Taking to the Skies:IT Flight Plan for Cloud Security

Todd Holloway

Marvell Semiconductor

Session ID: CLD-202

Session Classification: Intermediate

RSACONFERENCE2012

Learning Objectives

- Recognize challenges of a global security deployment
- Relate to why a cloud solution was selected
- Become familiar with lessons learned
- Identify recommended good practices

Today’s Agenda

- Web security challenges
- Requirements for a global solution
- The benefits of cloud security for cross-location protection
- Deployment experience and lessons learned
- Recommend good practices and key requirements for a cloud deployment

Company Overview

- Semiconductor
- Dozens of offices in many countries across the globe
- Thousands of endpoint machines

Security Challenges

- Many global locations
- Various types of competing solutions deployed by different teams
- Threat visibility limited
- Resources limited

Requirements for a Global Solution

- Unified policy and enforcement across all locations
- Policies can follows user/group/IP range, and is applied everywhere
- Consolidate point products (URL, APT, AV, etc)
- Flexible policy based on group/department
- Numerous deployment options (GRE tunnel, User auth optional, PAC file, etc.)

Terminology of Risk

- Asset – any entity which has value to the business
    - Contextual assets: the architectural attributes you have defined
    - Physical assets: buildings; equipment
    - Logical assets: information
    - Temporal assets: time

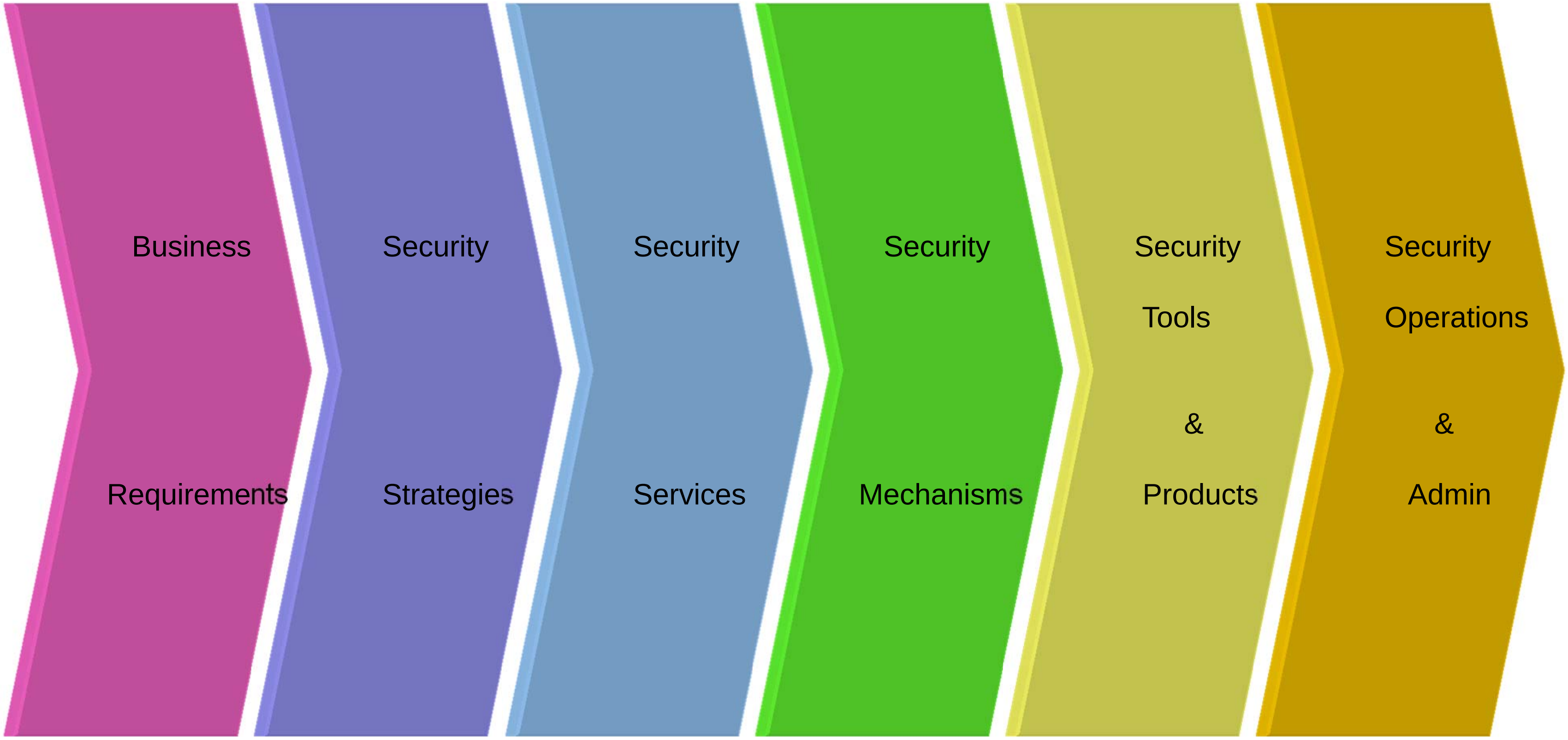
- Threat - any event which puts at risk a business function or a supporting business system

