New Requirements For Continuous Monitoring In The Cloud

Matt Alderman, Director, Product Management

November 4, 2011

Agenda

Brief History of Security, Compliance, & Continuous Monitoring

Federal Cloud Computing Strategy

- −The Case for Change
- −Cloud First

Future of Security, Compliance, & Continuous Monitoring

New Requirements for Continuous Monitoring in the Cloud

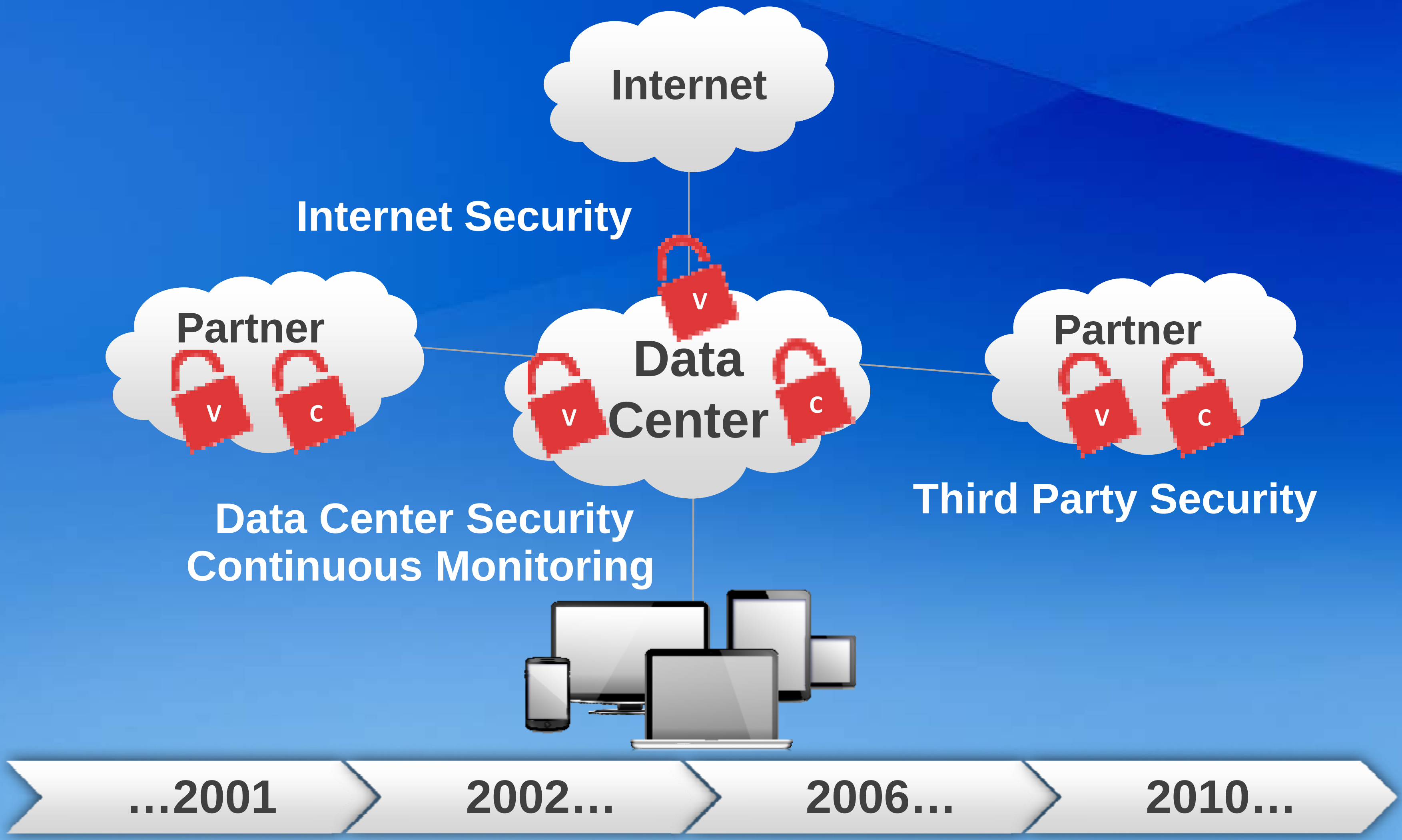
Implications for Federal Agencies

Leveraging the CM Reference Architecture

Industry Initiatives for Cloud Security

Q&A

Brief History of Security, Compliance, and Continuous Monitoring for Federal Agencies



Internet

Internet Security

Partner

Data Center

Partner

Third Party Security

Data Center Security
Continuous Monitoring

…2001

2002…

2006…

2010…

Federal Cloud Computing Strategy

The Case for Change

Economic Factors

- Low asset utilization (server utilization < 30% typical)
- Years required to build data centers for new services (over 2,000 data centers currently)
- Aggregated demand and accelerated system consolidation (Federal Data Center Consolidation Initiative)

