RedLock®

Security 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. 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

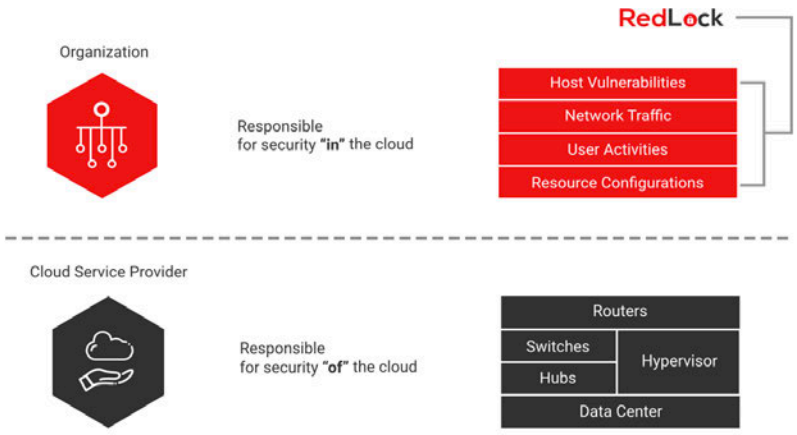


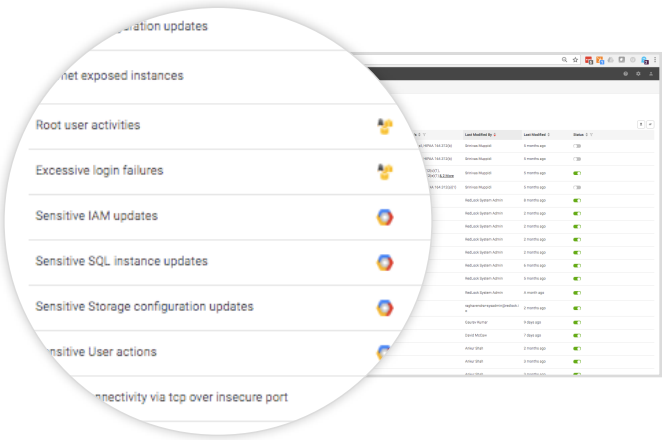
Figure 1: The Shared Responsibility Model

RedLock Enables Cloud Threat Defense

RedLock enables effective cloud threat defense across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud environments. The RedLock Cloud 360™ platform takes a new AI-driven approach to detect threats such as risky configurations, suspicious user activities, network intrusions, and host vulnerabilities.

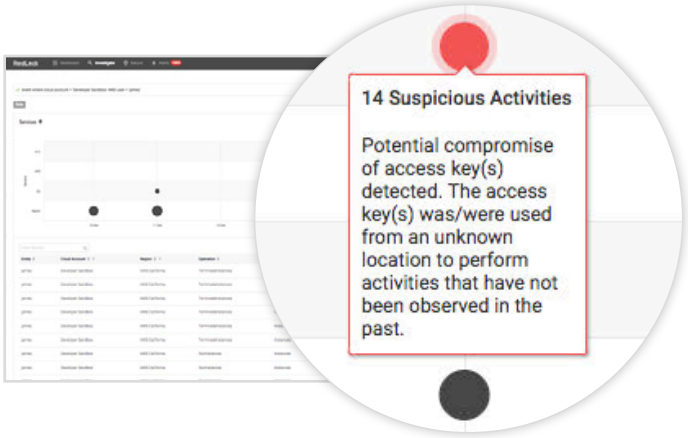
Risky Resource Configurations

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. Manual monitoring and auditing of configurations works in IT controlled environments, but is not really practical in user controlled cloud environments where change is constant. Consequently, we have seen a number of large scale breaches related to publicly exposed cloud storage services.



The RedLock Cloud 360 platform enables you to monitor cloud resources for configuration drift. The platform comes prepackaged with policies that adhere to industry standard best practices such as CIS, NIST, 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. As an example, an alert can be triggered if a user exposes an Amazon S3 bucket to the public.

