nCircle

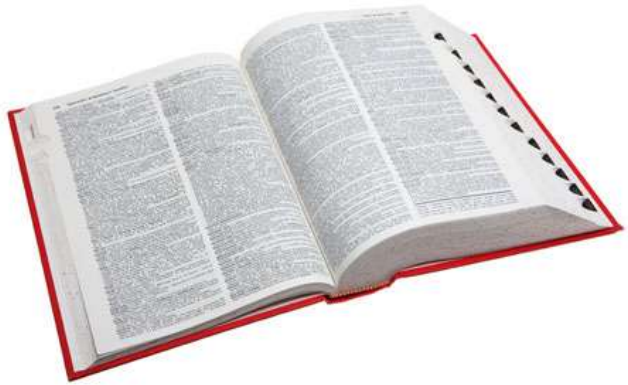
Continuous Monitoring 2.0:
Cloud-based benchmarking in industry and the federal government

Presented by:
Keren Cummins – Director, Federal Programs
Jim Acquaviva – VP, Product Strategy

Defining Terms

- **Continuous Monitoring** - the context of information security, is defined in 800-137 as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

- **Benchmarking** - the process of comparing one's business processes and performance metrics to industry bests and/or best practices from other industries. Dimensions typically measured are quality, time and cost.

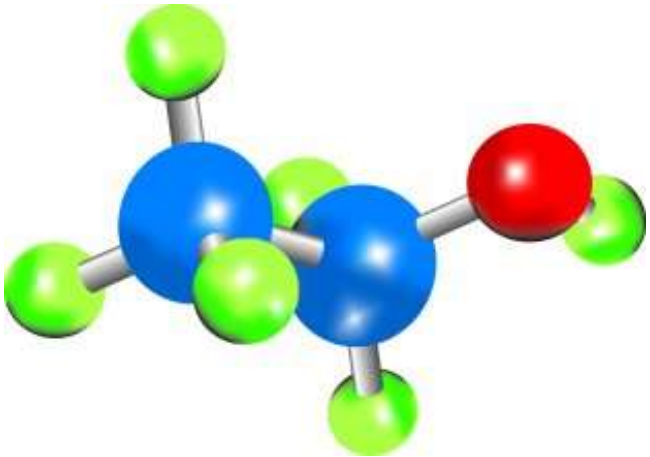


Game Changers

- State Department
  - 89% risk reduction in the first 12 months across the entire world
- USAID
  - FISMA C- to consistent A+'s for five years
- Center for Medicare/Medicaid Services
  - 80% risk reduction at 88 data centers and as high as 95% at one major center

Common Elements

- Breadth of engagement
- Simplicity of result
- Context
- Short cycle time



Why hasn't everyone done this?

- Or, why is this hard?
  - Metrics are hard
  - My organizational structure is different
  - My monitoring solution won't do that

The Challenge

- How can we replicate benchmarking success effectively?
  - With the organizations and tools that we already have in place?
  - For all our security programs (not just vulnerability management and configuration auditing)?

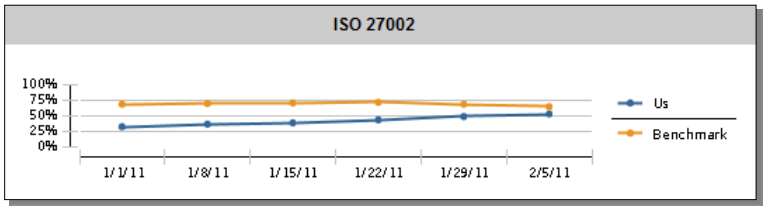
The CSO needs what the CFO has….

