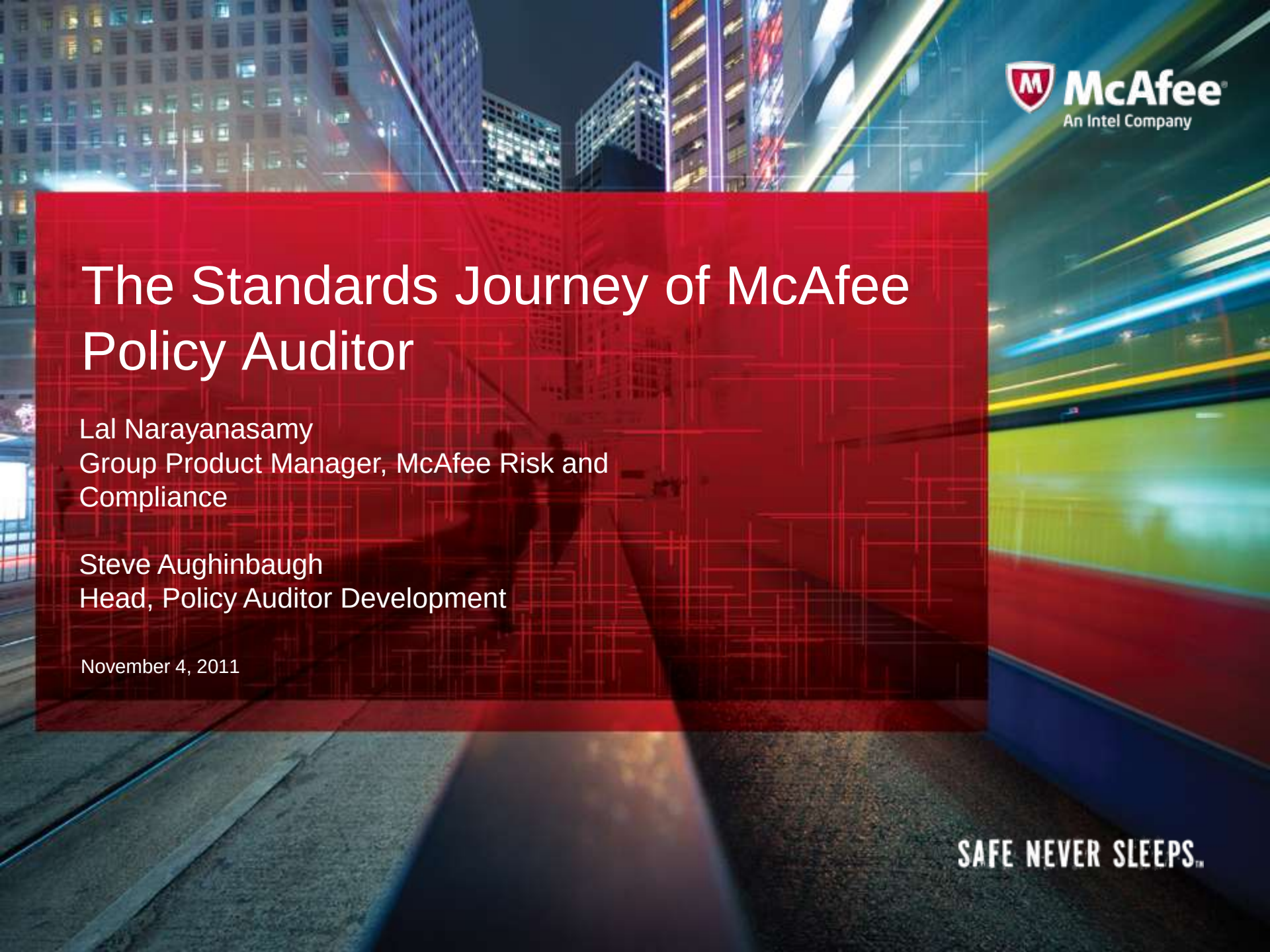


The Standards Journey of McAfee Policy Auditor

Lal Narayanasamy
Group Product Manager, McAfee Risk and Compliance

Steve Aughinbaugh
Head, Policy Auditor Development

November 4, 2011

Agenda

- **McAfee Policy Auditor – Overview**
- McAfee Policy Auditor and Standards
  - McAfee and SCAP
  - Evolution of McAfee Policy Auditor
  - Centrality of SCAP to product vision
- Realizing the vision - innovating further with SCAP in McAfee Policy Auditor
  - Localized content
  - Findings
  - Policy Auditor Custom Content Creator (PACC)
- McAfee Policy Auditor and SCAP in action – some examples
- The Future with standards
- Questions

