OPTIV

Cloud-Powered with Greater Security

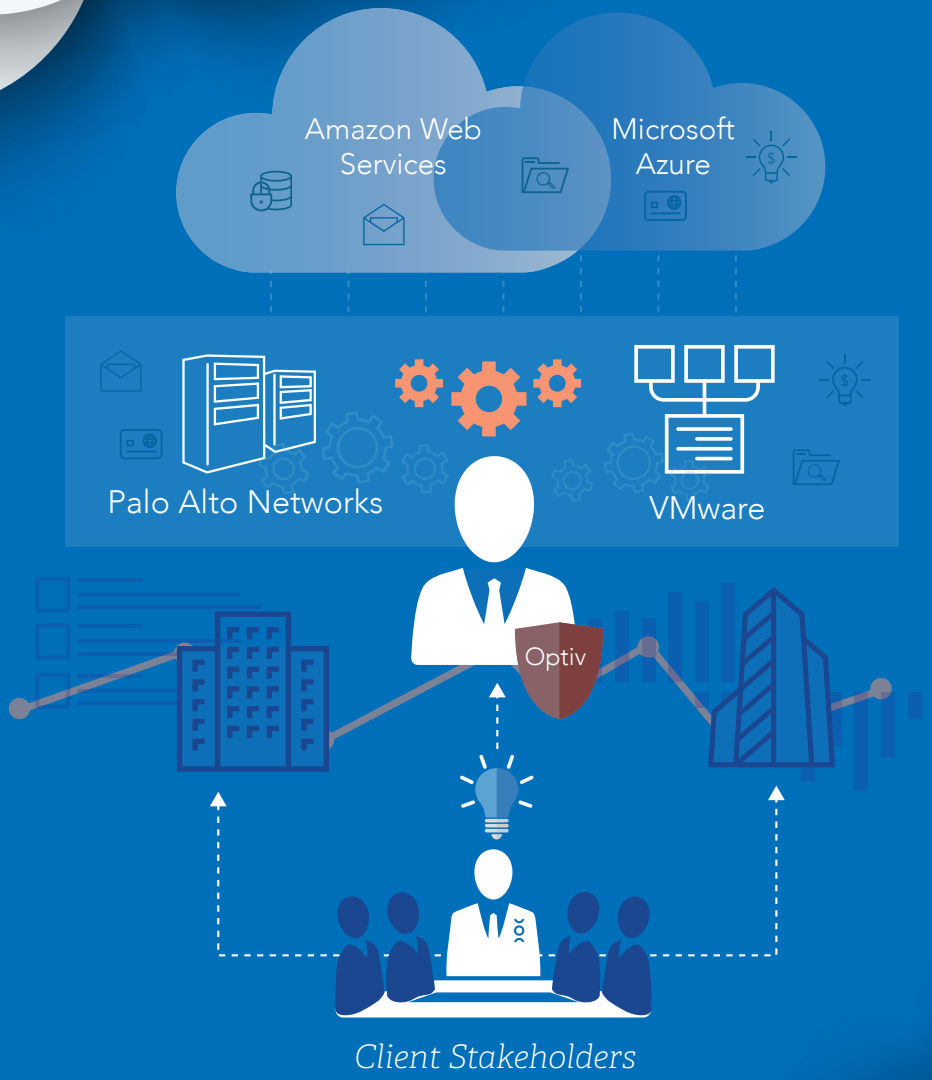
A Cyber Security Game Plan for Your Cloud

