# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Key Takeaways</td>
<td>4</td>
</tr>
<tr>
<td>01 - Data exposures are on the rise</td>
<td>5</td>
</tr>
<tr>
<td>02 - Vulnerabilities are being neglected in the cloud</td>
<td>7</td>
</tr>
<tr>
<td>03 - Risky users are flying under the radar</td>
<td>9</td>
</tr>
<tr>
<td>04 - Nefarious network activities are rampant</td>
<td>11</td>
</tr>
<tr>
<td>05 - Cloud attack kill chains are complex</td>
<td>13</td>
</tr>
<tr>
<td>About the Report</td>
<td>15</td>
</tr>
<tr>
<td>Ready to Take Action?</td>
<td>16</td>
</tr>
</tbody>
</table>
For years, *Game of Thrones* has enthralled audiences around the world as dynastic noble families fought to claim the Iron Throne. Each battle was epic and involved carefully crafted defensive and offensive strategies.

Defending today’s complex public cloud computing environments requires a similar sophisticated approach. The absence of a physical network boundary to the internet combined with the risk of accidental exposure by users with limited security expertise, increases the attack surface in the cloud by orders of magnitude. It is imperative for organizations to develop an effective strategy to protect their Amazon Web Services (AWS), Microsoft Azure, and Google Cloud environments.

The RedLock Cloud Security Intelligence (CSI) team studied threats across public cloud computing environments from June to September 2017 and published their findings in this report to highlight key issues.
1. Data exposures are on the rise

Fortune 1000 organizations have been in the news each week due to data exposures caused by cloud misconfigurations. Organizations are failing to adhere to established security best practices based on standards such as CIS Foundations and PCI DSS.

2. Vulnerabilities are being neglected in the cloud

Organizations are unable to leverage their existing vulnerability management investments to identify vulnerable hosts without context on cloud resources.

3. Risky users are flying under the radar

Poor security hygiene and ineffective monitoring is leading to increased account compromises, and prompting the need for better vigilance over user credentials and activities in public cloud computing environments.

4. Nefarious network activities are rampant

The incidence of network intrusions into public cloud computing environments are prompting the need for effective network monitoring.

5. Cloud attack kill chains are complex

Attacks on public cloud computing environments are growing in complexity and require a holistic approach to cloud threat defense.
2017 has seen its share of cloud misconfigurations that led to massive exposures. Deep Root Analytics exposed 198 million American voter records (99% of citizens), Time Warner Cable exposed 4 million records, and Dow Jones exposed 2.2 million records, just to name a few. One would imagine that there is growing awareness amongst organizations about the risks of cloud misconfigurations. As a result, the RedLock CSI team assessed database and storage resources in public cloud environments for public exposure.

**Key Findings**

The RedLock CSI researchers discovered that 53% of organizations using cloud storage services such as Amazon Simple Storage Service (Amazon S3) had inadvertently exposed one or more such services to the public. It appears that this is trending upwards despite growing awareness about the risks of misconfigurations; earlier in May this number was 40%.

Organizations simply cannot rely on security awareness trainings for users to avoid these kinds of mistakes. Proactive configuration monitoring needs to be in place to detect issues as soon as they arise.

The findings prompted the team to assess the overall compliance posture of public cloud computing environments against industry standards such as the CIS Foundations and the PCI data security standard. On average, organizations fail 45% of CIS checks and 46% of the violations were high severity issues such as network configurations that allow inbound SSH connections from the internet. In comparison, organizations fail 48% of PCI checks and 19% of the violations were high severity issues such as databases not being encrypted.
Data exposures are on the rise

Tips

1. Automatically discover resources as they are created in a public cloud computing environments.

2. Monitor configurations to ensure that they adhere to industry standards such as CIS and PCI.

3. Consider auto-remediation workflows to immediately resolve issues.
Vulnerabilities are being neglected in the cloud

The recent Equifax breach made headlines not only due to its sheer size (143 million records) but also due to the sensitivity of the data that the hackers made off with. Investigations revealed that the attack vector was a vulnerability in the Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application. U.S. CERT had reported the vulnerability back in March 2017.

