SKYBOX SECURITY

2019 CLOUD TRENDS

RESEARCH REPORT

About This Report

All information and data in this report without explicit reference is provided by the Skybox® Research Lab, a team of security analysts who daily scour data from dozens of security feeds and sources as well as investigate sites in the dark web. The Research Lab validates and enhances data through automated as well as manual analysis, with analysts adding their knowledge of attack trends, cyber events and TTPs of today's attackers. Their ongoing investigations determine which vulnerabilities are being exploited in the wild and used in distributed crimeware such as ransomware, malware, exploit kits and other attacks exploiting client– and server–side vulnerabilities. This information is incorporated in Skybox® Security's vulnerability management solution, which prioritizes the remediation of exposed and actively exploited vulnerabilities over that of other known vulnerabilities.

For more information on the methodology behind the Skybox Research Lab and to keep up with the latest vulnerability and threat intelligence, visit www.vulnerabilitycenter.com.

References to figures from "this year" refer to data sets from January 1 through September 30, 2019. References to figures from "Q3 2019" refer to data sets from July 1 through September 30, 2019.

EXECUTIVE SUMMARY

Cloud infrastructure as a service (IaaS) resources are known for having strong, innate security and are favored for being quick to deploy while helping to reduce costs and improve efficiency. Because of this, it's no surprise that these services are exploding in terms of popularity: one estimate suggests that 83 percent of enterprise workloads will be run on public cloud infrastructure by 2020[1].

While the hunger for cloud services is growing, this is often to the detriment of an organization's overall security. Deployments are moving forward at such a rapid speed that they can outpace the security initiatives needed to underpin their success. Devops teams are working under assumptions about "security in code" that don't consider the lifespan and permutations of their creations. These assumptions need to be dismantled in order to improve the overall security of cloud services and how they relate to other portions of the hybrid, corporate network.

This report asserts that gaining visibility of, and being able to securely manage, cloud services is the biggest cloud-related problem facing security teams today. To ensure the security of IaaS cloud, organizations need to establish new processes which can be used to eliminate misconfigurations and enforce more rigorous testing.

The report analyzes the increase in cloud IaaS–related vulnerabilities and demonstrates how third–party plugins and applications are expanding the attack surface and introducing new risk to the organization. In addition to providing the insight needed to inform the security of IaaS cloud deployments, the report also offers best practices for improving policy management capabilities to eliminate misconfigurations, demonstrates how to introduce network modeling and shares ways to strengthen overall cloud network security.

The devil's in the details when it comes to cloud security. This report aims to give security leaders the information that they need to understand which details matter most to their organizations and the tools that they need to improve their organizations' risk posture.

1 Source: Forbes - https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020#2e513c5b6261

KEY FINDINGS

Misconfigurations pose the greatest risk to cloud security

Although vulnerability counts relating to IaaS cloud services are climbing, they don't present the most important cloud-related risk to organizations. Misconfigurations of cloud IaaS and a lack of rigor in testing is damaging enterprises' risk posture.

The number of vulnerabilities reported which affect cloud IaaS is likely to increase by 50 percent by the end of 2019

The volume of vulnerabilities which exist within cloud IaaS products is increasing as the services continue to grow in popularity. The steady year-on-year growth reported here shows no sign of slowing down.

Cloud container vulnerabilities have increased by 82 percent over 2019

In July 2019's mid-year update to the Skybox *Vulnerability and Threat Trends Report*, Skybox reported that cloud container vulnerabilities had increased by 46 percent when compared to the same period in 2018. That share has since increased to 82 percent, highlighting cloud containers as a key area of concern.

Third-party plugins and applications are expanding the attack surface

Eight vulnerabilities which, if exploited, could lead to exposure of user data, were found in the popular plugin build system, Jenkins. Vulnerabilities which arise from third-party plugins and applications will increase, and their security is not the responsibility of the cloud vendor which may use them. Their security needs to be fully considered by customers.

TERMS AND PARAMETERS

The analysis within this report pertains largely to cloud IaaS providers. Any reference to vulnerability counts is drawn from National Vulnerability Database (NVD) reports.

Public vs. private IaaS: Data in this report does not differentiate between public and private cloud offerings: this is due to the lack of information available about public cloud services, as flaws are dealt with on the server–side before they reach the NVD. Also many cloud services offer a combination of both public and private cloud elements, making it difficult to separate the two.

