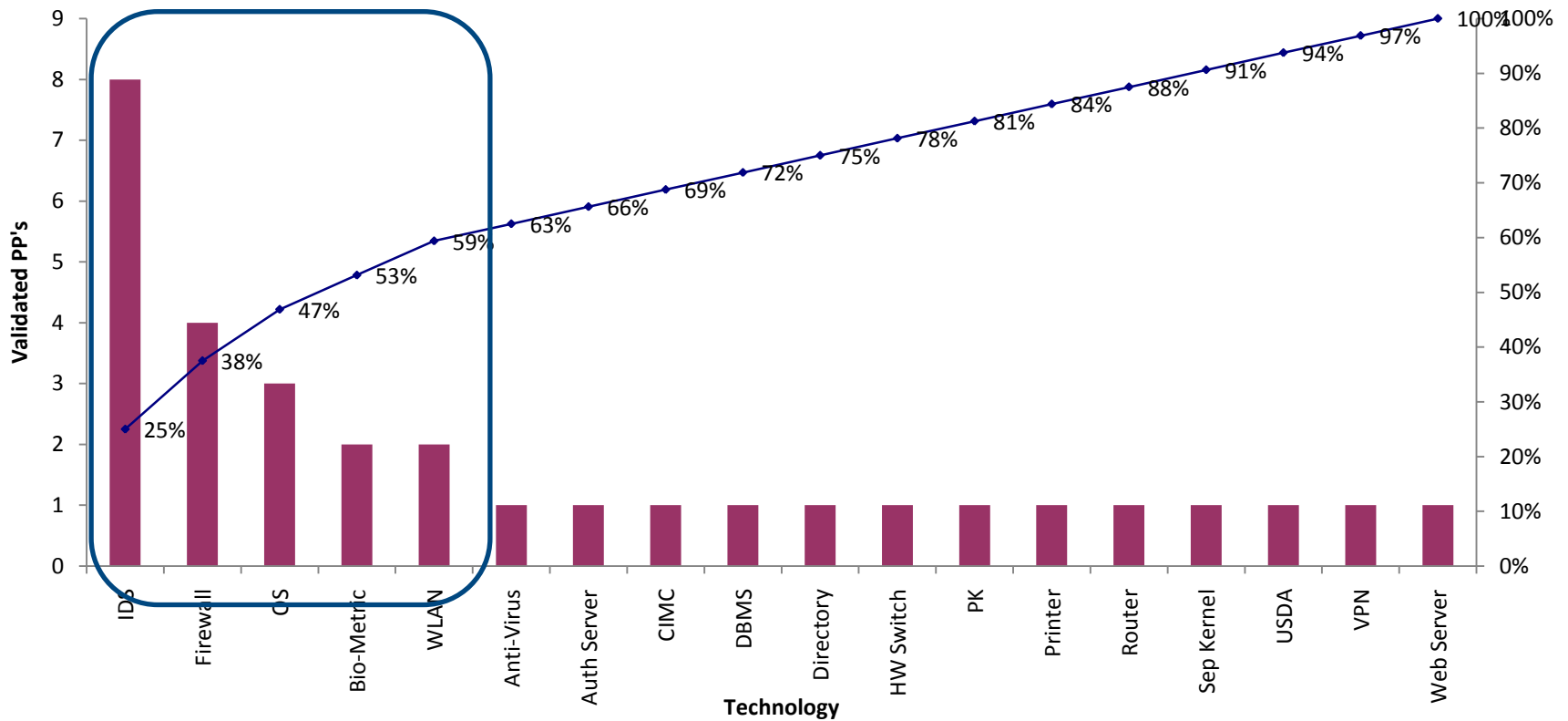
# what is ESM



## Enterprise Security Management



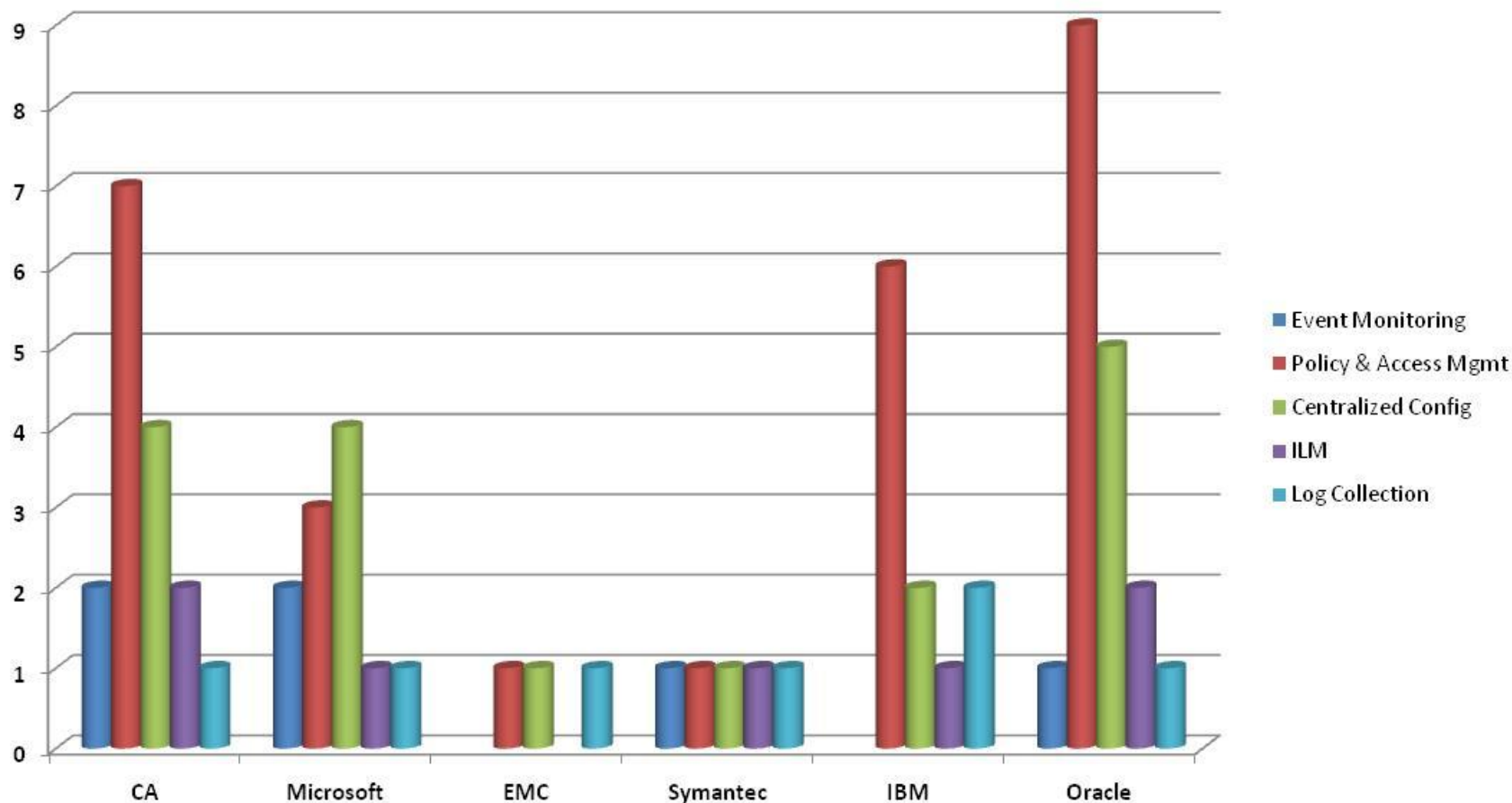
# existing PPs



60% of existing PP's cover only five technologies (out of 18)

