HOW TO SECURE YOUR BUSINESS IN A MULTI-CLOUD WORLD

For many organizations, the cloud has become the sole route to market for new application deployment. It affords greater agility and scalability, higher performance, and faster access to innovative technologies, all of which help a business gain a competitive edge. As a result, data and applications now reside in a multitude of cloud environments, including private and public clouds, spanning infrastructure, platform and software as a service – IaaS, PaaS and SaaS, respectively.

According to Gartner, multi-cloud strategies will be common for 70 percent of enterprises by 2019.[1] Despite this momentum, several barriers still slow adoption, and security remains a top concern. Also, although native public cloud security controls provide some degree of access control and identity management, breaches are often the result of improper use, misconfigurations or advanced threats.

Confidently accelerating the move to the cloud requires consistent, automated protections across multi-cloud deployments that prevent data loss and business downtime. This brief highlights an innovative security approach that minimizes the wide range of cloud risks that can cause breaches, while enabling organizations to achieve consistent and frictionless cloud protections for multi-cloud environments.

Traditional Cloud Security Approaches Are Insufficient

There are several security options to choose from when moving to the cloud. However, the approaches widely used today have proven insufficient in providing the holistic view of the cloud required to detect and prevent advanced threats and data breaches.

Native Public Cloud Security

Cloud security is a shared responsibility between the cloud provider and the customer. In IaaS, customers are responsible for protecting their applications and data running within the public cloud, whereas in SaaS, they are responsible solely for the security of their data. To aid with protection, cloud service providers offer basic native security services, including access controls and data protection tools. However, the level of security doesn't meet the requirements of the enterprise and is limited to only that cloud provider. Because organizations tend to use a variety of clouds, encompassing IaaS, PaaS and SaaS, fragmented security and management overhead often result.

Point Products

Using multiple security tools from multiple vendors to solve for specific use cases results in a fragmented security environment in which IT teams must manually correlate data to implement actionable security protections. This level of human intervention increases the likelihood for human error, leaving organizations exposed to threats and data breaches. For example, although useful to mitigate risks within SaaS environments, cloud access security brokers, or CASBs, have become another point security tool to administer, prone to human error and featuring operational complexity as well as increased costs that negatively impact IT administration overhead.

Legacy Network and Content Security

Security vendors today claim to offer the level of protection required to secure your cloud environments. However, what they refer to is often a virtualized instance of hardware placed in the public cloud. This approach is not truly cloud-integrated security, negating the on-demand nature of the cloud and agility benefits. Plus, it lacks the automation required to enable consistent, frictionless security across your entire multi-cloud environment.

Figure 1: Securing multi-cloud environments

What's Needed to Secure Multi-Cloud Environments?

Ideally, cloud security should speed application development and business growth while preventing data loss and business downtime. This requires three key capabilities: advanced application and data breach prevention, consistent protection across locations and clouds, and "frictionless" deployment and management.

To eliminate business disruption, organizations must protect their cloud assets. With today's sophisticated attacks, advanced enterprise-grade security is the only way to prevent successful breaches. More importantly, security capabilities must be delivered consistently across multi-cloud environments – private clouds, IaaS, PaaS and SaaS – in a frictionless manner, with minimal impact on the development lifecycle.

IaaS and PaaS Security Requirements

Initially, when organizations transitioned to the cloud, they virtualized their enterprise applications directly, using only the foundational IaaS components – compute, network and storage. Over time, applications were built to leverage cloud efficiencies. Now, applications consume multiple components from IaaS and PaaS services (see Figure 2). PaaS offerings significantly reduce development time and allow apps to scale efficiently based on demand.

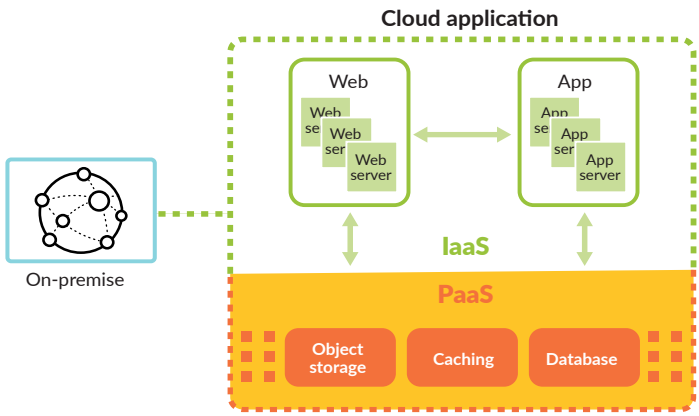

Figure 2: App development in IaaS and PaaS

To provide the enterprise-level security required for applications within IaaS and PaaS environments, a multi-dimensional approach is needed, including in-line, API-based and host-based protection components (see Figure 3).