Essentially, the Equifax application was left unpatched and exposed to the internet. While the importance of patching critical resources is well understood, many organizations simply cannot keep up. Research from the RedLock CSI team indicates that the host vulnerability situation is particularly dire in cloud computing environments, where the average lifespan of a workload is only 127 minutes.

Key Findings
The RedLock CSI team’s research revealed that 81% of organizations are not managing host vulnerabilities in the cloud. While most have existing investments in third party vulnerability scanning tools such as Qualys and Tenable, organizations are unable to map the data from these tools to gain cloud-specific context. Specifically, identifying hosts that are missing patches by IP addresses is not actionable, since IP addresses are constantly changing in the cloud.

Host vulnerability data needs to be correlated with host configurations in the cloud that can help identify the business purpose of the host and help prioritize patching. For example, is this host a webserver or a database server? Is it running in production or staging? In addition, the network traffic should be monitored to identify whether the vulnerabilities are actually exploitable.
02 Vulnerabilities are being neglected in the cloud

Tips

1. Continuously ingest third party vulnerability feeds into a cloud security monitoring solution to have centralized visibility with cloud-specific context.

2. Correlate vulnerability data with cloud configuration and network traffic data to identify the riskiest assets, and determine whether the vulnerabilities are actually exploitable from the internet.

3. Automatically classify workloads to establish criticality of the host, and prioritize remediation accordingly.
Risky users are flying under the radar

250 organizations leaking credentials to their cloud environments on internet-facing web servers

38% organizations with potential account compromises

89% account compromises detected due to changes in activities performed

The OneLogin breach earlier this year was a stark reminder about the importance of managing access and monitoring user activities in cloud computing environments. A hacker had obtained a set of access keys for OneLogin’s AWS environment and was able to access database tables containing sensitive data.

More recently, researchers disclosed that Viacom, the Fortune 500 corporation that owns Paramount Pictures, as well as cable channels such as MTV, Comedy Central, and Nickelodeon, exposed a vast array of internal access credentials and critical data that could be used to cause immense harm to the multinational corporation’s business operations. These incidents prompted the RedLock CSI team to investigate access hygiene and account compromise risks within cloud computing environments.

Key Findings

The team found 250 organizations (including large multi-national corporations) with similar issues where they were leaking access keys and secrets for their cloud computing environments on internet-facing web servers. In addition, hundreds of organizations were found to be leaking credentials via misconfigured services like Kubernetes and Jenkins.

This is concerning because keys often tend to have overly permissive access than is necessary for the role which creates greater exposure. In the OneLogin breach, the access keys that the hackers acquired had elevated privileges which allowed them to create instances for reconnaissance and ultimately access sensitive data.
Aside from closely managing access, organizations must also be vigilant about monitoring user activities within their cloud computing environments to detect insider threats or account compromises. This can be achieved using artificial intelligence to baseline user behavior and identify deviations from the norm. The RedLock CSI team determined that 38% of organizations have users whose accounts have potentially been compromised. There are a number of factors that help ascertain account compromises but in 89% of the cases, a change in the activities performed by a user was the leading indicator of compromise.

## Tips

1. **Enforce multi-factor authentication on all privileged user accounts.**

2. **Create a policy to automatically force periodic rotation of access keys.**

3. **Establish user behavior baselines and monitor for deviations to detect account takeovers or malicious insider activity.**
Nefarious network activities are rampant

A few weeks ago, hackers held 26000 MongoDB instances for ransom. In one case, the ransacked database contained three years of leukemia patient data that was being recorded to do research for better treatment plans. However, ransomware attacks on MongoDB instances began almost a year ago and MongoDB had posted an advisory back in January explaining how to prevent these attacks. Essentially, these unpatched databases were exposed to the internet and accessed by the hackers; the nefarious network activity had gone completely unnoticed by the impacted organizations.

This incident highlights the importance of having effective network intrusion detection solutions in place. However, this is non-trivial task and requires sifting through massive volumes of network data to find “a needle in a haystack”. The RedLock CSI team analyzed petabytes of network data for public cloud computing environments and only 0.5% of the traffic originated from suspicious IP addresses. However, a deeper analysis of the suspicious traffic uncovered some serious issues.