Technology Factors

- Better linked to emerging Cloud Computing technologies (e.g., mobile devices)
- Purchase “as-a-service” from trusted cloud providers
- Tap into private sector innovation

Federal Cloud Computing Strategy

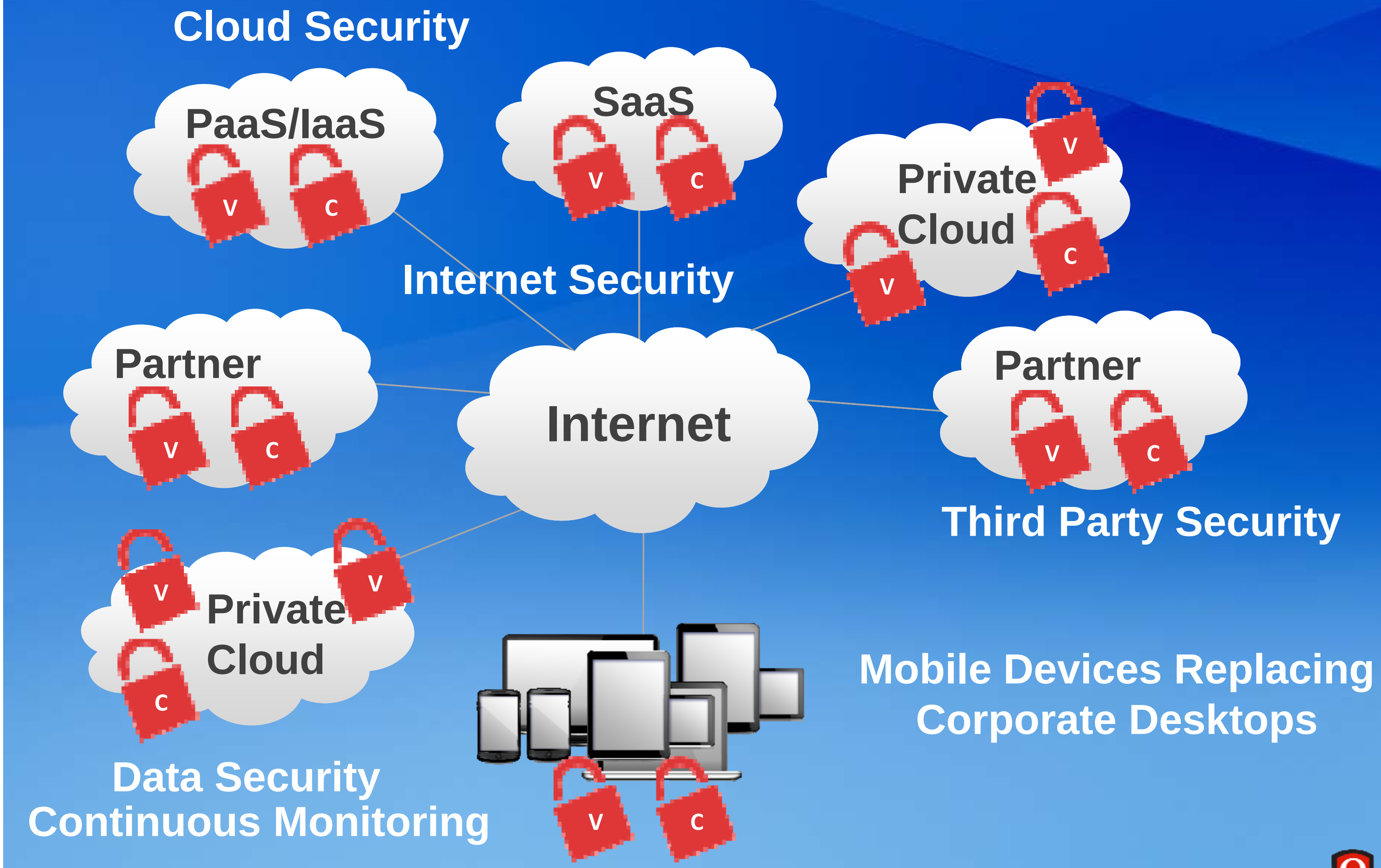
Cloud First

$20B of the Federal Government’s $80B budget is target for cloud computing solutions

Eliminate a minimum of 800 data centers by 2015

Each Federal agency will move 3 services to the cloud over the next 18 months

The Future of Security, Compliance, and Continuous Monitoring for Federal Agencies



