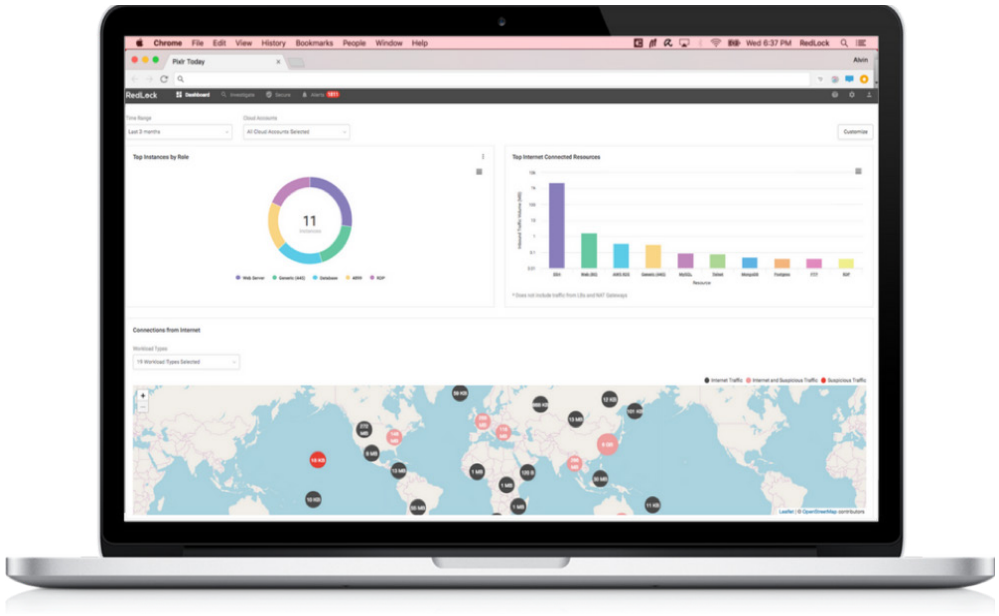
AT A GLANCE
REDLOCK

Continuous Visibility and Threat Defense for a Secure, Compliant Public Cloud

Threat defense at the speed of DevOps requires the ability to correlate disparate data sets and detect anomalous patterns across diverse resources.

With RedLock® by Palo Alto Networks, organizations can harness the power of machine learning to maintain compliance and govern security, even across the most fragmented multi-cloud environments.



Challenges

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 all increase the attack surface by orders of magnitude. The resulting pressure on SecOps teams is immense.

An organization's obligations in the Shared Responsibility Model include monitoring for risky configurations, anomalous user activities, suspicious network traffic and host vulnerabilities. Although point security products may be able to address each discrete challenge, they lack context and create alert fatigue.

A Better Approach: Continuous Threat Defense With Contextual Intelligence

To be truly effective, security needs comprehensive cloud context. For example, an organization that simply monitors its public cloud environments for risky configurations will receive an alert if an open security group is created. However, the severity of the threat is difficult to determine based on this data point alone. Alerts without context make it challenging to triage issues in a timely manner, ultimately leading to alert fatigue.

RedLock ranks every potential threat and network vulnerability via an intuitive A through F scale and delivers complete context through interactive diagrams. By using machine learning to correlate disparate data sets, including resource configurations, user activities, network traffic, host vulnerabilities/activities and threat intelligence, SOC teams can quickly prioritize responses based on the severity of each issue. In the earlier example, if the open security group were associated with an unpatched MongoDB® resource receiving traffic from a suspicious IP address, RedLock would raise a high-severity alert.

RedLock enables effective cloud threat defense across AWS®, Azure® and GCP™ environments.

AT A GLANCE
REDLOCK

Continuous Visibility and Threat Defense for a Secure, Compliant Public Cloud

Risky Resource Configurations

Because the cloud allows users to create, modify and dynamically scale resources, IT ops and security teams often have little involvement or oversight. Combined with the adoption of DevOps methodologies, this means manual monitoring and auditing of configurations in IT-controlled environments is impractical because it hinders development agility.

With prepackaged policies and single-click compliance reports for CIS, NIST and PCI, RedLock helps you monitor cloud resources for configuration drift. You can also build custom policies based on your organization's needs. RedLock continuously monitors for policy violations by existing resources as well as newly created resources that are generated dynamically. As an example, RedLock will trigger an alert if a user exposes an Amazon S3 bucket to the public.

Suspicious User Activities

Access to on-premises environments is typically locked down and centrally monitored by IT. In contrast, multiple users have privileged access to public cloud environments, which enables productivity but increases risk of exposure.