Products and services: Products and services selected for analysis were carefully chosen to focus on those with the most impact to major enterprises. This report also includes analysis of products that, while not exclusive to cloud, play a significant role in the use of cloud infrastructure, such as containers, orchestration platforms and devops tools.

Vulnerabilities: The process used to determine vulnerabilities in this report worked as follows:

- Identify cloud services and products that appeared in any vulnerability reports, filtering out any that did not pertain to the cloud
- Determine which vulnerabilities also existed in products which play a significant role in the use of cloud infrastructure

Understanding vulnerabilities and inherent risks of the technologies outlined in this report is important as they are often:

- Outside of the control of the customer as is the case with IaaS cloud service providers (CSPs) who are responsible for security of the underlying infrastructure
- Of greater risk the deeper they are in the cloud technology stack, impacting security of all services built on top of them (e.g., one container vulnerability can put countless microservices at risk)
- Overlooked or inaccessible to many security teams as security within the cloud may be outside their purview
- Easily replicated due to the fast and dynamic nature of the cloud

Using these methodologies, the report speaks to the real cloud-related problems facing corporations today and is intended to provide the insight needed to inform future cloud deployments.

RESULTS

It's important to remember that vulnerabilities do not present the greatest security risk to organizations' cloud environments. That title falls to the security protocols which surround the deployment of cloud IaaS resources — misconfigurations and lack of testing are leaving businesses exposed to security and compliance risks. Nevertheless, it is still necessary to understand more about cloud-related vulnerabilities (i.e., vulnerabilities that are either within products that are exclusive to cloud, or play a key role in the use of cloud IaaS) and also how their growth compares to the state-of-play for all vulnerabilities.

Overall Vulnerability Count Increases as Backlog Deepens

To understand cloud-related vulnerabilities in the bigger picture, let's first consider all vulnerabilities. NVD vulnerabilities have continued to accumulate in Q3 2019 in keeping with expected trends (for more information, see the 2019 mid-year edition of the *Vulnerability and Threat Trends Report*).[2]

Notably, there were 1,994 new vulnerabilities reported in August 2019. This is relatively high when compared to the 1,526 reports in the boom year, 2017, and nearly double the 2018 figure. This should not necessarily be cause for major alarm: these numbers suggest that the NVD is still working its way through a backlog of older vulnerabilities while still reporting on new instances.