McAfee Policy Auditor Overview

Agent based solution

- Deploy-Manage-Report via ePO
- Central policy management
- Scheduled audits

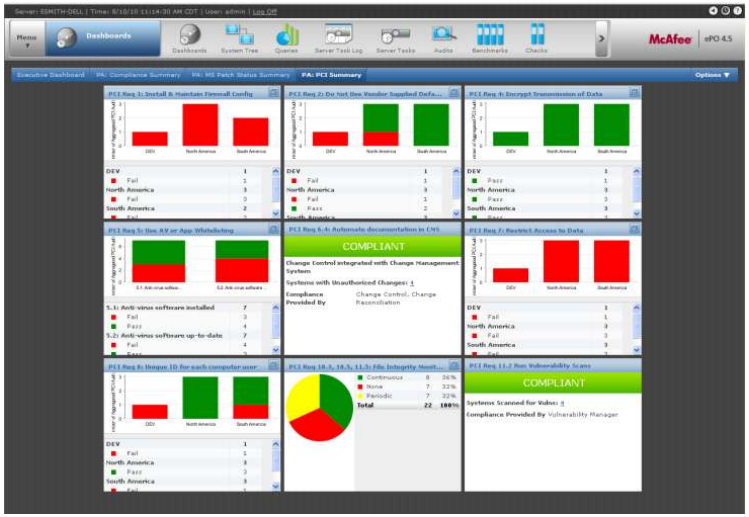
Standards based

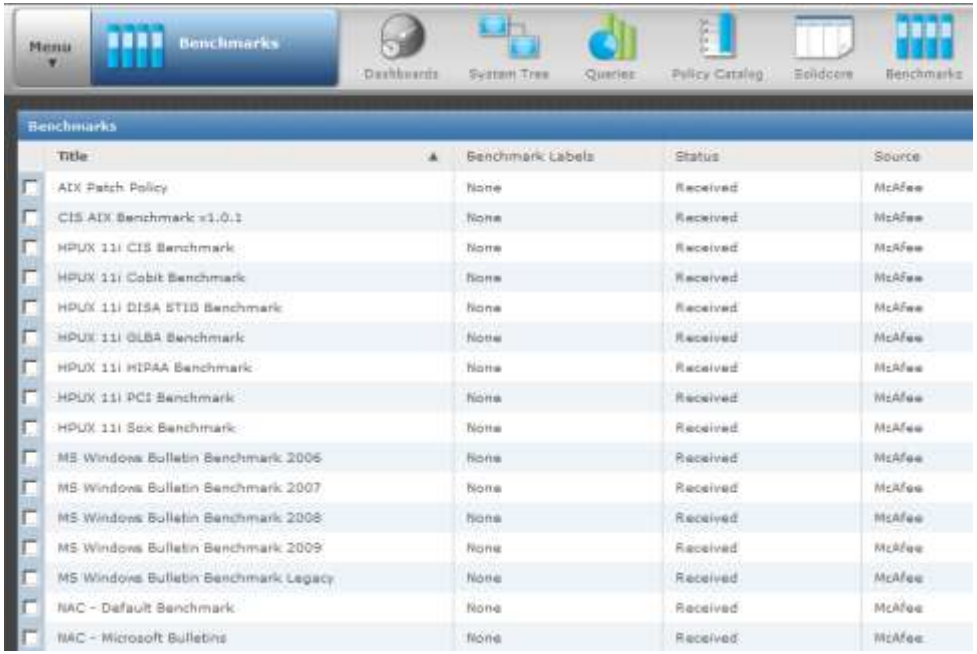
- SCAP
  - XCCDF, OVAL, CVSS, CVE

Published Industry templates

Configurable Baseline audits

Manage exceptions, waivers





McAfee Policy Auditor audit process flow

- Utilize ePO system tree and device discovery
- Policy Creation
- Scalable agent Assessments
- Single Management and Reporting Structure

