Tripwire Configuration Manager

Effective protection for cloud-based assets and apps

Tripwire® Configuration Manager gives you the ability to monitor the configuration of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), Salesforce, Zoom accounts and data storage from a single console. Misconfigurations are a leading cause of data breaches and security incidents involving cloud computing. Tripwire Configuration Manager uses current industry-standard security policies to automate the assessment of your applications, cloud accounts and storage so you don't have to.

Key Benefits

- Immediate assessment of application and cloud account configurations vs. industry-standard CIS Foundations Benchmarks
- Monitors cloud storage settings for buckets and blobs to ensure data is not inadvertently exposed or publicly visible
- Optional enforcement to minimize human effort-based misconfigurations
- Prioritization of non-compliant configurations using risk assessment
- Multi-cloud support to provide a single pane of glass view of cloud configurations
- Platform architecture allows existing Tripwire on-prem products to share data with Tripwire Configuration Manager
- Quickstart uses the existing cloud configuration as a baseline to speed startup
- Also available as a managed service

Rather than just providing misconfiguration alerts to over-burdened security staff, Tripwire Configuration Manager gives you the option to have your configuration automatically enforced. As a second time-saving measure, Tripwire Configuration Manager uses risk scoring to prioritize all misconfigurations so that security staff can focus on the most impactful problems first.

Configuration Assessment

As companies rush to migrate to the cloud, there is an influx of novice users that are misconfiguring critical security settings. The Verizon *2020 Data Breach Investigations Report* lists misconfigurations as one of the leading causes of breaches across nearly all industries, including retail, financial and healthcare[1]. Using automated search methods, attackers can quickly find these security gaps in an organization.

Tripwire Configuration Manager provides periodic assessment of security settings compared against an industry standard: the CIS Amazon Web Services Foundations Benchmark, published by the Center for Internet Security. You are immediately alerted to non-compliant settings that create dangerous security vulnerabilities.

Enforcement

Tripwire Configuration Manager provides the option of enforcing your security decisions. If a user changes a configuration in a way that takes it out of compliance, Tripwire Configuration Manager will automatically reset it to its previous, secure state. This reduces the time a configuration error is available for attack, and it offloads the tedious work of manually resetting configurations, freeing security personnel for more meaningful tasks.

Risk Scoring

The workload on security personnel is high and growing. Resources must be allocated to problems that represent the highest risk for the company. To aid in this prioritization effort, Tripwire Configuration Manager applies a risk score to any non-compliant configuration. This scoring is then used to create a prioritized list of problems for security staff to address.

Multi-Cloud

According to a recent survey conducted by RightScale, 84 percent of enterprises employ a multi-cloud strategy[2], resulting in a negative impact on security staff. Analysts must be familiar with the native tools used by each cloud service provider (CSP), and a separate console is required to manage each CSP environment. As the complexity of the environment increases, the operators' ability to find and remediate problems declines.

Tripwire Configuration Manager provides a single console to manage the configurations of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) environments. It presents an integrated view of cloud assets regardless of which CSP networks are used.

SaaS App Monitoring

If your organization uses Salesforce or Zoom, Tripwire Configuration Manager is able to scan those third-party applications' configuration states, in addition to your monitored public cloud accounts.

Ninety-four percent of companies now use one or more SaaS applications.[3] SaaS apps improve business efficiency but pose new security risks as well. The

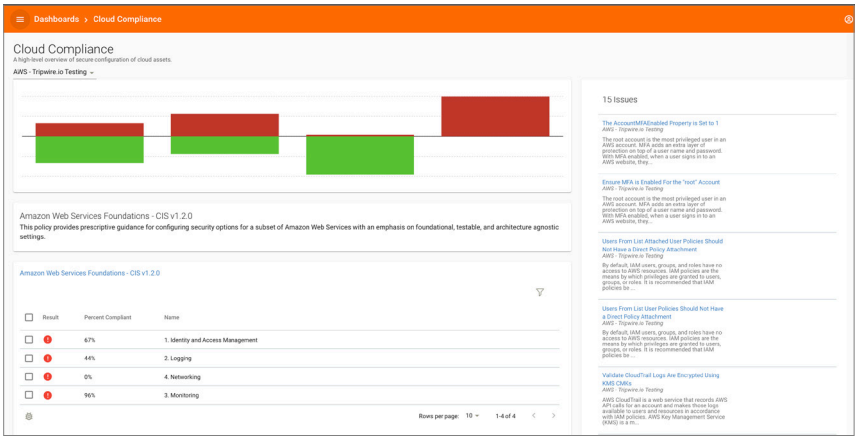

Fig 1a Tripwire Configuration Manager reviews configurations, compares them to a selected benchmark, then provides a summary of the errors found.

