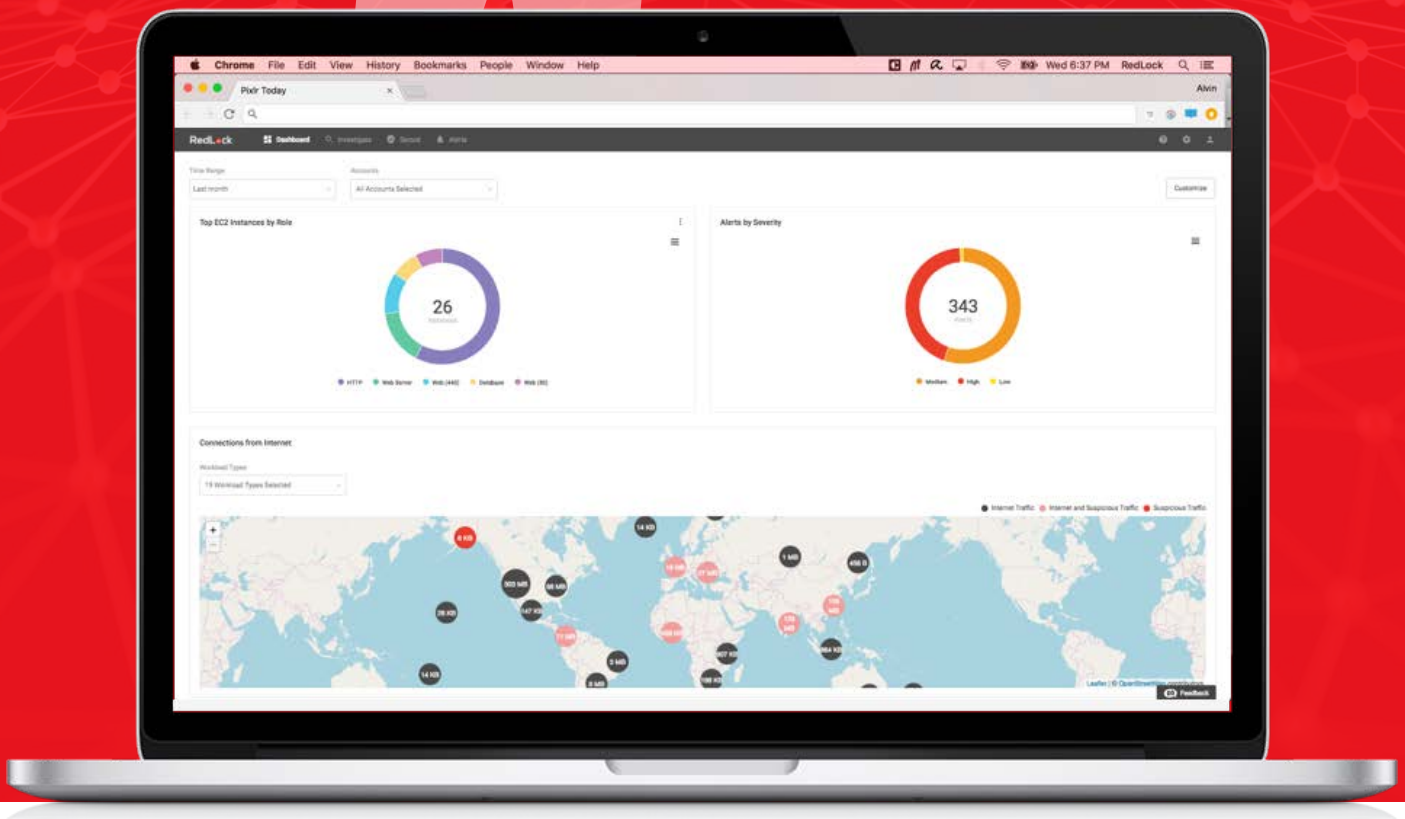
RedLock®

Google Cloud Platform Partner

Securing Google Cloud with RedLock® Cloud 360 Platform™



Compliance Assurance

Security Governance

SOC Enablement

Table of Content

Security in the Public Cloud is a Shared Responsibility

The adoption of public cloud computing among established businesses and startups is outpacing the adoption of new cybersecurity defenses. The absence of a physical network boundary to the internet, the risk of accidental exposure by users with limited security expertise, decentralized visibility, and the dynamic nature of the cloud increases the attack surface by orders of magnitude. The shared responsibility model of cloud security clearly outlines the respective responsibilities of cloud service providers and their customers. This is a difficult customer challenge, and Gartner forecasts that 95% of cloud security failures (and breaches) through 2020 will be the customer's fault. Your organization's obligations in the shared responsibility model include:

- Monitoring and remediating resource misconfigurations
- Detecting and remediating anomalous user activities
- Detecting and remediating suspicious network traffic
- Identifying vulnerable hosts

Cloud Security and Compliance Challenges

To effectively address cloud security, it is important to understand the changes that moving to the cloud presents and their implications on security, including:

- **DevOps Automation:** While the cloud enables agility by allowing users to create, modify, and scale storage, network and compute resources on-demand, this often occurs without any IT or security oversight. In traditional IT controlled environments, manual configuration monitoring and auditing works successfully, but is not practical in user-controlled (DevOps) cloud environments where change and personnel turnover is constant.

  > ***Implication:*** *Customers require an automated feedback loop to notify environment owners of security risks in an automated fashion, akin to their DevOps processes. Legacy point-in-time configuration scanning tools have generated too much noise that is not actionable.*

- **Decentralized Control:** In the cloud multiple users have privileged access, which enables productivity but creates greater risk. Reports of compromised access keys are becoming common. It is critical to monitor users across the entire cloud computing environment for suspicious activities. Unfortunately, the distributed nature of the cloud, consisting of users scattered across multiple accounts and regions, leads to decentralized visibility.

  > ***Implication:*** *Customers have accumulated substantial "security debt" in their cloud environments due to limited visibility and context regarding why configuration changes are being made, by whom, and what the impact is to their security posture.*

- **Disappearing Perimeter:** The presence of a physical perimeter around an on-premise network reduces the risk of exposure as any networking errors are physically blocked. The virtual perimeter in cloud environments is more vulnerable because errors open up the network to attacks. It is critical for organizations to vigilantly monitor network

traffic and detect suspicious activity. However, traditional network monitoring tools create security blind spots since they cannot be deployed for monitoring traffic to API-driven services in the cloud.

> ***Implication:*** *Customers must continuously monitor their cloud environments for suspicious network activity across all accounts.*

The RedLock Cloud 360 Platform

Feature Overview

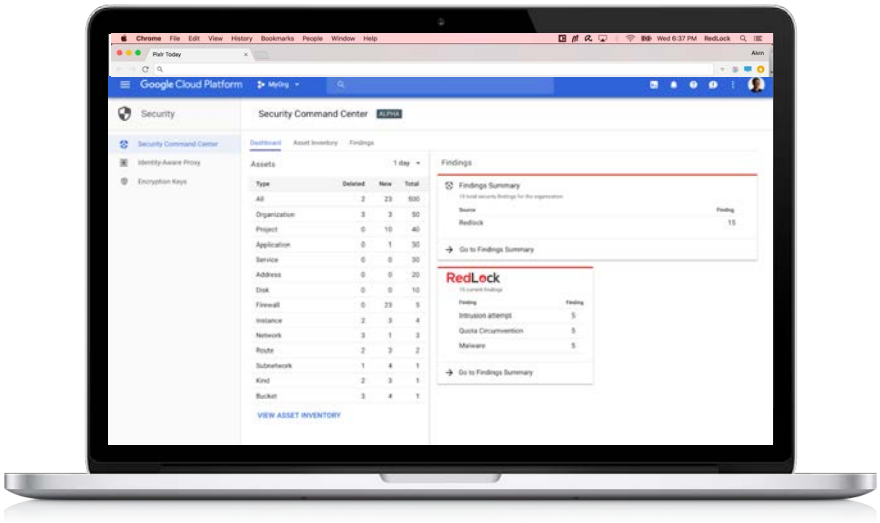
The RedLock Cloud 360 Platform is a cloud security and compliance solution that provides complete visibility and control within your Google Cloud environment. RedLock connects to your Google Cloud environment in minutes via APIs and continuously monitors to make sure your cloud resources are compliant with industry and organizational policies and it is protected from potential security threats. RedLock generates alerts when an issue is detected and provides context that enables incident response teams to quickly investigate and remediate problems. Dashboards provide insights into the overall security health of the organization. In addition, RedLock provides:

- **Comprehensive Visibility:** The RedLock Cloud 360 platform enables you to visualize your entire public cloud environment, down to every component within the environment. The platform dynamically discovers, maps, and visualizes the entire cloud infrastructure by aggregating and correlating configuration, user activity, and network traffic data. Combining this deep understanding of the cloud environment with artificial intelligence (AI) enriches the view with data from external sources such as threat intelligence feeds and vulnerability scanners. This comprehensive visibility lets you accurately and easily pinpoint risks. For example, the platform may indicate that databases are running in your cloud environment; you will want to ensure they do not communicate directly via the internet.
- **Compliance Reporting:** The RedLock Cloud 360 platform is prepackaged with policies that adhere to industry standard best practices such as CIS, NIST, SOC 2, and PCI. You can also create custom policies based on your organization's specific needs. The platform continuously monitors for violations to these policies by existing resources as well any new resources that are dynamically created. You can easily report on the compliance posture of your environment to auditors. For example, the platform can notify you if any of your databases are unencrypted.
- **Policy Guardrails:** The RedLock Cloud 360 platform lets you set guardrails for DevOps and enables them to be productive without compromising on security. This enables you to detect threats such as risky configurations, sensitive user activities, network intrusions, and host vulnerabilities. Using the example above, you could implement a policy to alert you if any MongoDB databases are running vulnerable versions of software.
- **Threat Detection:** RedLock automatically detects user and entity behavior anomalies across your entire cloud environment. The platform establishes behavior baselines and flags any deviations. For example, a potential access key compromise will be flagged if a user is determined to be using access keys from an unknown location to perform activities that have not been observed in the past.
- **Incident Investigation:** RedLock platform's deep understanding of the cloud environment, reduces investigation time from weeks or months to seconds. You can use the platform's interactive map to quickly pinpoint issues and perform upstream and downstream impact analysis. The platform provides you with DVR-like capability to view time-serialized activity for any

given resource. You can review the history of changes for a resource and better understand the root cause of an incident, past or present. For example, you can run a query to find all databases that were communicating directly via the internet last month. The resulting map will not only find all such instances but also highlight the resources that are potentially compromised. In this case, they are communicating with known malicious IP addresses.

- **Contextual Alerting and Adaptive Response:** The RedLock Cloud 360 platform enables you to quickly respond to an issue based on contextual alerts. Alerts are triggered based on patent-pending risk scoring methodology and provide context on all the risk factors associated with a resource. This makes it simple to prioritize the most important issues first. You can send alerts, orchestrate policy, or perform auto-remediation. The platform data can also be passed to third-party tools such as Slack, Demisto, and Splunk to remediate the issue. In the example of risky databases, a contextual alert will be generated with information on risk factors, which enables automated response.

Integration with Cloud Security Command Center



The RedLock integration with Google Cloud Security Command Center provides customers centralized visibility into security and compliance risks in Google Cloud environments. As part of the integration, RedLock monitors customer's Google Cloud environments and sends alerts pertaining to resource misconfigurations, compliance violations, network security risks and anomalous user activities to Cloud Security Command Center.

How it works

The RedLock Cloud 360 platform leverages disparate data sets including resource configurations, user activities, network traffic, and threat intelligence. It consumes this data from your Google Cloud environment, other cloud providers and third-party tools via APIs, and then applies artificial intelligence (AI) to correlate the massive volumes of data and enables a 3-step solution:

Discovery Cloud resources are automatically discovered as soon as they are created. RedLock profiles applications to provide context so that you have complete visibility across your environment at any given time. For example, it can discover when a virtual machine is instantiated and determine that it is a database running MongoDB software.