Measure Compliance Mandates Out-of-the-box

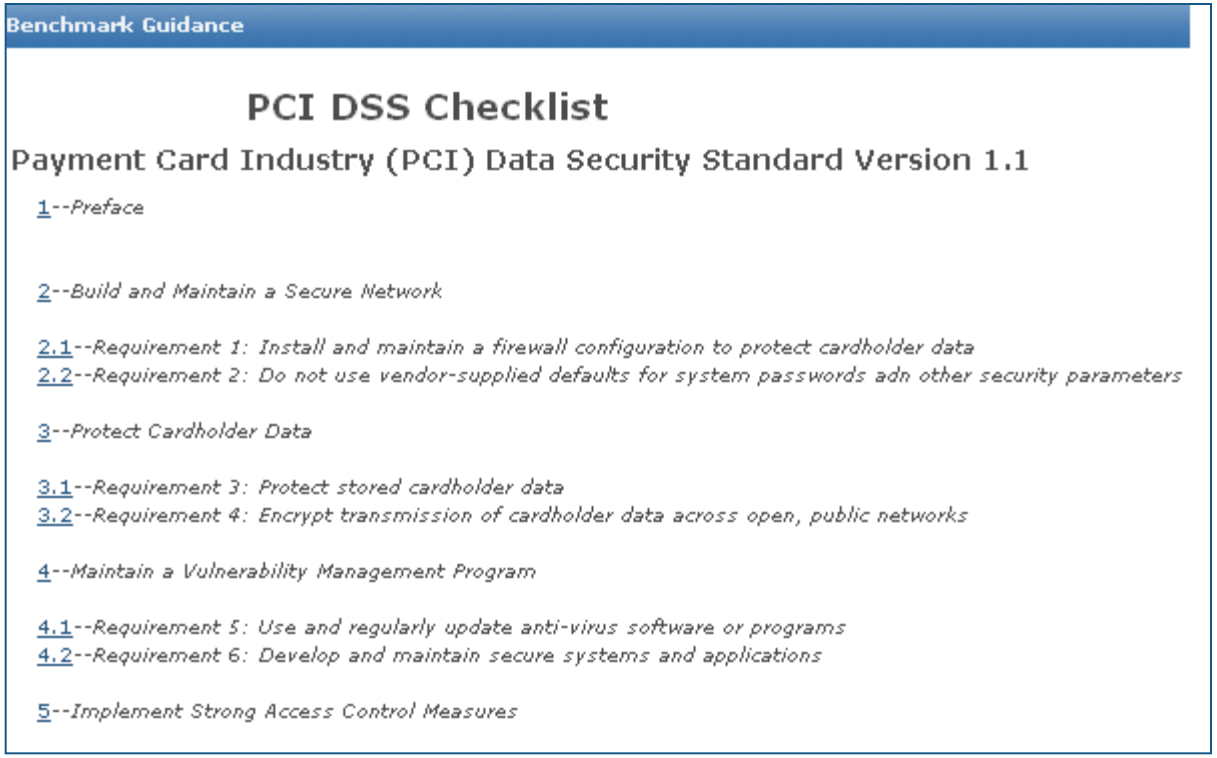
McAfee
An Intel Company

"Best Practice" Benchmarks

- Your CUSTOM
- FISMA
- FDCC*
- ISO 27001
- COBIT
- PCI DSS
- GLBA
- SOX
- HIPAA
- NERC

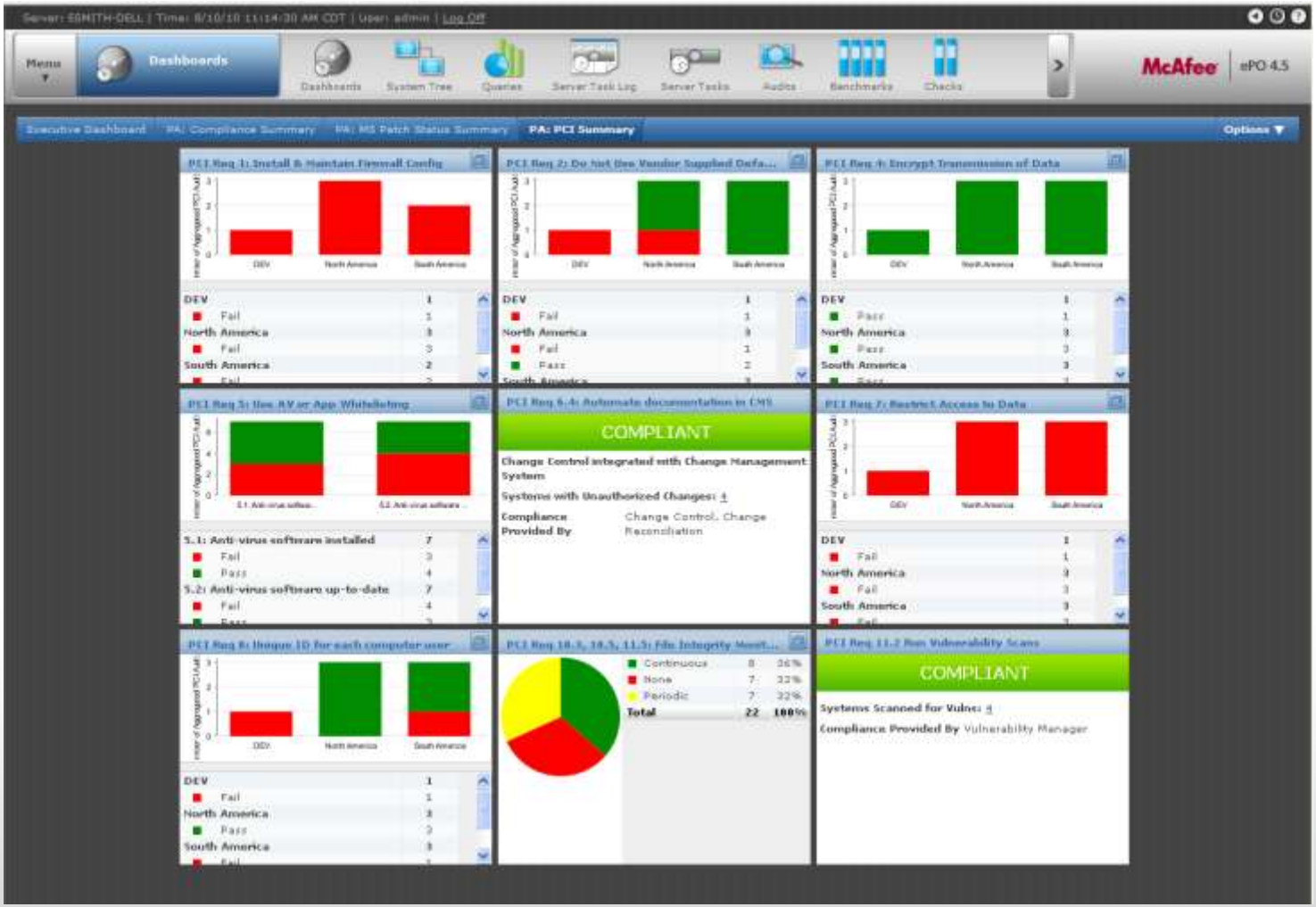
* One of the additional templates that can be easily imported from the NIST website

- Detailed compliance assessment of IT Controls
  - Password settings, account privileges, audit settings, file permissions, patch status
- Use of XCCDF and OVAL standards a key differentiator:
  - Enables organizations to easily import benchmarks created by authoritative security sources



Policy Auditor Patch Status Dashboard

Policy Auditor PCI Dashboard



Agenda

- McAfee Policy Auditor – Overview
- **McAfee Policy Auditor and Standards**
  - **McAfee and SCAP**
  - **Evolution of McAfee Policy Auditor**
  - **Centrality of SCAP to product vision**
- Realizing the vision - innovating further with SCAP in McAfee Policy Auditor
  - Localized content
  - Findings
  - Policy Auditor Custom Content Creator (PACC)
- McAfee Policy Auditor and SCAP in action – some examples
- The Future with standards
- Questions

History of SCAP at McAfee

- Had been using CVE and CVSS internally within our internal tools and databases
- Faced with multiple product development concerns
  - Needed to reduce costs of product development
    - Develop more products with a common code base
  - Needed to reduce the costs of content creation and maintenance
    - Too many small content teams focused on proprietary content formats
- SCAP usage in our products was a sound business decision
  - Provided a means to standardize content development
  - Provided a standardized reporting format
  - Allowed for us to build a common processing engine
- Later the OMB mandate reaffirmed we had made a good decision
- Now used extensively in all our threat feeds and internal infrastructure

McAfee Participation in SCAP Development

- **OVAL (Open Vulnerability & Assessment Language)**
  - McAfee OVAL Board Member

- **CVE (Common Vulnerabilities & Exposures) Standard**
  - One of the founding CVE Editorial Board Members

- **CCE (Common Configuration Enumeration)**
  - Member of CCE Working Group

- **CPE (Common Platform Enumeration)**
  - CPE Core Team member
  - Defined the initial need

- **NIST**
  - Initial Submitter to the NIST Security Configuration Checklists Repository
  - Presenter at the 2nd – 6th Annual IT Security Automation Conferences
  - Participated in SCAP Validation / Certification specification work
  - Working with NSA and NIST to define security automation architecture

- **XCCDF (Extensible Checklist Configuration Description Format)**
  - Past and current participant in NIST/NSA's XCCDF workshops and effort
  - Active XCCDF Working Group member

- **IETF (Extensible Checklist Configuration Description Format)**
  - Co-Chair of the SCAP Working Group discussions at IETF 79

McAfee SCAP Specification Uses

- **Product Uses:**
  - Policy and Compliance Validation
    - McAfee Policy Auditor
    - McAfee Vulnerability Manager
    - McAfee Network Access Control (MNAC)
  - Vulnerability Detection
    - McAfee Vulnerability Manager
  - Network Connection Health checks
    - McAfee Network Access Control (MNAC)
  - Risk Monitoring and Response
    - McAfee Risk Advisor
- **Security Information Services:**
  - Threat Publishing and Alerts
    - McAfee Threat Information Service
    - McAfee Risk Advisor
- **Internal Threat Research**