In collaboration with

paloalto NETWORKS

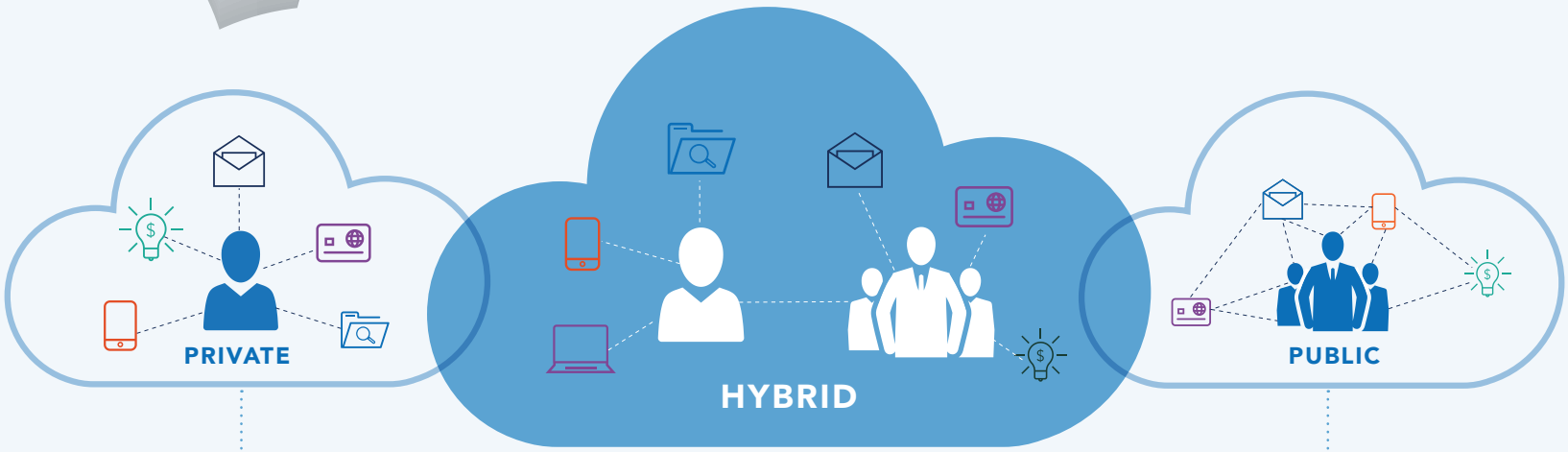
vmware

Mobilize your path to cloud with Optiv, Palo Alto Networks and VMware.



The rapid pace of application development and mastering data are major reasons companies are innovating and scaling their organization to reap the benefits of business agility and operational efficiencies.

The core drive for these technology trends is the cloud. Companies must embrace the cloud to achieve a sustainable competitive advantage. This could mean any one of three deployment models, but hybrid cloud appears to be the way forward. It provides companies with the benefits of the public cloud while allowing them to protect key assets on their private cloud.



- Single tenant implementation
- Owned and operated by IT organization
- Define your own data management and security policies
- Self-service and automation capabilities provide new agility

- Combination of private and one or more public clouds to maintain key infrastructure and data in private cloud while achieving the flexibility and scalability of the public cloud
- Allows IT organizations to become brokers of services

- Multi-tenant implementation
- Owned and operated by service providers such as Amazon Web Services (AWS) or Microsoft Azure
- Bound by multi-tenant data management policies
- Similar self-service and automation capabilities as private cloud

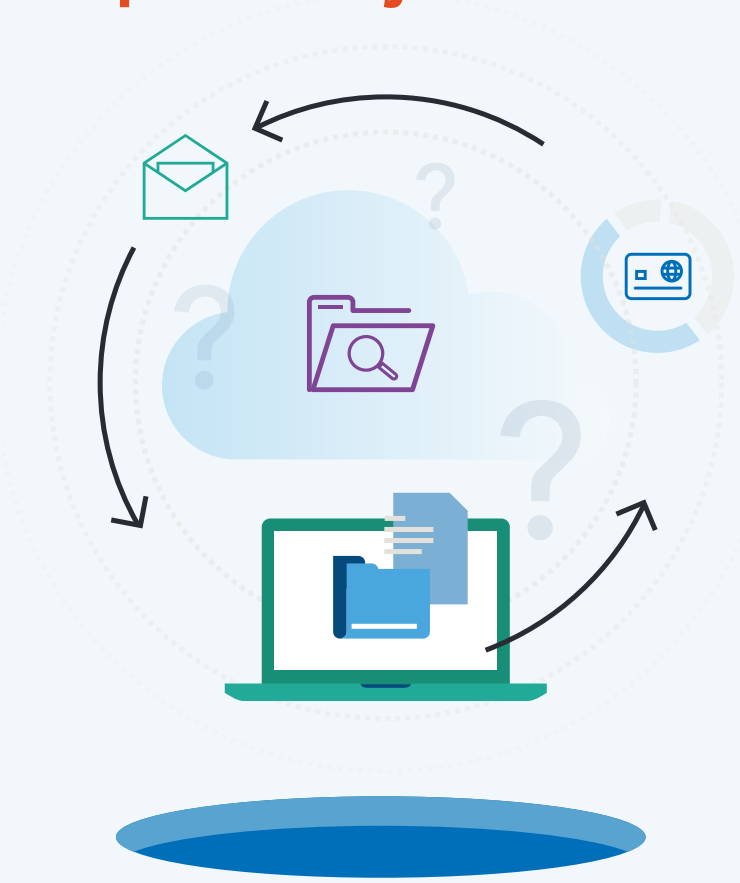
No matter the deployment method selected, every company faces the same dilemma: **securing its cloud**. Here are three of the most common pitfalls:

Pitfall #1
An unfortunate misconception that cloud service providers deliver embedded security measures that will protect the client's business.

