Automating the Continuous Compliance Process in the Decentralized Enterprise

by Bill Niester – Director, Public Sector Markets

October 28, 2009

A for Desire and Effort … But …

The Mandate: ***"The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC)."***

Results:

- **"…found widespread noncompliance with mandatory FDCC standards and noncompliance with directives issued by the Department's Chief Information Officer… testing revealed a lack of standardized software across the Department..."**
- **"We noted that only approximately 4.63 percent of the Department's laptops/desktops were fully compliant with FDCC."**
- **"…only 30 percent of the agencies had fully installed the FDCC on their computers…"**
- **"…policy adoption and implementation progress vary widely among sub-agencies and across the government as a whole."**

A Leap Forward is Necessary

AUTOMATION is the key to a successful leap forward

Security information must be collected

- Efficiently
  - Do more with less
- Securely
  - Ensure the protection of the system and the data
- Ubiquitously
  - Data available from all devices and to all users
- Quickly
  - We cannot sit and wait

Information Collection Models – an Evolutionary Analogy

MODEL: Use of Native Tools for Collection

Prehistoric Age

Humans threw stones and ate whatever they hit regardless of it was what they wanted

Modern Information Assurance Comparison

Run a scan or manual configuration analysis using basic "free" tools on an ad hoc basis when information is needed.

Pro's: Not as time consuming

Con's: Only assets known about, Point in time

Information Collection Models – an Evolutionary Analogy

MODEL: Outsourced Manual Collection

Prehistoric Age

Those who were skilled at tracking and rock throwing sold their services to the masses, gives rise to the hunting party.

Modern Information Assurance Comparison

Consulting organizations are created and used to execute the collection of security control information.

Pro's: Improved quality of information

Con's: Expensive, Low control of data

Information Collection Models – an Evolutionary Analogy

MODEL: Integrated Tool Development

Prehistoric Age

Humans developed specific tools from the basic tools for hunting such as bows and arrows and spears and built permanent traps to make sure food was constantly available.

Modern Information Assurance Comparison

Users take native OS and function specific tools, hire developers and consultants, build data centers and create dedicated infrastructures for continuous collection of data.

Pro's: High degree of control, Completeness of information

Con's: Expensive, High maintenance, Knowledge lock

Information Collection Models –
The Leap Forward

MODEL: Service Oriented Delivery

Prehistoric Age

Humans would have had food delivery services

Modern Information Assurance Comparison

A service delivered that simply provides a scalable and secure solution providing ubiquitous access to all the data collection capabilities required without the need to manage infrastructure

Pro's: Low management, Mission focus, Arguably more secure

Con's: Requires due diligence around security and performance

Enterprise Security Control Measurement

Agent or Agent-less that is the question!

Agents:

Pro

- Provides full access to device for complete access to data
- Limits network traffic
- Can be operated without central repository collection connection

Con

- Requires software installed on all target systems to be measured
- Complex to collect data from all agents
- Maintenance and upgrades are difficult
- Resource contention and feature creep
- Limited scalability

Enterprise Security Control Measurement

Agent or Agent-less that is the question!

Agent-Less:

Pro

- Ensures full enterprise reach
- Speedy deployment
- Enables centralized collection of findings
- Update cycle
- Zero target footprint outside of collection