McAfee Policy Auditor (PA) Evolution and SCAP – Past, Present and Future

McAfee
An Intel Company

Hercules/PA 4.5 (2006)

- Citadel acquired by McAfee
- Hercules (later renamed PA and Remediation Manager) CVE compliant

PA 5.0 (2008)

- Full ePO integration
- Waivers and exceptions management
- Benchmark and check editors

PA 5.0.1 (2009)

- SCAP certification attained
- Agent-agentless integration

PA 5.1(2009)

- Full localization – German, French, Spanish, Japanese, Chinese

PA 5.2(2009)

- "Findings"
- Periodic FIM
- SCAP content for Italian, Polish

PA 5.3 (2010)

- "Actionable findings" API
- OVAL 5.6 support
- PCI dashboard
- SCAP content for Swedish, Brazilian Portuguese

PA 6.0 (2011) - Current

- PACC tool to simplify custom content creation
- Cyberscope data extractor
- OVAL 5.7 – 5.9 support

PA 6.x (2012)

- SCAP 1.2 support

Agenda

- McAfee Policy Auditor – Overview
- McAfee Policy Auditor and Standards
  - McAfee and SCAP
  - Evolution of McAfee Policy Auditor
  - Centrality of SCAP to product vision
- Realizing the vision - innovating further with SCAP in McAfee Policy Auditor
  - Localized content
  - Findings
  - Policy Auditor Custom Content Creator (PACC)
- McAfee Policy Auditor and SCAP in action – examples
- The Future with standards
- Questions

Policy Auditor Vision

To be the technology of choice for compliance and IT security organizations in the private and public sector globally for actionable compliance validation and configuration assessment , distinguished by its:

- *ability to deliver rapid ROI*
- *adherence to industry standards (SCAP)*
- *depth of packaged content*
- *versatility in creation of custom content*
- *flexible modes of audit*
- *rich reporting and dash-boarding capabilities*
- *integration to McAfee SIEM and risk analytics*

Realizing the vision – 3 key innovations in-line with standards

Objective	Initiative
Expand reach to serve a global customer base in the private and public sectors	Localized/Internationalized product and content
Improving audit effectiveness and ROI – making audit results actionable	Findings
Versatility in security content – best-in-class packaged content; create custom content as needed	Policy Auditor Content Creator

Content Localization – the drivers and challenges

- Localization and internationalization driven by the need to serve a global customer base both in the private and public sectors
- GEO specific policies that need to have benchmarks created for them
  - ACSI 33, J-SOX, EU 8th Company Law Directive on Statutory Audit, etc.
- Localization of content – varying degree of support in standards
  - XCCDF and CPE support it
  - OVAL had limitations
  - CVE has limited translations
  - Others don't
- Need to deal with more than translations
  - Translations are a presentation issue
  - Able to assess a locale specific system accurately even if the presentation is in English
- Different types of content took different approaches to localizing
  - OS Patch Checks
  - Compliance and Configuration Checks
  - Application checks

Localized SCAP Content Coverage

- Existing McAfee developed SCAP Content
  - Benchmarks, Primitives, Patch Checks, Config Checks, Application Checks
- Created locale specific OVAL compliance checks
- Created locale/OS/version specific patches
- Targeted application checks for desktop security products
- Designed and implemented a process to provide localized content **using the existing SCAP specifications**
  - Creation of content
  - Testing of content
  - Publication of content

Language	Localized
English – US & International (EN)	Y
Chinese – Simplified (ZH-CN)	Y
Chinese - Traditional (ZH-TW)	Y
French (FR)	Y
German (DE)	Y
Italian (IT)	Y
Japanese (JP)	Y
Polish (PL)	Y
Spanish (ES)	Y
Swedish (SV)	Y
Portuguese – Brazilian (PT-BR)	Y

Findings - Drivers

- Provide data to satisfy Auditors
  - Auditors often require more detailed information about a pass or a fail
  - A configuration item passes, but what value does it have?
- Provide data needed to remediate systems
  - Why does the antivirus check fail?
    - because there is no AV?
    - Is the AV present but not a valid version?
    - Are the signature files up to date?
  - Why does the file permissions check fail?
    - Do unexpected accounts have access?
    - Does the file exist?
    - Does each expected account have proper permissions
- Simply provide clarifying data about the state of systems

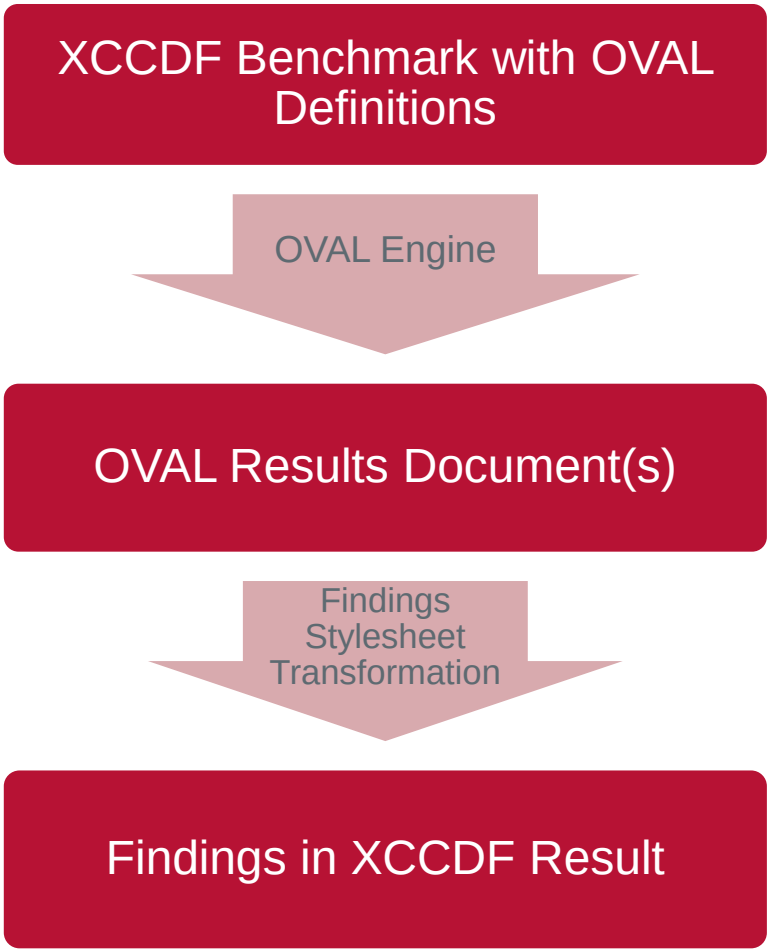
Findings – Key objectives

- For SCAP implementers
  - Findings must “fit in” with the rest of the SCAP infrastructure
  - Implementable with commonly available tools
- For Content Creators
  - Should have a low learning curve
- For SCAP Users
  - Should not require large resources at run time
  - Should reduce the volume of results to only significant data (high signal to noise ratio)
- For IT and Security personnel
  - Results should be clear, simple, and complete
  - Results should be localizable