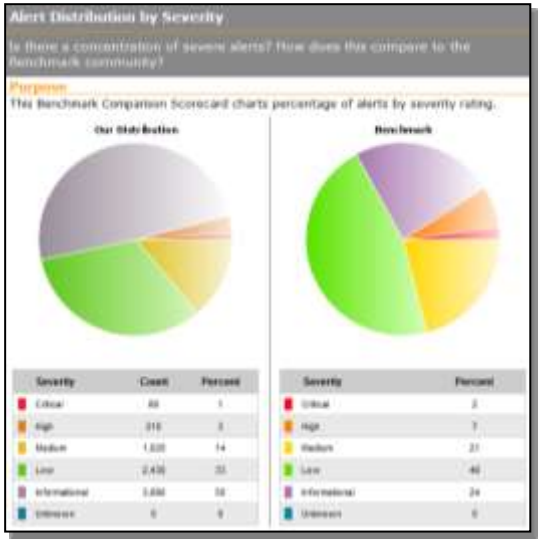
- CSO needs a metrics language to describe a company's security performance just like the CFO describes financial performance

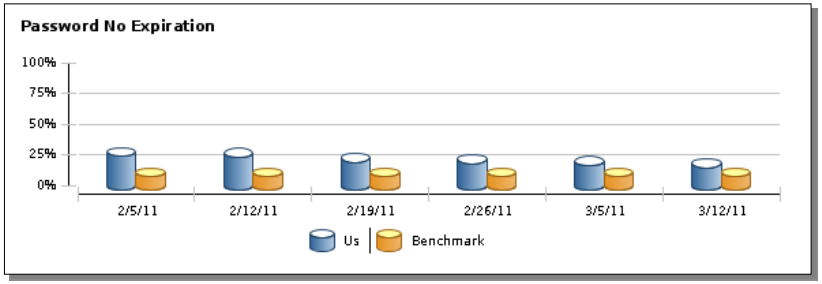
- CSO's can now field a formal security performance management program built on objective, fact based metrics that
  - Shows how security organization is protecting the company
  - Benchmarks performance vs. internal goals, and vs. industry peers
  - Trends performance over time

With a Security Performance Management Program, we can demonstrate that

- We are taking a comprehensive approach to security that is…
  - In line with our risk tolerance
  - At least equal to or better than our own industry's investment & performance
- We are producing hard data on an ongoing basis that we can rely on to make decisions
  - Investment
  - Execution
  - Resource allocation

