Trend Micro

CLOUD ONE™ – CONFORMITY

Cloud security and compliance posture management

Organizations are rapidly migrating to cloud computing and adopting innovations to help with new or existing cloud projects. For some, traversing this path has been a multi-year endeavor; others are learning about cloud technologies for the first time and discovering a world of possibility. However, with increased possibilities come new impacts on the business—the infrastructure, technology, security, and team dynamics need to adjust to this evolution.

While cloud computing leads to more automation, cloud engineering and operations teams now require greater visibility of all the moving parts across their infrastructure and platforms. This increase in complexity can result in the rise of cloud-related cybersecurity risk because of misconfigurations across storage, network, and identity. Furthermore, it can leave DevOps and cloud teams with a trail of unmanaged risks across multi-cloud environments in addition to performance, compliance, and operational concerns. This creates the perfect storm to negatively impact the business' reputation and bottom line.

INTRODUCING TREND MICRO CLOUD ONE™ – CONFORMITY

Conformity enables you to fulfill your side of the shared responsibility model with guardrails for your cloud. Providing continuous security, compliance, and governance in a cloud-native platform to help you manage misconfigurations of cloud resources and strengthen your security posture.

With almost 1,000 cloud infrastructure configuration checks out of the box, across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforrm™, your cloud services are scanned in real-time. This provides you with visibility of your entire cloud environment, your compliance score, contextual insights, and alerts for any risks in your cloud infrastructure.

> "Nearly all successful attacks on cloud services are as a result of misconfiguration, mismanagement, and mistakes. Continuously scanning workloads with cloud security posture management (CSPM) tools, covering identity, network, and storage configuration, is critical in identifying these problems."
>
> **"Endpoint and Server Security: Common Goals, Divergent Solutions"** published 01/2021
> ID: G00377795

> "Conformity is more than just a security tool. It provides me with situational awareness by giving me a global view of everything that I have inside my cloud—helping me manage it and take action."
>
> **Jason Cradit,**
> Principal Cloud Architect,
> 1898 & Co.

HOW DOES CONFORMITY WORK?

There is nothing to download or deploy. Simply sign up for a 30-day free trial, connect your cloud account, and in minutes you will have a comprehensive view of your cloud security posture. Conformity uses a custom access policy to view your cloud account metadata configuration settings—there is no read or write access to your data.
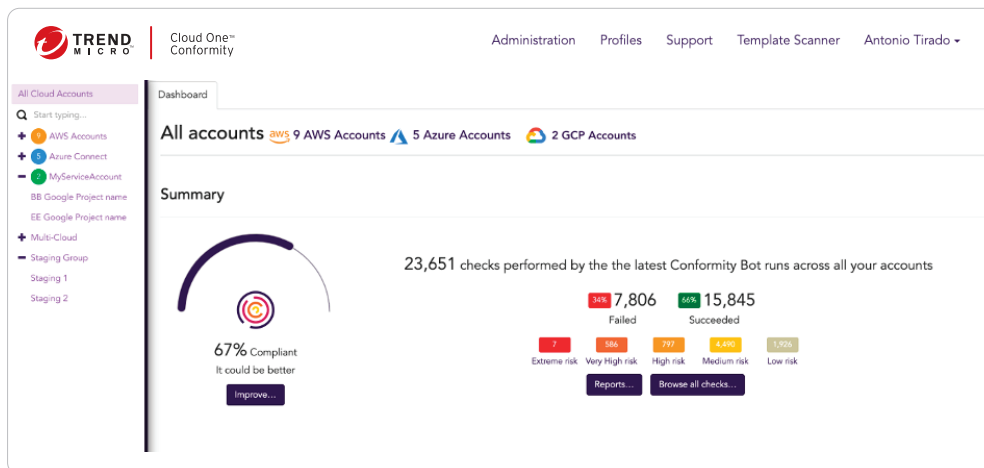

WHAT SETS US APART

World-class technology leaders are putting tremendous effort into building the most secure, optimized, resilient, and scalable cloud infrastructure for their businesses.

1. Continuously build your cloud infrastructure to industry best practices

Guardrails to innovate in the cloud with confidence. Each configuration recommendation in Conformity is founded on the design principles of the Well-Architected Frameworks, enabling you to create best-of-breed infrastructure and preventing common technical pitfalls. This ensures your infrastructure is truly benefiting from all of the advantages your cloud services platform offers.

The Well-Architected Framework is made of up six pillars: security, operational excellence, reliability, performance efficiency, cost optimization, and sustainability. Each recommendation and remediation step displays which pillar it supports, giving you assurance that your cloud infrastructure is configured and deployed securely while your systems and sensitive data are properly protected. Leverage auto-remediation capabilities for any rules you want to be automatically addressed.
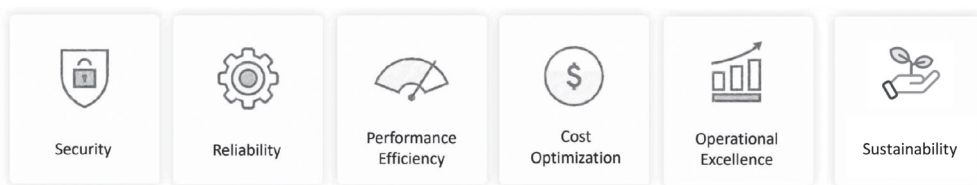
Fast Facts

- Extensive depth and breadth of coverage on AWS, Azure, and Google Cloud services.

