RedLock

Business Case

for Cloud Threat Defense

Table of Content

Executive Summary

RedLock enables effective threat defense across Amazon Web Services, Microsoft Azure, and Google Cloud environments. The RedLock Cloud 360TM platform takes a new machine learning-assisted approach that correlates disparate security data sets to provide comprehensive visibility, detect threats, and enable rapid response across fragmented cloud environments. With RedLock, organizations can ensure compliance, govern security, and enable security operations across public cloud computing environments.

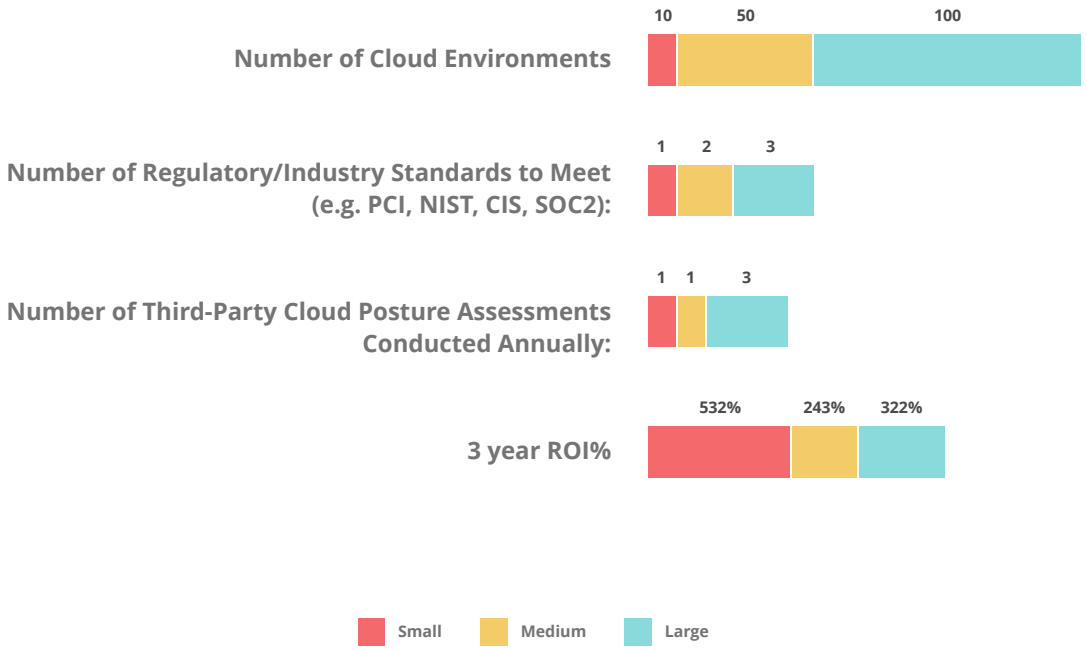
To better understand the benefits, costs, issues and risks associated with implementing a cloud threat defense solution, RedLock surveyed its customer base to understand the specific areas of savings and cost avoidance. Customers use RedLock's cloud-native software-as-a-service (SaaS) solution for a variety of use cases: visibility, security governance, compliance assurance, reduced third-party tools and labor requirements, and reduced financial risk due to security breaches. RedLock customers reported the following benefits:

RedLock Benefits

Impact	Cost Avoidance	Benefits
Security Operations	• Avoid manual cloud posture assessment costs • Reduced efforts to investigate and resolve potential security risks • Avoid development and maintenance of a log management system • Reduced financial risk due to security breaches	• Eliminate the cost, management and overhead associated with third-party cloud posture (penetration testing) assessments • Reduce time-to-remediation with actionable alerts prioritized by risk ranking • Eliminate the need for homegrown or third-party SIEM systems • Significantly reduce the probability of economic, asset or brand loss due to security breaches in your cloud environments
Compliance	• Eliminate efforts to manually map traditional compliance controls to public cloud • Reduced labor to comply with audit verification requirements	• Save time, resources and money with out-of-the-box compliance reporting based on industry standards such as PCI, NIST, SOC 2, HIPAA, CIS, GDPR, and more
DevOps	• Avoid delays and rework required with trying to force-fit traditional security controls into public cloud	• Provide security and compliance teams continuous visibility into public cloud environments • Integrate automated remediation into development workflows

Key Findings of RedLock Cost-Benefit Analysis

Based on sample sizes of representative customer cloud environments, the three-year ROI% for RedLock are estimated* as:



*Note that these do not include RedLock license costs and should be subtracted from this model).