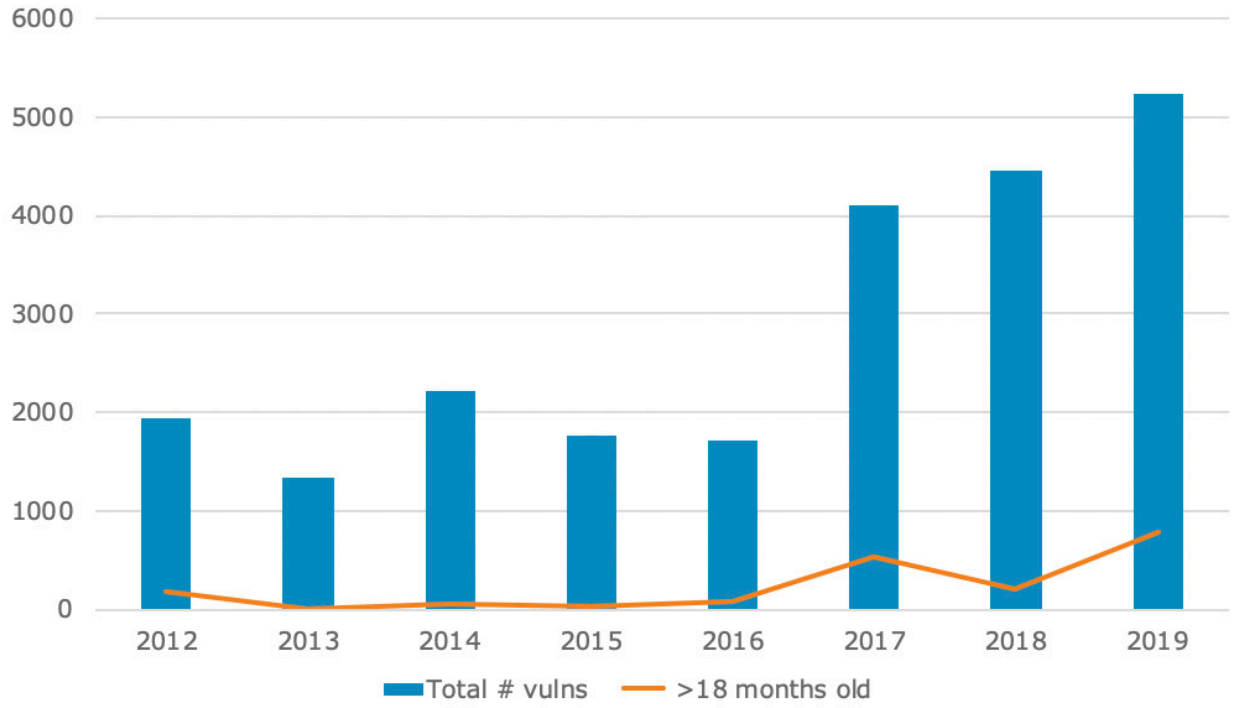

FIG 1 | New and backlogged vulnerabilities cataloged in Q3s by year

2 Source: CVE Details - https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

Cloud IaaS Vulnerabilities Increase

The number of new vulnerabilities identified within IaaS resources is escalating. Although the overall vulnerability counts may seem relatively small, the fact that the number of reported CVEs grew by 50 percent between 2017 and 2018 is worth acknowledging. It's possible that we'll see a similar increase by the end of 2019: our research shows that the total number of new cloud vulnerabilities reported so far this year is on course to outnumber 2018's count by over a third.