Cloud Security

PaaS/IaaS

SaaS

Private Cloud

Internet Security

Partner

Internet

Partner

Third Party Security

Private Cloud

Mobile Devices Replacing Corporate Desktops

Data Security
Continuous Monitoring

New Requirements for Continuous Monitoring in the Cloud

Challenges

- Cloud Limitations:
  - Loss of Visibility
  - Loss of Control

Requirements

- Secure Data in the Cloud
  - Data Ownership (CM-8, RA-2)
  - Data Separation/Segregation (AC-4, SC-2, SC-4)
  - Data Encryption (SC-8, SC-9, SC-13)
  - Data Backup/Recovery (CP-9, CP-10)
  - Data Destruction (MP-6)
  - Access Control (AC-3, AC-19)
  - Activity/Log Management (AU-2, AU-12)
  - Incident Response (IR-4, IR-5, IR-6, IR-8)
  - Security Controls (CA-7, CM-6, RA-5, SI-6)
  - Patch Management (CM-2, SI-2)

- Verify Security of Data in the Cloud (AC-20, CA-2, CA-7, RA-5, SA-9)

New Requirements for Continuous Monitoring in the Cloud

Challenges

- Cloud Limitations:
  - Loss of Visibility
  - Loss of Control

- Technical Challenges:
  - Scalability of traditional hierarchical continuous monitoring instances
  - Scheduling/Control of continuous monitoring instances
  - Normalization of data

Implications for Federal Agencies

Continuous Monitoring

- Internal Cloud
- External Cloud
  - FedRAMP

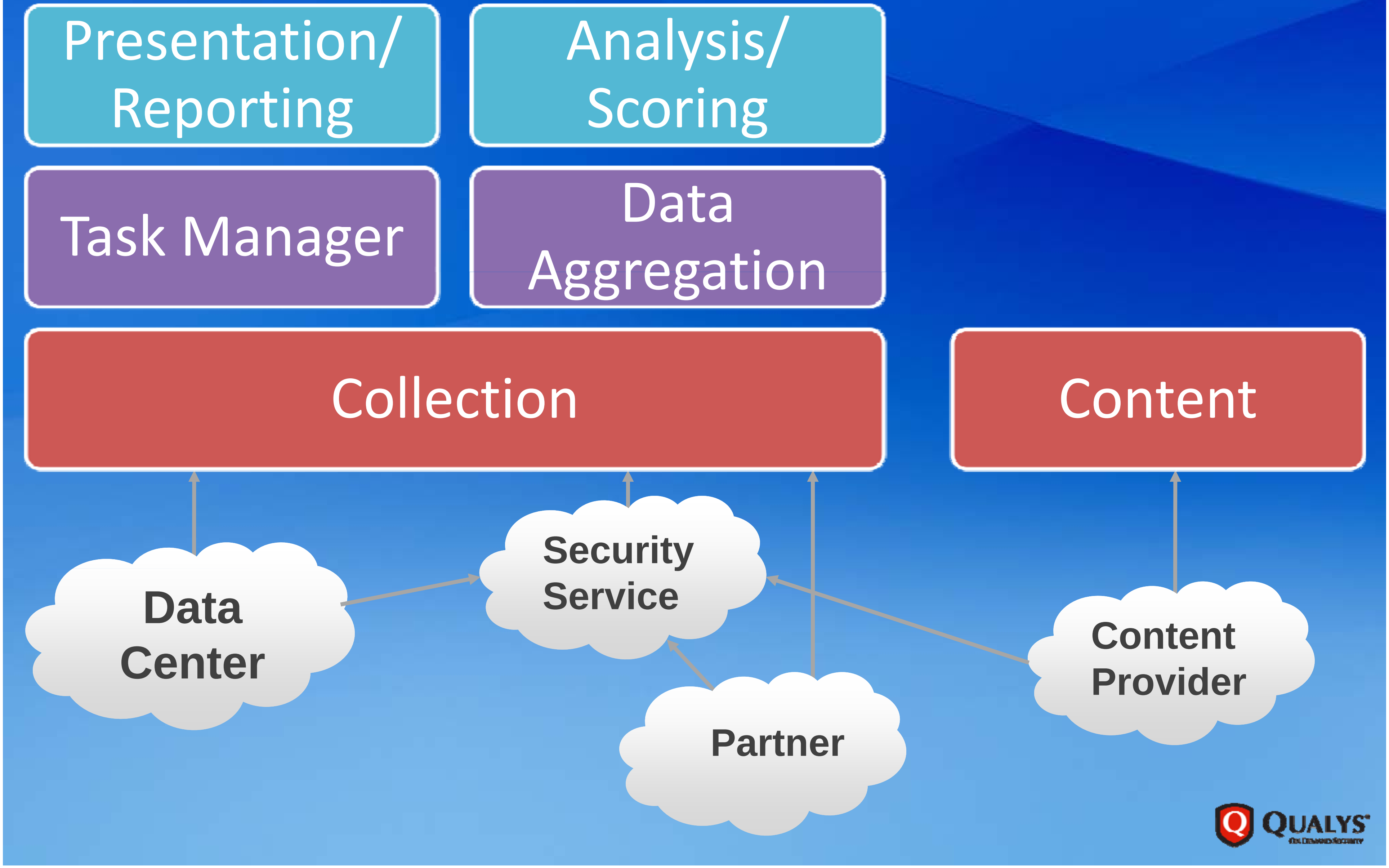
Mobile Security

- Data continues to move externally
- What tools help verify security/compliance?