Pitfall #2
Lack of visibility from executive-level stakeholders of sanctioned and unsanctioned cloud SaaS-based application services used by employees.

Pitfall #3
A belief by business stakeholders that they only have two options when protecting their business.

Uncertainty Over Shared Responsibility in the Cloud



Pitfall #1

An unfortunate misconception that cloud service providers deliver embedded security measures that will protect the client's business.

This cannot be further from the truth. A true enterprise cloud security solution will always require the knowledge and experience necessary in securing workloads wherever they reside.

Are you securing your assets properly in the cloud?

Lack of Visibility of Cloud Applications

Pitfall #2

Lack of visibility from executive-level stakeholders of sanctioned and unsanctioned cloud SaaS-based application services used by employees.

This gives rise to a weak cloud security program that is exposed to cyber attacks and data breaches. When it comes to where your data is located, being aware of what you don't know is half the battle. Cloud Access Security Brokers (CASB) can help identify the security risks in over 900 applications found in the enterprise that are both sanctioned and unsanctioned.

Do you know where ALL your applications are in the cloud?

Ambiguity in Securing the Cloud

Pitfall #3

A belief by business stakeholders that they only have two options when protecting their business.

The first option is to ignore security altogether at first, not because it's unnecessary, but because security policy deployment cannot keep pace with the rate of change within the cloud. The second option is to lift traditional security technologies that are port-bound into the cloud. Neither of these options addresses all the critical requirements needed to protect cloud environments. With a comprehensive assessment, you can identify all the risks and implement a cost effective security solution that meets the needs of every business unit without impacting agility or security.

Do you know all of the options for protecting your cloud?

With a well thought out plan, your organization can achieve a fully-realized cloud security program. **Key requirements for securing the cloud include:**

REQUIREMENT # 1

Understand your cloud security program maturity and desired state.

The evolution to the cloud has accelerated the need to think holistically about security up and down the supply chain. Core elements to implementing a fully-realized cloud security program include assessing the current program state, defining the desired outcome and building a roadmap for maturing capabilities.

Optiv's Cloud Security Architecture Program uses a programmatic approach with key stakeholders to assess the current state of the cloud security program and problems to resolve, define business drivers and achievable objectives, build a roadmap for maturing capabilities within an operational and actionable framework and provide metrics that monitor results.

REQUIREMENT # 2

Use consistent security in both physical and virtualized form factors.

Use the same levels of application control and threat prevention to protect both your cloud computing environment and your physical network.

Palo Alto Networks® enables greater security for your data center – be it physical or cloud-based – using a consistent set of next-generation firewall and advanced threat prevention features deployed in either a physical appliance or virtualized form factor. Native management tools help streamline policy deployment and eliminate the time gap between virtual workload deployment and security policy update, allowing you to operate at the speed of the cloud.

REQUIREMENT # 3

Extend visibility and granular control into SaaS applications wherever they are located.

To maintain the same level of security within the network as data flows to SaaS applications, you must attain visibility and granular control into these SaaS applications.

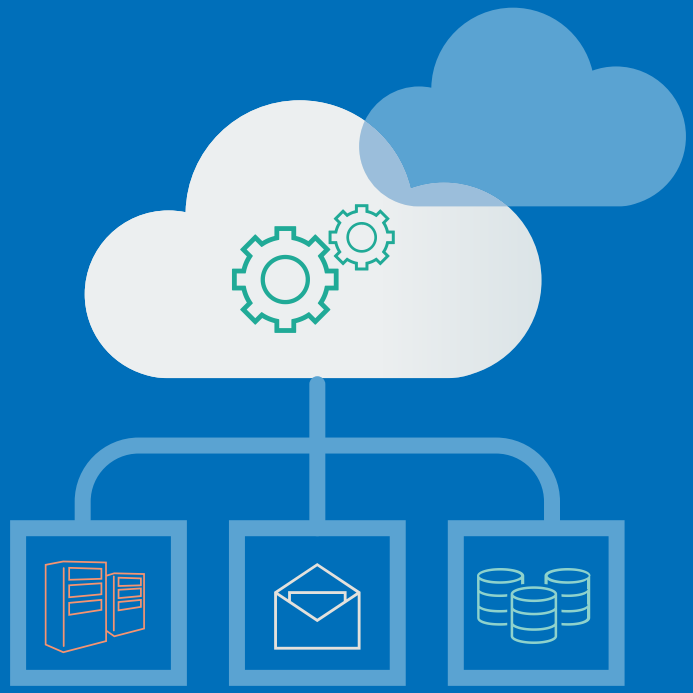
Palo Alto Networks Aperture extends the visibility and granular control of your security platform into SaaS applications themselves – an area traditionally invisible to IT. Aperture solves this problem by looking into SaaS applications directly, providing full visibility into the day-to-day activities of users and data. Granular controls help ensure policy is maintained to eliminate data exposure and threat risks.