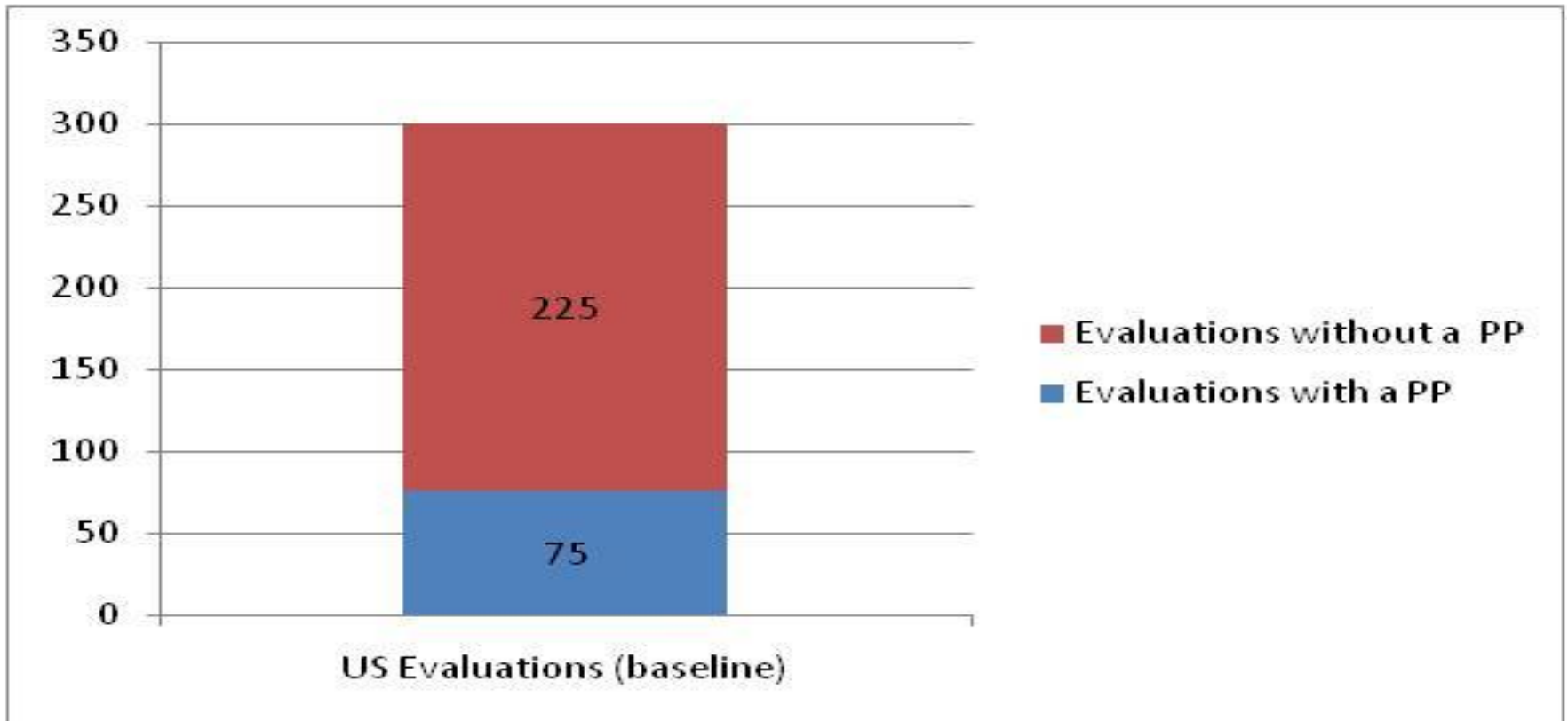
# number of ESM products available

by major vendors



- Policy & Access Mgmt make up 42% of ESM products available
- At least 64 products in the space

# CC evaluations in the US



- 23 PP's in the US only support 25% of products evaluated
- 16% of compliant evaluations had multiple claims
- With new ESM PP's, at least 64 products would be PP compliant
- 18 out of 23 CA evaluations would have been eligible for ESM PP's if they existed (78%)

# goal of the survey

- Two goals:
  - Prioritization of the 1<sup>st</sup> ESM PP
  - Importance of the CC and its elements to government customers

# survey demographics

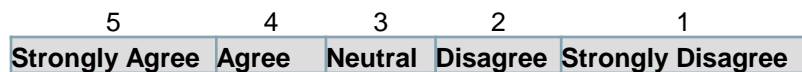
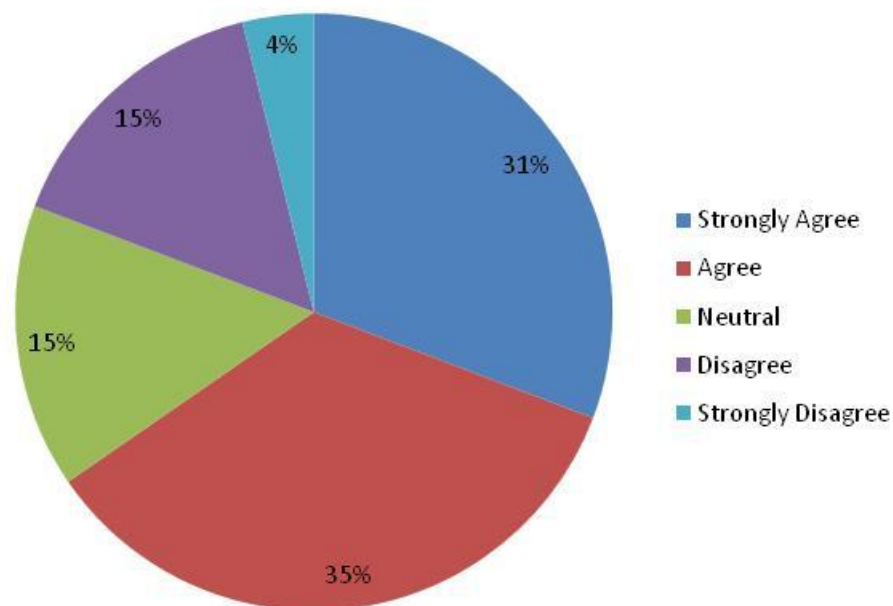
includes selection of 12 data points (survey questions)