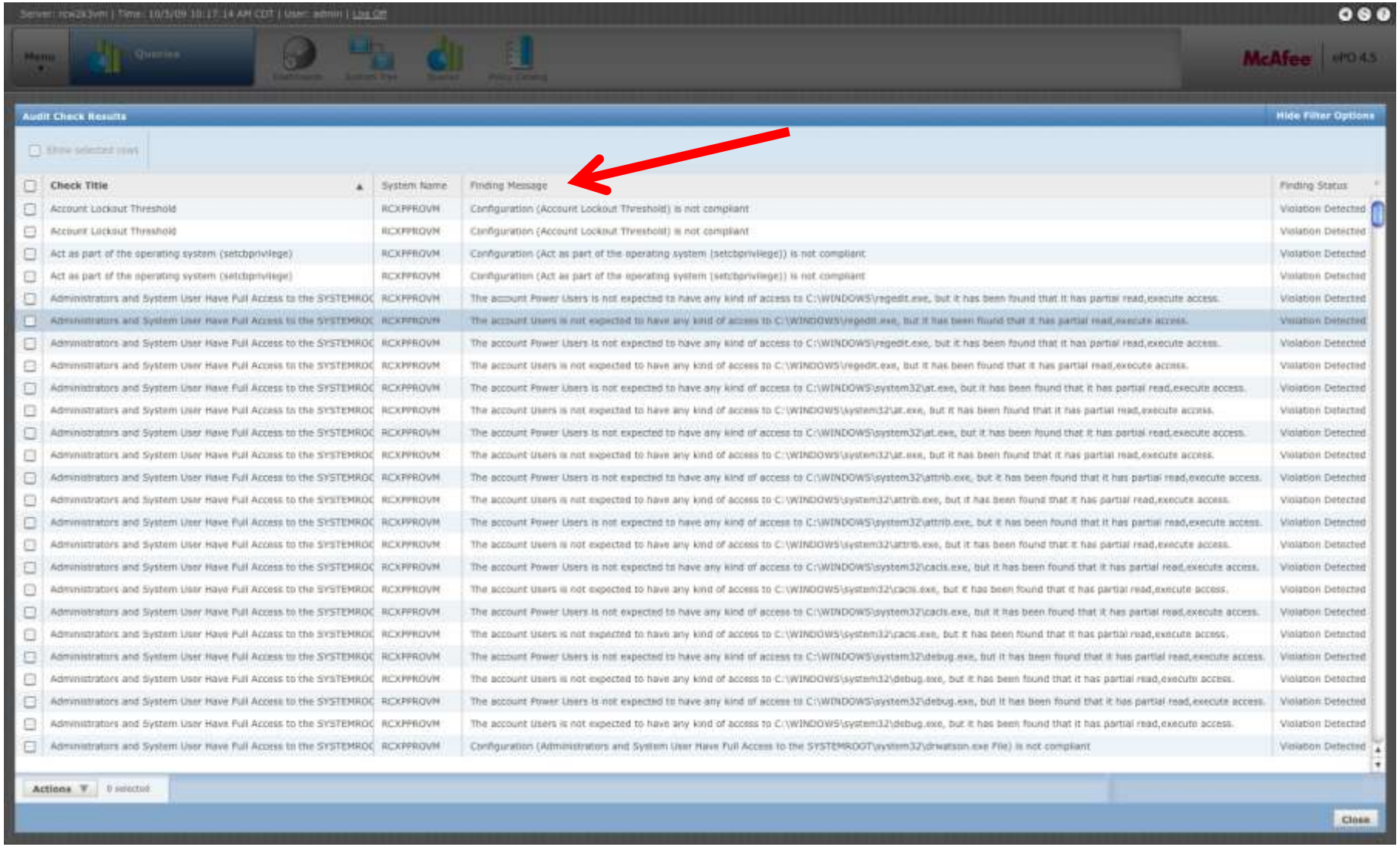
High Level Approach

- Process the OVAL results documents via XSL stylesheets to extract only relevant results information
- Each OVAL definition needing detailed results will have its own stylesheet
- XCCDF Results schema extended to provide a location for a Findings xml schema-compliant