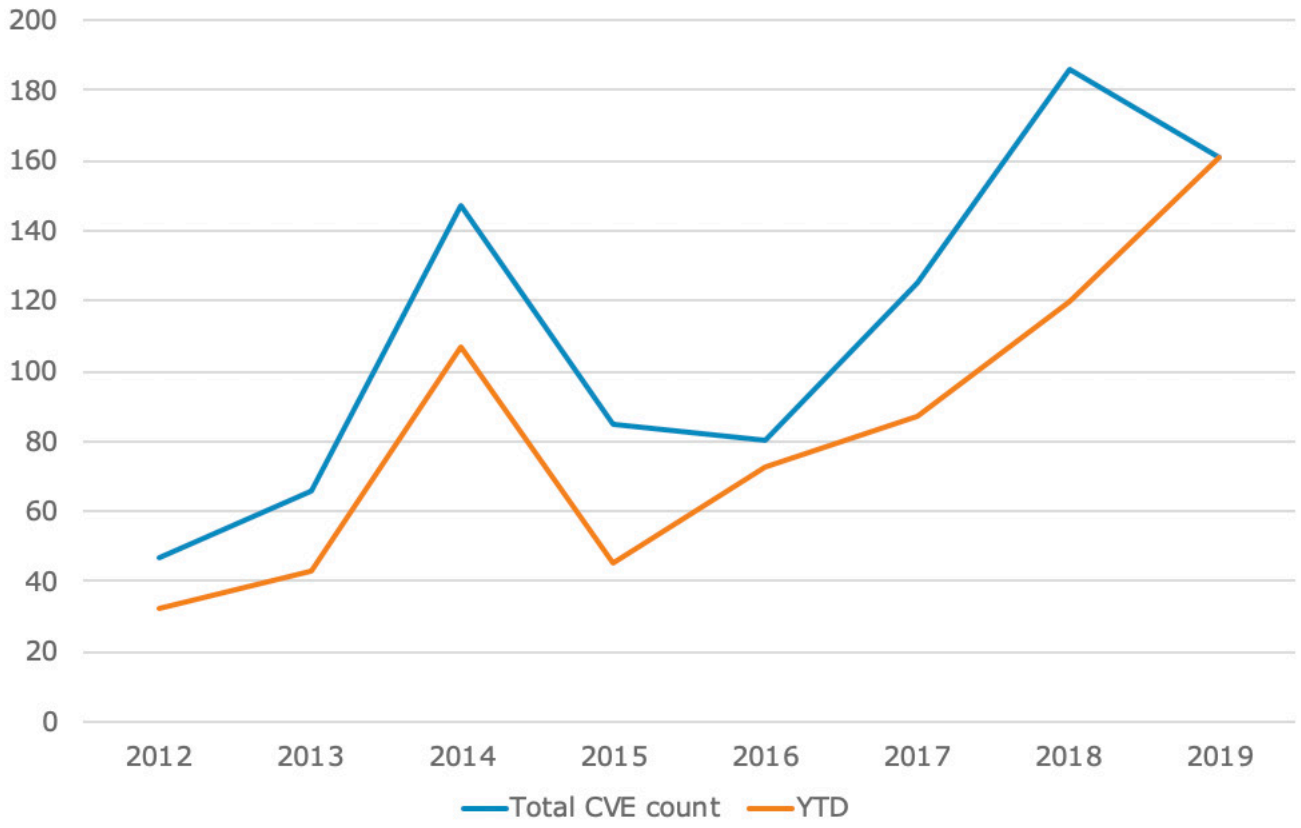

FIG 2 | Cloud IaaS vulnerability counts for year totals and year-to-date (i.e., January 1 through September 30 each year)

IBM is Most Vulnerable Cloud Vendor

The most vulnerable cloud vendor, by this research paper's definition, is the one with the largest number of NVD reports, combined with self-reports. It's important to note that there are known issues with the accuracy of NVD's figures. Smaller products and services are often overlooked by the NVD — this is not because they are more secure, but purely because the company is not big enough to be recognized. As such, this report also looks at vendor self-reports to help build a wider, more in-depth picture of the reality of vulnerabilities within IaaS vendors.

IBM's keenness to self-report its own vulnerabilities has led to it being named the most vulnerable cloud vendor, thus the title is not to say it is the most insecure. IBM has a number of cloud products[3], covering a wide range of applications with overlapping functionality and shared components, and a security vulnerability management function (IBM PSIRT) that is known for its transparency — it publishes detailed advisories and individual fixes on its own products even when the affected component has been bundled from a third party.

> Vulnerabilities that exist in bundled third-party components are very easily spread and are harder to detect from just looking at NVD. It is therefore likely that more vulnerabilities exist within vendor products than we are able to count.

> It's also worth noting that these vulnerability counts are still small. This could be because that these types of flaws have lived in the shadows for a long time: they were largely undiscovered, unreported or not critical enough to draw the attention of the industry.

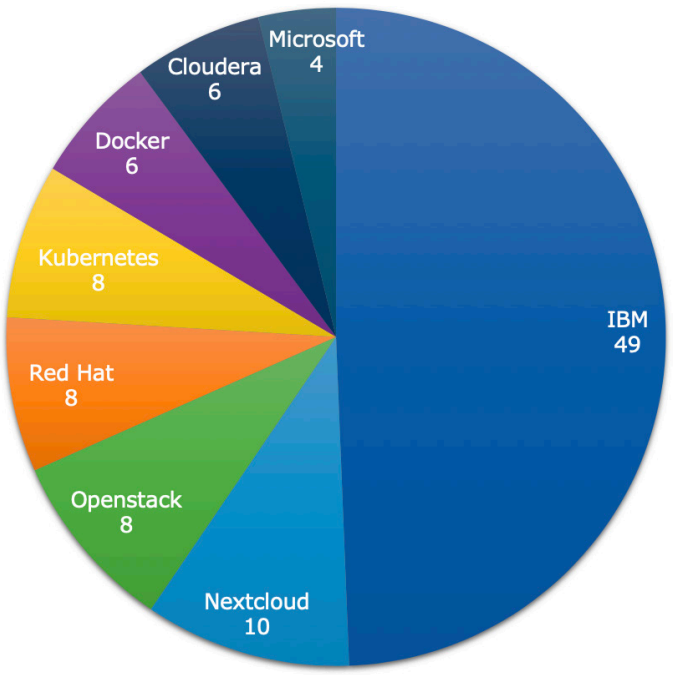

FIG 3 | Number of IaaS-related vulnerabilities per vendor

3 Source: IBM - https://www.ibm.com/cloud/products

Container Vulnerabilities Continue to Rise

Containers, which create a distinction between virtual servers hosted on a shared machine without emulating a full server environment, have recently been growing in popularity as businesses look for new ways to boost efficiency, particularly in relation to the cloud. The number of vulnerabilities within containers has been steadily increasing over the last couple of years: this year, there is a marked increase of 82 percent when compared with the same period in 2018.

