Securing Microsoft Azure with RedLock® Cloud 360 Platform™

Implement effective cloud threat defense for Microsoft Azure with the RedLock Cloud 360 platform:

- Get visibility into assets and applications across your entire Azure environment
- Report on the security and compliance posture across your Azure environment
- Enable DevOps by setting guardrails and monitoring for threats such as risky configurations, sensitive user activities, network intrusions, and host vulnerabilities
- Detect account compromises and insider threats with anomaly detection capabilities
- Investigate current threats or past incidents and quickly determine the root cause
- Receive contextual alerts to prioritize issues and respond appropriately

RedLock Enables Cloud Threat Defense for Microsoft Azure

Public cloud computing adoption is outpacing 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. While point security solutions may be able to address each discrete challenge, they lack context and create alert fatigue.

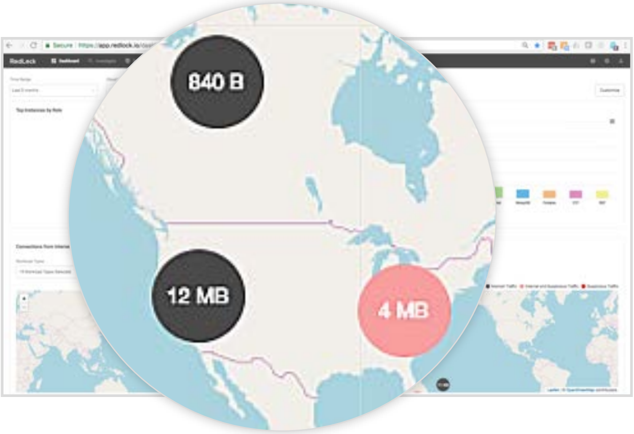
At RedLock, we believe that more information - and context - leads to better security decision making. Which is why RedLock dynamically discovers cloud resource changes and continuously correlates raw, siloed data sources including user activity, resource configurations, network traffic, threat intelligence, and vulnerability feeds to provide a complete view of public cloud risk. The RedLock Cloud 360™ platform takes a new AI-driven approach and enables organizations to fulfill their obligations in the shared responsibility model, including:

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

RedLock Cloud 360 Platform

Comprehensive Visibility

The RedLock Cloud 360 platform enables you to visualize your entire Azure environment, down to every component within the environment. The platform dynamically discovers cloud resources and applications by continuously correlating configuration, user activity, and network traffic data. Combining this deep understanding of the Azure environment with data from external sources such as threat intelligence feeds and vulnerability scanners, enables it to produce context around risks. For example, the platform may discover that databases running MongoDB exist within your cloud environment.



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

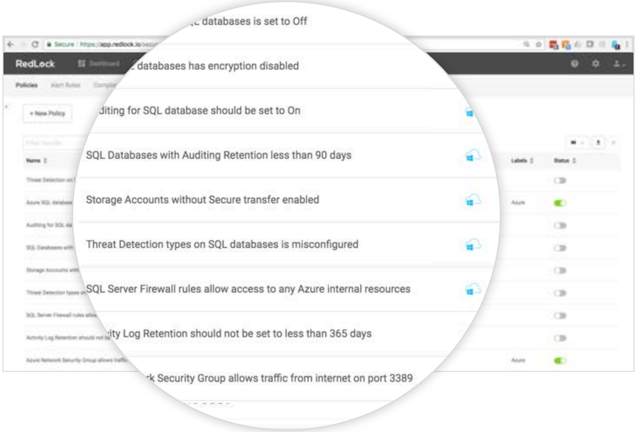
Compliance Reporting

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 Azure 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.

Similar to a credit score, the platform computes risk scores for every resource based on the severity of business risks, violations, and anomalies. This quickly identifies the riskiest resources and enables you to quantify your overall security posture to management or the board. Using the example above, you could implement a policy to alert you if any MongoDB databases are running vulnerable versions of software.