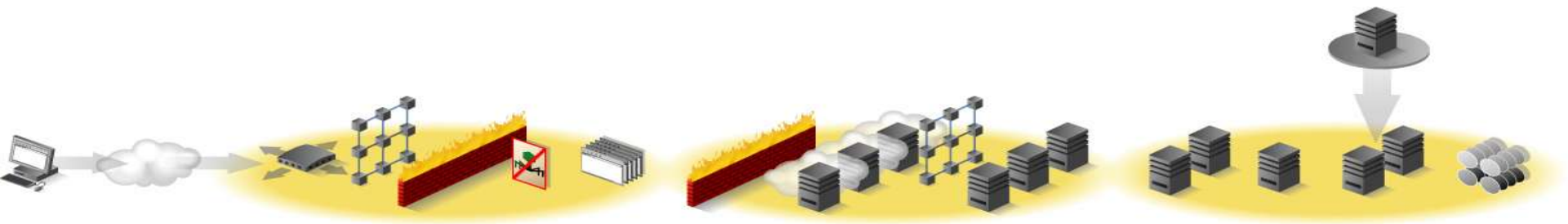




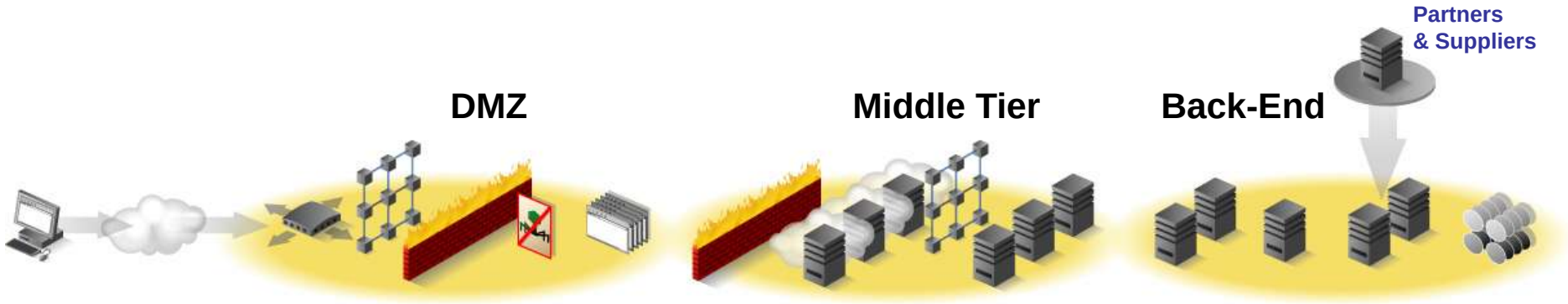


Security Metrics & Scorecards– cornerstone of an effective IT GRC assessment

- Metrics affirm the existence and effectiveness of security controls
- Scorecards enable and evidence management oversight; communicate performance and evaluate corrective actions
- Well constructed Metrics and Scorecards:
  - Continuously monitor controls
  - Deliver trusted, timely, and actionable decision making information
  - Identify and communicate concentration of risks
  - Align security initiatives with business objectives



Measuring security is a top CISO priority but it's challenging….



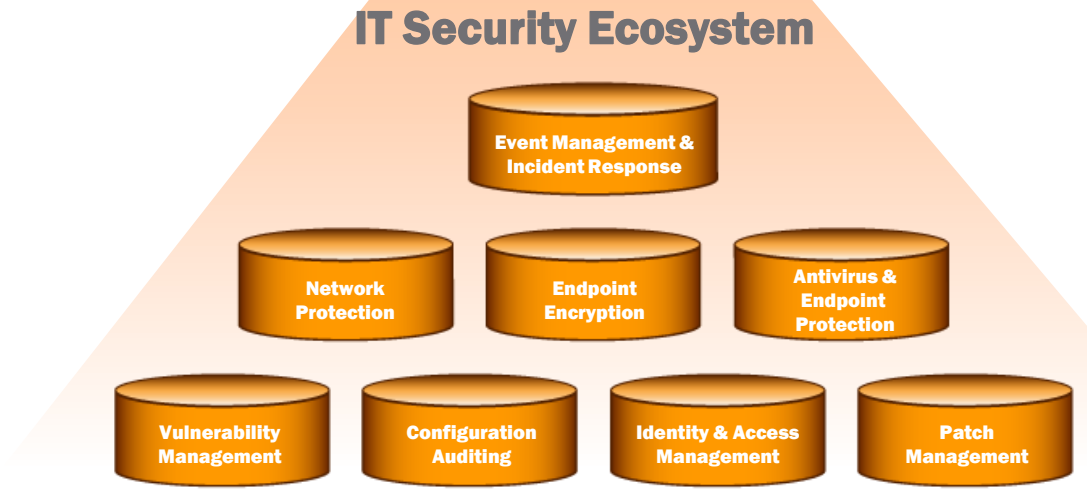
IAM	Firewall	Antivirus	Web Filtering	IDS/IPS	System Mgt	Patch	Audit & Compliance	SEIM	Databases
MS AD	Checkpoint	Symantec	Web Sense	McAfee	HP	WSUS	nCircle	ArchSight	Oracle
Tivoli	Juniper	McAfee	Barracuda	Source Fire	IBM Tivoli	SCCM	RSA	enVison	SQL Server
CA	Cisco	Trend Micro	Surf Control		CA	PatchLink	Agiliance	Intellitatics	DB2
Oracle	Symantec	Sophos			BMC Remedy				Postgres

- **Heterogeneous and dispersed silo's of vital IT information**
- **Variety of contributors and application sources each doing it differently**
- **Need to fuse together silo's and map results to a business context**
- **Challenging to reliably and consistently calculate**
- **Exacting to communicate effectively to wide variety of audiences**

An Effective Security Performance Management Solution

- Measure performance to goals
- Benchmark with peer groups
- Cover the entire IT Ecosystem
- Objective, Fact- based metrics
- Answer the critical questions

✓ *How secure and compliant is our enterprise?*
✓ *How do we compare to others?*
✓ *Are we investing effectively?*