Terminology of Risk

- Impact - a description and measurement of the outcome of a threat upon attributes (assets or organizational goals)

- Vulnerability - a weakness in a business system which could lead to the realization of a threat, thus resulting in the organization suffering an impact

Traceability for Completeness



Business Requirements

Security Strategies

Security Services

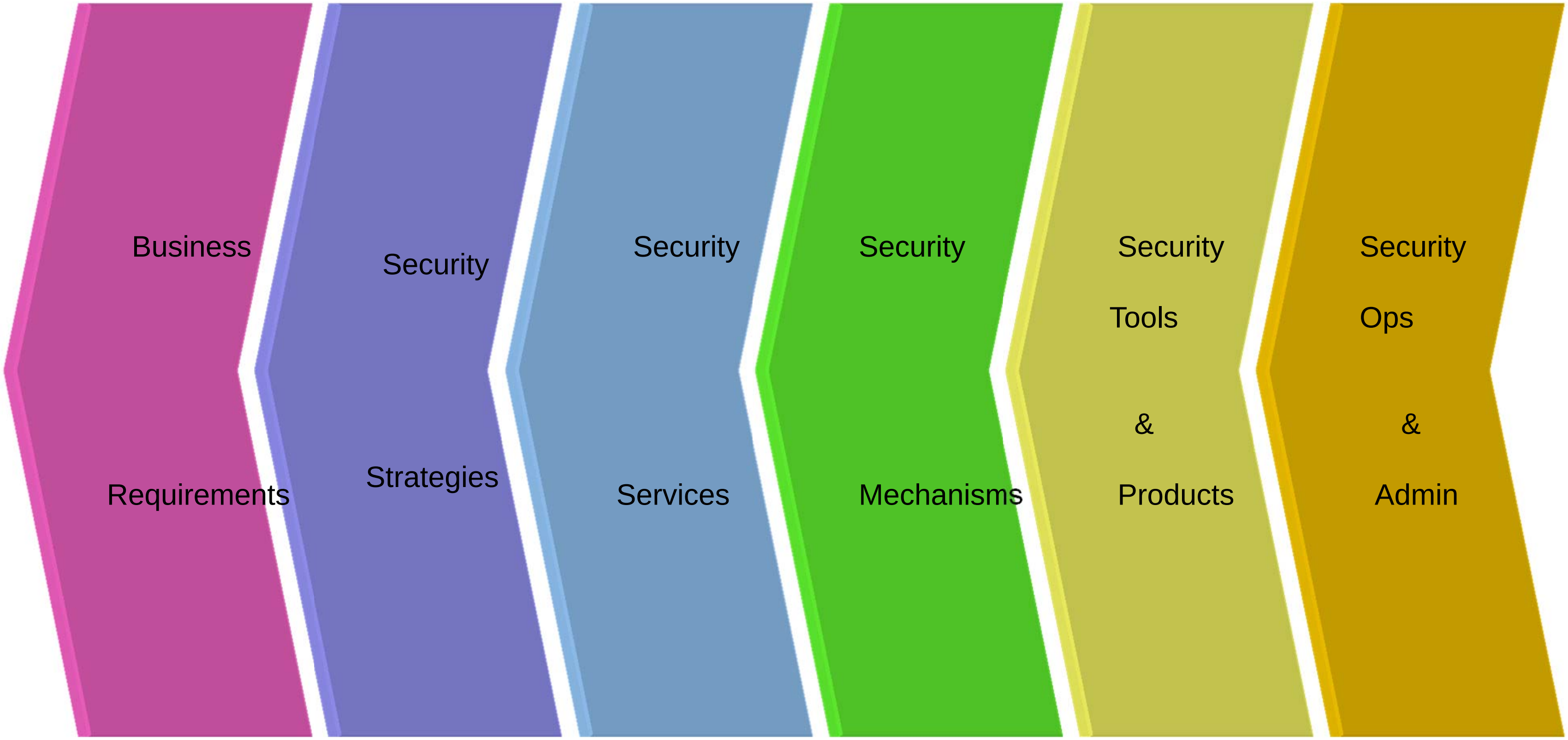
Security Mechanisms

Security Tools & Products

Security Operations & Admin

Every business requirement for security is met and the residual risk is acceptable to the business