- Data sampling:
  - 27 completed surveys
  - E-mailed to US DoD agencies and Australasian agencies
  - Survey posted on NIAP, Australasian, and British scheme sites
  - Available for five weeks on NIAP, three on other sites
  - Survey respondents included representatives from Japan, Canada, US, Australia, and Spain

**Data Source: Confirmit survey tool (250 records)**

# survey results: operational mission

My agency currently uses ESM Tools to achieve its operational mission

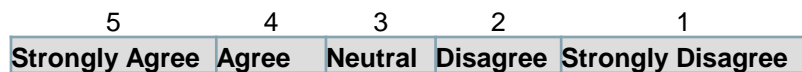
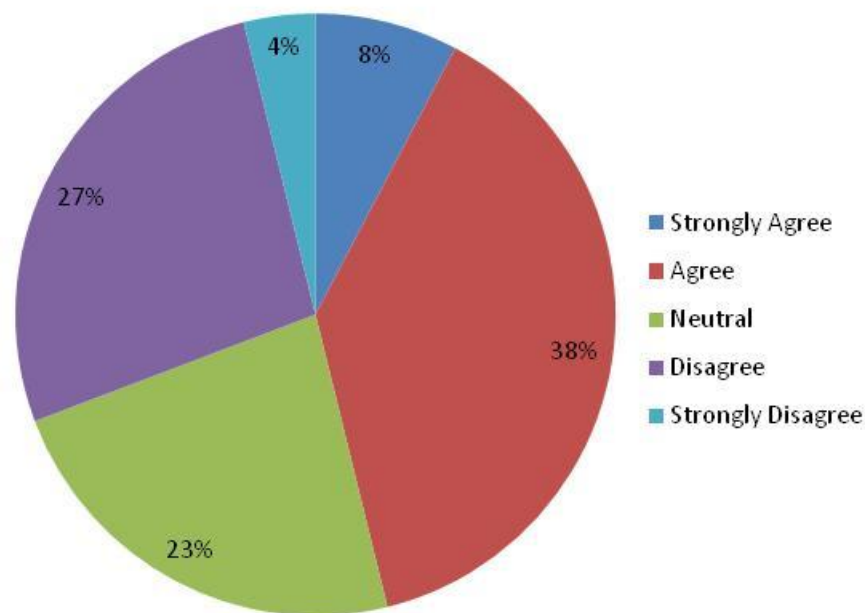


**Avg: 3.7**

**2/3 of respondents use ESM tools**

# survey results: operational mission

The ESM Products we use meet our Security requirements

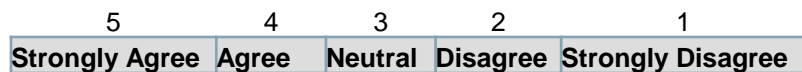
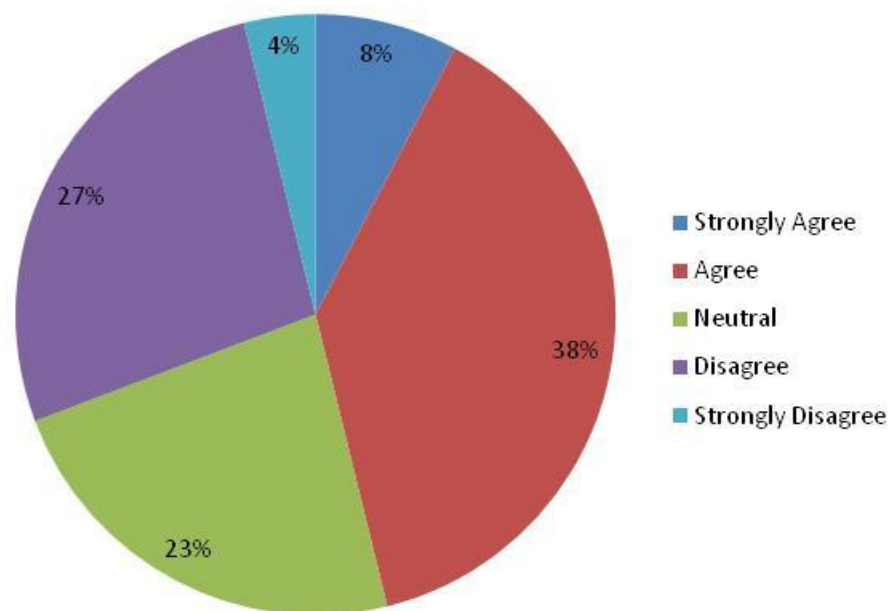


**Avg: 3.1**

**46% Agree, but 31% are unsatisfied with their ESM products**

# survey results: operational mission

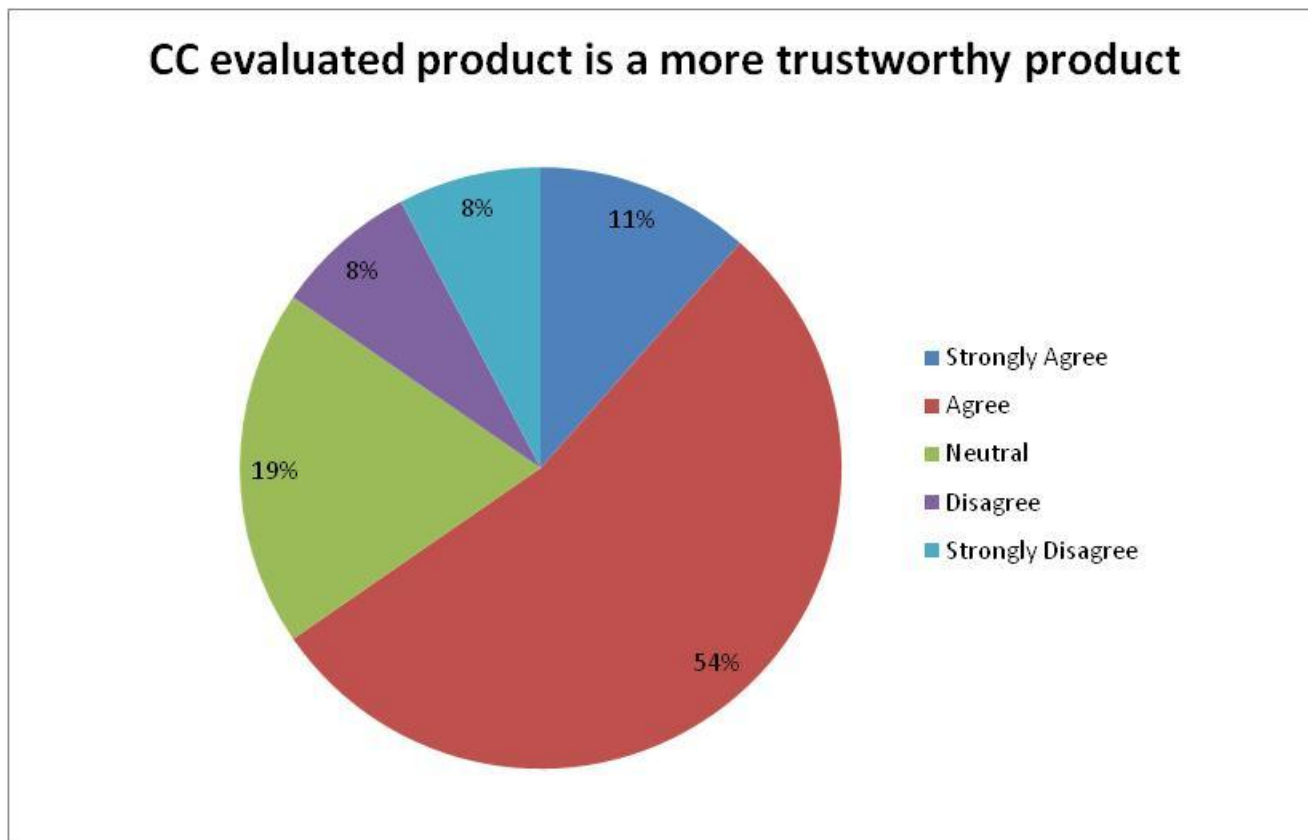
ESM products that integrate well together are very important.