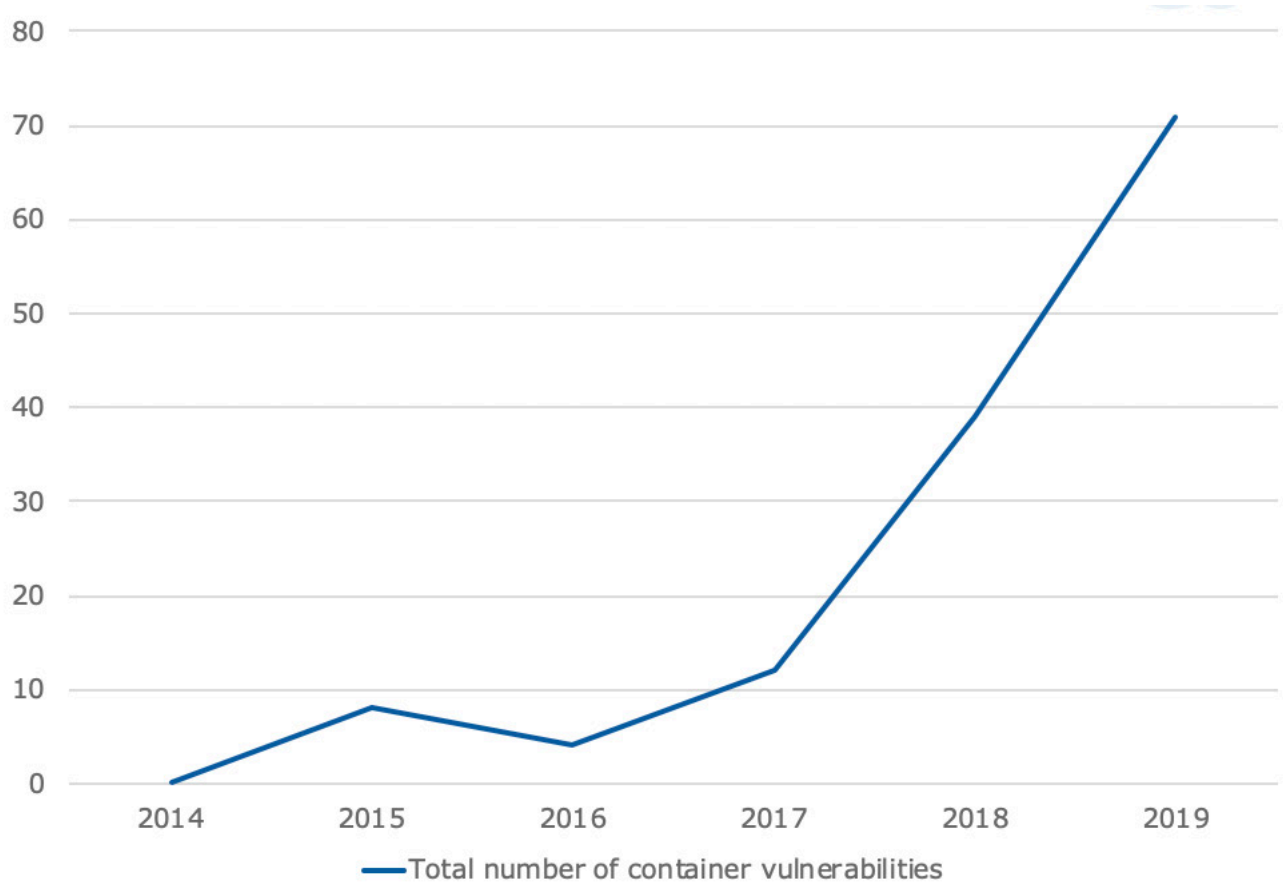

FIG 4 | Year-on-year increase of vulnerabilities within containers

Exploits

While there are no reports of IaaS or container vulnerabilities exploited in the wild, there have been a small number of published working proofs-of-concept (PoCs) that highlight the need for organizations to ensure the security of their cloud technology and maintain rigorous patching processes.

Of particular note is a simple PoC disclosed in late August which affected Docker for Windows[4]. The PoC demonstrated how the program's login command could be co-opted to run other programs of an attacker's choice. This is due to Docker's dependence on insecure locations within the Windows Program Data directory. If an attacker were able to place an executable file within the directory, and if a legitimate user of the system were then to attempt to log in as they normally would, the attacker would be given free rein to negatively impact the OS. A patch for this flaw was subsequently released.

There are also simple exploits that could be used by attackers relating to some inbuilt insecurities within cloud devices, including bad passwords and open buckets[5]. In order to counteract these flaws, it's critical for organizations to employ strong levels of cyber hygiene during the deployment and throughout the management of any cloud initiative.