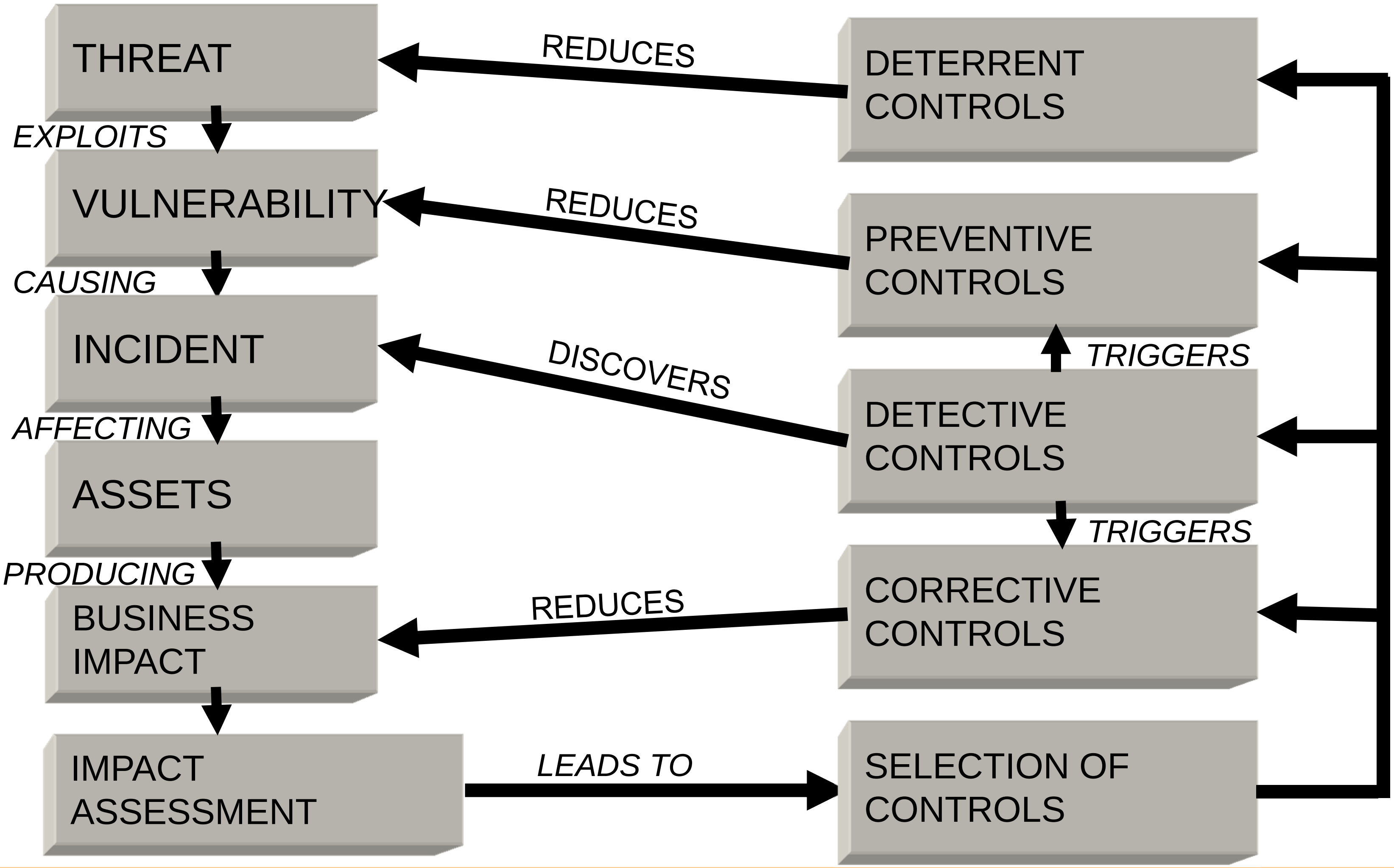
Traceability for Justification



Every operational or technological security element can be justified by reference to a risk-prioritized business requirement

