SECURITY AUTOMATION FOR PRIVATE CLOUD ENVIRONMENTS

Praveen Karunakaran, CCSK, CISSP, CISSP-ISSAP, CISM
Security Lead - HP Cloud Services
24 Sep 2011

Agenda

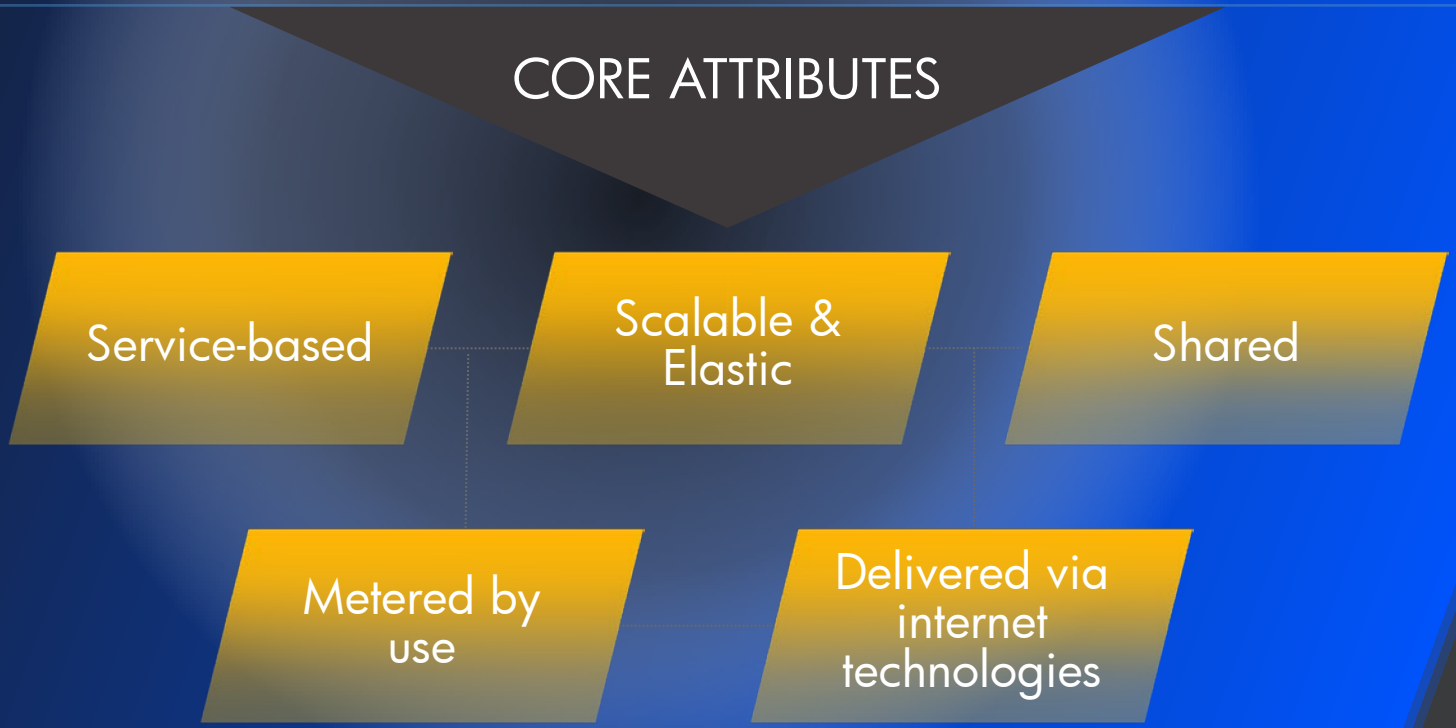
- Introduction/ Overview
- Business and Technical Drivers
- Limitations of Traditional Security Solutions
- Cloud Security Requirements
- Security Automation - Architecture Requirements
- Deployment Approach
- Summary