4 Source: Morgan Henry Roman- https://medium.com/@morgan.henry.roman/elevation-of-privilege-in-docker-for-windows-2fd8450b478e

5 Source: The Test Labs- https://thetestlabs.io/code/exploiting-common-serverless-security-flaws-in-aws/

INSIGHTS

Understanding the Shared Responsibility Model

Amazon, the current leading provider of public cloud services[6], operates with total clarity in the way that, while they take responsibility for all flaws within their services, they place the authority over everything running on their infrastructure in the hands of the customer. They specify that "AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications"[7].

An incident this year illustrated this divide. When a string of vulnerabilities in popular container management software Kubernetes made a splash, Amazon issued two successive advisories[8,9]. Both warned customers of a flaw in the Kubernetes kubectl tool that allowed file system intrusion and, by extension, arbitrary code execution.

6 Source: Flexera - https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/#Container%20Use%20Is%20Up,%20and%20Kubernetes%20Use%20Is%20Skyrocketing

7 Source: Amazon - https://aws.amazon.com/compliance/shared-responsibility-model/

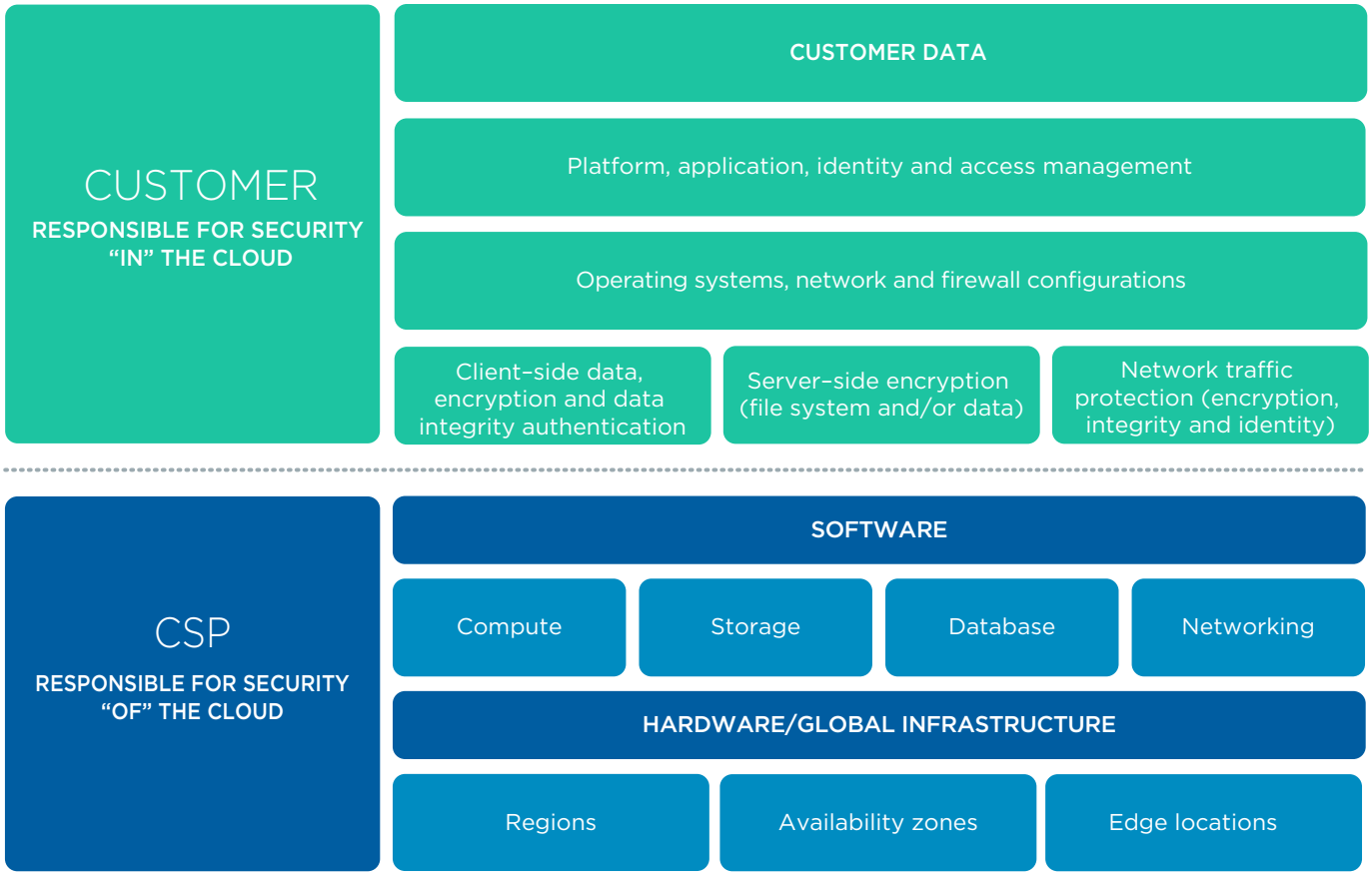

FIG 5 | An example of the shared responsibility model as described by Amazon

The kubectl copy command had been found susceptible to unintended directory traversal such that it could place files from within a container anywhere on the host machine and unpack them on the spot (CVE-2019-1002101). In June, there was a slight variation on this flaw still floating around in kubectl code that had been overlooked in the March fix, which was then addressed (CVE-2019-11246). It turned out that the latter change had diverted the problem to elsewhere in the program but did not fix the underlying issue, so yet another clean-up fix intended to finally close the hole was issued (CVE-2019-11249).

The kubectl module had been passed on to customers in Amazon's Kubernetes-loaded machine images until July, implicating the company in a software flow they neither develop nor support. As such, once the details of this cascade of vulnerabilities came to light, they took a minimal approach to remediation by leaving the onus of patching and installation to their customers. In fact, since kubectl was nonessential to the Amazon machine images it shipped with, the decision was made to cut their losses and simply remove it from all images as of a given date. Customers were informed of the need to upgrade by communication of the advisories.

Ultimately, the responsibility for securing any cloud service falls at the feet of the CISO and their security team.

There should be no assumptions about the responsibilities of the cloud service provider — even if they take responsibility for patching flaws within their technology, it's still the job of the security team to protect their organization's critical networks. This is even more true when considering the security which surrounds cloud apps and other cloud services. The vendor is not responsible for ensuring watertight configuration, segmentation, nor is it responsible for rigorous testing and monitoring "in" the cloud. These are all processes that should be owned and perfected by their customers.