Detection: The platform detects a variety of risks. It can detect if resource configurations drift from policy-defined best practices. The platform creates behavior baselines for each user and any deviations are flagged to detect issues such as account compromises or insider threats. The platform monitors network traffic and flags suspicious activity. In addition, hosts that are vulnerable or potentially compromised can be quickly identified.

Respond: The RedLock Cloud 360 platform employs proprietary risk scoring algorithms to help prioritize and remediate the highest risks within your environment. To facilitate rapid response and remediation, the platform integrates with incident response tools such as Slack, Demisto, Splunk, and QRadar.

Deploying RedLock for Google Cloud Environments

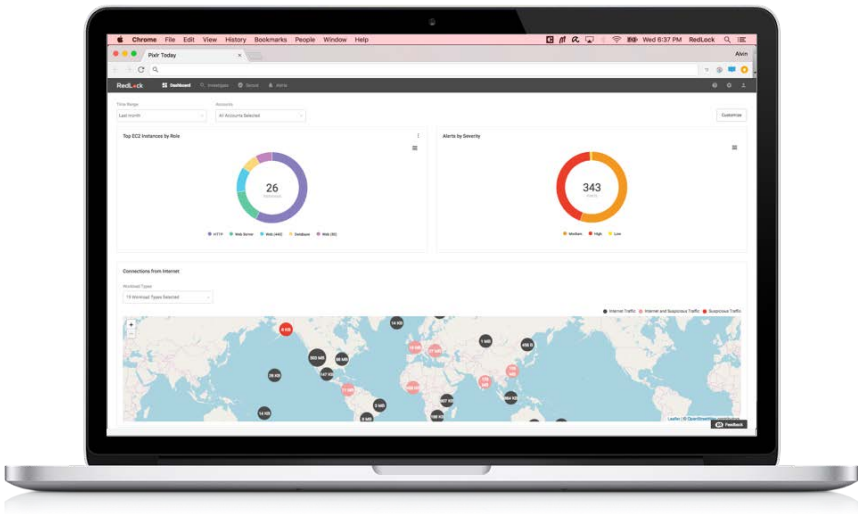
To use RedLock with your Google Cloud environment:

- Create a Google Cloud Account in RedLock. RedLock must be provided with 'read-only' access to Google Cloud services to enable resource monitoring. The identities of both systems are established through security keys generated in Google Cloud. You will need your security key and provide a name for your Google Cloud account.
- In the RedLock Configuration section, provide the Service Account Key (JSON file) that you downloaded from Google Cloud. Once processed, verify the details displayed correspond to the intended project security key.
- Once the connection is successfully set up, the Audit Log indicates a green tick mark in the status section. The Google Cloud Account is now successfully created and displayed in the Cloud Accounts list. You can now start monitoring your Google Cloud environment.

Operationalizing Cloud Threat Defense

Centralized Visibility

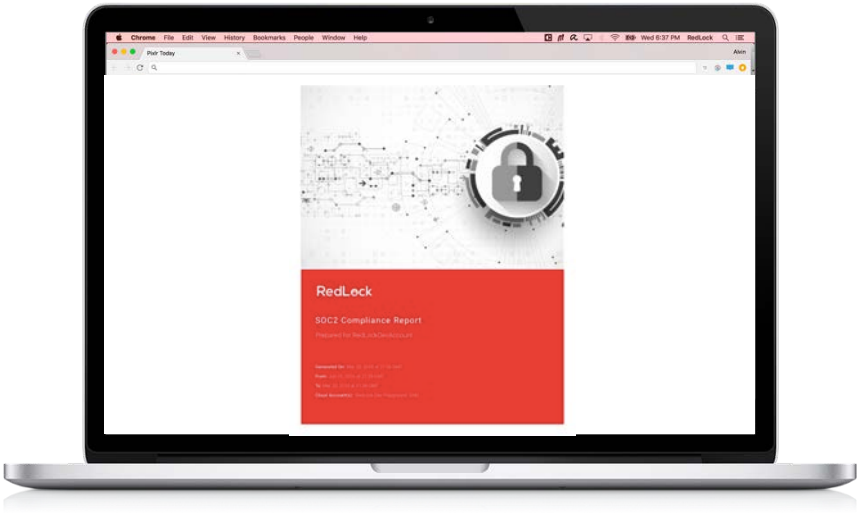
RedLock's intuitive, comprehensive dashboard provides visibility into your Google Cloud. You have option to view current or historical data based on predefined or custom time ranges. The dashboard provides a performance view of resources, traffic, connections, and user actions in a graphical or tabular format, and includes:



* Monitored Accounts and Resources	* Policy violations by Type over time
* Open Alerts	* Top Policy Violations
* Risk Rating by Scanned Accounts	* Top Internet Connected Resources
* Top Compute Engine instances by role	* Connections from the Internet Map
* Alerts by severity	

Risky Configuration Monitoring

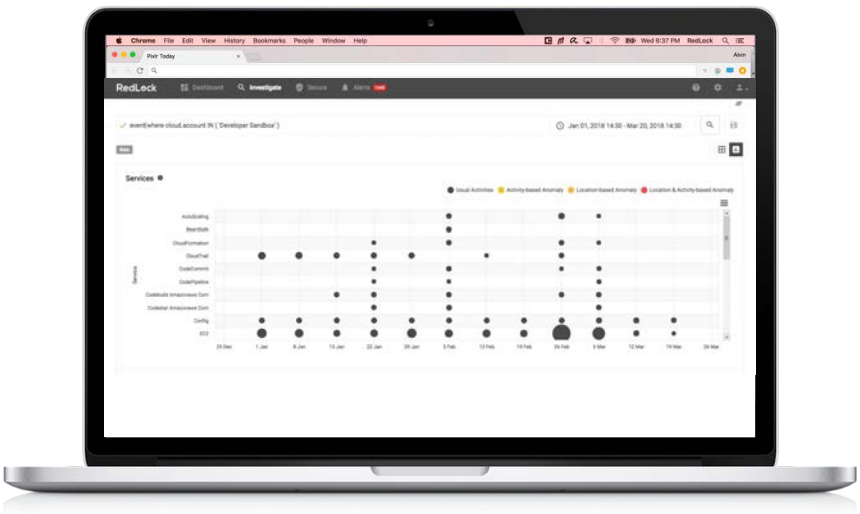
While the cloud enables agility by allowing users to create, modify, and retire resources on-demand, this often occurs without any oversight. How can you be assured that your cloud environments are not exposed due to risky configurations?



How can you determine if your cloud resource configurations are compliant? And how do you prove your cloud environment compliance status to your auditors? RedLock provides pre-packaged policies for common compliance standards such as CIS, NIST, PCI, and HIPAA to monitor Google Cloud environments. Any misconfiguration of Google Cloud resources such as Google Compute Engine, Google Cloud Storage, and Cloud Datastore will be immediately detected and raise alerts. In addition, RedLock provides compliance reports as a standard feature.

Account Compromise and Insider Threat Detection

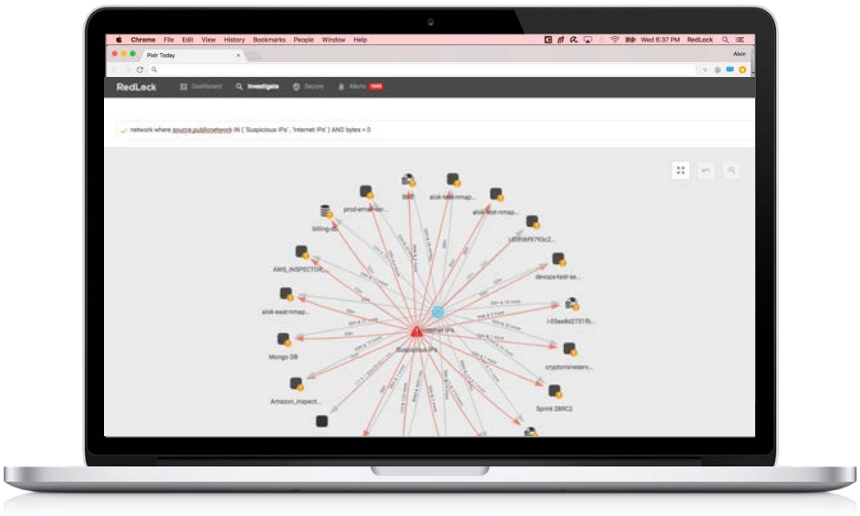
Do you suspect account-hijacking attempts in your environment? Are you seeing insider threats or internal users performing unusual activities?
In cloud environments, multiple users have privileged access which enables productivity but creates a greater risk of exposure. It is imperative to monitor users across your entire Google Cloud environment for anomalous activities. Unfortunately, the distributed nature of the cloud consisting of multiple accounts and regions makes this difficult.