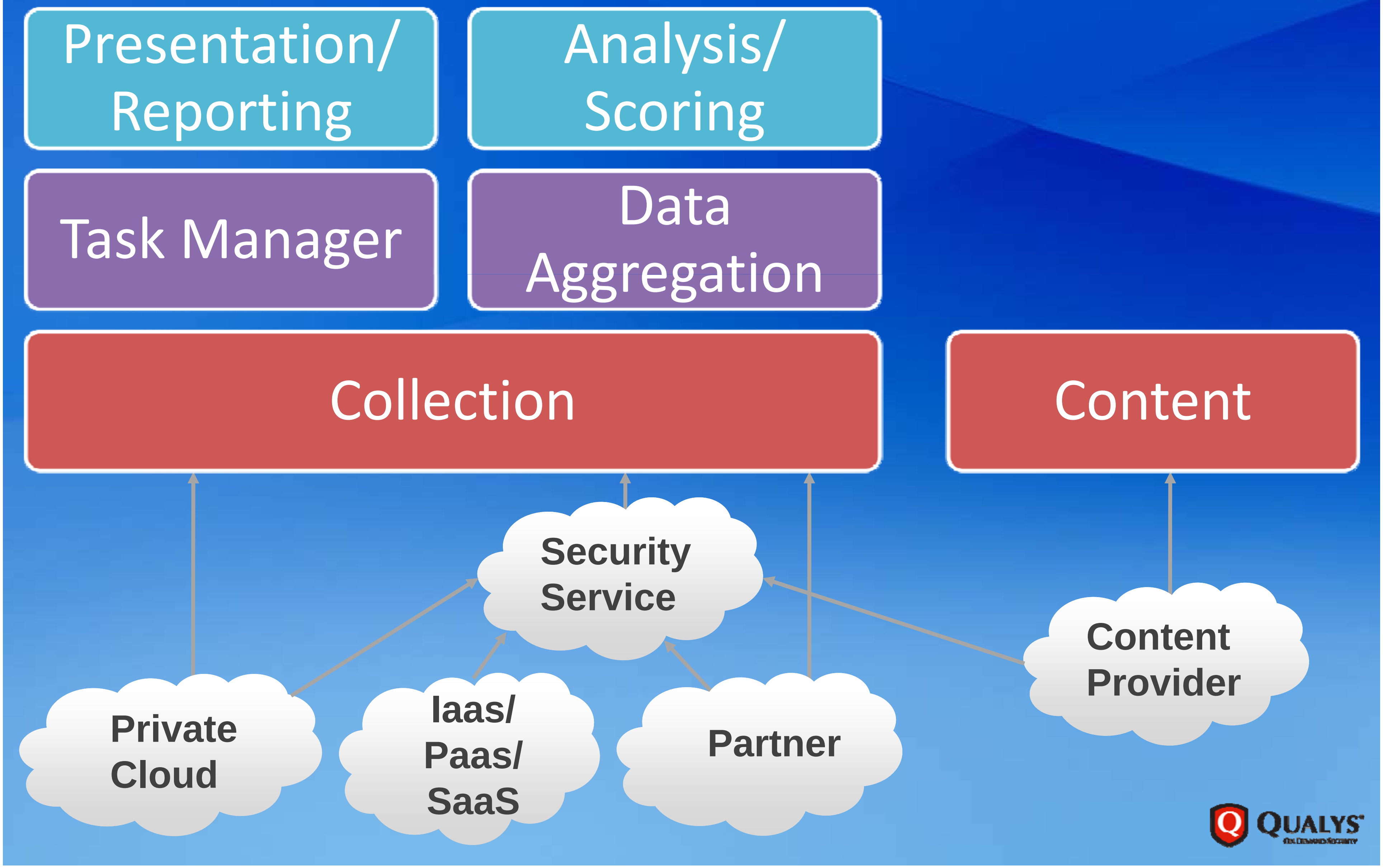
Reporting

- Correlate internal and external results
- Central reporting

Leveraging the CM Reference Architecture



Leveraging the CM Reference Architecture



Industry Initiatives for Cloud Security

CSA cloud security alliance℠

- https://cloudsecurityalliance.org/

CloudAudit

- http://cloudaudit.org/

OPEN DATA CENTER ALLIANCE

- http://www.opendatacenteralliance.org/

Thank You

Matt Alderman

malderman@qualys.com