**Avg: 4.1**

**Almost 50% believe that integrated products are very important**

# survey results: common criteria

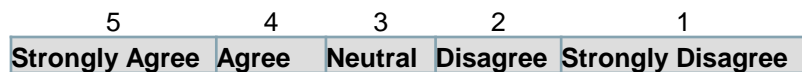
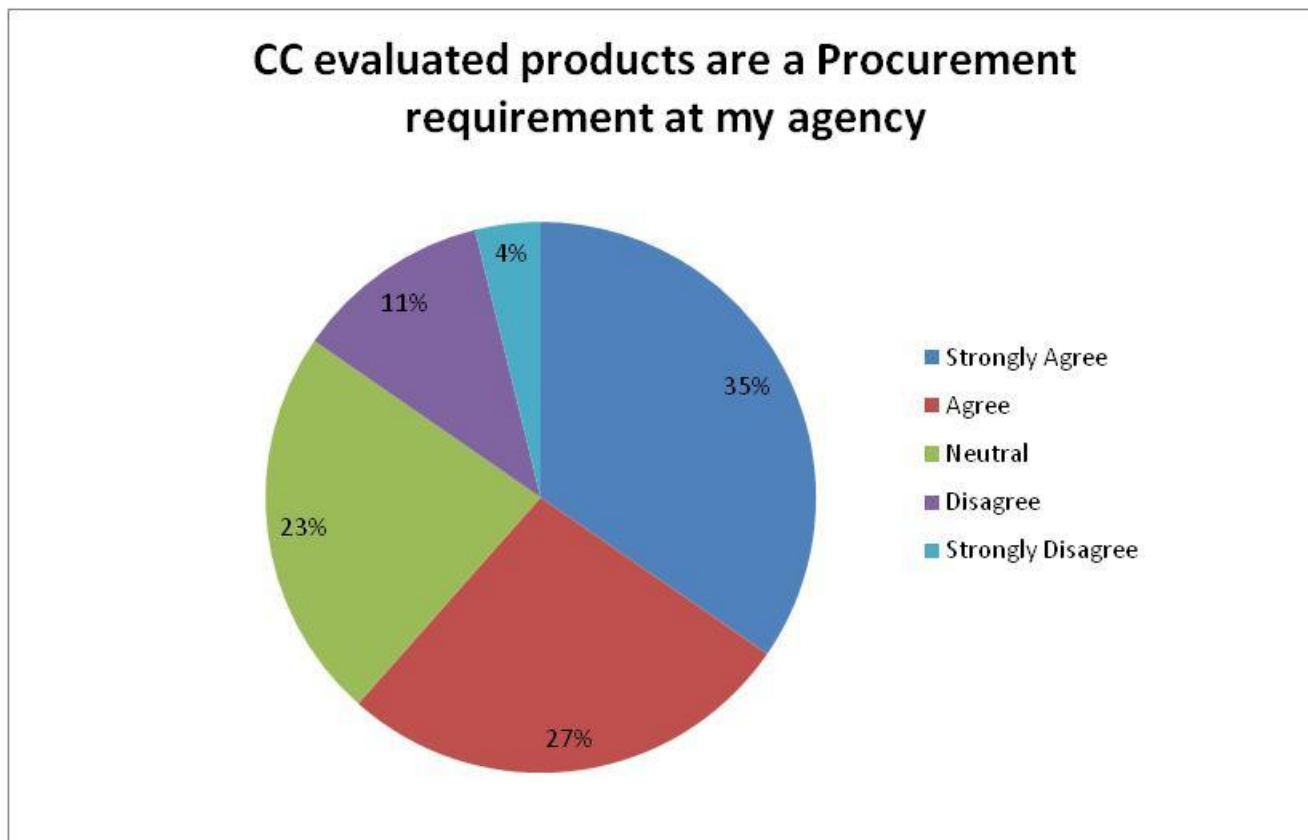


5 4 3 2 1  
Strongly Agree Agree Neutral Disagree Strongly Disagree

**Avg: 3.5**

**65% believe that CC evaluated products are more trustworthy**

# survey results: common criteria



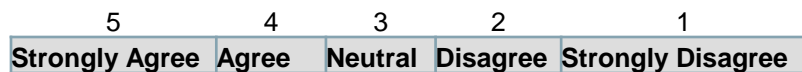
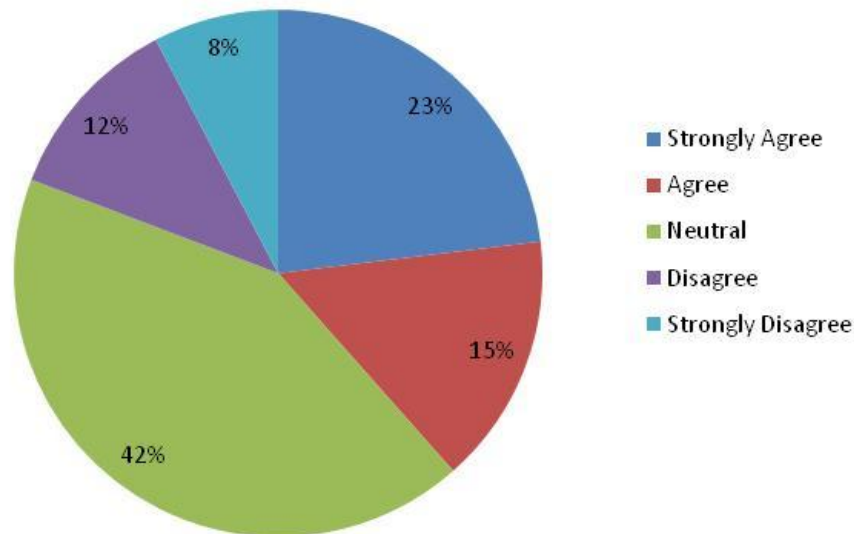
**Avg: 3.8**