REQUIREMENT # 4

Migrate network and security services into the virtualization layer.

Businesses that possess network architectures rooted in hardware can't match the speed or security of those running virtualized networking. By moving network and security services into the data center virtualization layer, network virtualization enables IT to create, snapshot, store, move, delete and restore entire application environments with the same simplicity and speed available when spinning up virtual machines. This, in turn, enables levels of security and efficiency that were previously not possible.

VMware NSX is the network virtualization platform of the software defined data center. It takes the functionality formerly embedded in network hardware – such as switching, routing and firewalling – and abstracts it to the hypervisor. The integration of virtualized security and distributed firewalling directly into the infrastructure enables micro-segmentation and granular security delivered to the individual workload.



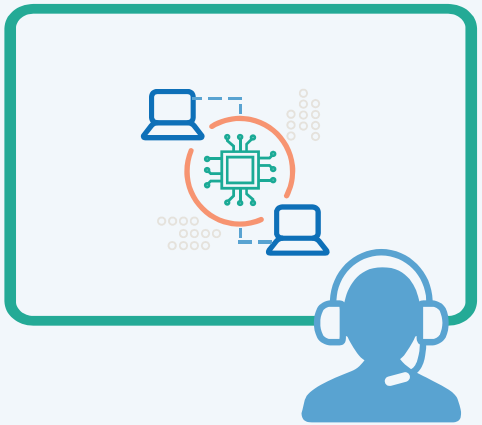
REQUIREMENT
5

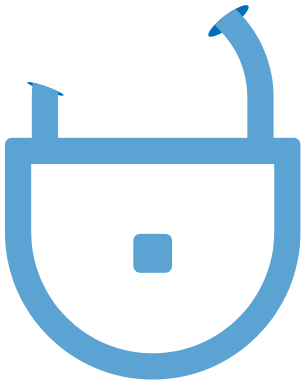
Centrally manage and automate security deployments.

Physical network security is still deployed in almost every organization, so it's critical that you have the ability to manage both hardware and virtual form factor deployments from a centralized location using the same management infrastructure and interface.

Palo Alto Networks Panorama™ network security management allows you to centrally manage all of your Palo Alto Networks next-generation firewalls, both physical and virtual form factor, ensuring policy consistency and cohesiveness. Using the same look and feel that the individual device management interface carries, Panorama eliminates any learning curve associated with switching from one user interface to another.

VMware NSX integrates directly with Panorama to extend the virtualized next-generation firewall from Palo Alto Networks automatically and transparently to every ESXi server. Context is shared between VMware NSX and Palo Alto Networks centralized management platform, enabling security teams to dynamically apply security policies to virtualized application creation and changes.





Optiv, along with our partners Palo Alto Networks and VMware, can help you migrate to the cloud so you can reap the full benefits of a cloud-powered business while minimizing security compromises.

Palo Alto Networks Experience

- Diamond Level Partner – Highest level and most certifications
- 107 ACE (Accredited Configuration Engineers) and 31 CNSE (Certified Network Security Engineers) on staff
- Over 150 Palo Alto Networks projects in 2015
- 2011-2016 Americas Partner of the Year
- 2016 Americas Excellence Award for Support
- 2016 Americas Professional Service Partner of the Year

VMware Experience

- NSX Elite Partner – Highest Level VMware NSX Partner
- 15 VCP-NV's on Staff
- Partner Professional Services Certified

Optiv delivers a comprehensive suite of solutions and services to help enterprise-class organizations plan, build and run effective cloud security programs.

We combine extensive research, specialized expertise and field experience with powerful partnerships with industry leaders like Palo Alto Networks and VMware to help you achieve your security objectives.

Ready to get started?

Visit optiv.com/solutions/cloud-security

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896 | **www.optiv.com**

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

1.17 | V1