Questions & Answers

Please hold question until the end

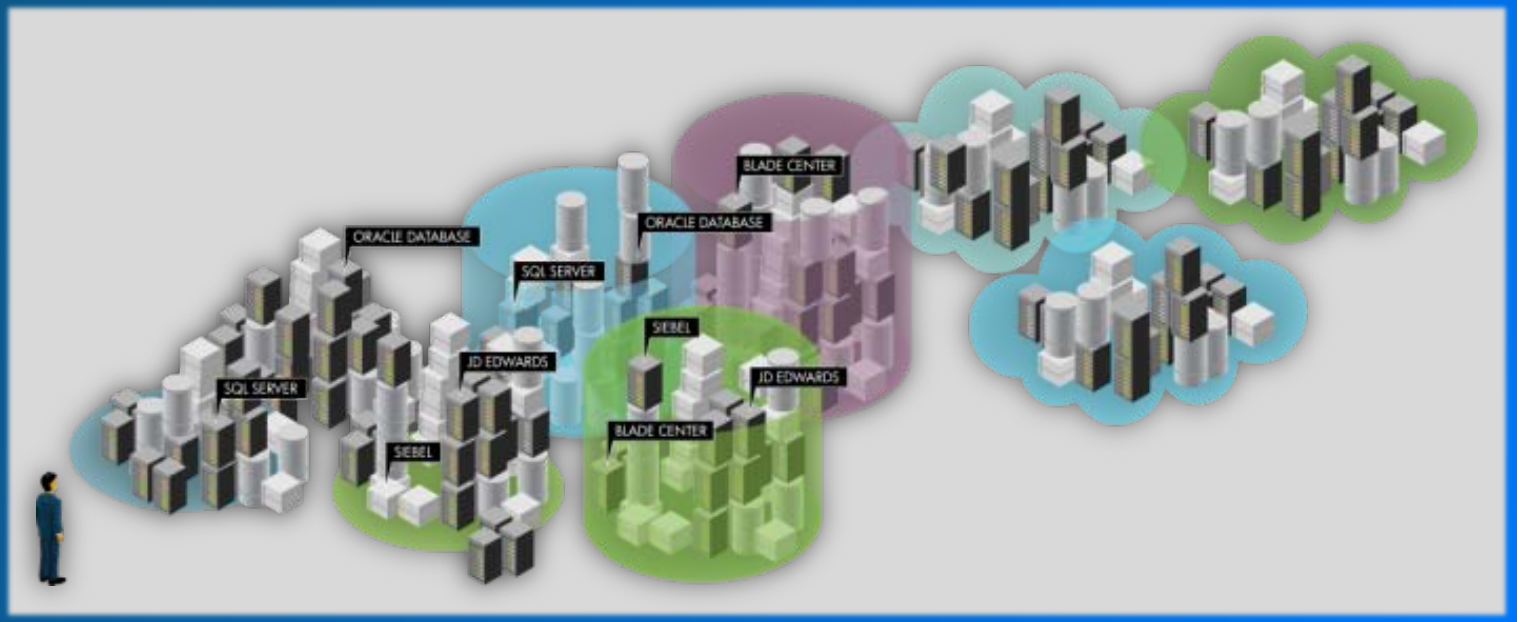
WHAT IS CLOUD

Cloud services are highly scalable and elastic technology-enabled services, delivered and consumed over a network through an as-needed, pay-per-use business model