It is imperative to monitor users for suspicious activities across your entire cloud environment. Unfortunately, the distributed architecture of public cloud environments – with users scattered across multiple accounts and regions – leads to decentralized visibility.

RedLock enables you to detect issues, such as account compromises and insider threats within your public cloud deployments, by establishing behavior baselines and flagging deviations. For example, a potential access key compromise will be flagged if a user is accessing keys from an unknown location to perform previously unobserved activities.

Network Intrusions

A physical perimeter around an on-premises network reduces the risk of exposure by completely blocking any networking vulnerabilities. In contrast, the virtual perimeter in public cloud environments is significantly more vulnerable because a single programmatic error could expose the entire network to attacks.

It's critical that organizations vigilantly monitor their network traffic and detect suspicious activity. However, traditional network monitoring tools create security blind spots since they cannot be deployed to monitor traffic to or from API-driven services in the cloud. Palo Alto Networks Unit 42 cloud research team uncovered malicious cryptomining activity that had gone undetected at multiple well-known organizations.

RedLock enables you to detect network intrusions and suspicious actions by correlating network traffic data with data from your public cloud environment and third-party threat intelligence sources. For example, RedLock will trigger an alert if a MongoDB resource accepts a connection from a suspicious IP address.

Host Vulnerabilities

Unpatched hosts and access vulnerabilities in cloud environments are quickly exploited in today's automated threat landscape. Organizations have relied on dedicated vulnerability management tools in on-premises environments, but these tools are far too static and slow for dynamic cloud environments. They only periodically scan the environment to identify, based on IP address, hosts with missing patches. Because public cloud environments are highly elastic and IP addresses frequently change, the results can be unreliable.

RedLock identifies risks, such as host vulnerabilities, through context-based machine learning. It builds a more complete picture of your security posture by correlating data from your public cloud environment as well as vulnerability data from third-party tools. This enables you to monitor for vulnerabilities and seamlessly prioritize remediation efforts based on risk score. You can also search for vulnerabilities across your entire environment in minutes based on severity; Common Vulnerabilities and Exposures, aka CVE, IDs; 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 affected.

AT A GLANCE
REDLOCK

Continuous Visibility and Threat Defense for a Secure, Compliant Public Cloud

RedLock Approach	Benefits
Comprehensive Visibility and Monitoring	Visualize your entire multi-cloud environment, down to each and every component. RedLock dynamically discovers cloud resources and applications by continuously correlating configuration, user activity and network traffic data. Combined with data from external sources, such as threat intelligence feeds and vulnerability scanners, only RedLock provides the context required to quickly and accurately pinpoint risks without creating alert fatigue.
Compliance Reporting	Get single-click reports for common compliance standards. RedLock provides prepackaged policies that adhere to industry-standard best practices, and also supports custom policies. With continuous monitoring for policy violations by both existing and new resources, you can continuously maintain a robust compliance posture at the speed of DevOps.
Policy Guardrails	Enable "DevSecOps" by setting policy guardrails for DevOps teams, so they can maintain development agility without accidentally exposing sensitive data or admin keys. RedLock detects risky configurations, sensitive user activities, network intrusions, host vulnerabilities and more, and computes risk scores for every resource based on the severity of business risks, violations and anomalies, so you can quickly respond to risks and maintain a strong security posture.
Threat Detection	Detect user and entity behavior anomalies across your entire multi-cloud environment with RedLock by automatically establishing behavior baselines and flagging any deviations or anomalies.
Incident Investigation	Reduce investigation time from weeks – or months – to seconds. RedLock's visualized analytics and near-native integration with public cloud environments help you quickly pinpoint issues. Comprehensive logs display time-stamped activity for every resource, meaning you can review the history of a resource to better understand the root cause of an incident, whether past or present.
Contextual Alerting & Adaptive Response	Quickly respond to issues based on contextual alerts, triggered based on a patent-pending risk scoring methodology that delivers unmatched contextual intelligence on all risk factors associated with a resource. This makes it simple to prioritize the most critical risks. You can also send alerts, orchestrate policy or perform auto-remediation.

Figure 1: RedLock approach and benefits

Security Operating Platform

RedLock provides comprehensive visibility, threat detection and rapid response across your public cloud environments, including Amazon Web Services, Microsoft Azure and Google Cloud Platform. The specialized combination of continuous monitoring, compliance assurance and security analytics purpose-built for the public cloud enables security teams to rapidly respond to critical threats by replacing manual investigation with automated reports, threat prioritization and remediation. RedLock's near-native integration and API-based approach allows security to be embedded directly into the application development process, enabling DevSecOps.

RedLock is part of the Palo Alto Networks Security Operating Platform, providing enterprise 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 larger enterprise, 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 environment; or have been moved to a SaaS application, we can protect them.