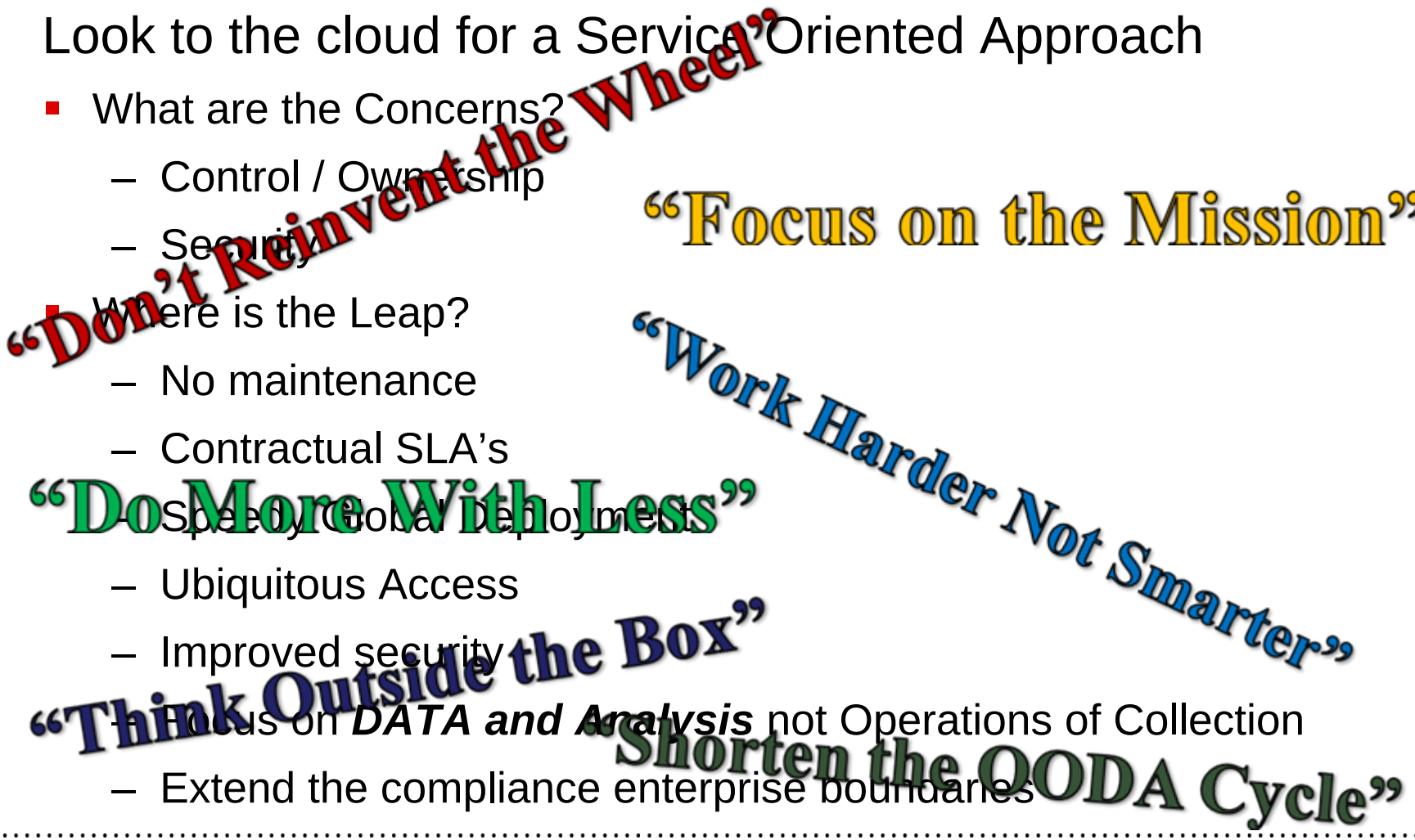
Con

- May limit set of information collected
- Generates network traffic
- Requires credentialed scan to gather local system information

Standards are a great start -Where do we leap?

Look to the cloud for a Service Oriented Approach

- What are the Concerns?
  - Control / Ownership
  - Security
- Where is the Leap?
  - No maintenance
  - Contractual SLA's
  - Speedy Global Deployments
  - Ubiquitous Access
  - Improved security
  - Focus on ***DATA and Analysis*** not Operations of Collection
  - Extend the compliance enterprise boundaries



QUALYS®

So where does that leave us…

- The need to know the enterprise security posture is accelerating
- Existing methodologies and models for information collection are not working
- We as an industry need to start thinking in a new service oriented mindset
- Cooperation, trust and an open mind are the key to the leap forward

Q&A

Thank You

Bill Niester – Director Public Sector Markets
bniester@qualys.com
(734) 646-6940

QUALYS®