Public Cloud Security Requirement

The adoption of the public cloud is remarkable; the worldwide public cloud services market is projected to grow 21.4 percent in 2018 to total $186.4 billion, up from $153.5 billion in 2017, according to Gartner, Inc. But this rapid growth introduces new risks. Gartner forecasts that 95% of cloud security failures through 2022 will be the customer's fault1.

As you evaluate solutions for ensuring cloud compliance and security, discussions regarding repurposing legacy data-center security solutions, building your own security and compliance solution, or buying a cloud-native security product may have become a top-of-mind topic. According to a survey by Crowd Research Partners, only 16% of organizations found their existing security measures were adequate to protect them in the cloud.

While building a solution internally may sound attractive, the reality is quite different. Dozens of point cloud security tools do exist, but most are ineffective for comprehensively addressing the most common and pressing cloud security challenges:

- **Visibility:** Unlike a traditional on-premise data center, where an organization has complete visibility and control over all assets, migrating to the cloud introduces major blind spots. Keeping track of assets and accurately identifying risks is challenging due to the cloud's ephemeral nature, fragmented ownership by individual lines of businesses, multiple regions, and multiple service providers. Simply put, a Configuration Management Database (CMDB) for the cloud is typically non-existent in most organizations.

- **Compliance Management:** Cloud service providers are releasing new capabilities into their platforms daily, as organizations demand new features and developers want to adopt the latest technologies. Environments are changing by the minute. With such speed of change, how does one map traditional compliance and regulatory controls from the on-premise era to the cloud? And more importantly, how do you produce auditor-friendly historical reporting to prove these environments were in compliance at all times?

- **Threat Detection:** Discovering a variety of risks in the cloud is essential for a safe, hygienic environment. Detecting if resource configurations drift from policy-defined best practices, identifying account compromises or insider threats, and pinpointing suspicious network traffic are all elements of an effective cloud threat defense. None of the these can be solved with traditional security tools.

- **Incident Response:** Having hundreds or thousands of data points about your cloud environments is, by itself, not enough to effectively respond to cloud threats. You must be able to respond based on a holistic view of your environments. This requires correlaing disparate data from your assets: resource configurations, user activities, network traffic, and host vulnerabilities/activities, third party threat intelligence sources, etc., to produce the necessary context. Only then will you have information for actionable alerts, enabling prioritized response based on the severity of issue.

Beyond these fundamental cloud security challenges are the additional implications of what building your own cloud threat defense solution means to people, processes and technology in your organization. Other questions to consider are:

- When I have a breach or a misconfiguration, how will I know and how will I respond?
- What hardware and software will I need to develop a custom solution?
- How will I staff the maintenance and upkeep of a custom solution?
- Can I afford the 9 to 24-month cycle to build my own solution?
- Can I monitor all my cloud resources from a single pane of glass?
- Do I have the right people to design and build a cloud threat defense solution?
- What are the impacts to my DevOps and SecOps teams?

Savings and Benefits with RedLock

The RedLock Cloud 360 platform yields measurable savings and benefits in the following areas:

Reduced Labor to Meet Compliance Requirements

Cloud resource compliance reporting and auditing is challenging, time consuming and expensive. RedLock estimates that it initially takes 480 hours to map controls to each compliance standard and produce the required reports. In subsequent years, it takes 240 hours for maintenance, reporting, and audit support. With the RedLock Cloud 360 platform, mapping cloud resource configurations to compliance frameworks such as CIS, NIST, SOC 2, PCI, HIPAA and GDPR is a standard, out-of-the box feature. This can free up substantial resources to work on other strategic efforts.

Third-Party Cloud Posture Assessment Cost Avoidance

Periodically assessing risks in cloud environments is an area where most organizations do not have the in-house expertise or tools to be effective. As such, organizations rely on third parties who specialize in this area to conduct these tests on an annual basis. We estimate such assessments take anywhere from 3 to 5 business days of a Consultant's time per cloud account, all of which can be eliminated with continuous security monitoring using RedLock.