**Only 15% do not require CC on the Procurement clipboard**

# survey results: common criteria

One interpretation of this question is that this decision is on a case by case basis

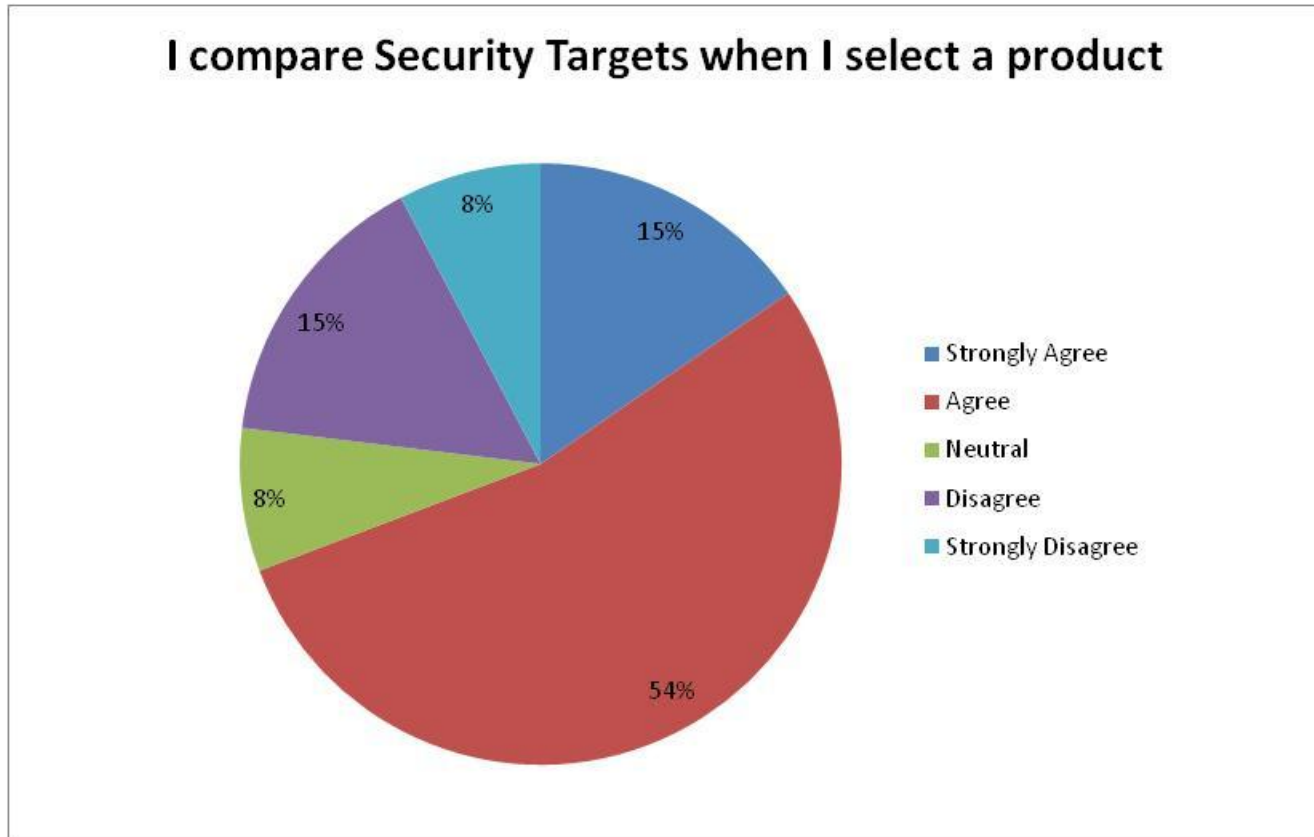
If a security product is not CC evaluated, I will need to replace it with a CC evaluated product



**Avg: 3.4**

**This decision varies based on agency , country and other factors**

# survey results: procurement decisions



5 4 3 2 1  
Strongly Agree Agree Neutral Disagree Strongly Disagree

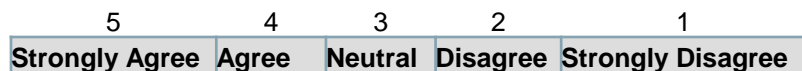
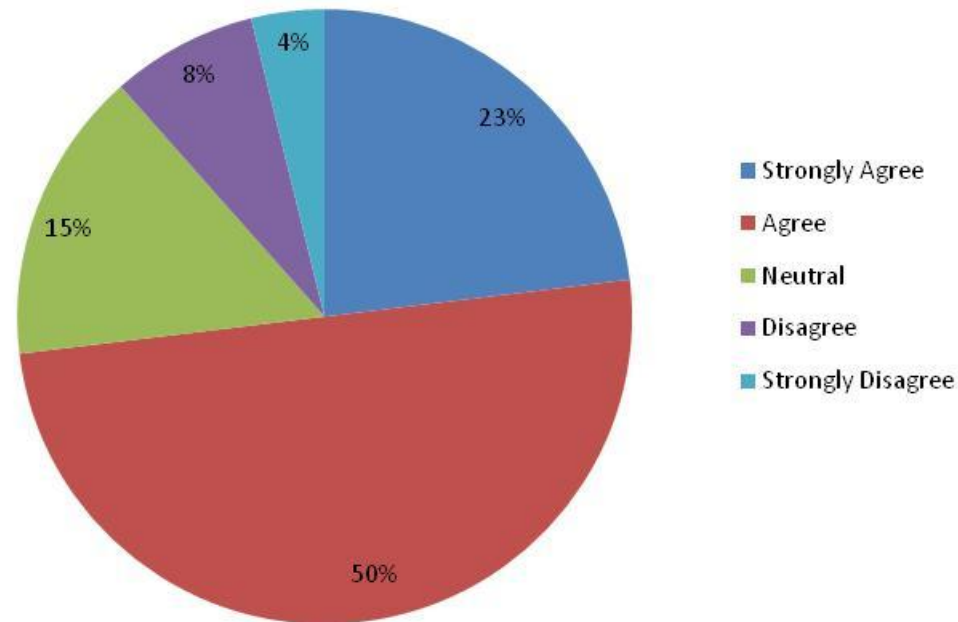
**Avg: 3.5**

