tripwire

Best Practice Guide for Multi-Cloud Security

Advanced Vulnerability Management with Tripwire IP360

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

When you opt to use multiple cloud providers, you're implementing a multi-cloud strategy. This practice is increasingly common, and can refer to mixing SaaS (software as a service) and PaaS (platform as a service) offerings as well as public cloud environments that fall under the IaaS (infrastructure as a service) category. The most common public cloud environments today are Amazon Web Services (AWS), Microsoft Azure and Google Cloud.

Security professionals responsible for securing multi-cloud environments are often stuck trying to apply the old principles of vulnerability management (VM) to these new environments with varying success. The truth is, multi-cloud environments require special consideration when deploying VM tools.

This best practice guide outlines the methods of deploying and using Tripwire® IP360™ in a multi-cloud environment with public cloud providers.

Multi-Cloud Benefits and Challenges

Organizations and agencies have an unprecedented range of options for data storage. You can manage your data on-premises, fully in the cloud, or in a hybrid environment wherein both on-premises and cloud computing are used. A multi-cloud strategy doesn't mean you have to do away with your on-premises or hybrid cloud setup, either; you can have both a hybrid and multi-cloud approach at once. There are a number of reasons a multi-cloud strategy is becoming more popular:

» Multi-cloud approaches reduce reliance on a single vendor, also known as "vendor lock-in."

» This also mitigates fears of data loss or downtime if there's an issue in any one environment.

» Multi-cloud strategies allow you to take advantage of the perks of several providers at once.

In addition to the benefits, multi-cloud strategies do create additional challenges as well:

» It can be difficult to assess where to allot your resources for maximum ROI.

» It's harder to stay compliant with regulatory standards while operating in multiple clouds.

» Most organizations lack the necessary tools to run successful multi-cloud vulnerability management.

Vulnerability Management Basics

Cyber attacks generally exploit known vulnerabilities. The way to make sure that you know about your system's vulnerabilities before your adversaries do is the practice of vulnerability management.

80% of IT decision-makers say new approaches are needed to successfully operate in multi-cloud environments.

— What the New Multi-Cloud World Means to IT, BMC infographic

Scanning

Vulnerability management functions by way of continuous, scheduled scanning. These scans can pick up known vulnerabilities, misconfigured assets, uninventoried endpoints, slips in compliance and many other network instances that hackers see as an invitation.

Scanning can be performed via agent-based or agentless methods—and there are pros and cons to both approaches. Agents can provide access to environments, including some cloud environments, where remote network scanning is difficult or prohibited. They also reduce the requirement to maintain and track endpoint credentials required for agentless scanning, and may provide better tracking in a dynamic IP environment. Agentless scans can also identify information that isn't stored on network devices, like SSL certificates. However, it's not a matter of choosing one over the other. The strongest vulnerability management strategy will employ both types of vulnerability assessment.

In a multi-cloud environment, you'll want a solution that builds agents into the deployment pipeline for virtual images. That means a robust vulnerability management solution will already be present when an image spins up, to feed scan results back to your device profiler.

Prioritization

Once your scanning operations flag vulnerabilities and provide vulnerability risk assessments, how do you take action? It's crucial that your vulnerability management solution delivers your scan results in order of priority so you know which vulnerabilities to tackle first.

Tripwire IP360 in Multi-cloud Environments

Tripwire IP360 not only provides comprehensive asset discovery, inventory and prioritization—it also does so across your entire multi-cloud environment. That means you can stay within regulatory compliance and maintain a stringent cybersecurity posture no matter how many public cloud vendors you're using at once. Tripwire IP360 virtual appliances can be deployed in AWS, Azure and Google Cloud.

Tripwire VnE Manager

Regardless of your type of cloud environment and your decisions around agentless or agent-based vulnerability management scans, the information you collect will end up on your Tripwire® VnE Manager. This is the centralized management appliance that utilizes a fully-hardened Linux-based operating system, strong encryption for communications and frequent system and vulnerability signature updates provided by Tripwire VERT (Vulnerability and Exposure Research Team). Tripwire VnE Manager is optimized for asset discovery, vulnerability scanning and reporting for fast, easy and cost-effective deployment.

How Tripwire Device Profilers work in multi-cloud environments

You can deploy Tripwire's scan engine, the Tripwire Device Profiler (DP), in each type of cloud environment discussed above. Tripwire DPs can perform both agentless or agent-based scanning.

The Rise of Multi-Cloud Computing

According to a 2017 Cloudify survey, 50 percent of organizations already have more than one IaaS vendor in play. A similar survey by Enterprise Management Associates puts that number at 61 percent, with 35 percent of organizations using four or more public clouds at once.

Generally, you can't have a scan engine scanning from one cloud into another—Tripwire DPs generate a lot of outbound traffic that can look like an attack when transmitted from one cloud environment to another. With Tripwire technology designed for multi-cloud environments, DP virtual images collect data and route it back your VnE Manager.