databases is set to Off

databases has encryption disabled

diting for SQL database should be set to On

SQL Databases with Auditing Retention less than 90 days

Storage Accounts without Secure transfer enabled

Threat Detection types on SQL databases is misconfigured

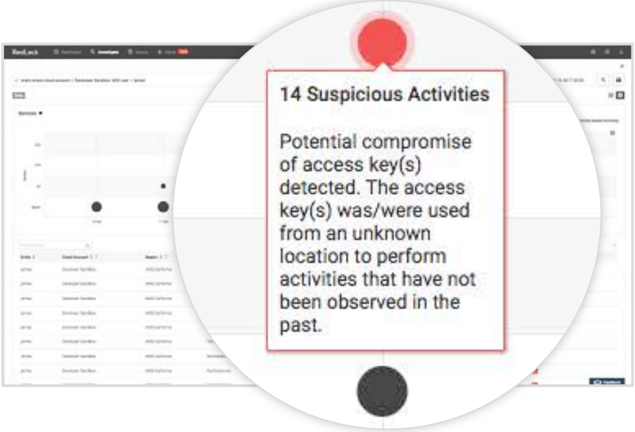
SQL Server Firewall rules allow access to any Azure internal resources

ity Log Retention should not be set to less than 365 days

k Security Group allows traffic from internet on port 3389

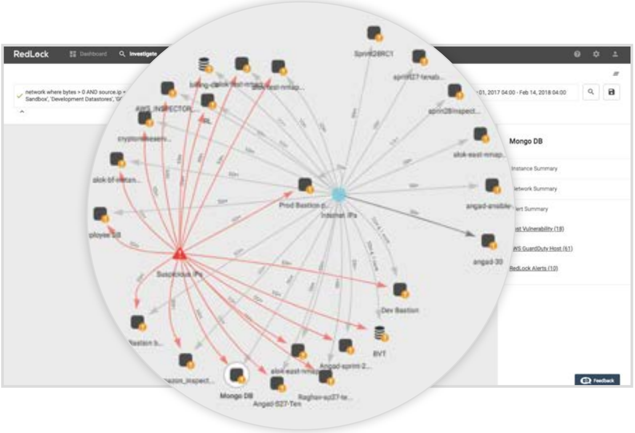
Threat Detection

The RedLock Cloud 360 platform automatically detects user and entity behavior anomalies across your entire Azure 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.



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.

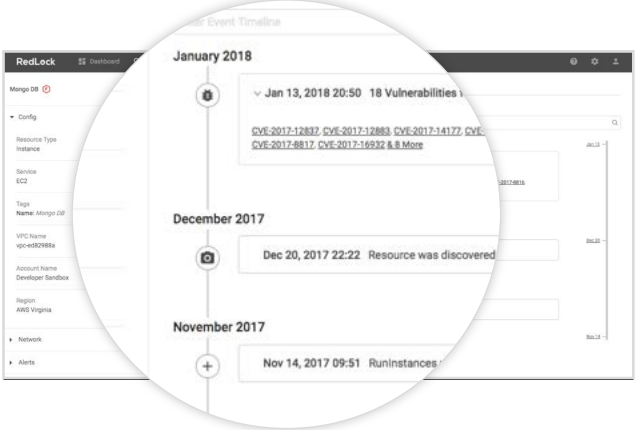


Incident Investigation

The RedLock Cloud 360 platform's deep understanding of the Azure environment, reduces investigation time from weeks or months to seconds. You can use the platform's graph analytics to quickly pinpoint issues and perform upstream and downstream impact analysis. The platform provides you with a 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 & 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 alerts can also be sent 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.



Mongo DB

Config

Resource Type
Instance

Service
EC2

Tags
Name: *Mongo DB*

VPC Name
vpc-ed82988a

Account Name
Developer Sandbox

Region
AWS Virginia

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

Developing a Cloud Threat Defense Roadmap for Microsoft Azure

RedLock enables organizations to develop their cloud threat defense program across entire Azure environments 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 pre-packaged 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 Azure environments in minutes.

Stage 1 - Adopt	Stage 2 - Expand	Stage 3 - Scale
Cloud Footprint: ● Dozens of workloads ● Few cloud accounts	**Cloud Footprint:** ● Hundreds of workloads ● Many cloud accounts	**Cloud Footprint:** ● Multiple cloud providers ● Thousands of workloads ● Dozens of cloud accounts
Objectives: ● Compliance assurance ● Security governance	**Objectives:** ● Central visibility ● Threat detection ● Vulnerability mgmt **+ Stage 1 Objectives**	**Objectives:** ● Auto-remediation ● Incident Investigation **+ Stage 2 Objectives**

RedLock

Cloud Threat Defense Maturity Model