**69% of procurement officers read Security Targets**

# survey results: procurement decisions

PP's are the only way gov't agencies can compare apples to apples – clearly respondents recognize the value

Having a CC evaluated ESM product that is compliant to a PP is very important to me

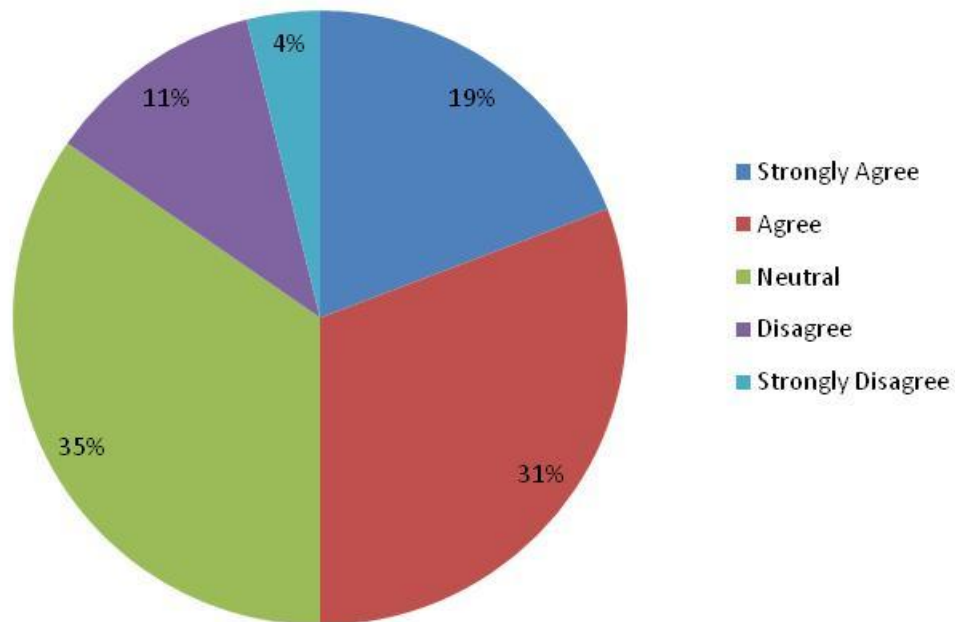


**Avg: 3.8**

**73% of respondents think PP's are important**

# survey results: procurement decisions

I plan on replacing existing security tools with one or more ESM products



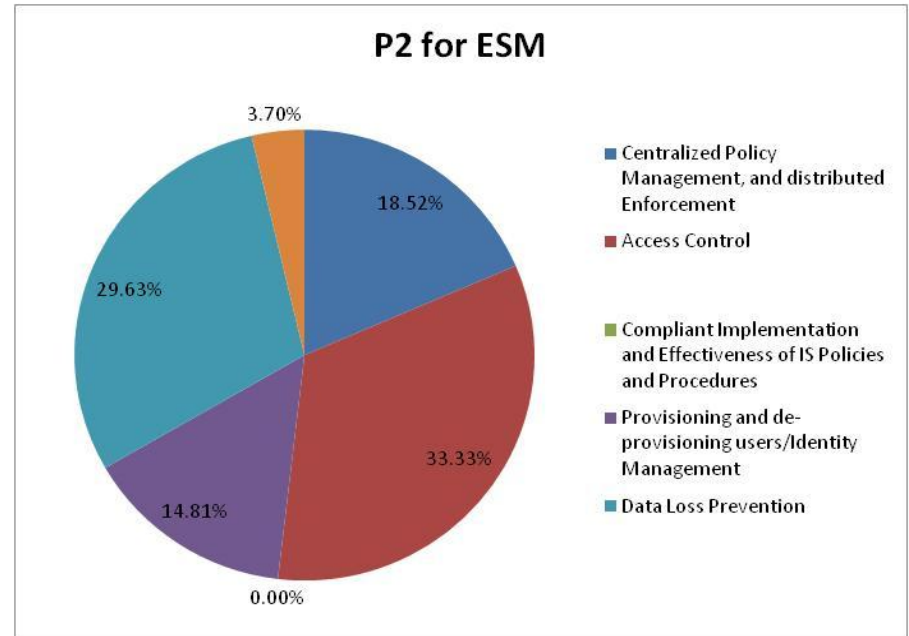
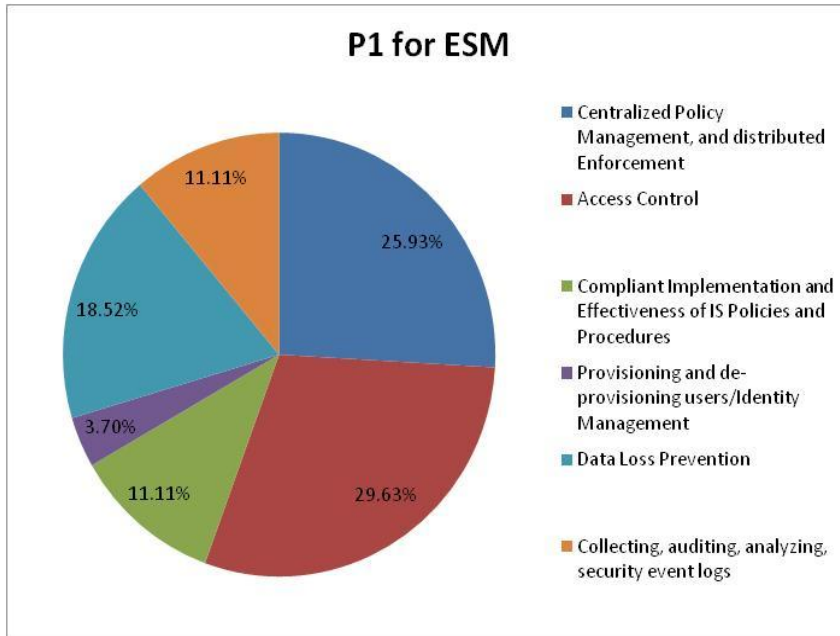
5 4 3 2 1  
Strongly Agree Agree Neutral Disagree Strongly Disagree

