tripwire

SOLUTION BRIEF

Smarter Cloud Infrastructure Security

Vulnerability and Configuration Management with Tripwire

"Cloud environments are inherently shared environments. This simple fact makes system hardening and rigorous access control especially important in the cloud. If you are using Amazon Web Services, you must make sure your cloud assets are compliant with the Center for Internet Security's AWS Foundations Benchmark."

— Matt Williams, Tripwire Technical Product Manager

The trend of mass migration to the cloud brings benefits like lower operating costs, easier deployability, and the flexibility of an elastic environment. However, it's crucial to understand that the responsibility to secure your cloud infrastructure still falls on your organization.

Cloud providers allow organizations to take advantage of their infrastructure, resulting in a shared model for security. As tempting as it is to leave security up to your provider, cloud security is a shared responsibility. The line of responsibility is clearly drawn out within the SOC2 report of each cloud provider.

Keeping Up with the Hybrid Cloud

While a hybrid approach offers the best of both worlds, organizations must determine their data's security state while juggling regulatory compliance demands and issues around visibility within the public cloud. The same security and compliance requirements for on-premise assets are required for assets managed in the cloud. To complicate matters further, security teams must figure out what their cloud providers' built-in security covers—and where they need to pick up the slack.

Security techniques haven't evolved fast enough to keep up with the speed and demand of cloud providers like AWS, Azure, and Google Cloud Platform (GCP). Basic security principles remain the same, but their application is different in this faced-paced environment. There are two main services consumed by organizations from these cloud providers: infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS). While there are some security services built into these, the responsibility for

managing configuration and vulnerability risks falls on the customer.

While there are some vendors who handle security in the cloud, very few can monitor multi-cloud, on-premise and hybrid environments. Whether your organization chooses to consume IaaS or PaaS from one or more cloud vendors, Tripwire is uniquely positioned to help secure your organization.

Take Control of the Migration Process

As you move your development from traditional on-premise data centers to a hybrid or cloud-only system, you need to figure out how to ensure this migration is done right. But only 21 percent of organizations include security teams in the cloud provider selection process, according to the Ponemon Institute.[1]

To get back in the driver's seat and secure your cloud migration, use Tripwire solutions to verify that the infrastructure being deployed in the cloud is done so in accordance with your organization's risk posture and security hardening guidelines. Cybersecurity challenges are different in the cloud, and the best way to overcome them is to apply basic security controls with an automated zero trust model.

Tripwire Axon with Full Automation

Tripwire Axon® is a multiservice, scalable, high-performance data collection platform. It was designed to solve the challenges associated with accurate and complete security and compliance visibility across a broad range of systems. It optimizes the collection, aggregation and application of data, and enables users to collect endpoint data once and reuse it across multiple security and compliance controls.

Tripwire Axon agents can be installed using your provisioning tool—such as Puppet, Chef or Ansible—of choice. When alive, they call home (the console) to self-register and determine what needs to be checked. They then run these checks and provide feedback to the console for analysis. The console can then send an action to either pass/continue, fail/restart, or alert an administrator so that an appropriate response is taken.

Monitoring Infrastructure-as-a-Service (IaaS)

Organizations shifting their infrastructure to the cloud need to ensure that virtual images are configured according to their organization's hardening guidelines and that their IaaS doesn't introduce an unacceptable level of vulnerability risk. Tripwire allows customers to check the risk posture of each image as it comes alive by deploying the Tripwire Axon® platform on each cloud image. Tripwire Axon agents can be deployed autonomously using your deployment tool of choice. Once the images comes alive, the agents self-register and test themselves for vulnerability and configuration compliance risk. This risk is then reported to the security team in the same interface as the on-premise assets, giving the security team a single pane of glass to the risk. If the images are persistent, subsequent assessments can be triggered by a change or after a certain amount of time.

Monitoring Platform-as-a-Service (PaaS)

Instead of deploying infrastructure in the cloud, some development teams choose to use various PaaS offerings to build their applications. Tripwire Cloud Management Assessor, an extension to Tripwire Enterprise, allows you to view the consoles experiencing change within your hybrid cloud environment. Through its clear and simple dashboard, you can drill down deeper for detailed change context. It can also show you how aligned your hybrid cloud is with the CIS Controls. Deep reporting shows pass/fail results for CIS benchmarks. View your failures list to get easy step-by-step remediation instructions.

Bringing Change Management to the Cloud

While the operational process should deploy each fresh image correctly, they should still be verified. As infrastructure is deployed in the cloud, Tripwire solutions can verify the configuration of the images as well as ensure that the vulnerability risk is at an acceptable level. If the image remains persistent in the cloud, Tripwire Enterprise can also monitor for changes, as changes on images should happen further left in the pipeline, not in production. Therefore, when a change is detected, Tripwire Enterprise can send a message to deprovision and spin up a new image, or, depending on the severity of the change and use case of the image, an alert can be sent to the appropriate team.

While monitoring the configuration of the cloud account or platform in use,

Tripwire Enterprise can either alert or take an action if a change is detected. Using APIs, an automated process can take place depending on the severity of the change detected. For example, if a storage blob or bucket becomes open to the public, a high-severity incident process can be initiated.

Using a Zero Trust Model

This guidance should be considered from within a zero trust model, meaning that user access should be highly limited. The only account that should be making changes is the provisioning tool. Additionally, organizations should consider automating many facets of their model in order to improve efficacy. So how can organizations meet these cloud security best practices?

Fortunately, this is where dedicated security solutions can help. Cloud-fluent security solutions can be deployed in a zero trust model to dynamically tell you how a system is configured, what the vulnerability risk is, and if something changed that shouldn't have—all of this without manual user intervention.

Schedule Your Demo Today

Let us take you through a demo of Tripwire cybersecurity solutions and answer any of your questions. Visit **tripwire.com/contact/request-demo**

"Cloud service providers allow customers to build complex private network environments suitable for processing even the most sensitive data. The confidentiality of this data rests on security controls, unlike those commonly used on-prem, and a slight mistake can ultimately expose this sensitive data to the public Internet. Network administrators need to keep a close eye on the external view of all IP space allocated for their cloud. Vulnerability scanners like Tripwire IP360™ make it easy to recognize exposed services and close them up before attackers can exploit them."

— Craig Young, Tripwire Vulnerability and Exposures Research Team (VERT)

Sources

1 https://techbeacon.com/data-security-hybrid-it-top-challenges-how-tackle-them

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

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

SBSCI1a 1903