Proactively Secure Your Cloud Computing Platform

Dr. Krutartha Patel
Security Engineer
Agenda

1. Cloud Security – IMPERATIVE
2. Positives and Challenges
3. Physical and Virtual Gateways
4. Leveraging Investment
Strong Drivers for Move to the Cloud

- **Compute Power**
- **Reduced Costs**
- **Business Continuity**

- Scalable, elastic infrastructure
- Pay only for what you use
- Resilience and disaster recovery
Cloud Delivery Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Vendors</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IaaS</strong></td>
<td>Rent Hardware Software Networks</td>
<td>IT</td>
</tr>
<tr>
<td>Infrastructure-as-a-Service</td>
<td>amazon web services™, Rackspace IT Hosting</td>
<td></td>
</tr>
<tr>
<td><strong>PaaS</strong></td>
<td>Rent Hardware and Software</td>
<td>Developers</td>
</tr>
<tr>
<td>Platform-as-a-Service</td>
<td>Google App Engine, Windows Azure</td>
<td></td>
</tr>
<tr>
<td><strong>SaaS</strong></td>
<td>Rent Applications Such as Email</td>
<td>End Users</td>
</tr>
<tr>
<td>Software-as-a-Service</td>
<td>Google Apps, Salesforce</td>
<td></td>
</tr>
</tbody>
</table>
IT Infrastructure Deployment Models

Physical

- Traditional enterprise

Virtual

- Virtualization, better utilization

Private Cloud (On-Premise)

- Owned and operated by organization

Public Cloud (Off-Premise)

- Resources on demand and pay-per-use
<table>
<thead>
<tr>
<th></th>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cloud Security – IMPERATIVE</td>
</tr>
<tr>
<td>2</td>
<td>Positives and Challenges</td>
</tr>
<tr>
<td>3</td>
<td>Physical and Virtual Gateways</td>
</tr>
<tr>
<td>4</td>
<td>Leveraging Investment</td>
</tr>
</tbody>
</table>
Cloud Security Positives

- Scalable Security
- Expert Security
- Global Intelligence
- Multi-Layer Security
- Cost Effectiveness
Cloud Security Challenges

- Network Attacks
- Multi Tenancy
- Access Control
- Data Security
- Compliance and Regulations
1. Cloud Security – IMPERATIVE
2. Positives and Challenges
3. Physical and Virtual Gateways
4. Leveraging Investment
Case Study - Amazon Web Services

Virtual Gateways for Amazon Public Cloud

Secure Your Infrastructure in AWS Public Cloud
Amazon VPC Topology

- Direct connectivity to Internet or over VPN
- Amazon VPC internet gateway
- Amazon VPC router
- Check Point Virtual Appliance for VPC
- AWS EC2 instances in private subnets
Central Management and Enforcement

Diagram showing the connection between Amazon VPC and branches to the headquarters (HQ).
Virtualization Security Challenges

- Protection from external threats
- Inspect traffic between Virtual Machines (VMs)
- Secure new Virtual Machines automatically
Virtualization Security Challenges

Security Challenges in Virtual Environments
Virtualization Security Challenges

Security Challenges in Virtual Environments (Data Center/Cloud)

Ensure Security in dynamic environments

Maintain zero-downtime during Virtual Machines live migration
Secure the Virtual Infrastructure

Inter-VM Traffic Inspection Protects Virtual Machines

- Seamless security within the Hypervisor
- IMPORTANT to Integrate using VM Vendor APIs
- Central Management, Granular Policy design
Public or Private Clouds

Multiple Virtual Systems in ONE Physical...

Virtualized Gateways Simplify Cloud Security
Public or Private Clouds

Multiple Virtual Systems in ONE Physical ..

Virtualized Gateways Simplify Cloud Security
Cloud Security Challenges

- Network Attacks
  - Firewall, IPS
- Multi Tenancy
  - Gateways in Virtual Infrastructure
- Access Control
  - Firewall, VPN
- Data Security
  - Data Loss Prevention
- Compliancy
  - Security Management
Agenda

1. Cloud Security – IMPERATIVE
2. Positives and Challenges
3. Physical and Virtual Gateways
4. Leveraging Investment
Leveraging Investment

One-click Activation of functionality

From the central management console

Application Control
Identify and control usage of thousands of applications based on user and machine identity.
Thank You