REDLOCK ON MICROSOFT AZURE

Protect all resources in your Azure environment with RedLock by Palo Alto Networks

Benefits of RedLock on Azure

- Visualize every connected resource across your Azure environment
- Maintain continuous compliance and easily generate reports across your Azure environment
- Enable secure DevOps by setting guardrails with real-time 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 more quickly
- Integrate seamlessly with native Azure services, including Azure Security Center

RedLock Simplifies Cloud Threat Defense for Microsoft Azure

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 point security products may be able to address individual challenges, they are unable to provide holistic protection in an environment where resources are constantly changing.

RedLock® – Palo Alto Networks cloud security and compliance service – 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. Through an innovative, machine learning-driven approach, RedLock 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 Microsoft Azure

Unmatched Visibility

Visualize your entire Microsoft Azure® environment, down to every component. RedLock dynamically discovers cloud resources and applications by continuously correlating configuration, user activity and network traffic data. Combining this comprehensive understanding of the Azure environment with data from external sources, such as threat intelligence feeds and vulnerability scanners, enables RedLock to deliver complete context for each risk.

Simplified Cloud Compliance

RedLock 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. RedLock continuously monitors for policy violations across all connected resources and supports one-click reports for simplified audits of your Azure environment.

Policy Guardrails

RedLock 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. RedLock 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

RedLock automatically detects anomalies in user and other behavior across your entire Azure 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.

Incident Investigation

With deep understanding of the Azure environment, RedLock 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

RedLock 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 third-party tools, such as Slack®, Demisto® and Splunk®, to remediate issues. In the case of a risky database, RedLock will generate a contextual alert with information on risk factors to enable automated response.

RedLock Integration With Azure Security Center

RedLock integrates with Azure Security Center to provide centralized visibility into security and compliance risks across your entire Azure environment. With this, your security teams can quickly gather data, identify threats and take action before business damage or loss occurs.

Developing a Cloud Threat Defense Roadmap for Microsoft Azure

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

- **Compliance assurance:** Mapping cloud resource configurations to compliance frameworks, such as CIS, GDPR, PCI and HIPAA, can be extremely time-consuming. Using prepackaged policies, RedLock 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. RedLock enables architecture validation by establishing policy guardrails to detect and auto-remediate risks across resource configurations, network architecture and user activities. With RedLock, you can finally support DevOps agility without compromising on security.
- **SOC enablement:** Security operations teams are inundated with alerts that provide little context on the issues, which makes it hard to triage issues in a timely manner. RedLock makes it possible to identify vulnerabilities, detect threats, investigate current or past incidents, and remediate issues across your entire Azure environment 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 management **+ Stage 1 objectives**	**Objectives:** • Auto-remediation • Incident investigation **+ Stage 2 objectives**

Figure 1: Cloud Threat Defense Maturity Model

Security Operating Platform

RedLock provides comprehensive visibility, threat detection and rapid response across your entire public cloud environment, including Amazon Web Services, Microsoft Azure and Google Cloud Platform. 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 investigation with automated reports, threat prioritization and remediation. With its API-based approach, RedLock delivers superior cloud-native security.

RedLock is part of the Palo Alto Networks Security Operating Platform, providing organizations with a multidimensional approach to public cloud security delivered through inline, API- 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, such as AWS®, Azure or GCP™; or have been moved to a SaaS application, we can protect them.

Visit our website to learn more: paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com