# Prisma Cloud on GCP

## Protect all resources in your Google Cloud Platform environment with Prisma Cloud

### Benefits of Prisma Cloud on GCP

- Visualize every connected resource across your entire GCP environment.
- Maintain continuous compliance and easily generate reports across your GCP environment.
- Enable secure DevOps by setting guardrails with realtime monitoring for threats, such as risky configurations, sensitive user activities, network intrusions, and host vulnerabilities.
- Use anomaly detection capabilities to root out account compromises and insider threats.
- Investigate current threats or past incidents and quickly determine root causes.
- Get contextual alerts to help your team prioritize issues and respond quickly.
- Integrate seamlessly with native GCP services, including Cloud Security Command Center.

### Prisma Cloud Simplifies Cloud Threat Defense on GCP

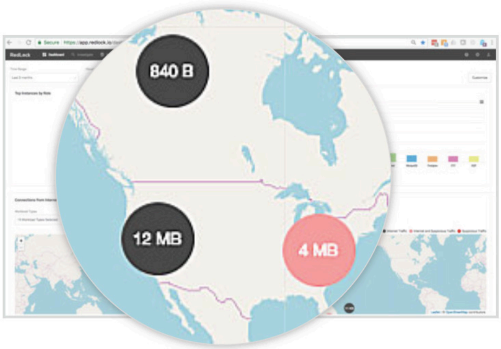
Public cloud computing adoption is outpacing cybersecurity defenses. The absence of a physical network boundary to the internet, risk of accidental exposure by inexperienced users, decentralized visibility, and the dynamic nature of the cloud increase the attack surface by orders of magnitude. Although security point products may be able to address individual challenges, they are unable to provide holistic protection in an environment where resources are constantly changing, such as in Google Cloud.

Prisma™ Cloud is a security and compliance service that discovers cloud resource changes and continuously correlates raw, siloed data sources, including user activity, resource configurations, network traffic, threat intelligence, and vulnerability feeds, to provide a complete view of public cloud risk. Through an innovative, machine learning-driven approach, Prisma Cloud enables organizations to quickly prioritize risks, maintain agile development, and effectively fulfill their obligations in the Shared Responsibility Model.

### Key Features and Benefits to Secure GCP

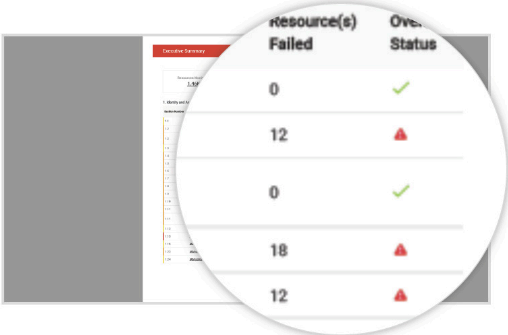
*Unmatched Visibility*

Visualize your entire Google Cloud Platform (GCP™) environment, down to every component. Prisma Cloud dynamically discovers cloud resources and applications by continuously correlating configuration, user activity, and network traffic data. Combining this comprehensive understanding of the GCP environment with data from external sources, such as threat intelligence feeds and vulnerability scanners, Prisma Cloud delivers complete context for each risk.



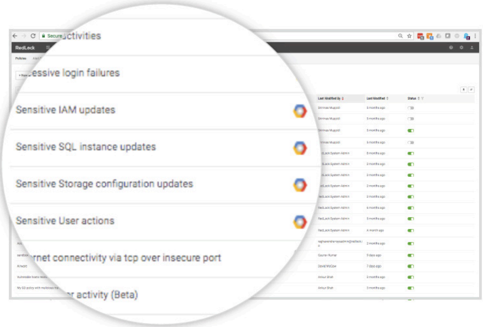
### *Simplified Cloud Compliance*

Prisma Cloud includes pre-built policies that adhere to industry-standard best practices, such as those put forth by CIS, GDPR, NIST, SOC 2, and PCI. You can also create custom policies based on your organization's specific needs. Prisma Cloud continuously monitors for policy violations across all connected resources and supports one-click reports for simplified audits of your GCP environment.



Executive Summary

| Resource(s) Failed | Ove... Status |
|---|---|
| 0 | ✓ |
| 12 | ▲ |
| 0 | ✓ |
| 18 | ▲ |
| 12 | ▲ |

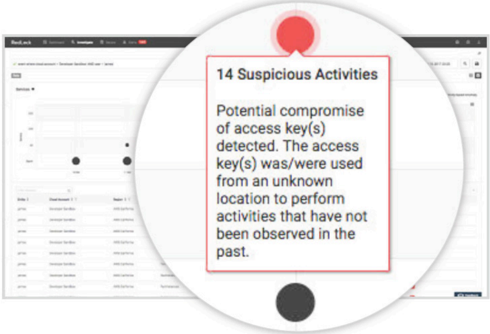

...ctivities
...essive login failures
Sensitive IAM updates
Sensitive SQL instance updates
Sensitive Storage configuration updates
Sensitive User actions
...rnet connectivity via tcp over insecure port
...r activity (Beta)

### *Policy Guardrails*

Prisma Cloud lets you set guardrails for DevOps to maintain agile development without compromising on security. This enables you to detect threats, such as risky configurations, sensitive user activities, network intrusions, and host vulnerabilities. Prisma Cloud automatically ranks risk scores for every resource, based on the severity of business risks, violations, and anomalies, helping SecOps quickly identify the riskiest resources and prioritize remediation efforts accordingly.