Suspicious User Activities

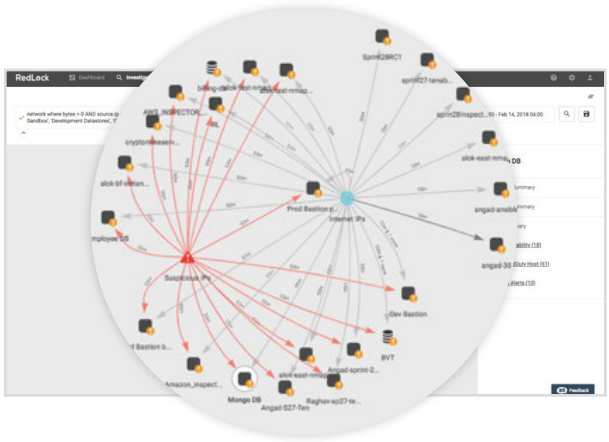


Access to on-premise environments is typically tightly locked down and centrally monitored by IT. In contrast, multiple users have privileged access to public cloud environments, which enables productivity but creates greater risk of exposure. Recent breaches have illustrated the damaging consequences of compromised access credentials. As a result, it is imperative to monitor users across your entire cloud computing environment for suspicious activities. Unfortunately, the distributed architecture of public cloud environments consisting of users scattered across multiple accounts and regions leads to decentralized visibility.

The RedLock Cloud 360 platform enables you to detect issues such as account compromises and insider threats in your public 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.

Network Intrusions

The presence of a physical perimeter around an on-premise network reduces the risk of exposure as any networking errors are physically blocked. In contrast, the virtual perimeter in public cloud environments is more vulnerable because a single programmatic error could open up the network to attacks. The RedLock research team uncovered nefarious crypto mining activity at a number of organizations such as Tesla, Gemalto, and Aviva which had completely gone undetected by the organizations. This illustrates that 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

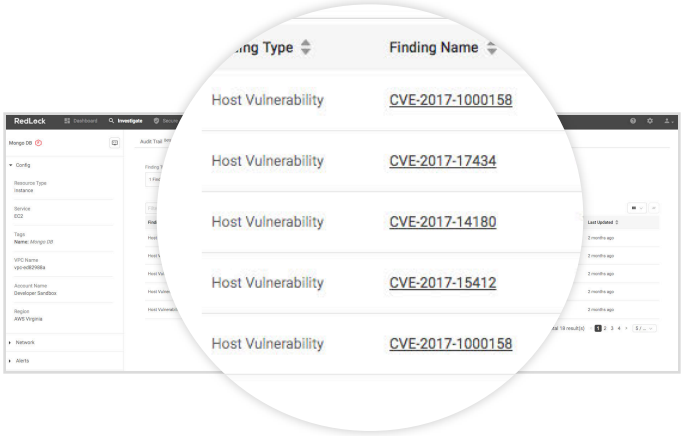


monitoring traffic to API-driven services in the cloud.

The RedLock Cloud 360 platform enables you to detect network intrusions. The platform correlates network traffic data with data from your public cloud environment and third party threat intelligence sources to detect suspicious activities. For example, an alert will be triggered if a MongoDB resource accepts a connection from a suspicious IP address.

Host Vulnerabilities

Unpatched hosts in cloud computing environments are just as vulnerable to attack as those in on-premise environments and the impact can be devastating. While standalone vulnerability management tools can be used in on-premise environments which are relatively static, they are ineffective in dynamic cloud environments. These tools perform periodic scans of an environment to identify hosts with missing patches based on IP address. However, public cloud environments are constantly changing and IP addresses are elastic, which makes the results unreliable.



The RedLock Cloud 360 platform provides the context that is necessary to be able to identify risks such as host vulnerabilities. It correlates security data from your public cloud environment with vulnerability data from third party tools. This enables you to monitor for vulnerabilities and prioritize remediation for resources with high risk scores. You can also search for vulnerabilities across your entire environment in minutes based on severity, CVE IDs (Common Vulnerabilities and Exposures), and other attributes. For instance, you can run a query in a matter of minutes to determine if any of the hosts in your environment are impacted by the Spectre and Meltdown vulnerabilities.

Effective Cloud Threat Defense Requires Context

While organizations can address each responsibility in the shared security model as an individual problem, comprehensive cloud context is necessary to be effective. For example, organizations that are simply monitoring their public cloud environments for risky configurations will receive an alert if an open security group is created. However, the severity of the threat is hard to determine based on this data point alone. Alerts without context makes it hard to triage issues in a timely manner and ultimately leads to alert fatigue.

The RedLock Cloud 360 platform provides the necessary context by using AI to correlate disparate data sets including resource configurations, user activities, network traffic, host vulnerabilities/activities, and threat intelligence. This enables you to prioritize response based on the severity of issue. For the example above, the platform would raise a high severity alert if the open security group is associated with an unpatched MongoDB resource that is receiving traffic from a suspicious IP address.