WHAT'S DRIVING THE MOVE TO CLOUD

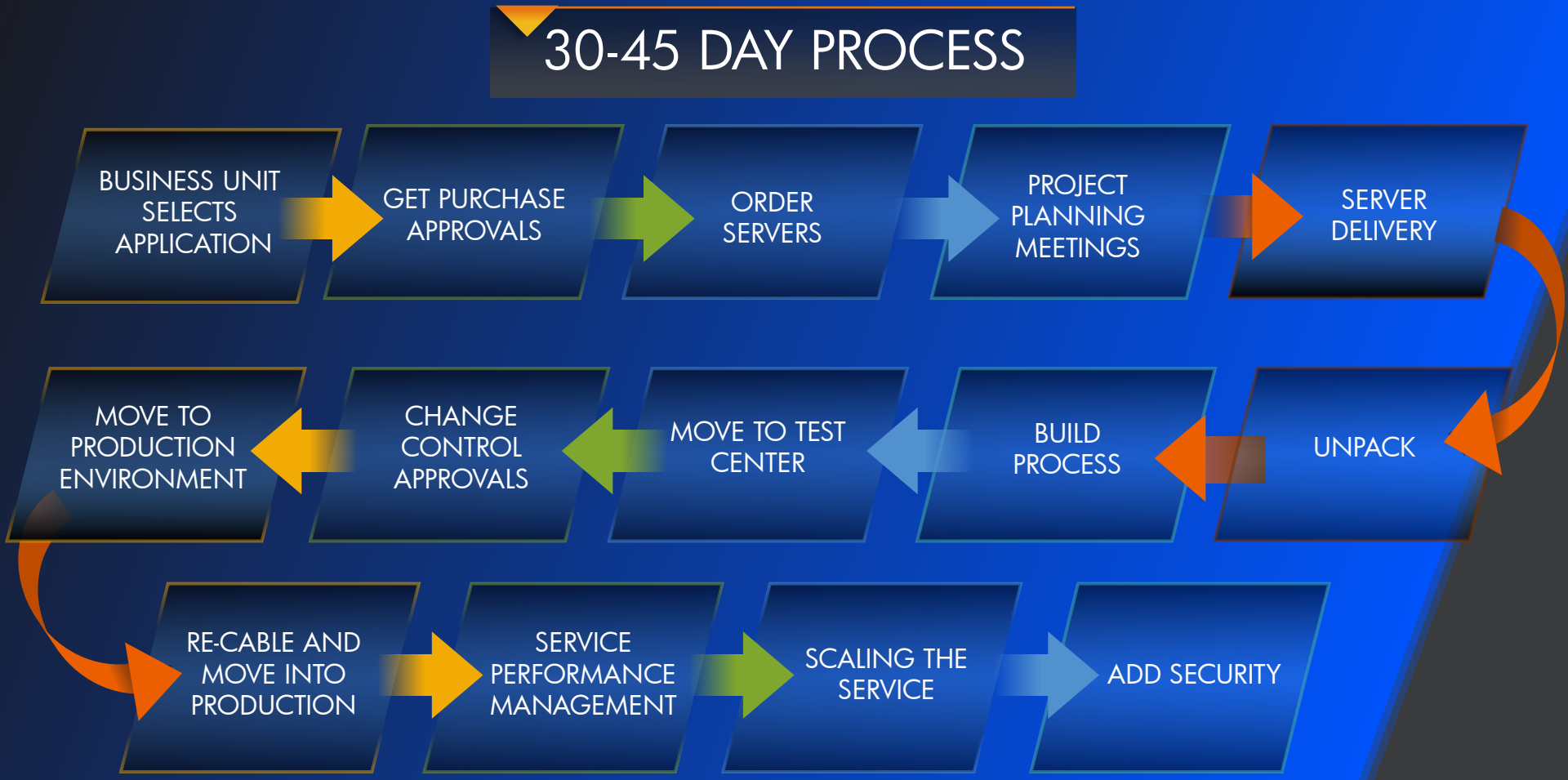
- 70% of businesses considering or using Private Clouds
- Business is adopting cloud 5x faster than IT
- 70% of IT resources captive in maintenance and operations



Business drivers: Speed, flexibility and economics
IT challenges: Sprawl, control and integration

NON CLOUD ENVIRONMENT REALITY

Building New Systems



CLOUD PARADIGM: NEW WORLD ORDER

60 MINUTES TO 6 HOURS

PRIVATE CLOUD SERVICES

Private Cloud Services provides maximum ROI in an efficient and flexible consumption model:

1. No capital investment needed
2. Flexible, scalable and automated
3. Built for running production applications
4. Designed for high levels of performance, uptime, security and privacy

PRIVATE CLOUD - FEATURES

On Demand Service Delivery

CUSTOMER PORTAL WITH SELF-SERVICE FEATURES

CENTRALIZED GOVERNANCE AND SECURITY MODEL

UTILIZATION BASED BILLING

INSTANT SCALABILITY & AVAILABILITY

OPTIMIZED FOR BUSINESS APPLICATIONS

INTEGRATION WITH PARTNER TECHNOLOGIES

SECURING THE CLOUD

SECURITY FOR PRIVATE CLOUD

Problem Statement

- Complex and dynamic operational model
- Abstraction of compute and resources are not bonded to a physical boundary
- Cloud resources like virtual systems, virtual storage, virtual networks etc., are provisioned in real time and there is a requirement to protect these resources when they are provisioned
- The security solutions used in traditional IT environments limit the flexibility, the rapidity of changes, and limit the cost savings enabled by the abstraction of resources in cloud

Security Requirements for Private Cloud Infrastructure

- Security Tools as Distributed Policy Enforcement Points
- Integration with Centralized Security Management Tool
- Real-Time and Automated Security Service Provisioning & De-Provisioning
- Policy Driven Network Segmentation
- Multi Tenancy and Resource Isolation
- Compliance with Industry Standards

SECURITY SERVICE AUTOMATION

Automating Security Deployment and Operations in Private Cloud Environment

AUTOMATION FOR SECURITY SERVICE PROVISIONING

- ✓ Fully Automated Security Service provisioning lifecycle
- ✓ Customizable Security Services for individual clients
- ✓ Systematically managed changes
- ✓ Lesser Time for Service Provisioning

COMPREHENSIVE SECURITY POLICY DATABASE

- ✓ Comprehensive Security Policy Database
- ✓ Customizable Security Templates
- ✓ Vendor Neutral Security Policies
- ✓ Provision to add Custom Security Requirements

MULTIPLE SECURITY VENDORS

- ✓ Option to chose the preferred security vendor
- ✓ Migrate from one vendor to another without changing the Security Policies

PRIVATE CLOUD – SECURITY AUTOMATION

Foundation for Cloud Security Automation

SELF SERVICE PORTAL

ORDER & SERVICE MANAGEMENT

ASSET TAGGING

SECURITY POLICY DATABASE

SECURITY STANDARD /COMPLIANCE REQUIREMENTS

SECURITY AUTOMATION AND INTEGRATION LAYER (API)