KM8

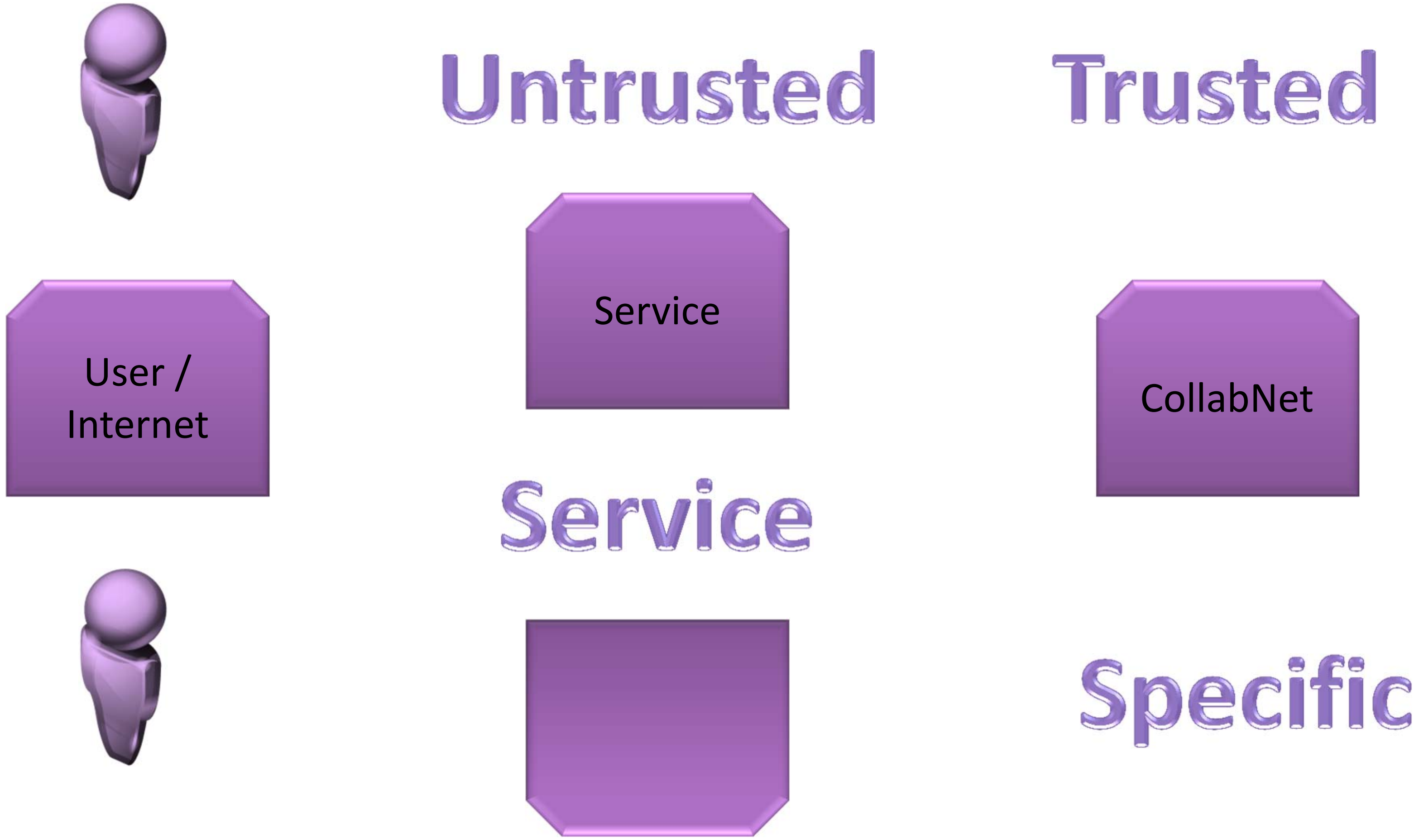
Security Controls: Right Place, Right Time



Slide 11

KM8	Not sure where the start point is to read this slide-perhaps you could indicate by color or number Ken McClung, 12/7/2011

My Perimeter Architectural Zones



Untrusted

Trusted

User / Internet

Service

CollabNet

Service

Specific

The Benefits of Cloud Security for Cross-Location Protection

- Less need for IT presence in each location
- Administered through a single interface across all locations
- Cross-location reporting consolidated in single console, all in the cloud
- Minimal to no hardware, software to ship, install, manage

Deployment Experience and Lessons Learned

- Active directory tie-in?
- SSO/SAML future?
- Can take days, not months?
- Policy migration to the cloud
- Transition?
- GRE vs. VPN vs. PAC?

Applying Best Practices and Key Requirements for a Cloud Deployment

- Perform an ROI calculation of on-premise vs. cloud services
  - Look for well-architected web service that provides economic savings and meets functionality requirements.
- Consider the broad range of user devices and configurations in your environment
- Consider level of Malware Protection vs. traditional or other cloud solutions
  - Many solutions focus on web filtering but may have limited malware protection capability
- Consider elasticity and scalability of your cloud solution

Applying What You Have Learned Today

- Learn risk terminology
  - It will elevate the topic of security from tools to solutions
  - Allow you to talk with non-security people about security
- How to think strategically
  - SABSA: www.sabsa.org
  - Cloud Security Alliance: cloudsecurityalliance.org
  - TOGAF: www.opengroup.org

Q&A

About me:

Todd Holloway tholloway@gmail.com

http://www.linkedin.com/in/riskmgmt