SOLUTION BRIEF

Monitoring Ephemeral Assets in the Dynamic Cloud

Simplify Asset Management and Improve Security with Tripwire Enterprise

Highlights

Monitoring for change in a dynamic cloud environment can be extremely difficult. Tripwire Enterprise simplifies the management of ephemeral assets in a variety of cloud environments with automated scanning, on- and off-boarding, dynamic waivers, and more.

In the cloud, flexibility is key. A major driver of cloud infrastructure adoption is the degree to which it can elastically scale with usage needs as they fluctuate from one day to the next. Sharing security responsibilities with the cloud provider can also relieve some of the burdens of busy security teams. But for all the merits of cloud infrastructure's flexibility, it also means compliance and security processes have to keep up.

Tripwire® Enterprise makes this possible. Beyond enforcing security configuration management (SCM) controls across your on-premises and public, private, and multi-cloud infrastructures, it applies special automated techniques to accommodate the short lifecycle of ephemeral assets. It does this by initiating configuration scans on these assets as they appear, conducting automatic on- and off-boarding to keep systems orderly and compliant, and by issuing dynamic waivers as needed to ensure peak operational availability.

The Need for Ephemeral Asset Security

In addition to elastic assets, which continually grow and shrink in number, ephemeral assets are those that exist for a short window of time to execute a specific task. For example, file systems act as ephemeral assets that come and go as dictated by Kubernetes workloads. Ephemeral assets can be spun up and down to manage containers or other aspects of the cloud computing load.

It may seem like the speed at which ephemeral assets come and go would make it less critical to ensure each one was deployed in a secure and compliant way.

There are two main reasons why this is false:

1. Ephemeral assets add up quickly: Assets that are only briefly used can still easily accumulate. This unassuming digital clutter can hide a potential compliance issue or attack vector.
2. They can enlarge the attack surface: A misconfigured base image will create an ever-expanding attack surface when identical copies are launched into your cloud environment.

Security teams need to fortify cloud infrastructures for effective security, continuous compliance, and reliable IT operations—even when assets dynamically come and go at a rapid pace. Tripwire Enterprise ensures the secure configuration and integrity of ephemeral assets with automated on- and off-boarding you can rely on.

How Tripwire Manages Dynamic Infrastructure

Tripwire Enterprise sets the standard for SCM, ensuring configurations are appropriately set so that they don't defy a mandated compliance policy or create opportunities for cybercriminals. For traditional on-prem assets, it schedules scans at regular intervals. Ephemeral assets can't be scanned in this manner, as their entire existence may take place between scans.

For this reason, Tripwire Enterprise automatically scans these assets immediately upon their deployment. When an ephemeral asset spins up, it initiates these automatic scans in addition to its regularly-scheduled cadence. This process applies to your organization's entire cloud infrastructure.

Automated Onboarding

Increases in resource demand within cloud environments can lead to large spikes in the number of new ephemeral assets to monitor. One common instance of this is when updated systems are deployed to take the place of existing infrastructure or when failure states trigger new builds. Rolling updates are a great way to maintain a consistent, immutable infrastructure while staying on top of new patches and installed package updates. Or if automation in your environment responds to an unwanted change or newly discovered vulnerability by triggering a new build, you can also see a large influx of assets spinning up.

As large numbers of new assets come online to take over for the systems that are being decommissioned, it is important to know that everything is being rolled out with a secure configuration. Capturing the secure baseline of critical files is a necessary step to detecting and remediating misconfigurations as they occur. The short-lived assets that spin up at times like these can be hard to catch and scan before they spin back down. Scheduled scanning alone will not be able to ensure that such assets are monitored at all.

The automated onboarding provided by Tripwire Enterprise makes it possible for users to configure the templates of their ephemeral assets to be automatically scanned as they register with the Tripwire Enterprise console. Tripwire Axon® agent tagging provides for the designation of specific systems that need rules to be run at the moment of registration. Security teams can selectively choose which systems require scanning during a scheduled window versus those that should be auto-onboarded between scheduled scans.

Auto-onboarded nodes that fall into the scope of your organization's compliance policies will have a score available as soon as their initial scan completes, allowing you to see your compliance state and score as soon as your systems come online and complete their first scan.