VIRTUALIZATION PLATFORMS

SECURITY TOOL VENDORS

DEPLOYMENT & MONITORING

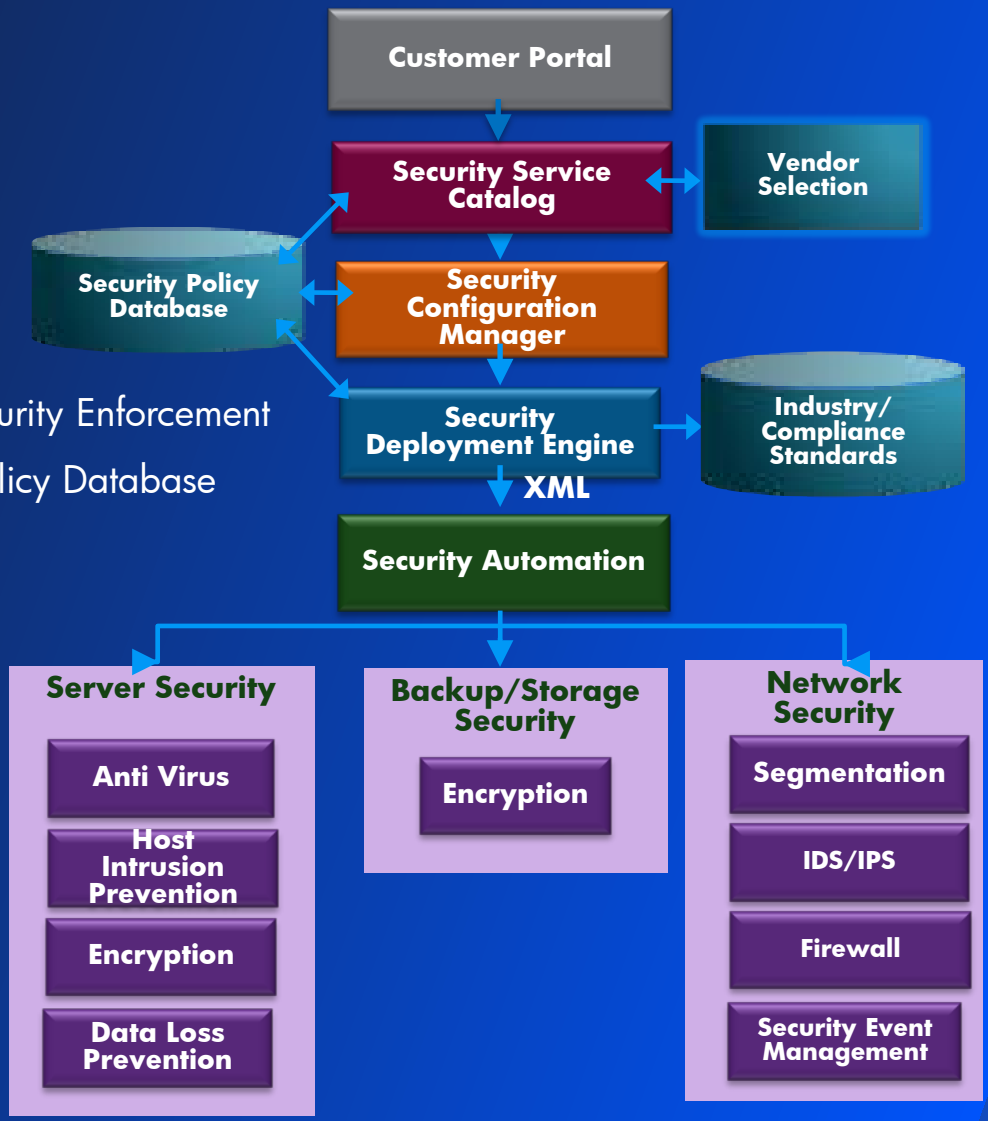
SECURITY DASH BOARD

- ✓Increased Security
- ✓Reduced Human Labor

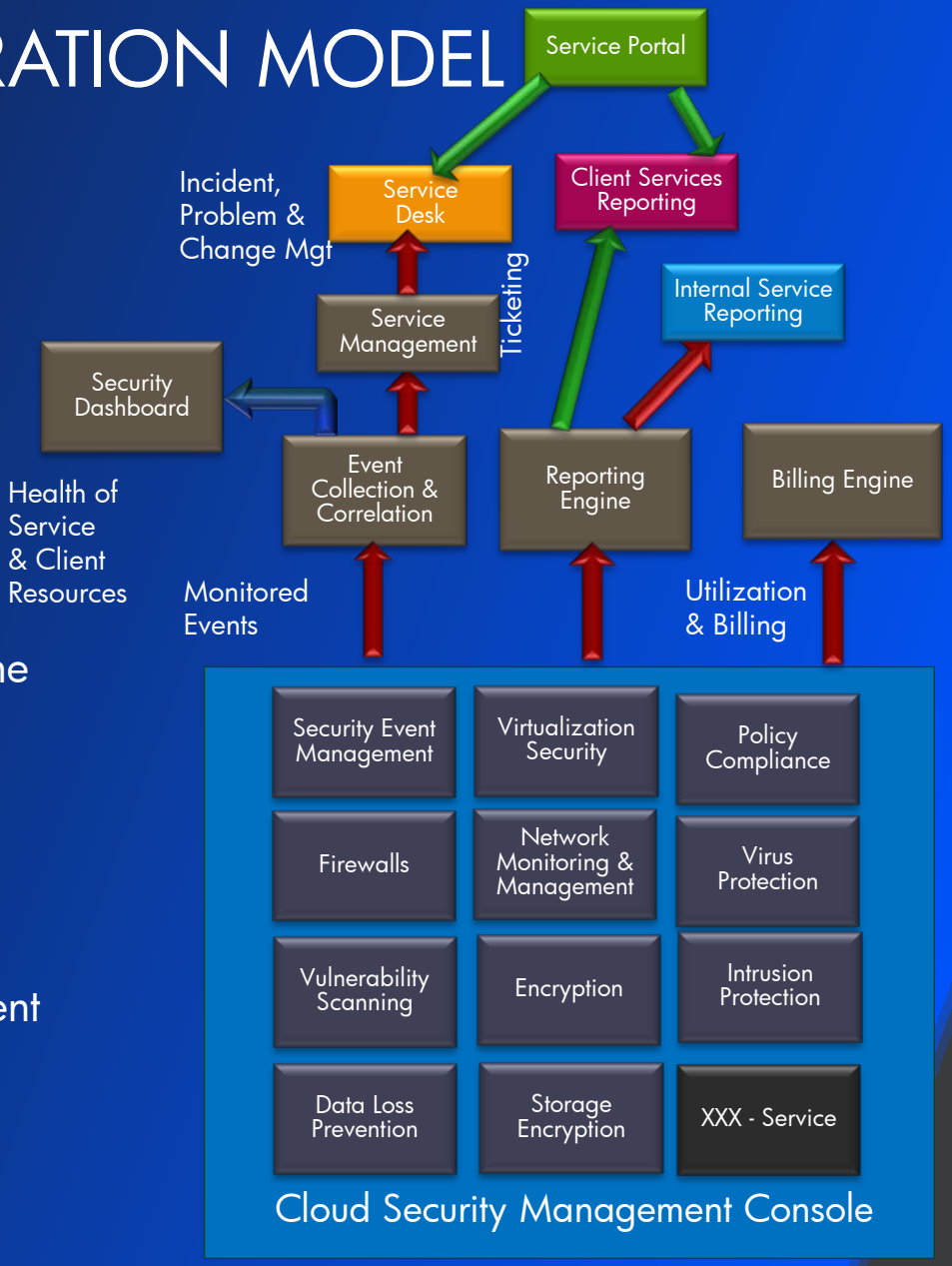
- ✓Minimal Provisioning Errors
- ✓Reduced Overall Risk
- ✓Reduced Cost

SECURITY AUTOMATION ARCHITECTURE

- Customer Specific System Attributes
- Standard Set of Security APIs
- Security Zones and Policy Based Security Enforcement
- Platform and Vendor Independent Policy Database
- Multiple Security Vendors