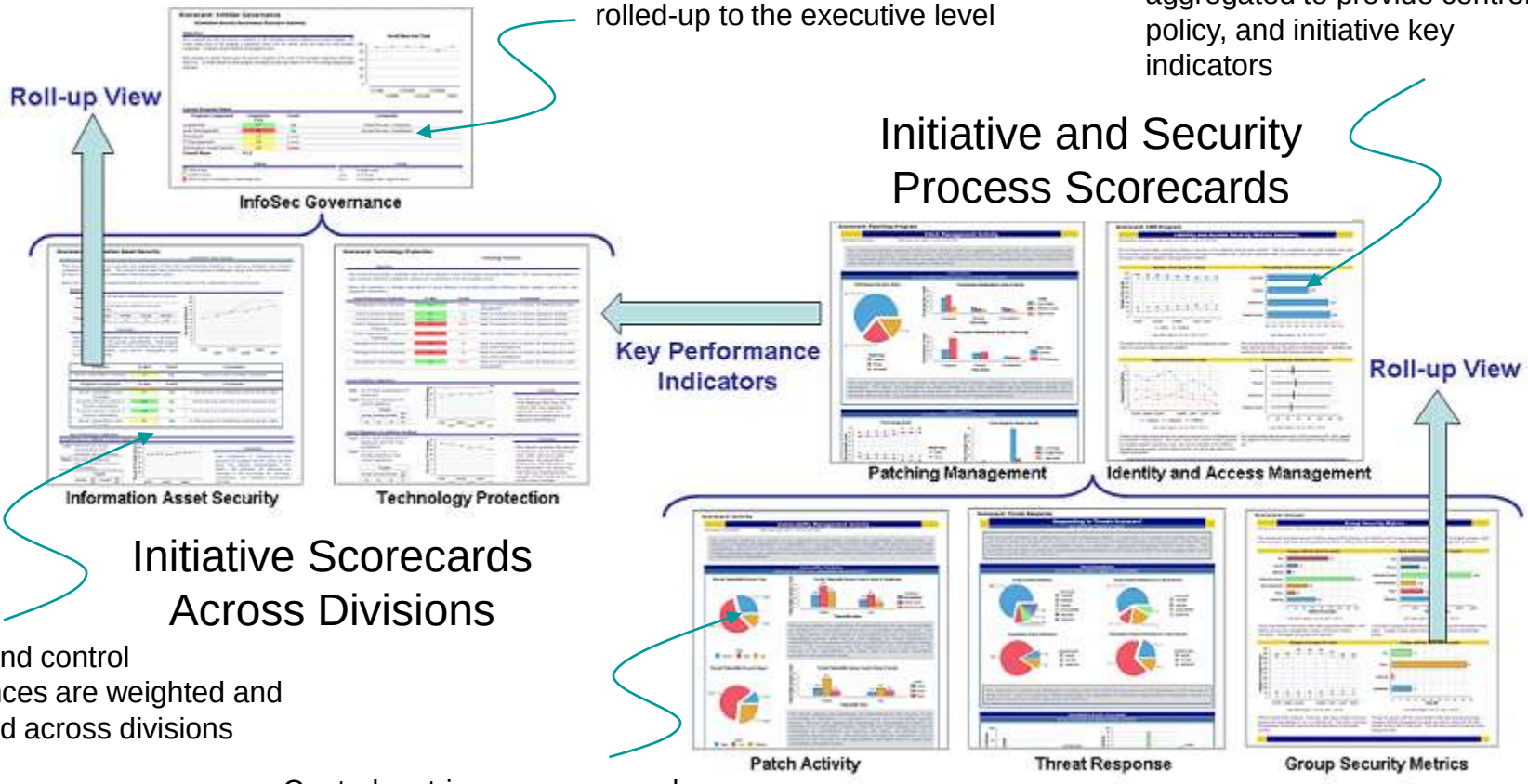


Communicate security and compliance posture: Metrics & Scorecards Roll-ups and drill-in's

Overview by Initiatives and by Divisions

Overviews of Initiatives and Profiles of Users and Assets are rolled-up to the executive level

Metric results are weighted and aggregated to provide control, policy, and initiative key indicators