Reduced Labor to Investigate and Resolve Security Risks

SOC teams typically do not have the expertise or the tools to investigate and act on security alerts generated from cloud service providers (CSP) or other open source security tools, such as AWS Guard Duty, Security Monkey, etc. This problem only becomes worse with organizations adopting multiple cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

RedLock addresses these challenges by providing SOC teams with the unified ability to monitor, measure and prioritize risks across all public cloud environments. RedLock alerts contain all the relevant information, including but not limited to the nature of the risk, when it was introduced and by whom, its impact on the environment, exploitation status, and details on how to remediate the risk. Armed with this information, SOC analysts can reduce investigation time by 75% by focusing on the alerts with the highest priority, and take action without having to engage in out-of-band conversations with DevOps teams, or manually investigate issues using multiple tools.

Cost Avoidance of a Third-Party Log Aggregation Solution

SIEMs (Security Information and Event Management systems) are expensive to use, as their cost is driven by the amount of data that is ingested. This is in addition to associated hardware costs, and part or full-time system administrators to maintain these systems. With RedLock, this data aggregation is included in the platform, thus enabling customers to only feed relevant alerts into the enterprise SIEM, and reduce storage costs by 95%. RedLock estimates it can help customers avoid $5,000 per account cloud environment for hardware and software for log aggregation, plus up to one full time headcount.

Reduced Financial Risk Due to Security Breaches

In 2017, the Ponemon Institute estimated the average cost of a security breach was $7,350,000, and the likelihood of a security breach was 6%. With RedLock, organizations can comprehensively identify cloud security risks, and use the platform's in-depth analytics to quickly understand the exact nature and ramifications of the risks, and resolve issues faster. By getting ahead of the threats and vulnerabilities, RedLock estimates it can reduce likelihood of breaches by 50% in the first year of operation, and 75% in years two and beyond once the outstanding security exposures are addressed.

Financial Analysis

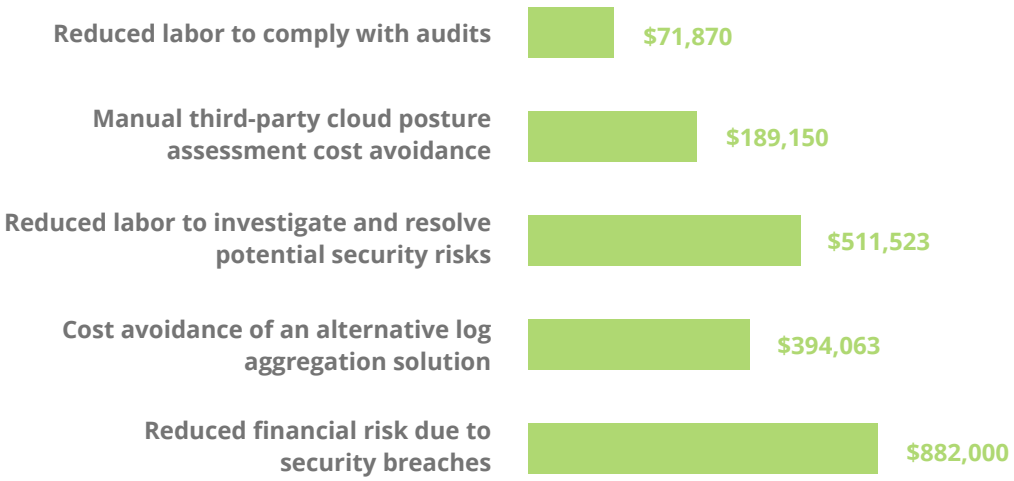
With these customer-based estimates, the following models represent the detailed RedLock savings for three different environments. Again, note these do not include RedLock license costs and should be subtracted from this model.

5  Average Alerts Per Cloud Account per Day	**$150,00**  Fully Loaded FTE Cost
$250  Third-Party Consulting Hourly Rate	**24**  # of Hours Per Cloud Account for Third-Party Testing Activity
60  Time to Investigate & Resolve Each Cloud Alert Manually (in minutes)	**15**  Time to Investigate & Resolve Each Cloud Alert with RedLock (in minutes)

Model 1: Small Cloud Environment

10	1	1
# of Cloud Environments:	# of Regulatory/Industry Standards to Meet (e.g. PCI, NIST, CIS, SOC2)	# of Third-Party Cloud Posture Assessments Conducted Annually