- Nearly 1,000 real-time industry best practice checks. No need to build your own.

- Real-time monitoring and alerts.

- Extremely actionable and easy to use.

- Includes remediation guides and auto-remediation.

- Seamless integrations with key ticketing and communication channels like Slack, ServiceNow, Jira, PagerDuty, Microsoft Teams, and more.

- CloudFormation and TerraForm template scanner capability scans IaC templates

2. Manage compliance at scale in the cloud

Industry standards and compliance requirements are constantly changing. Benefit from continuous scans against compliance and industry standards in your cloud infrastructure and immediately act on high-risk policy violations against SOC2, ISO 27001, NIST, CIS, GDPR, PCI DSS, GDPR, HIPAA, and more.

Leverage standardized or custom reports, auditing your infrastructure for misconfigurations with an endless combination of filters. Run exportable reports on your cloud environments for internal and external audits against benchmark standards.

3. Democratize cloud operational excellence

Instill confidence in developers by providing guardrails that enable agile development and a secure, optimized cloud infrastructure. Our Conformity Knowledge Base is a continually growing library containing almost 1,000 step-by-step remediation guides for public cloud infrastructure configurations. This empowers developers and engineers to better understand how to build superior cloud architecture, regardless of their security or technical expertise.

This readily available remediation information allows organizations to move quickly with their cloud migration, DevOps processes, or other cloud projects without the fear of introducing misconfigurations, vulnerabilities, or reliability risks.
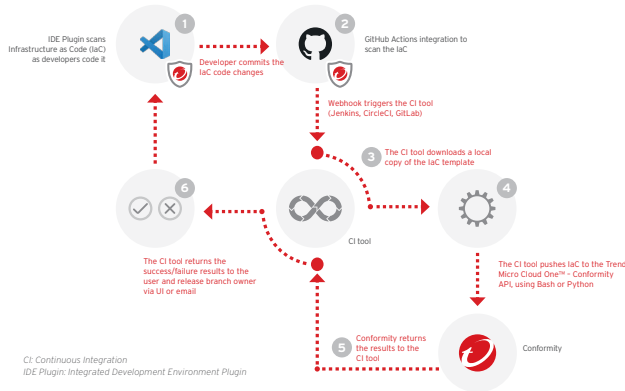
PROACTIVE PREVENTION AND AUTOMATION

In addition to providing real-time threat monitoring and auto-remediation for your cloud environments, you'll quickly realize the value of shifting security and compliance to the earliest phase of your CI/CD pipeline. With our Infrastructure as code (IaC) template scanning, templates can instantly be run through the Conformity API during the coding process. This will enable automated, proactive prevention of misconfigurations and give you peace of mind that the code moving into your cloud infrastructure is fully compliant and aligned to industry best practices.

Embed the CloudFormation Template Scanning API into Your CI/CD Pipeline

1 — IDE Plugin scans Infrastructure as Code (IaC) as developers code it
— Developer commits the IaC code changes
2 — GitHub Actions integration to scan the IaC
— Webhook triggers the CI tool (Jenkins, CircleCI, GitLab)
3 — The CI tool downloads a local copy of the IaC template
4 — The CI tool pushes IaC to the Trend Micro Cloud One™ – Conformity API, using Bash or Python
5 — Conformity returns the results to the CI tool
6 — The CI tool returns the success/failure results to the user and release branch owner via UI or email

CI tool
Conformity

CI: Continuous Integration
IDE Plugin: Integrated Development Environment Plugin

SET UP CONFORMITY IN MINUTES

Conformity is designed so you can be up and running within minutes. After you have connected your AWS, Azure, or Google Cloud account, you'll see the overall risk posture of your cloud environment. You can replicate rules and communication preferences across accounts to give development teams proper security guardrails.

MEET WORKFLOW AND COMPLIANCE REQUIREMENTS

Conformity currently integrates with the following communication channels, workflow systems, and compliance standards.

INTEGRATION WITH:

slack · Jira · Teams · zendesk · amazon SNS
pagerduty · servicenow · EMAIL · SMS · New Relic

CONTINUOUS COMPLIANCE MONITORING FOR:

GDPR · AICPA SOC · PCI · ISO 27001 Certified · NIST · HIPAA COMPLIANT

And more compliance standards available...

aws partner network
Advanced
Technology Partner
Security Competency
Cloud Management Tools Competency

> "Having Conformity continuously monitor our AWS infrastructure and notify us in real time of any critical issues ensures we remain compliant with best practices, and any potential threats to our applications or data are resolved before they impact our business."
>
> Team Lead of Information Security, GrubHub

TREND MICRO™
Securing Your Connected World