Developing a Cloud Threat Defense Roadmap

RedLock enables organizations to develop their cloud threat defense program from inception to maturity with the following capabilities :

- **Compliance Assurance:** Mapping cloud resource configurations to compliance frameworks such as CIS, PCI, and HIPAA can be challenging. RedLock enables monitoring, auto-remediating, and reporting on compliance using out-of-the-box policies.
- **Security Governance:** Security governance is challenging in dynamic public cloud computing environments due to the lack of visibility and control over changes. RedLock enables architecture validation by establishing policy guardrails to detect and auto-remediate risks across resource configurations, network architecture, and user activities. With RedLock, organizations can finally achieve DevSecOps.
- **SOC Enablement:** Security operations teams today are being inundated by alerts that provide little context on the issues, which makes it hard to triage issues in a timely manner. RedLock enables identifying vulnerabilities, detecting threats, investigating current or past incidents, and auto-remediating issues across entire cloud computing environment in minutes.

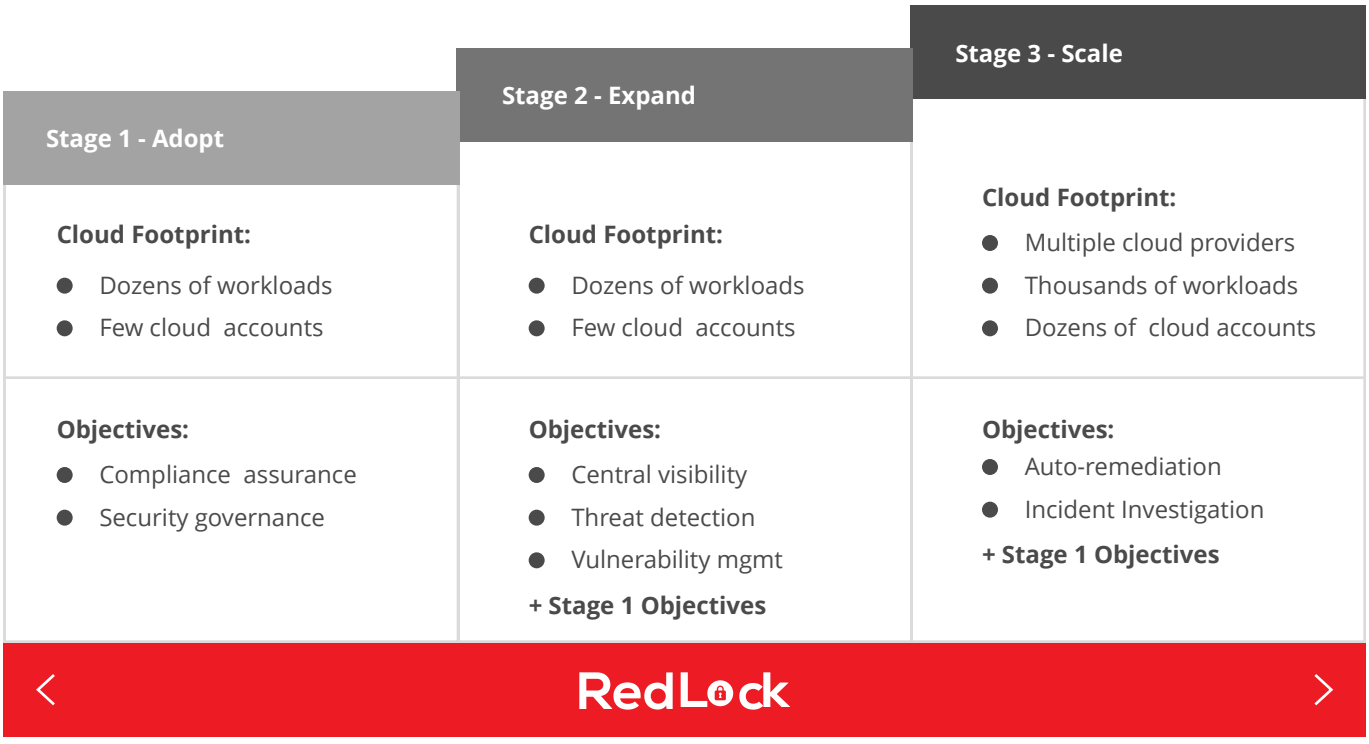


Figure 2: Cloud Threat Defense Maturity Model