CSA APAC cloud security alliance® ASIA PACIFIC REGION

Security Service Goes Cloud

Claudius Lam

Chairman, Cloud Security Alliance HK & Macau Chapter

cloudsecurityalliance.org facebook.com/csaapac1
Cloud Security Alliance cloudsa_apac csa_china

“Increasingly, organizations are asking what can’t go to the cloud, rather than what can…”

Source: Gartner Blog Network. The end of the beginning of cloud computing by Lydia Leong

Many Choices

Cloud Security Challenges

- Visibility
- Agility
- Purchasing
- Compliance

Why do I need additional security in the cloud?

Threats:

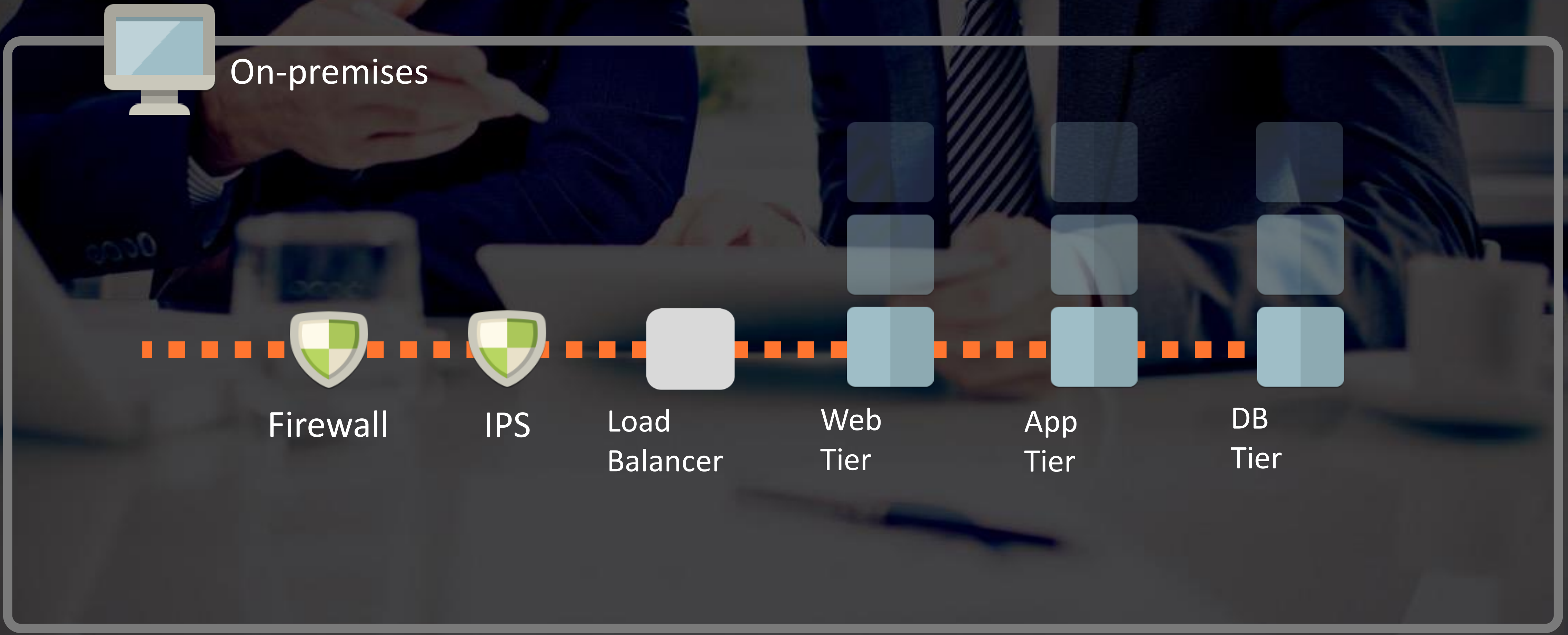
- Network attack
- Vulnerabilities
- Malware
- Insider threats

Compliance:

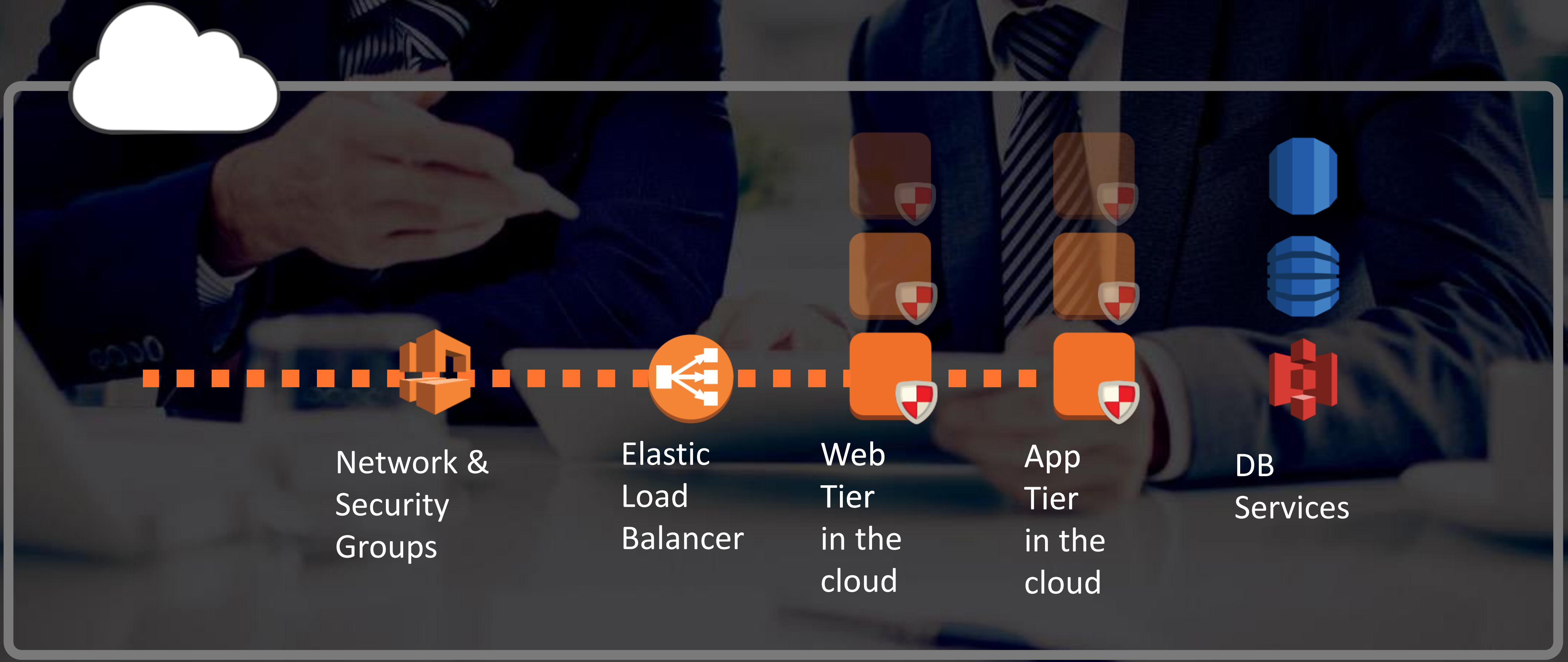
- PCI DSS
- HIPAA
- Internal

Traditional on-premises security

Applied at the perimeter



Build a workload-centric security strategy



Avoid bottlenecks with automated host-based protection

What do you need?