**Avg: 3.5**

**50% are planning on purchasing new ESM products**

# survey results- 1<sup>st</sup> ESM PP choice

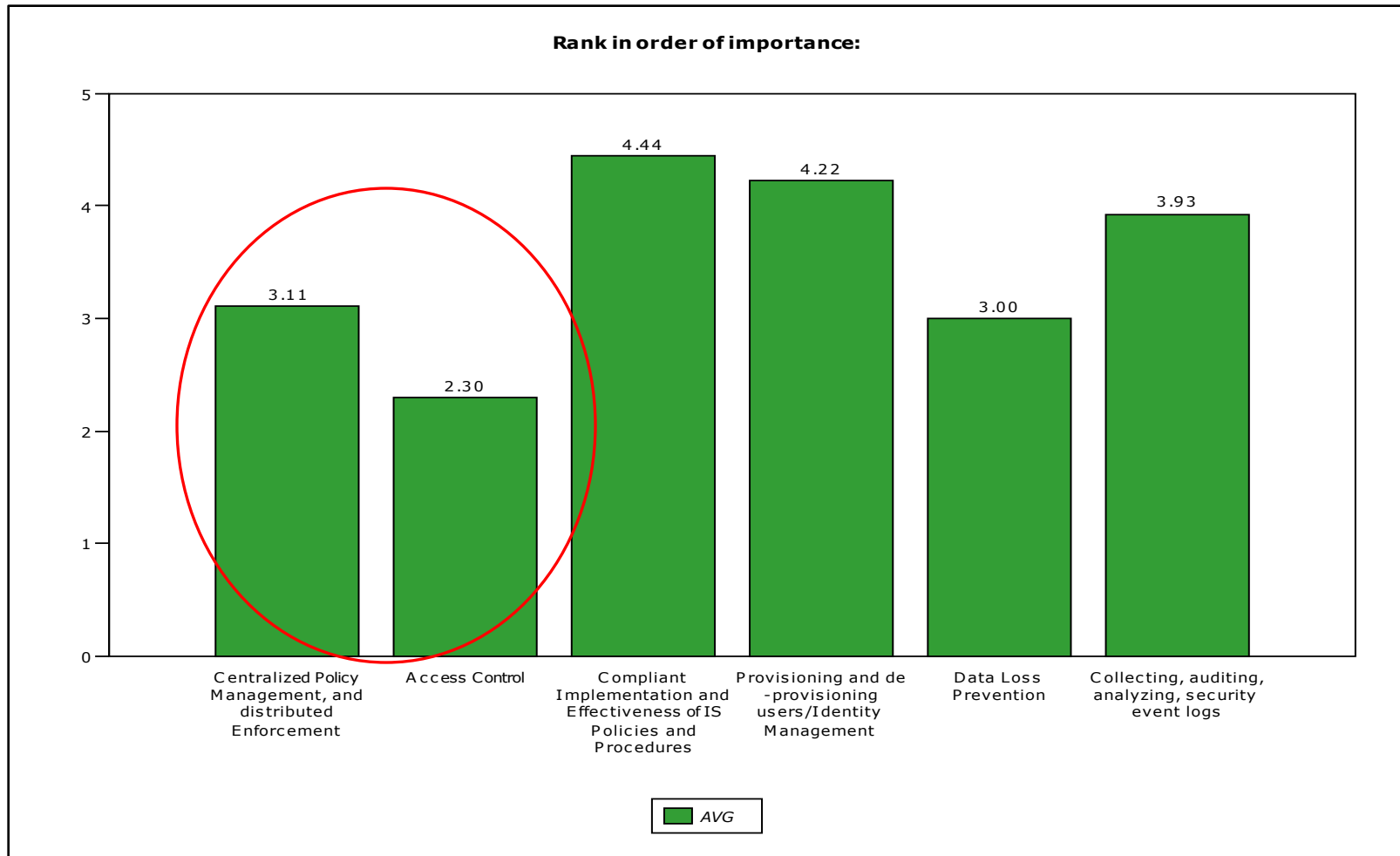
access control is CLEAR #1 priority



**63% of respondents said that AC was in top 2 priorities**

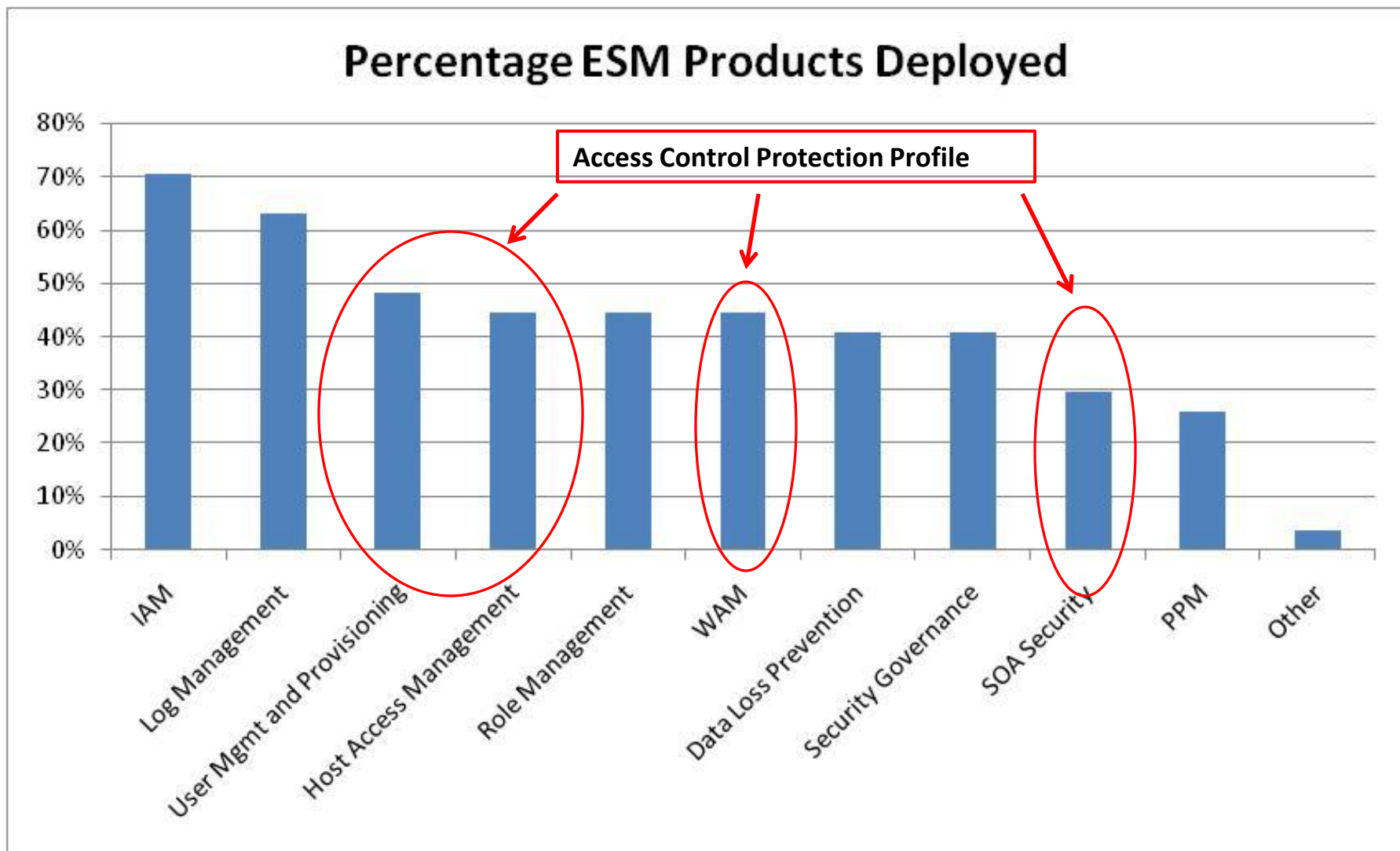
# survey results

## access control is CLEAR #1 priority



**86% of respondents said that either AC or Policy were highest priority**

# survey results– deployed products



# 1st protection profile--decision

✓ Customers suggest AC as the 1<sup>st</sup> one

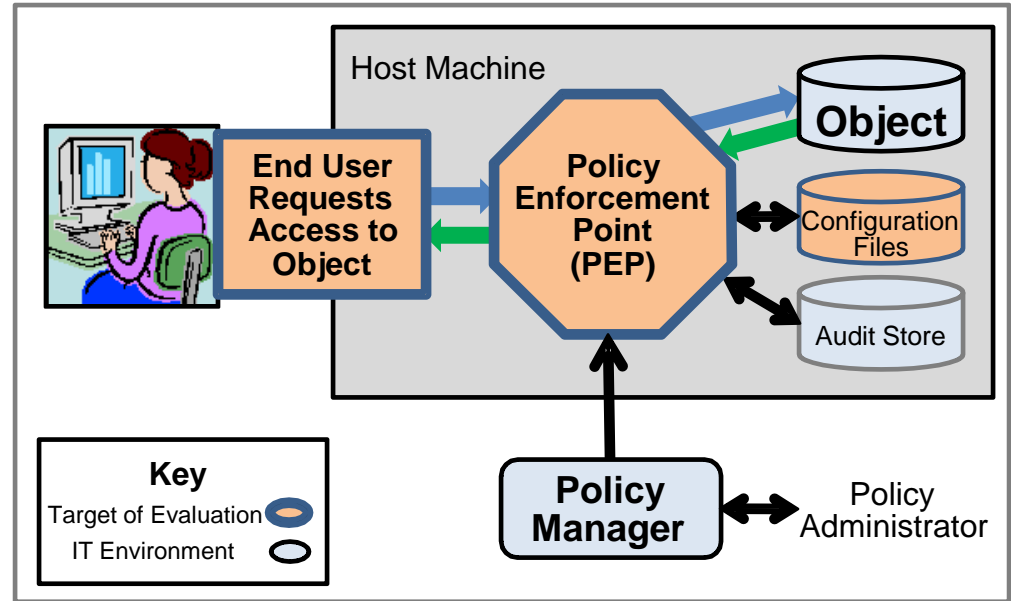
✓ Access Control PP is focused on implementing the policy from a Policy Manager (another PP later).

✓ Key threats to Access Control enforcement is communication to/from the Policy Manager and Configuration files






✓ Functional requirements include:

- ✓ Audit Generation (FAU)
- ✓ Access Control Policy (FDP)
- ✓ Data Authentication (new)
- ✓ Non-Repudiation (new)

- ✓ Authorization Validation (new)
- ✓ Data Validation (new)
- ✓ Fault Tolerance (new)
- ✓ Self Testing (new)



# products that could be evaluated against new PP (sample)

 <p>Identity Management</p>	 <p>Compliance and configuration</p>	 <p>Policy/Access</p>	 <p>Monitoring and response</p>	 <p>Standardized logging</p>
CA Identity Manager	CA GRC Manager	CA Siteminder	CA Auditor for z/OS	CA Enterprise Log Manager
	SC Operations Manager, SC Configuration Manager & SC VMM	SC Operations Manager, SC Configuration Manager, SC Essentials	SC Operations Manager & SC Essentials	SC Operations Manager*
Symantec Alteris	Symantec CCS/FTK	Symantec Alteris	Symantec SSIM	Symantec Alteris
	EMC RSA Access Manager	EMC RSA Envision		EMC RSA Envision
Oracle Identity Manager	Oracle Enterprise Manager	Oracle Access Manager	Oracle Audit Vault	Oracle Audit Vault
IBM Tivoli Identity Manager	IBM Tivoli Compliance Insight Manager (TCIM), Security Information Event Manager (TSIEM)	IBM Tivoli Unified Single Sign-On, Tivoli Security Policy Manager		IBM Common Audit and Reporting (CARS) & TCIM

# the team, so far (growing!)

We are always looking for more participants!



NATIONAL SECURITY AGENCY



CENTRAL SECURITY SERVICE



# Questions?

**Joshua Brickman, PMP**

CA Technologies

Director of Federal Certification Program Office

(508) 628-8917

[Joshua.Brickman@ca.com](mailto:Joshua.Brickman@ca.com)

# Legal Notice

- THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised of the possibility of such damages.
- CA does not provide legal advice. Neither this presentation nor any CA software product shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein.