Benefits

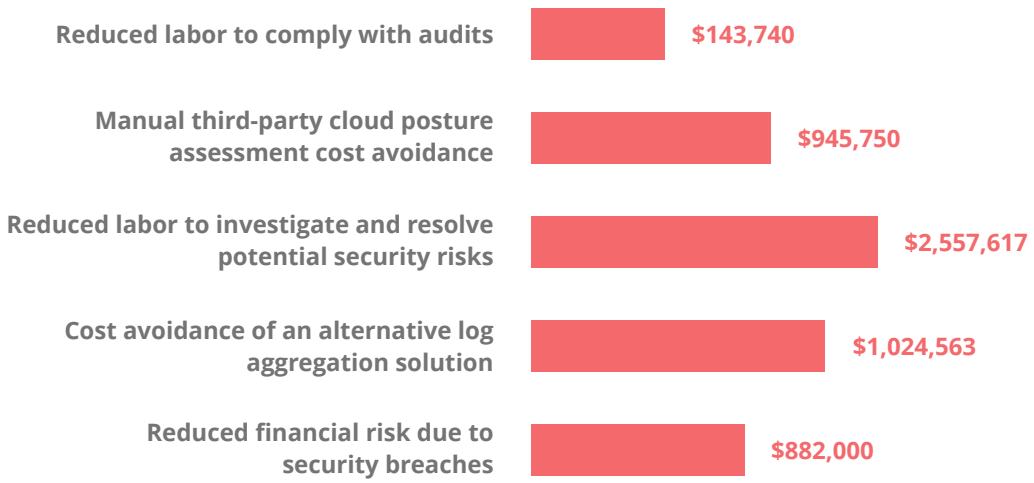


Total Benefit Over 3 Years: $2,048,606

Model 2: Medium Cloud Environment

50	2	1
# of Cloud Environments:	# of Regulatory/Industry Standards to Meet (e.g. PCI, NIST, CIS, SOC2)	# of Third-Party Cloud Posture Assessments Conducted Annually

Benefits

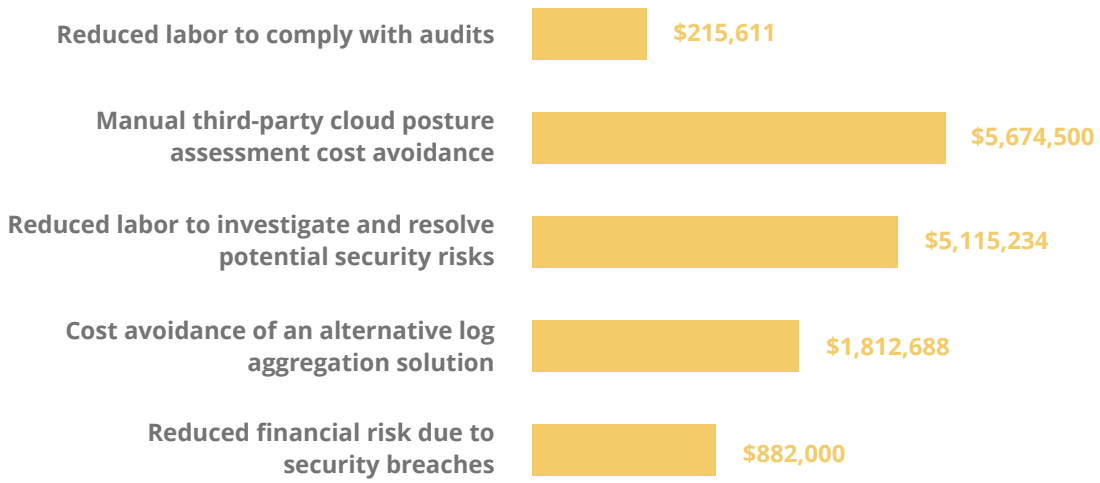


Total Benefit Over 3 Years: $5,553,670

Model 3: Large Cloud Environment

100	3	3
# of Cloud Environments:	# of Regulatory/Industry Standards to Meet (e.g. PCI, NIST, CIS, SOC2)	# of Third-Party Cloud Posture Assessments Conducted Annually

Benefits



Total Benefit Over 3 Years: $13,700,032

Conclusion

Organizations can expect to save substantial money, time and resources, while also ensuring compliance and maintaining a strong security posture when using RedLock. Savings accrue in many areas, including reduced labor associated with: audits, third-party posture assessment, threat investigation, and third-party tool management. Ancillary systems such as third-party SIEMs can be avoided altogether. Perhaps most importantly, RedLock can reduce the likelihood of a security breach, further protecting organizational assets.