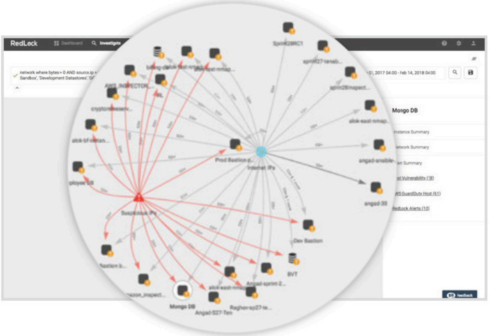
### *Threat Detection*

Prisma Cloud automatically detects anomalies in user and other behavior across your entire GCP environment, establishing behavior baselines and flagging any deviations. For example, a potential access key compromise will be flagged if a user is determined to be using access keys from two locations at similar times that are geographically impossible.



14 Suspicious Activities

Potential compromise of access key(s) detected. The access key(s) was/were used from an unknown location to perform activities that have not been observed in the past.

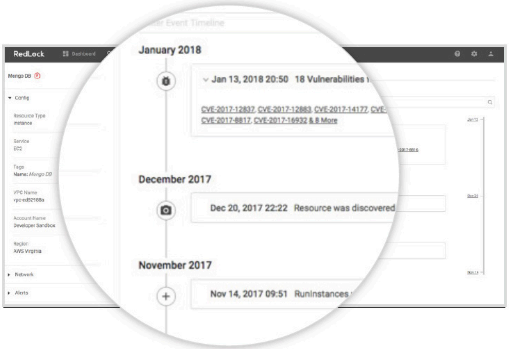


### *Incident Investigation*

With deep understanding of the GCP environment, Prisma Cloud reduces investigation time to seconds. You can quickly pinpoint issues, perform upstream and downstream impact analysis, and review the history of changes to a resource to better understand the root cause of an incident. For example, you can run a query to find all databases that were communicating directly via the internet last month. The resulting map will find all such instances and highlight the resources that are potentially compromised.

### *Contextual Alerting and Adaptive Response*

Prisma Cloud enables your teams to quickly respond to issues based on contextual alerts. These alerts, triggered based on a patent-pending risk scoring methodology, provide context on all risk factors associated with a resource, making it simple to prioritize the most important issues. You can send alerts, orchestrate policy, or perform auto-remediation. You can even route alerts to tools such as Slack®, Splunk®, and our own Demisto® to remediate issues. In the case of a risky database, Prisma Cloud will generate a contextual alert with information on risk factors to enable automated response.



January 2018

Jan 13, 2018 20:50 18 Vulnerabilities

CVE-2017-12837, CVE-2017-12883, CVE-2017-14177, CVE-...
CVE-2017-8817, CVE-2017-16932 & 8 More

December 2017

Dec 20, 2017 22:22 Resource was discovered

November 2017

Nov 14, 2017 09:51 RunInstances

### Integration with Cloud Security Command Center

Prisma Cloud integrates with Google's Cloud Security Command Center to provide you with visibility into security and compliance risks across your entire GCP environment. This means security teams can quickly gather data, identify threats, and take action before business damage or loss occurs.

### Developing a Cloud Threat Defense Roadmap for GCP

Prisma Cloud enables you to develop a cloud threat defense program across your entire GCP environment, from inception to maturity, with the following capabilities:

- **Compliance assurance:** Mapping cloud resource configurations to compliance frameworks, such as CIS, GDPR, PCI DSS, and HIPAA, can be extremely time-consuming. Using prepackaged policies, Prisma Cloud enables continuous monitoring, auto-remediation, and one-click reporting, simplifying the process of staying compliant.
- **Security governance:** Incomplete visibility and imprecise control over changes in dynamic public cloud computing environments can make security governance difficult. Prisma Cloud enables architecture validation by establishing policy guardrails to detect and auto-remediate risks across resource configurations, network architecture, and user activities. With Prisma Cloud, you can finally support DevOps agility without compromising on security.
- **SOC enablement**: Security operations teams are inundated with alerts that provide little context on issues, which makes it hard to triage those issues in a timely manner. Prisma Cloud makes it possible to identify vulnerabilities, detect threats, investigate current or past incidents, and remediate those issues across your entire GCP environment in minutes.

| Stage 1: Adopt | Stage 2: Expand | Stage 3: Scale |
|---|---|---|
| **Cloud Footprint:**<br>• Dozens of workloads<br>• Few cloud accounts | **Cloud Footprint:**<br>• Hundreds of workloads<br>• Many cloud accounts | **Cloud Footprint:**<br>• Multiple cloud providers<br>• Thousands of workloads<br>• Dozens of cloud accounts |
| **O ves:**<br>• Compliance assurance<br>• Security governance | **O ves:**<br>• Central visibility<br>• Threat detection<br>• Vulnerability management<br>**+ Stag es** | **O es:**<br>• Auto-remediation<br>• Incident investigation<br>**+ Stag es** |

**Figure 1:** Cloud Threat Defense Maturity Model

### Prisma Cloud Security Suite

Prisma Cloud provides comprehensive visibility, threat detection and rapid response across your entire public cloud environment, including Google Cloud Platform, Amazon Web Services (AWS®), and Microsoft Azure®. A unique combination of continuous monitoring, compliance assurance, and security analytics enables security teams to respond more quickly to the most critical threats by replacing manual investigations with automated reports, threat prioritization, and remediation. With its API-based approach, Prisma Cloud delivers superior cloud-native security.

Prisma Cloud is part of the Palo Alto Networks Security Operating Platform®, providing organizations with a multidimensional approach to public cloud security delivered through inline, API-based, and host-based protection technologies working together to minimize opportunities for attack.

The Security Operating Platform extends protection to your entire network, with comprehensive protection regardless of location. Whether your applications reside on-premises; have been virtualized and need protection in a private cloud, such as VMware NSX®, Cisco ACI®, KVM or OpenStack®; are extended to a public cloud; or have been moved to a SaaS application, we can protect them.

Visit our website to learn more: www.paloaltonetworks.com.