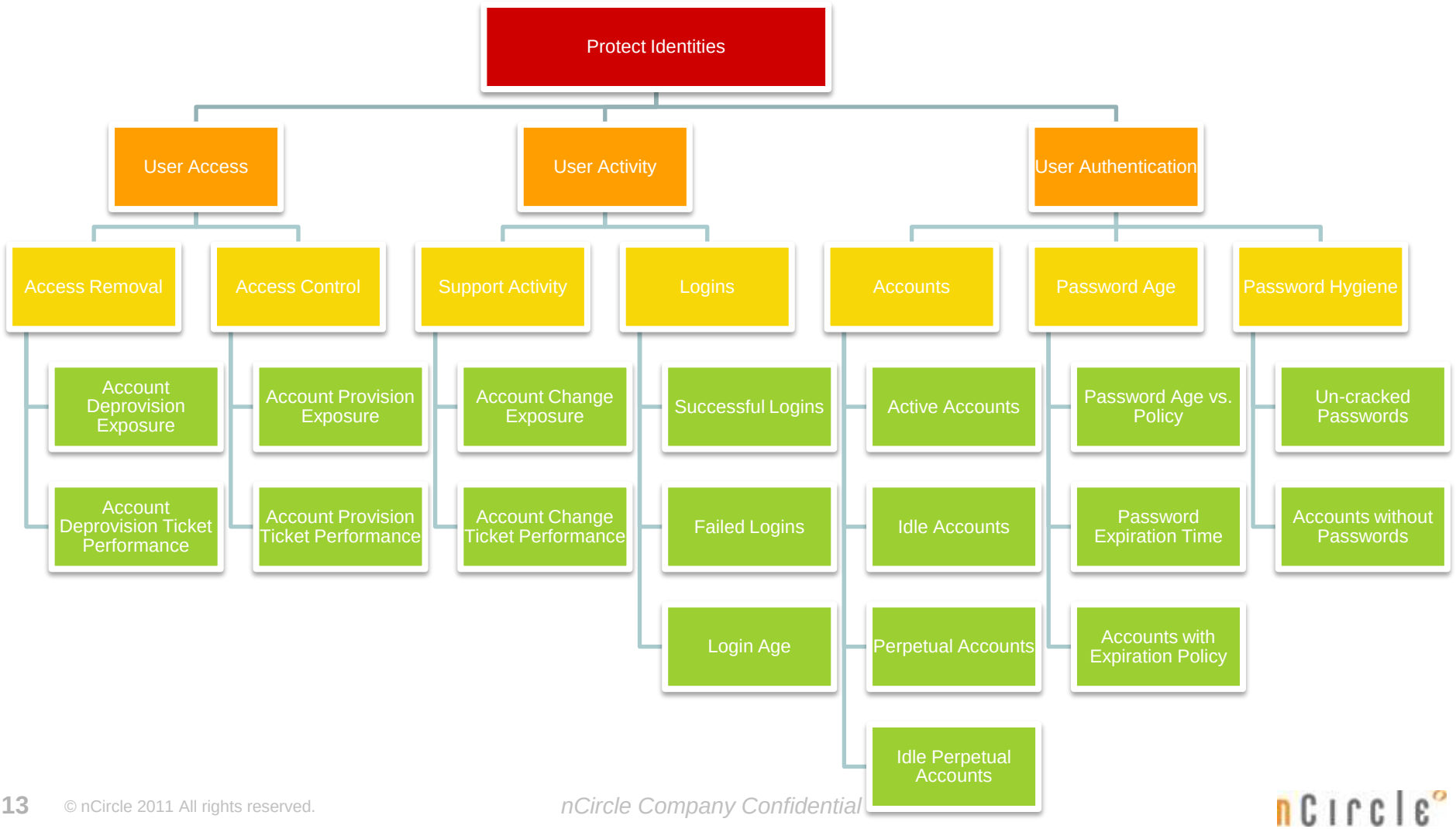
Initiative Scorecards Across Divisions

Initiative and control performances are weighted and aggregated across divisions

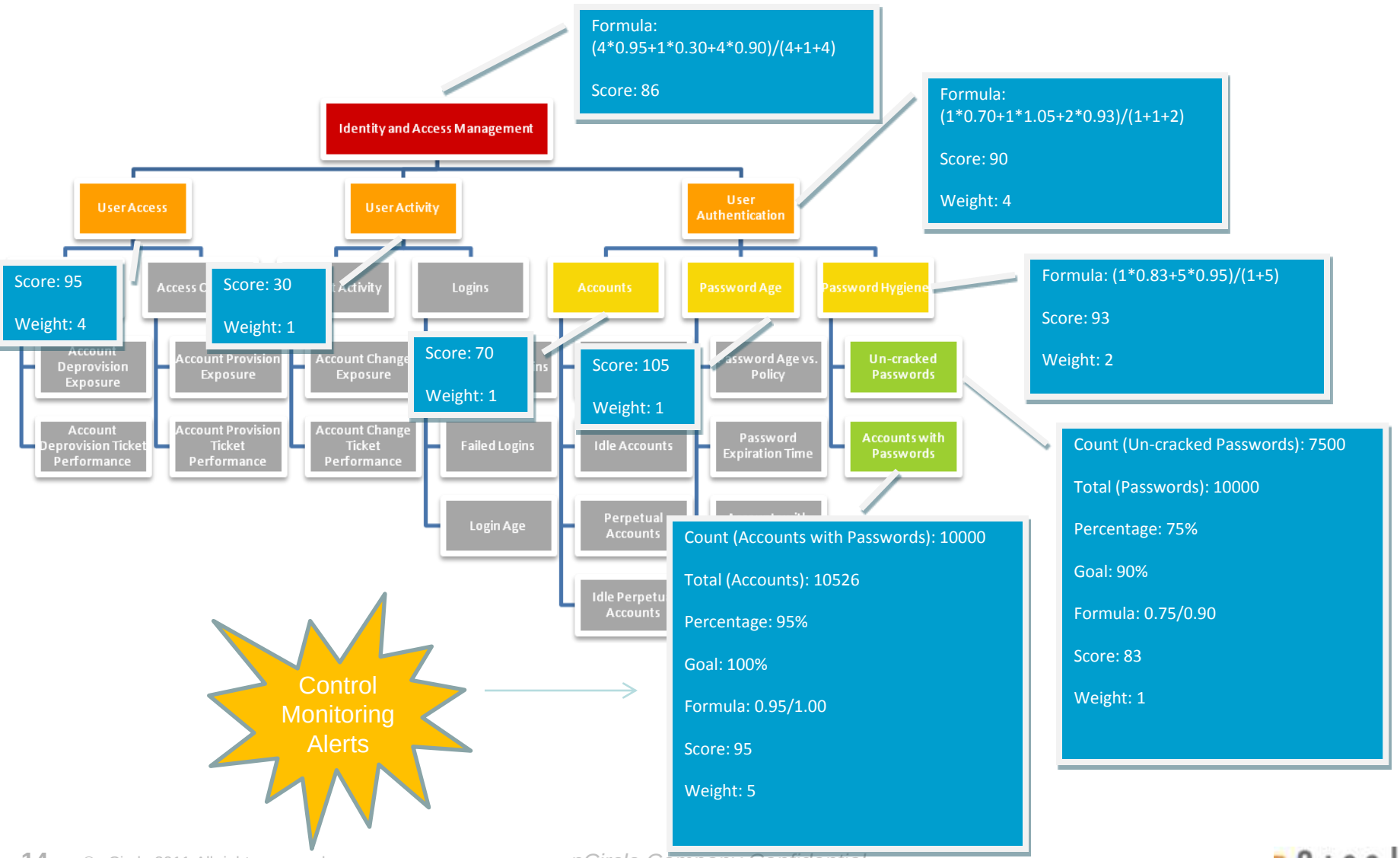
Control metrics are composed of metric results compared to policies and goals

Detailed Operational Security Metrics and Scorecards

Initiative Roll Up
Example - Identity & Access Management



Score Calculation Overview



Benchmark Initiative – Key Metrics

- ~453 accounts established
- 48% joined more than one Benchmark
- New account sign ups accelerating
- 117 of the 140 new accounts do not have nCircle products

	Sign Ups	Joined Benchmark	
		#	%
Q1	103	53	51%
Q2	141	63	45%
Q3	130	97	105%
Q4 to date	79	51	90%
Total	453	264	72%

Benchmark	Joined
IP360	109
IP360	10
CCM	36
McAfee EPO	28
SYMC SEP	26
Microsoft AD	30
Qualys	40
Rapid7	29
WSUS	16
Total	324