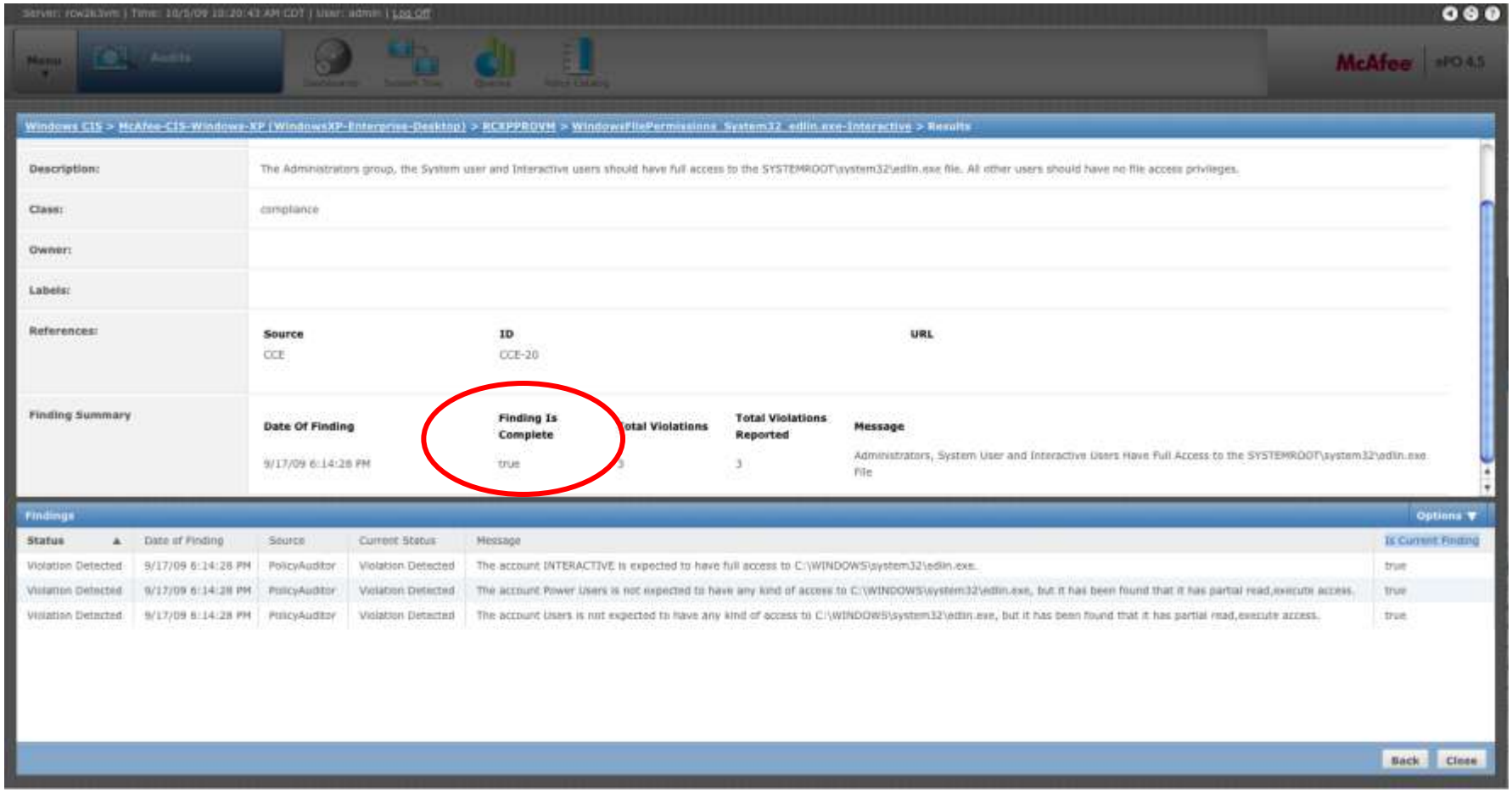
High Level Approach



Example Query Result w/Findings



Example Audit Result w/Findings



Status of Findings Today

- A distinguishing feature of McAfee Policy Auditor
- Being actively used by iPost today
- Extends the integration of OVAL and XCCDF to provide users with a missing capability
- Makes SCAP content more useful to customers without forcing them to interpret XML results to get what they operationally need
- Being contributed to extend the SCAP set of standards
- Open specification is being provided to not just customers but to the community for others to integrate and benefit from

Policy Auditor Content Creator - Drivers

- Provide customers an easier way of creating custom security content when needed
- Customers to primarily use McAfee provided packaged content, but create new content or tailor existing benchmarks when needed
- Use and benefit from a standards-based tool like Policy Auditor without having to be an XCCDF or OVAL expert
- Create custom content with findings