Key Findings

The team discovered that 37% of databases are accepting inbound connection requests from the internet. This is a very poor security practice as databases should never be directly exposed to the internet. To make matters worse, the research revealed that 7% of these databases are receiving requests from suspicious IP addresses which indicates that they have been compromised. The team noted that this can lead to serious exposure since 64% of databases are not encrypted.
Tips

1. Ensure services are configured to accept traffic from the internet on an as-needed basis.

2. Introduce behavioral modeling capabilities that can identify the roles of each host. For example, have the ability to distinguish a host running a web server from one that is running a database service like MongoDB, since policies for both hosts would be very different.

3. Monitor environment for suspicious traffic to cloud resources, particularly those that are not load balancers or web gateways.

4. Implement a “deny all” default outbound firewall policy.

5. Ensure databases are encrypted to prevent data exfiltration in the event of a breach.
Cloud attack kill chains are complex

The RedLock CSI team recently exposed hackers that were using organizations’ AWS computing resources to mine Bitcoins. The impacted organizations included large multinational corporations such as Aviva and Gemalto. Given the concerns around nation-state hackers stealing bitcoins to fund political campaigns, it is important to deconstruct the kill chain of this attack and proactively implement measures to defend against advanced cloud threats.

Key Findings

The investigation began when the RedLock CSI team found a number of Kubernetes administrative consoles deployed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform that were not password protected. These instances were effectively open to the public and created a window of opportunity for hackers. Having a configuration monitoring solution in place across the cloud computing environments could have exposed this serious misconfiguration.

Upon deeper analysis, the team discovered that hackers were executing a Bitcoin mining command from one of the Kubernetes containers. The instance had effectively been turned into a parasitic bot that was performing nefarious activity over the internet. This highlights the need for effective network monitoring solutions in public cloud computing environments to detect suspicious activity.

To make matters worse, the team found access keys and secret tokens stored in plaintext within these unprotected Kubernetes instances. Hackers could use these to access critical infrastructure and cause more damage. It is imperative to monitor
The incident highlights the need for a holistic approach to security in the cloud. A combination of configuration, user activity, and network activity monitoring is necessary to detect these complex threats in public cloud computing environments.

Tips

1. Monitor cloud resources to detect misconfigurations and auto-remediate issues.

2. Monitor inbound and outbound network traffic and correlate with resource configurations to spot suspicious activity.

3. Monitor user activity for suspicious behavior to detect insider threats or account compromises.
RedLock CSI Team

RedLock enables effective security governance across Amazon Web Services, Microsoft Azure, and Google Cloud environments. The RedLock Cloud 360™ platform takes a new AI-driven approach that correlates disparate security data sets including network traffic, user activities, risky configurations, and threat intelligence, to provide a unified view of risks across fragmented cloud environments. With RedLock, organizations can manage risks, validate architecture, and enable security operations across cloud computing environments.

The RedLock Cloud Security Intelligence (CSI) team consists of elite security analysts, data scientists, and data engineers with deep security expertise. The team's mission is to enable organizations to confidently adopt public cloud computing by researching cloud threats, advising organizations on cloud security best practices, and frequently publishing out-of-the-box policies in the RedLock Cloud 360™ platform.

The CSI team has discovered millions of exposed records that contain sensitive data belonging to dozens of organizations ranging from small businesses to Fortune 50 companies. The team notifies the affected organizations and publishes security advisories to raise awareness about the issues.

Report Methodology

The data in this report is based on analysis across RedLock’s customers’ environments which comprises of over five million resources that are processing petabytes of network traffic. In addition, the team also actively probed the internet for vulnerabilities in public cloud computing environments.
Get a Free Risk Assessment

Get started in minutes and obtain a free risk assessment across your cloud footprint without hindering agile development. It will provide the following insights:

- Are there any resources with risky configurations?
- Are there unpatched hosts in your environment?
- Have there been any network intrusions?
- Are there any insider threats?
- Have any accounts been compromised?


Download Cloud Security Buyer’s Guide

Download the Cloud Security Buyer’s Guide to get 20+ tips based on the NIST Cybersecurity Framework and manage risks across your public cloud computing environment.

“The RedLock Cloud 360™ platform provides Veeva with the tools it needs to continuously monitor our environment, quickly identify and respond to issues, and provide improved visibility on its compliance posture.”

David Tsao
Global Information Security Officer (CISO), Veeva Systems