TechTarget | Custom Media
White Paper

Comprehensive Security for AWS in Hybrid Cloud Deployments

Every research study tells us hybrid cloud is the future of IT infrastructure. However, securing workloads, containers, and instances in a hybrid cloud environment demands an updated security design, beyond what legacy approaches can offer. Many aspects of the legacy approach are a poor match for the dynamism, agility, and speed of the cloud. For example, many older security models are too monolithic and rigid to operate at speed or scale. In many cases, security deployment isn't integrated with cloud services, resulting in unprotected or vulnerable instances. Compliance requirements are another element that is overlooked. Furthermore, bolting security onto hybrid cloud environments severely limits visibility, making end-to-end visibility impossible, which leads to several problems.

For all these reasons, organizations that want to safely enable the hybrid cloud need cloud native security. The foundation of cloud native security is the integration of the security platform with the cloud services. This architecture ensures process fit across cloud services so nothing is overlooked or missed as IT utilizes the dynamic nature of the cloud. Cloud native integration ensures both consistent deployment of security tools for each cloud service instance and consistent security policy implementation. The same is true for compliance and governance policies. Further, with visibility across an integrated security stack, enhanced protections for workloads, containers, and instances are assured. A full-lifecycle approach eliminates potential blind spots and vulnerabilities. However, the biggest gain a cloud native approach offers for IT may be the operational simplicity that this fundamental integration provides every day.

Another key component to enabling a secure hybrid cloud is ensuring scalability and agility. A cloud native solution will simplify the entire protection process, supporting security at scale. One of the most important benefits of a modern approach to development is that "time to market" is reduced, providing faster deployment of solutions. With a cloud native and integrated approach to security, protection is always on, reducing vulnerable windows or unprotected instances. With automated solutions, these two benefits can be gained without constant intervention or interruption to the IT or security teams.

Joint AWS and Palo Alto Networks Solution for Secure Hybrid Cloud

Palo Alto Networks and Amazon Web Services (AWS®) have worked closely in partnership for many years, focusing on eliminating common problems for using cloud services. This new joint solution integrates the AWS Outposts™ hybrid cloud solution with two fundamental Palo Alto Networks solutions: Prisma® Cloud, the cloud native security platform, and VM-Series Virtual Next-Generation Firewalls (NGFWs) for inline threat prevention and network security. This comprehensive set of integrations provides a secure platform that delivers all the benefits of hybrid cloud and cloud native security, delivering both cloud and on-premises infrastructure that automatically protects new workloads or instances.

Integration of AWS Outposts and VM-Series Virtual NGFW

The integration of AWS Outposts for running AWS cloud on-premises with the VM-Series NGFWs provides a single network security solution for all AWS instances across cloud and on-premises environments. This offering delivers both inline threat prevention and network security to protect outbound, inbound, and east-west traffic, regardless of physical location. In addition, this integration aligns the network security posture with AWS to simplify operations and better support cloud agility. With this new joint approach, protection is improved.

Integration of AWS Outposts and Prisma Cloud

The integration of AWS Outposts and Prisma Cloud ensures cloud security posture management (CSPM) is consistent across the entire hybrid cloud infrastructure. Using a single integrated solution provides comprehensive visibility across cloud and on-premises infrastructure in a single pane of glass. This is vitally important for providing effective protection. The use of a comprehensive platform makes visibility, compliance, and governance much simpler. The single solution protects several different environments, such as containers, hosts, and serverless instances, and provides a simpler path for deploying DevSecOps methodologies.

Benefits to Customers from This Joint Solution

Many organizations find moving to a hybrid cloud model increases complexity instead of reducing it. Transferring products and services formerly supported by legacy IT processes to a dynamic hybrid cloud environment is a mismatch. Security approaches that require too much manual intervention, call for synchronizing and organizing many different products, or have visibility into only specific infrastructure segments tend to both restrict and complicate hybrid cloud environments. Put simply, legacy security processes cannot match the dynamism and agility of the hybrid cloud. Prisma Cloud is purpose-built to solve this problem by delivering several important benefits to customers:

1. Improved Efficiency Through Simplified Operations

Complexity not only wastes resources, but also results in more mistakes as elements are missed or overlooked. The ability to extend a single policy model across cloud and on-premises infrastructure is powerful. Monitoring with a single security platform instead of many point solutions also reduces alerts and alert fatigue. Automated issue prioritization highlights the most important alerts. This simplification across the full application lifecycle makes it easy for developers to find issues early in development, rather than later in production at a greater cost. The solution delivers runtime defense and network-based threat prevention as well. Lastly, the elimination of "unicorn" products in your development lifecycle means IT and security teams do not require expertise to operate several different security products.

2. Support for Secure and Simplified Auto Scaling

The adoption of this joint AWS and Palo Alto Networks solution supports and enables secure and agile auto scaling for the hybrid cloud. The integration simplifies protection when adding or removing compute, storage, and network services to meet workload demands. Ensuring that any new resources or instances are fully protected without having to manually check or add protection speeds up operations and removes the chance of oversight or errors creating vulnerabilities.

3. Improved Security with More Visibility Across the Hybrid Cloud

Securing and managing IT infrastructure often comes down to a simple maxim: "If it isn't visible, it isn't protected." Hybrid clouds can be a challenge for visibility since some implementations result in silos. The AWS and Palo Alto Networks security integration solves the hybrid visibility problem by discovering and protecting all cloud assets and resources across the lifecycle, using automation to reduce the load on both IT and security operations. In addition, the protection across the entire lifecycle (build/deploy/run) results in less operational risk and fewer issues for more rapid innovation. Cloud native integration also makes it possible to provide complete telemetry and timelines across the entire stack to support improved threat analysis and forensics. Finally, correlated visibility across clouds and across all application traffic, whether packaged or custom apps, makes it possible to protect all apps better.

4. Simplification of Governance and Compliance

Supporting the demands of governance and compliance has become a critical task for IT. However, with fragmented hybrid infrastructures, ensuring that all directives are met is challenging. Errors and misconfigurations are possible without any awareness of them. The AWS and Palo Alto Networks joint offering solves these problems with integrated cloud native visibility, compliance, and governance. The joint hybrid infrastructure platform offers simple one-click reporting, automated and consistent protection, and pre-built cloud policies that can also be deployed with a single click. This gives IT and security professionals the confidence that any statements or attestations of compliance or governance are accurate and true.

Key Takeaways

The joint AWS and Palo Alto Networks solution for delivering agile, secure, and compliant hybrid cloud infrastructure represents a huge step forward for simplified hybrid cloud security. With security and cloud services combined into a single logical entity consistent across the organization and clouds, IT teams can achieve the agility and scalability they want with comprehensive vulnerability management and runtime protection, yet without dedicating huge amounts of resources or expertise. More importantly, this joint offering improves time to market, provides greater operational efficiency for cloud delivery, and automates the meeting of compliance and governance demands.

This comprehensive cloud security platform has been created with the goal of meeting both current and future challenges in hybrid cloud security. For more information about this solution, please visit Palo Alto Networks online.

paloalto NETWORKS

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

This content was commissioned by Palo Alto Networks and produced by TechTarget Inc.