RedLock
Cloud Threat Defense

4 Emerging Cloud Security Threats

February 2018

73% of organizations are allowing root user activities

16% of organizations with potential account compromises

1 Account compromises are on the rise

Poor user and API access hygiene is leading to an increase in account compromises.

When combined with ineffective visibility and user activity monitoring, it makes organizations even more vulnerable to breaches, Tesla being a recent victim.

8% of organizations had cryptojacking activity within their environments

2 Changing tides: from stealing data to stealing compute

The soaring value of cryptocurrencies is prompting hackers to shift their focus from stealing data to stealing compute power in an organization's public cloud environment.

The nefarious network activity is going completely unnoticed due to a lack of effective network monitoring.

58% organizations publicly exposed at least one cloud storage service

66% of databases are not encrypted

3 Long road ahead to GDPR readiness

Risky resource configurations can be attributed to a large number of the breaches in public cloud environments in 2017.

With GDPR coming into effect in a few months, organizations are under the gun to identify and address these issues as quickly as possible.

4 Spectre and Meltdown vulnerabilities - a rude awakening

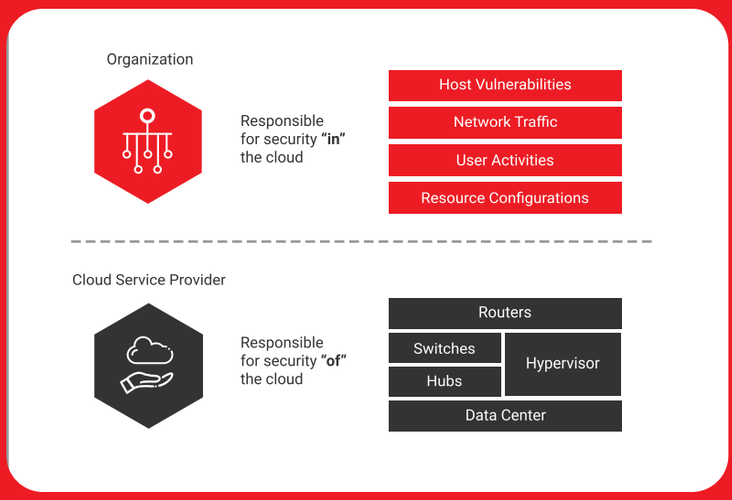
The impact of the Spectre and Meltdown vulnerabilities on public cloud environments was a wakeup call for organizations to address vulnerability management in the cloud.

Unfortunately, organizations are unable to leverage their standalone on-premise tools to achieve this since they were not designed for cloud architectures.

83% of vulnerable hosts are receiving suspicious traffic

15% of vulnerable hosts flagged as compromised by Amazon GuardDuty

Security is a Shared Responsibility



Want tips to avoid these pitfalls?
https://info.redlock.io/cloud-security-trends-feb2018

Ready to take action?
https://info.redlock.io/cloud-risk-assessment