Attributes of a Successful Benchmark Initiative

1. Consensus
2. Relevance
3. Consistency
4. Transparency
5. Privacy

Benchmarking Performance Internally & Externally

External Comparison Benchmarks	Internal Performance Benchmarks
Rolling 12 Month Community Average	Established Goals or Baselines
Performance Quadrants	Internal Performance Comparisons
Weekly Trended Benchmarks	Specific to Risk and Value
Refined Benchmarks	Targeted Conditions & Thresholds
Refinement by Size, Industry, Geography	Policy Analysis vs. Benchmark

Valuable Peer Benchmarks

Benchmark Performance Quadrants

Participant Results

Benchmark Performance Standard

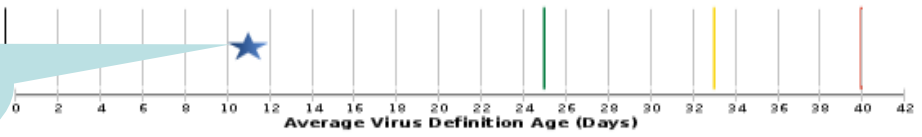
Weekly Performance Benchmark

Average Virus Definition Age

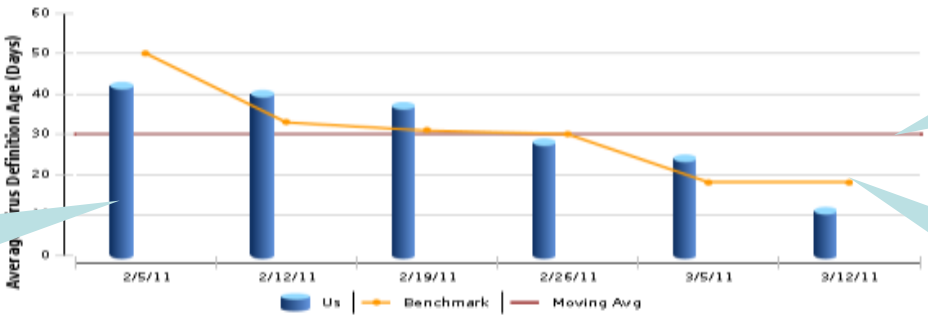
How frequently are virus definitions updated? How does this compare to the Benchmark community?

Purpose

This Benchmark Comparison Scorecard charts our average virus definition age compared to nCircle Benchmark results.



We are in the First Quartile Quartile 1: 25 Quartile 2: 33 Quartile 3: 40



As of period ending on: Mar 12, 2011

Analysis

Bars at or below the line indicate that our average virus definition age is within benchmark norms. This information can be used to determine whether virus definitions are updated according to policy and determine if adjustments to policy should be made.

Further Analysis

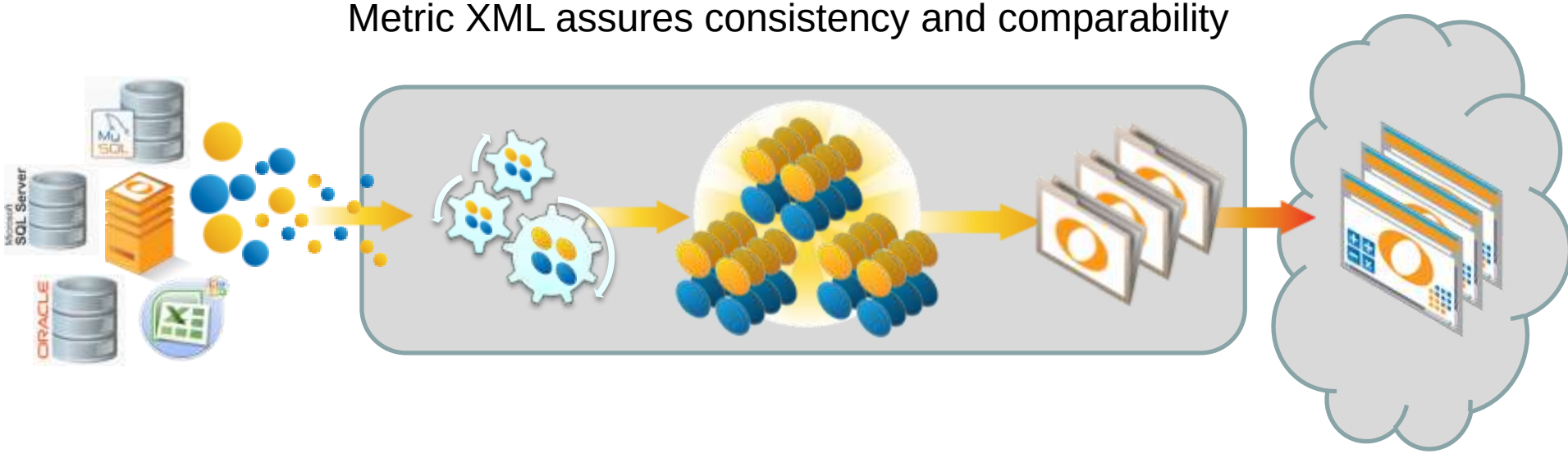
Examine the impact our average virus definition age has on detecting virus events. See the Virus Remediation Activity Scorecard, available in the Basic Endpoint Protection Benchmark Metrics Pack.