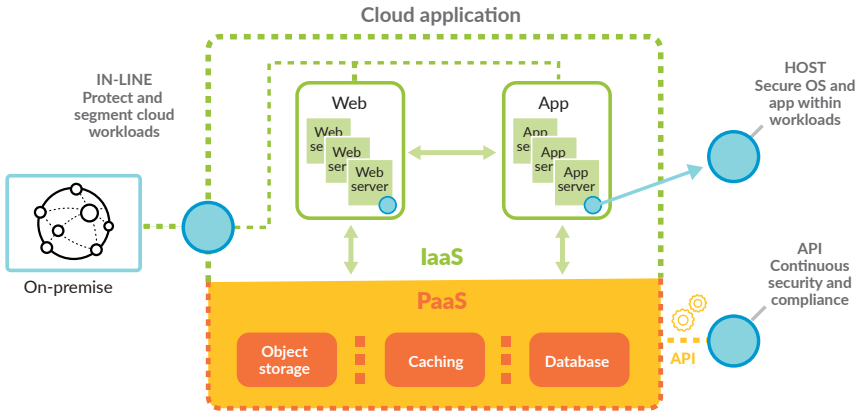

Figure 3: Critical cloud protections for IaaS and PaaS

- **In-line:** Protect and segment cloud workloads to safeguard against internal and external threats. By investigating communications in your cloud environment, you'll gain application-level visibility into north-south traffic flowing in and out of your cloud environment as well as east-west traffic between workloads. Segmentation policies ensure appropriate levels of interaction between various cloud workloads, such as web applications and database workloads.
- **API-based:** Provide continuous discovery and monitoring, data security and compliance reporting. The API-based approach is transparent to developers and enables security teams to discover and monitor cloud resources and assets for any suspicious activity; secure storage services by preventing misconfigurations; and comply with industry standards, such as CIS, ISO and SOC 2, as well as regulations, such as GDPR, HIPAA, PCI DSS and NIST; with customizable reports and controls.
- **Host-based:** Secure the operating system and applications within workloads. A lightweight host agent deployed within the cloud instance detects any zero-day exploits and ensures the integrity of the operating system and applications. As attackers uncover vulnerabilities, the agent-based approach can provide protection until organizations are able to patch components.

To provide a consistent, "frictionless" security posture throughout the multi-cloud infrastructure, security should essentially become part of the development process through automation. Developers do not need to be security experts so long as automated, consistent protections can be inserted into the environment. In addition, it's critical to understand that security requirements for IaaS and PaaS must be delivered through a consistent security posture that supports applications and data across the three major cloud service platforms: Amazon® Web Services, Microsoft® Azure® and Google® Cloud Platform.

SaaS Security Requirements

Easy to set up and use for collaboration, SaaS applications have changed the way organizations do business. They've also introduced new security risks in the process, including malware propagation and sensitive data exposure, often resulting from uncontrolled SaaS application usage. The push to address these security gaps led to the creation of the CASB category.

The following are the deployment modes by which to deliver CASB functions, along with additional recommendations to ensure comprehensive security for your SaaS applications and data:

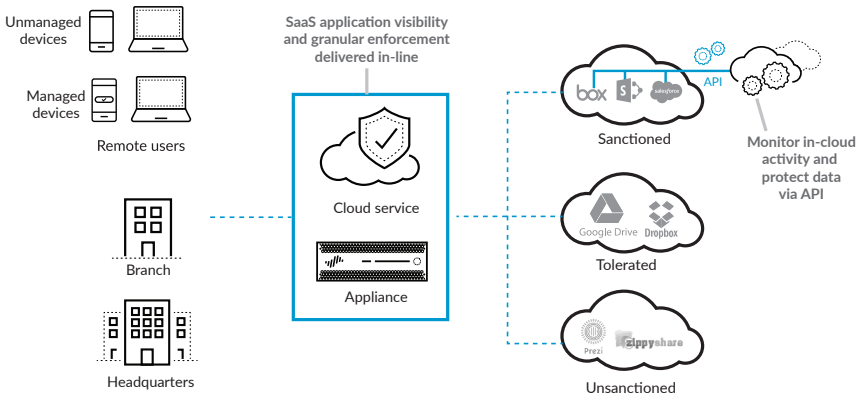

Figure 4: SaaS approach

- **In-line deployment** provides SaaS application visibility and control. When delivered as a cloud service, you can reduce the deployment complexity and cost of managing global infrastructure. Through in-line protection provided by hardware appliances or as a cloud service, organizations can prevent exfiltration of sensitive data across all cloud applications. Understand SaaS usage across your users, and build policy to control your risk exposure accordingly.
- **API deployment** provides deeper protections for sanctioned, enterprise-approved applications and performs several CASB functions, including granular data security inspection on all data at rest in the cloud application or service, as well as ongoing monitoring of user activity and administrative configurations.

In the same way IaaS and PaaS cloud components must be secured, SaaS applications, such as Box, Dropbox®, GitHub®, Google Drive and Salesforce®, must also be protected with a consistent security posture, regardless of application and cloud provider.

Securing Private Clouds

Organizations are rapidly embracing multi-cloud architectures, not only inclusive of the public cloud. Many organizations will continue to support on-premise applications within traditional data centers or private clouds. Protecting these data centers requires a comprehensive, consistent security strategy. Additional information is available at https://www.paloaltonetworks.com/solutions/initiatives/private-cloud.

Use Collective Intelligence to Prevent Threats

Consistent security across your multi-cloud environment is essential to the growth and productivity of your business. The only way to achieve this is through continuous, coordinated sharing of threat information across an integrated security platform. Beyond securing your multi-cloud environment, a comprehensive security platform spans the network and endpoints as well. These security mechanisms – in clouds, networks and endpoints – essentially act as sensor and enforcement points, working together to arm your business with the collective intelligence required to prevent successful cyberattacks.

Visit our cloud security page to learn more: https://www.paloaltonetworks.com/products/secure-the-cloud.

1 Gartner: The Future of the Data Center in the Cloud Era, David J. Cappuccio, 19 June 2015

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

how-to-secure-your-business-in a-multi-cloud-world-wp-050818