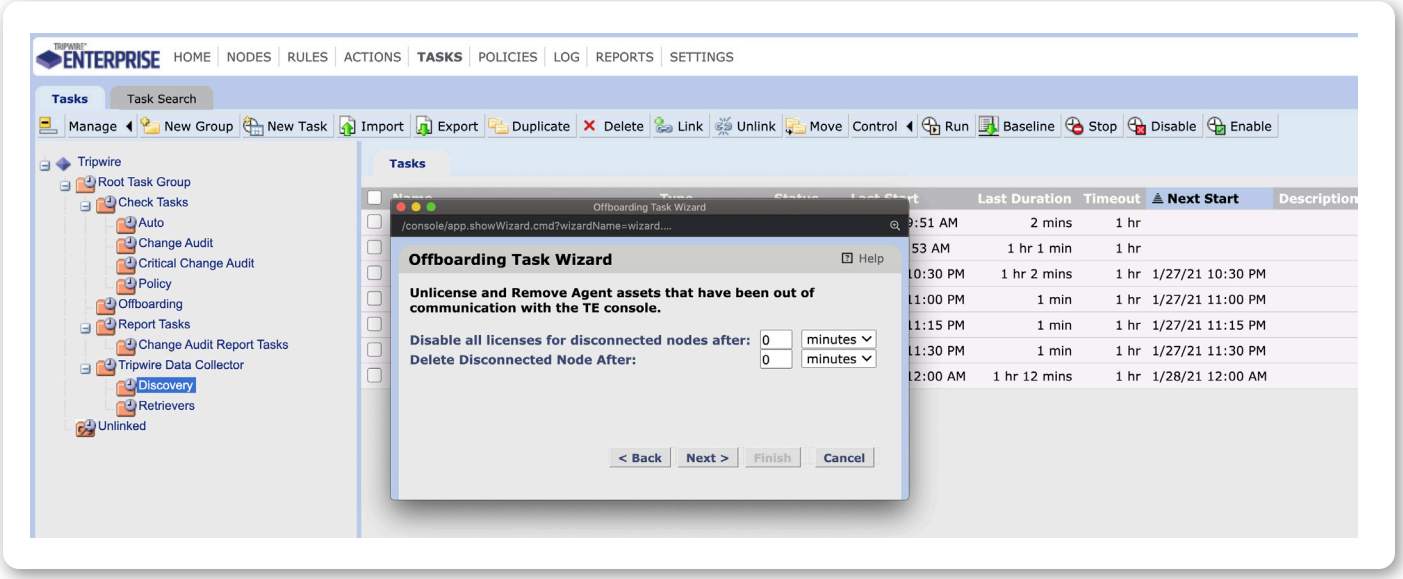

Fig. 1 The Offboarding Task Wizard enables Tripwire Enterprise to automatically disable and remove ephemeral assets that are no longer in use.

Automated Offboarding

As mentioned above, ephemeral assets can quickly accumulate after being purpose-built for a particular moment in time. In all of the scenarios where automatically deployed assets spin up in the cloud, you must also consider the automated process of decommissioning them. If automation was required to handle the incoming systems, it is going to be just as necessary to handle their removal.

What if your cloud infrastructure could essentially clean up after itself? Tripwire Enterprise automatically offboards ephemeral assets that are no longer in use.

Automated offboarding simplifies the process of decommissioning existing nodes as needed. This is done using tasks within the console that allow system administrators to decide how long Tripwire Axon agents are permitted to be out of communication with the console. Assets that stay out of communication longer than the designated period of time can be unlicensed or ultimately deleted. Using these tasks, you can specify the groups of nodes that offboarding should apply to and even set different time limits for different groups of assets.

However, there are instances in which it would be beneficial to hold off on permanently deleting these assets because of organizational change management process requirements. In this case, nodes and data can be left in place to be removed by administrators at an approved point in time. On the other hand, organizations may wish to move directly to deleting the assets in question to clean up the environment for the purposes of long-term reporting.

Dynamic Waivers

In a cloud environment, it is often necessary to have a clear method to document the business requirements or mitigating factors that would make an asset eligible for a compliance waiver. Next, it is important that those waivers apply to the asset assets in question as soon as they come online.

When working with static, long-lived assets, it is possible to create a highly detailed rationale for waivers to apply to particular systems that fail a given compliance check. There may also be business requirements or mitigating factors to explain or justify the failure. In the case of dynamic, ephemeral assets, using waivers becomes more complex. Using Tripwire Enterprise, security administrators can define waiver rationales for groups or classes of assets—even for those ephemeral assets that do not yet exist at the time the documentation for these waivers is created.

Tripwire Enterprise allows security administrators to define the scope of compliance waivers based on node groups. As soon as an asset spins up and is categorized or tagged into the appropriate groups in Tripwire Enterprise, the waivers that apply to that node group will apply automatically. The policy score for the newly created asset will reflect those waivers.

Summary

Monitoring for change in a dynamic cloud environment can be extremely difficult. Ephemeral assets that spin up for a short amount of time may not appear to be high-priority security concerns, but security administrators are not off the hook for proving these assets are deployed in a secure and compliant way. Tripwire Enterprise simplifies the management of ephemeral assets in a variety of cloud environments with automated scanning, on- and off-boarding, dynamic waivers, and more.

Schedule Your Demo Today

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

tripwire®

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

SBMEADC1a 2102