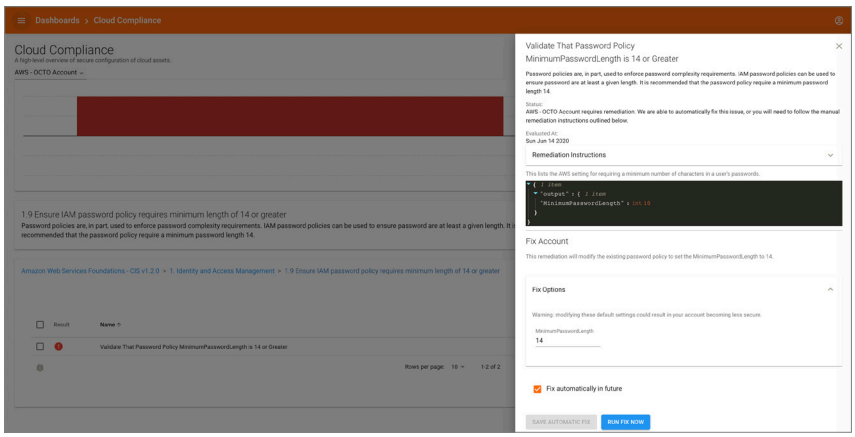

Fig 1b If the operator probes into any problem listed, a detailed description of the misconfiguration is provided. The user is also given the option to trigger automated enforcement at this stage.

Supported Benchmarks

- CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 1
- CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 2
- CIS Benchmark for Amazon Elastic Kubernetes Service (EKS) v1.0.0, Level 1
- CIS Benchmark for Amazon Elastic Kubernetes Service (EKS) v1.0.0, Level 2
- CIS Microsoft Azure Foundations Benchmark, v1.1.0, Level 1
- CIS Microsoft Azure Foundations Benchmark, v1.1.0, Level 2
- CIS Benchmark for Google Cloud Platform Foundation v1.1.0, Level 1
- CIS Benchmark for Google Cloud Platform Foundation v1.1.0, Level 2
- CIS Benchmark for Zoom Benchmark v.1.1.0, Level 1
- CIS Benchmark for Zoom Benchmark v.1.1.0, Level 2
- Google Kubernetes GKE policy
- Tripwire AWS Best Practices

department or individual who implements these apps becomes responsible for their configuration security—otherwise, threat actors can gain access to conference calls or view sensitive customer data. These risks can only be mitigated if the SaaS is securely configured and monitored for change by employees who have the expertise, tools and processes needed to do the job.

Tripwire Configuration Manager allows you to view Salesforce and Zoom's SaaS configurations in a single pane of glass to see how their configurations compare to best practice frameworks such as CIS. It also provides audit reporting on those configurations, reducing the amount of time your teams spend audit preparation. Salesforce monitoring is currently based on Tripwire Best Practices, which have been refined by the Professional Services and SE teams based on extensive customer feedback and iterative tuning based on major industry standards.

Tripwire's Integrated Platform

Tripwire Configuration Manager works as part of the Tripwire security platform. Data provided by Tripwire IP360™ vulnerability scanning and the Tripwire Enterprise file integrity monitoring and compliance systems can feed data into a common reporting engine. This approach provides a single pane of glass for operators monitoring a large number of controls for both on-prem and cloud assets.

The addition of Tripwire Configuration Manager to this platform enables existing Tripwire customers to add cloud asset monitoring to their existing on-prem controls.

Tripwire Configuration Manager reviews AWS and Azure configurations and compares them to the CIS Amazon Web Services Foundations Benchmark. Additional available benchmarks include CIS Microsoft Azure Foundations and CIS Amazon Elastic Kubernetes Services (EKS). When a non-compliant setting is found, it first provides a summary of the errors found.

If the operator probes into any problem listed, a detailed description of the misconfiguration is provided. The user is also given the option to trigger automated enforcement at this stage.

Easy Start

Changing to a new control can be an time-consuming effort, in part because new policies must be created and tested. Tripwire Configuration Manager simplifies this process. The user can log into their account and instruct Tripwire Configuration Manager to accept the existing configuration as a baseline for all subsequent change monitoring. Within five minutes, the system can begin enforcement operations without the need to hold credentials or set up roles.

Managed Service

Tripwire Configuration Manager is also offered as a Tripwire ExpertOps℠ managed service. Tripwire experts manage your tools so that your employees are free to perform other tasks.

Schedule Your Demo Today

Let us take you through a demo and answer any of your questions. Visit **tripwire.me/demo**

Sources

1 *"2020 Data Breach Investigations Report."* Verizon Enterprise, 2020, enterprise.verizon.com/resources/reports/dbir/.

2 *"Cloud Computing Trends: 2019 State of the Cloud Survey."* Flexera Blog, 8 Apr. 2020, www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/.

3 Alves, Phil. *"60 SaaS Statistics and Trends for 2020."* DevSquad, 22 Jan. 2020, devsquad.com/blog/saas-statistics/.