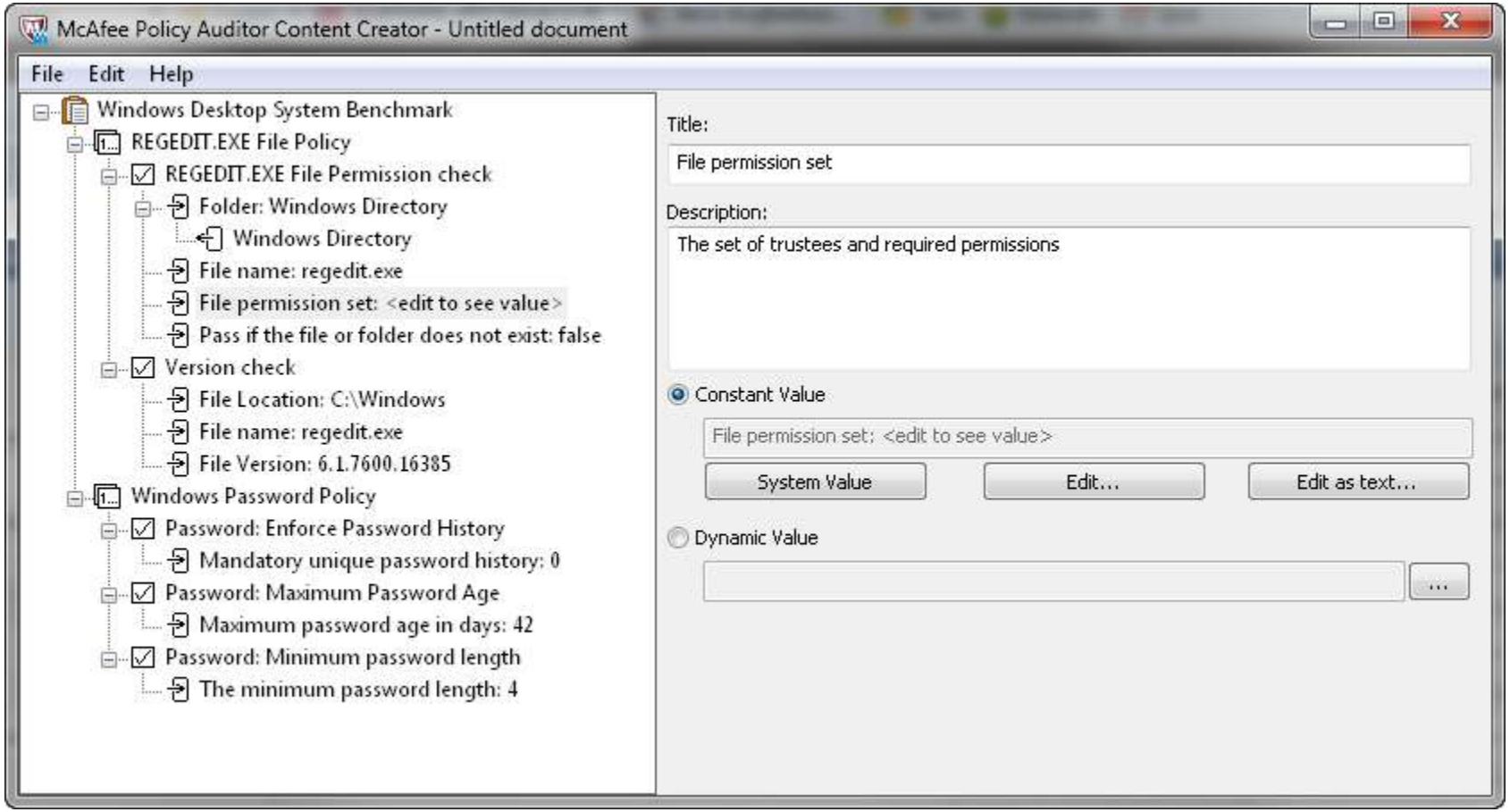
Policy Auditor Content Creator Overview

- Introduced in the current version, Policy Auditor 6.0
- Used to create custom benchmarks and checks
- Windows GUI Application
- Install on any Windows system supported by the PA Windows agent
- New benchmarks can be created from McAfee templates then auto populate the test values
- Can be used to build any benchmarks or checks for any OS but non-Windows checks will not have use of system browsers
- System browsers
  - Files system
  - Registry
  - Trustees/Users
  - And more …
- Export to XCCDF or OVAL (then import into PA for deployment)

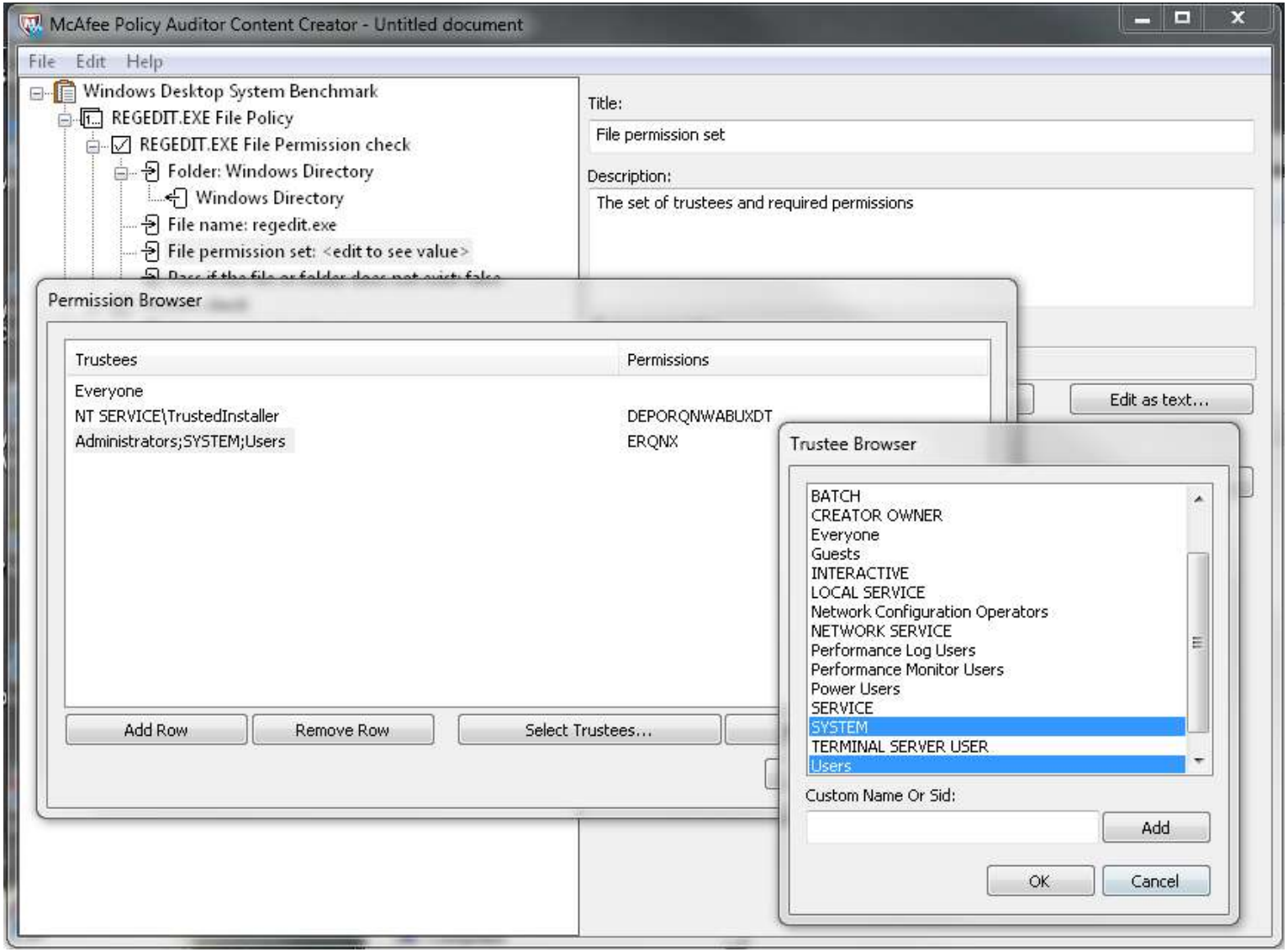
PA Content Creator Overview (continued)

- The PACC tool is not a general purpose XCCDF/OVAL editor. It is a purpose built tool used to create content for Policy Auditor using a specific set of security relate rules.
- The complete XCCDF/OVAL language is very complicated and difficult to learn and use. The PACC tool can be used without any knowledge of XCCDF or OVAL.
- The PACC tool uses XCCDF and OVAL (as well as PA Findings) as the export format to move the benchmarks and rules into Policy Auditor. Benchmarks can and should be saved in the PACC tools local BME formatted files.
- We plan to release updates to the PACC tool frequently, perhaps every 2 to 3 months as needs dictate