The RedLock Cloud 360 platform develops a baseline of normal user activity. It consumes Audit Logs from across your entire Google Cloud environment. Any unusual activities are flagged as anomalies and can be investigated with easy-to-use forensics tools, enabling you to detect account compromises and insider threats.

Network Intrusion Detection

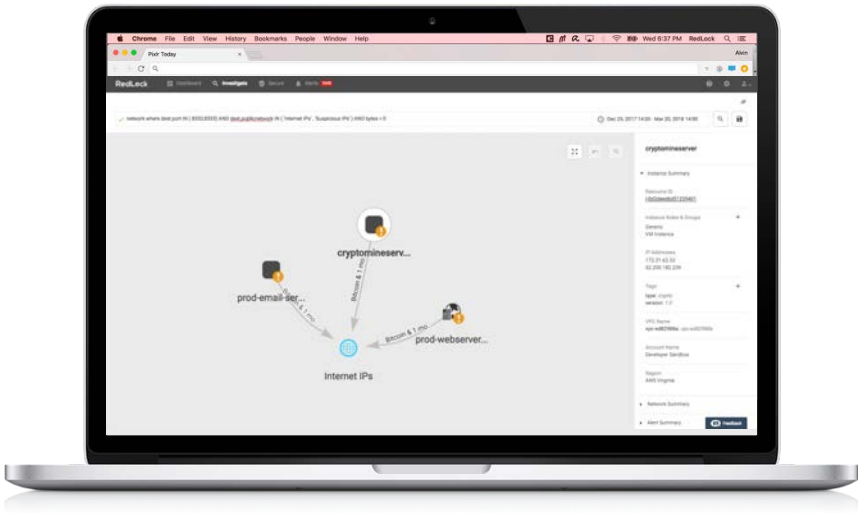
The absence of a physical network boundary to the Internet increases the attack surface in the cloud by orders of magnitude. Monitoring network traffic is necessary for detecting suspicious activity, such as which resources are receiving data from



suspicious IPs, or which database servers have connections from the Internet? Traditional tools create security blind spots since they cannot be deployed for monitoring traffic to API-driven services. RedLock consumes data from across your entire Google Cloud environment and correlates them with configuration data and third party threat intelligence feeds, to surface, investigate, and respond to threats.

Cryptojacking and Host Compromise Detection

Cryptojacking, the practice of stealing compute resources to mine cryptocurrency, has been highlighted in a number of recent news stories. The most prominent incident is the Tesla attack, where hackers were performing crypto mining from one of Tesla's Kubernetes pods. The RedLock Cloud 360 platform can detect cryptojacking in real-time (see screenshot below), as well as host-level compromises such as hosts acting as spam bots, or hosts exhibiting unusual patterns of behavior.



Integrations

RedLock provides multiple pre-packaged integration options, which can be used to integrate RedLock into existing workflows and technologies, including:

Email

Configure your email to work with RedLock to receive alerts to your inbox.

Slack

Slack is an online instant messaging and collaboration system that enables you to centralize all your notifications, including alerts from RedLock.

Splunk

Splunk is a software platform to search, analyze and visualize machine-generated data gathered from the websites, applications, sensors, devices etc. RedLock alerts can be remediated using existing workflows.