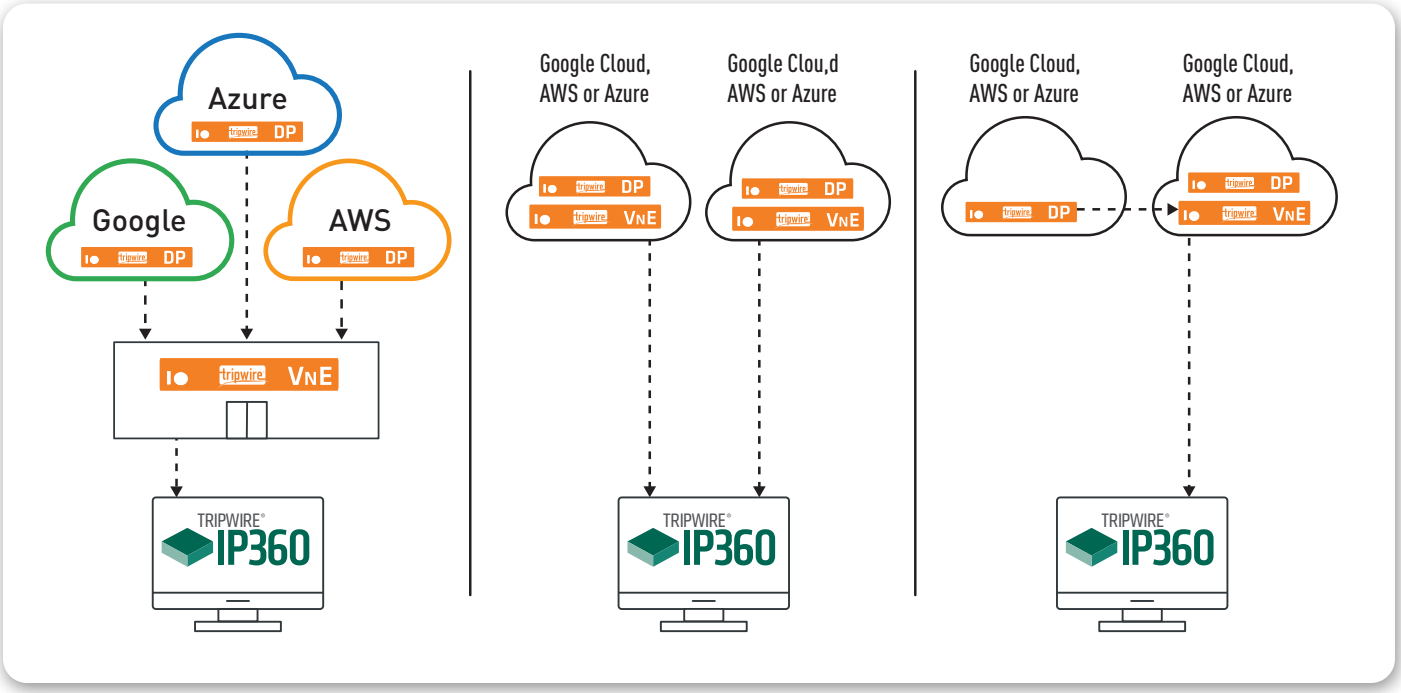

Fig. 1 Regardless of which services you use, Tripwire provides flexible multi-cloud deployment options for VnE Managers and Device Profilers.

Eight Steps to a Successful Multi-Cloud Deployment

When you're ready to leverage the benefits of a multi-cloud approach with Tripwire IP360's powerful vulnerability management, follow these best practice steps to get started:

1. Review the concept of the shared security model in the cloud with your business partners to make sure they understand the benefits and risks of moving to the cloud. Reinforce that VM and security controls are an essential part of a cloud strategy.
2. Inventory which cloud environments are being used or planned by your organization and choose your cloud vendors.
3. Understand the accounts and deployment zones where you need visibility to monitor for vulnerabilities. Deploy Tripwire DP scanning resources to get the needed coverage.
4. Understand the nature of the application in the cloud. Server replacement IaaS may be a good fit for network scanning. Highly dynamic environments will need agents or integration with the cloud tools.
5. Decide where you want to collect this info in the VnE Manager—on-prem, in one of the cloud environments, or one for each cloud environment.
6. Enable remote scanning Tripwire DP virtual images in your public cloud environments.
7. Regularly review the results from your cloud assessments and follow remediation instructions.
8. Assess the security of your cloud services with a tool like Tripwire Configuration Manager.

Summary

Multi-cloud environments call for sophisticated vulnerability management solutions. Whether your organization or agency uses on-premises, cloud or hybrid systems, Tripwire IP360 provides comprehensive asset discovery and inventory. Take advantage of the most granular risk scoring and prioritization reporting on the market in order to address vulnerabilities quickly and thoroughly.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

BRMCSBPG2a 2112