nCircle

Scorecard Published: 4/4/2011

Architecture for consistent measurement & confident benchmarking

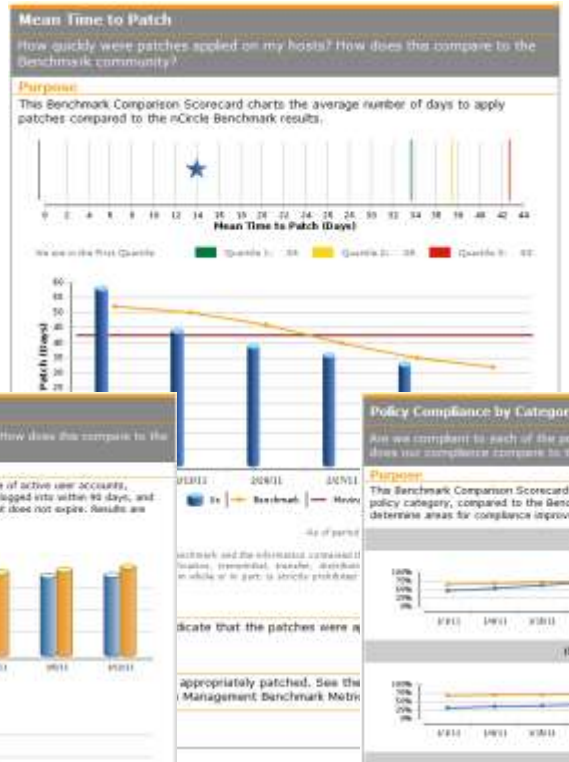
Metric XML assures consistency and comparability

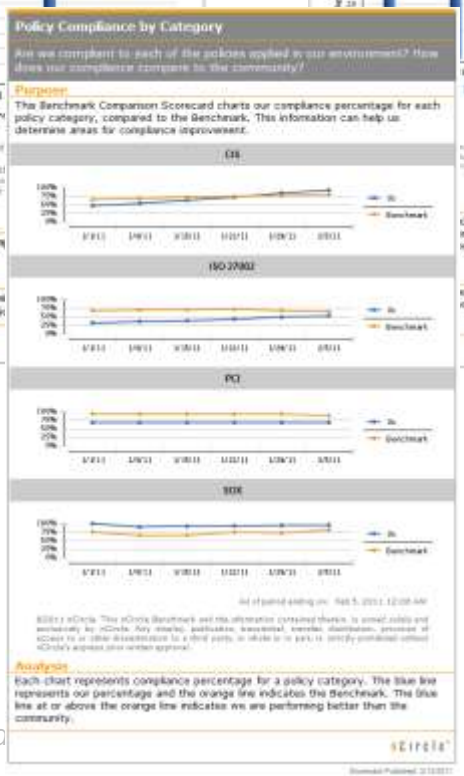


Data Sources **Data Adapter** **Data Sets** **Metrics** **Scorecards**

Delivers Transparency, Auditability, Security & Data Integrity

Analyze performance against Benchmarks





Analyze performance against Benchmarks & Identify underperforming areas

A Federal Benchmark Community?

- Questions
- Is this useful?
- Basis for metrics: similar to commercial or uniquely federal?
- Definition of community: participate in commercial, uniquely government, uniquely federal?
- Cloud-based? Hosted how?