Policy Auditor Content Creator UI



Policy Auditor Content Creator Browser



Agenda

- McAfee Policy Auditor – Overview
- McAfee Policy Auditor and Standards
  - McAfee and SCAP
  - Evolution of McAfee Policy Auditor
  - Centrality of SCAP to product vision
- Realizing the vision - innovating further with SCAP in McAfee Policy Auditor
  - Localized content
  - Findings
  - Policy Auditor Custom Content Creator (PACC)
- **McAfee Policy Auditor and SCAP in action – some examples**
- The Future with standards
- Questions

McAfee Policy Auditor and SCAP in action…

- A leading global financial services company conducts periodic patch audits following every Patch Tuesday using McAfee-supplied SCAP content on 100K Windows servers
  - Policy Auditor and SCAP content provide a scalable and effective compliance validation option that can be managed through a single agent and single management console
- A Europe-based automaker performs ISO 27001 and 27002 assessments using McAfee-supplied SCAP content on 22K Windows and SuSE servers; automaker also performs audits to internal standards and will be using the PACC tool to generate the require custom content
  - Policy Auditor and the SCAP security content therein automated a previously inefficient process characterized by manual processes and disparate solutions
  - Localized security content and findings extend solution's reach for audit and remediation

McAfee Policy Auditor and SCAP in action…(continued)

- Several Federal departments and agencies (civilian and defense) perform FDCC and USGCB assessments using Policy Auditor
  - Built-in Cyberscope data extractor helps agencies submit system state data to DHS Cyberscope portal in a timely fashion

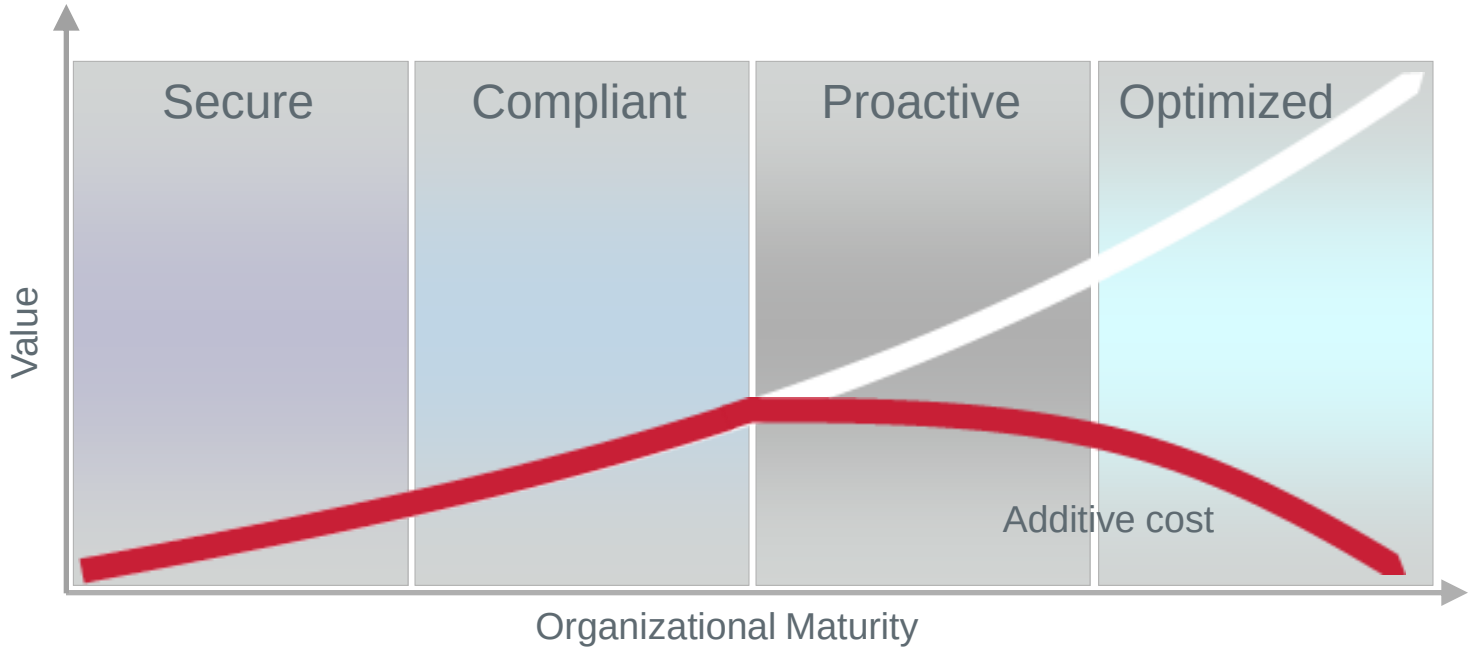
- A major Federal department uses Policy Auditor to perform assessments daily on critical assets the results from which are fed into the iPost reporting tool and risk dashboard to perform daily risk assessments

Agenda

- McAfee Policy Auditor – Overview
- McAfee Policy Auditor and Standards
  - McAfee and SCAP
  - Evolution of McAfee Policy Auditor
  - Centrality of SCAP to product vision
- Realizing the vision - innovating further with SCAP in McAfee Policy Auditor
  - Localized content
  - Findings
  - Policy Auditor Custom Content Creator (PACC)
- McAfee Policy Auditor and SCAP in action – examples
- **The Future with standards**
- Questions

Automation and Standards in Compliance Validation – Driving to an Optimized State

The relationship to cost and security and compliance diverge during progression to the managed and optimized states.



- Maturity of process reduces audits from months to days and enables sustainable compliance
- Cost savings occur through reduction of point products and increased automation

McAfee Policy Auditor and Standards – The Future

- Help grow standards-adoption worldwide for security and compliance
  - Replicate success in US public sector world-wide
  - Spur standards adoption in the private sector
- Adopt additional standards to bring additional value to customers and lower compliance pains
  - OCIL for manual controls, self-assessments
  - CRE for remediation
  - Emerging standards like CybOX for integration to SIEM and risk assessment tools
- Share and grow standards with the community
  - findings
  - localization

Other areas in security automation and SCAP we are tracking…

- Enhanced roll up reporting
- Asset tracking and integration
- Content distribution
- Content and results signing
- Additional network device integration
- Event monitoring
- Remediation
- Security knowledge products

Questions?


McAfee®
An Intel Company