Intrusion Detection & Prevention

DevOps friendly Security

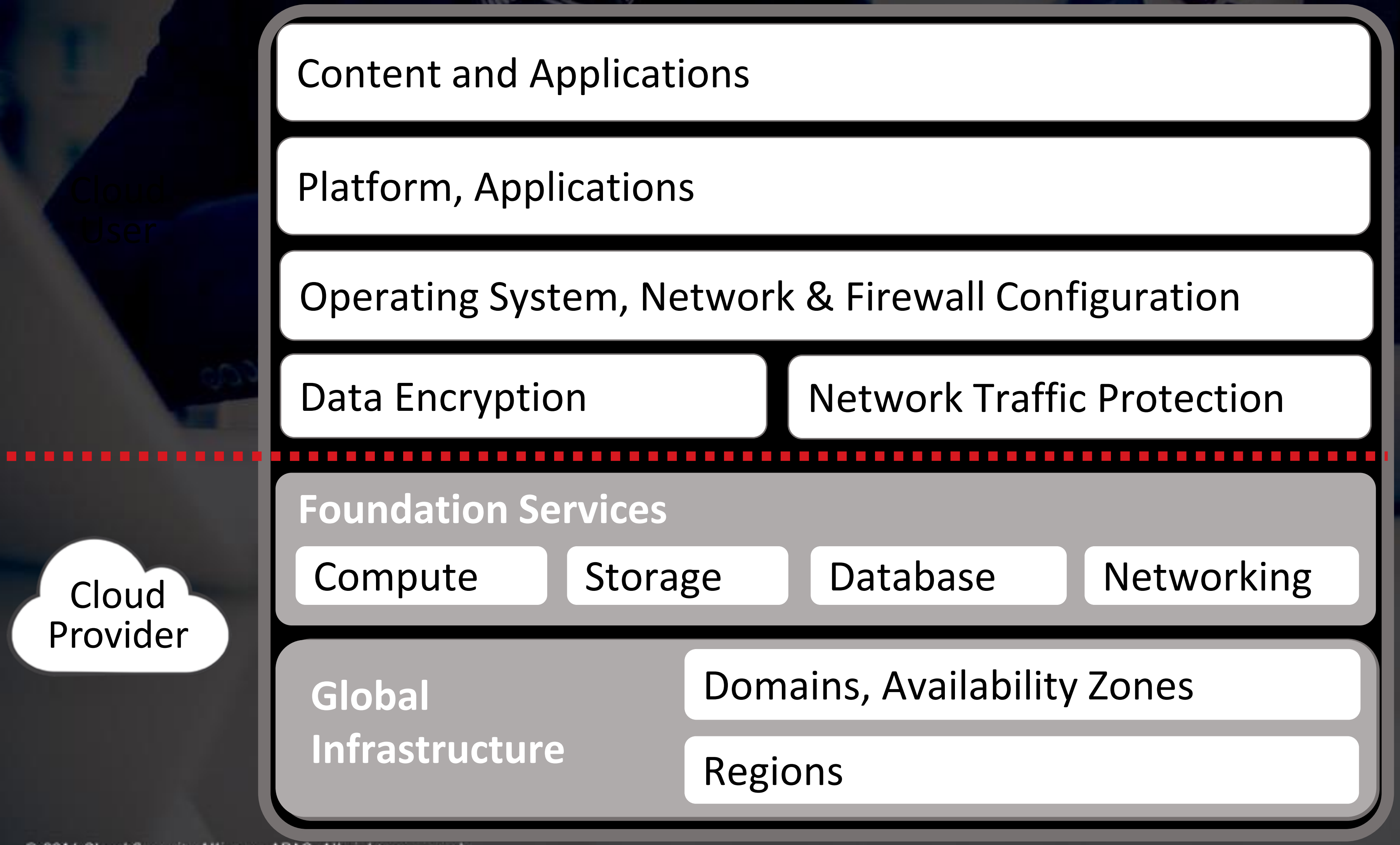
Actionable Insight

Advanced Security Functionality

Virtual Patching

All in a single, host-based tool

Cloud Security is a Shared Responsibility



Cloud User

Content and Applications

Platform, Applications

Operating System, Network & Firewall Configuration

Data Encryption

Network Traffic Protection

Cloud Provider

Foundation Services

Compute

Storage

Database

Networking

Global Infrastructure

Domains, Availability Zones

Regions

Cloud providers deliver a secure infrastructure.

But YOU need to protect what you put IN the cloud—your workloads.

Shared responsibility for compliance

Cloud Provider

- Facilities
- Physical security of hardware
- Network infrastructure
- Virtualization infrastructure

Cloud User

- File & System integrity monitoring
- Intrusion detection & prevention
- Firewall
- Anti-malware
- Vulnerability scanning & updating

PCI DSS compliance

PCI DSS Requirement	Responsibility
Install and maintain a firewall configuration to protect cardholder data	Shared
Do not use vendor-supplied defaults for passwords or other security parameters	Shared
Protect stored cardholder data	Shared
Encrypt transmission of cardholder data	User
use and regularly update anti-virus software	User
Develop and maintain secure systems and applications	Shared
Restrict access to cardholder data by business need to know	Shared
Assign a unique ID to each person with computer access	Shared
Restrict physical access to cardholder data	Cloud Provider
Track and monitor all access to network resources and cardholder data	Shared
Regularly test security systems and processes	Shared
Maintain a policy that addresses info security for all personnel	Shared

Center for Internet Security

SANS

SANS/CIS TOP 20 CRITICAL SECURITY CONTROLS

1. Inventory of Authorized & Unauthorized Devices	11. Secure Configurations for Network Devices
2. Inventory of Authorized & Unauthorized Software	12. Boundary Defense
3. Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations & Servers	13. Data Protection
4. Continuous Vulnerability Assessment & Remediation	14. Controlled Access Base on the Need to Know
5. Controlled Use of Administrative Privileges	15. Wireless Access Control
6. Maintenance, Monitoring & Analysis of Audit Logs	16. Account Monitoring & Control
7. Email and Web Browser Protections	17. Security Skills Assessment & Appropriate Training to Fill Gaps
8. Malware Defenses	18. Application Software Security
9. Limitation and Control of Network Ports, Protocols and Services	19. Incident Response Management
10. Data Recovery Capability	20. Penetration Tests & Red Team Exercises

Best Practices for Securing AWS Workloads*

- Understand Your Shared Responsibilities
- Get Visibility of Cloud-based Workloads
- Bake Security Into Workloads from Development
- Adopt a "No Patch" Strategy for Live Environments
- Use AWS Security Groups but Leverage a Third-Party Firewall for Advanced Functionality
- Adopt a Workload-Centric Security Strategy

* Source: Gartner research note – Best practices for securing workloads in Amazon Web Services, April 2015

What deployment option is best for you?

	Vendor As a Service	Azure Marketplace	AWS Marketplace	Software
Hourly pricing	Available			Not Available
Security data & traffic	in vendor’s VPC	SaaS	Stays in your VPC	Stays in your data center or VPC
Infrastructure Operations & Costs	Handled by vendor	Customer responsibility		
PCI DSS compliance	Not recommended		Built to help accelerate PCI DSS compliance	
Control manager	Run by vendor, security managed by customer		Customer runs in data center or VPC	
Security controls	All modules: Network (IPS, firewall), System (integrity monitoring, log inspection) & Anti-malware			
Instance-based protection	Yes			
Automation	API, scriptable, via the console			

Thank You

csahkm.org