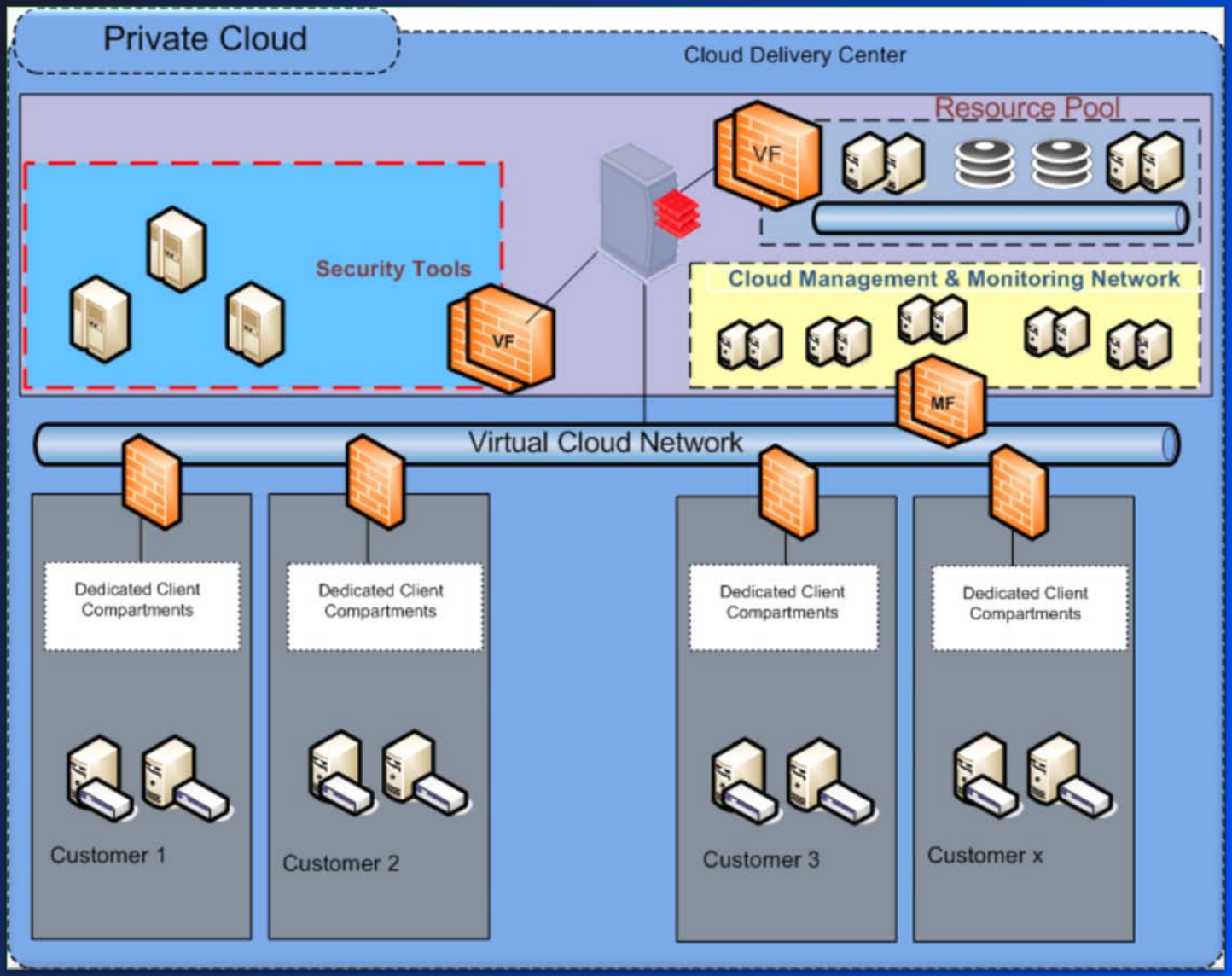


DELIVERY AND OPERATION MODEL



The Operational Architecture provides the post-provisioning support for Security services. It includes:

- Capabilities to interface directly with cloud resources supporting security management and monitoring.
- Security event collection & Management
- Incident, Problem, Change & Request Management
- Internal & Customer Service Reporting



SUMMARY

- In a cloud infrastructure, security solutions like Firewalls, IDS/IPS, AV, Vulnerability Management etc., should work as distributed policy enforcement points integrated directly into a centralized security management tool
- Real-time and automated security provisioning, network segmentation, compartmentalization and resource isolation are the key success factors for a cloud delivery model
- Developing a Comprehensive Security Policy Database and Integration of Security into Cloud using a Standard Set of Security APIs is a complex process
- Require careful design and integration of various security components within a well designed architecture, and a well designed and tested auto-provisioning rules (policies)

Q&A