# Backup

# data collection plan

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
My agency currently uses Enterprise Security Management (ESM) Tools to achieve its operational mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The ESM Products my agency uses meet our Security requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ESM products that integrate well together are very important.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

A Common Criteria evaluated product is a more trustworthy product	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Common Criteria evaluated products are a Procurement requirement at my agency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If a security product is not CC evaluated, (even if it's working well and meeting my needs) I will need to replace it with an Common Criteria evaluated product	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I compare Security Targets when I select a product	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Having a CC evaluated ESM product that is compliant to a Protection Profile is very important to me	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I plan on replacing existing security tools with one or more ESM products	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

# data collection plan, continued

## Criticality of ESM Security Features:

Please rank in order of importance where "1" is the "most important" and "6" is the "least important".

- Centralized Policy Management, and distributed Enforcement
- Access Control
- Compliant Implementation and Effectiveness of IS Policies and Procedures
- Provisioning and de-provisioning users/Identity Management
- Data Loss Prevention
- Collecting, auditing, analyzing, security event logs

# data collection plan, continued

---

Please select the products that you have deployed **(check all that apply)**:

- Service Oriented Architecture (SOA) Security
- Identity Access Management
- Host Access Management
- Data Loss/Leak Prevention
- Log Management
- Security Governance
- Privileged Password Management
- User Management and Provisioning
- Role Management
- Web Access Management
- Other

---

In what country are you currently located?

Please select your answer

---

Number of ESM end users in your organization:

- 1 to 1,000
- 1,001 to 5,000
- 5,000+

---

Demographic Questions - by submitting this you are consenting to receive the survey results.

First Name

Last Name

Organization Represented

E-Mail