8 Source: Amazon - https://aws.amazon.com/security/security-bulletins/AWS-2019-006/

9 Source: Amazon - https://aws.amazon.com/security/security-bulletins/AWS-2019-007/

Third-Party Plugins and Applications Have Expanded the Attack Surface

The increasing popularity of cloud services has brought with it an influx of third-party plugins and applications that are both in use by cloud vendors and directly by organizations themselves. These plugins can be quickly spun up and deployed, with each new iteration expanding the organization's attack surface.

The threat present in these third–party plugins and applications became clear during Q3 2019, when eight vulnerabilities were discovered in Jenkins, an automation and software build system for which is widely used to develop tools which increase agility and improve process orchestration. Jenkins itself is not a cloud–specific platform, but it does host plugins which are used by devops teams to improve efficiencies within their cloud deployments.

Interestingly, the Jenkins vulnerabilities share a few common traits which all underscore the risk that third–party plugins, in general, could introduce into a cloud environment. If exploited, all of the vulnerabilities could lead to the exposure of their users' identifying information, leading to bypasses of authentication and authorization checks. Some become dangerous only when chained with other exploits, but all are potential weakest points in the cloud environments that they serve.

The vulnerable plugins were developed independently and collaborated on using the Jenkins Project's own open–source web platform. They comprise interfaces with Docker and the Java cloud application development platform JClouds, both of which have multiple request forgery issues; Google Kubernetes Engine, which leaks access tokens; and two found to store passwords in config files: a plugin for IBM Application Security on Cloud and one for Skytap Cloud Continuous Integration.

The number of third–party cloud plugins in development and use is only going to increase. Although these plugins may be considered a minor investment and concern to large enterprises, if they are not properly secured and segmented then they could introduce new risk. These are not just throwaway services: their security needs to be fully considered, and they need to be properly configured and tested.

RECOMMENDATIONS

How to Improve Policy Management Capabilities in the Cloud

Working with IaaS resources can be a double-edged sword. While these services offer organizations a welcome opportunity to maintain control of access points and ensure compliance with internal and external policy requirements, they can also be easily misconfigured.

To avoid improper configuration, businesses need to enforce strict multi-factor authentication and be stringent with the authorization of managed policies. They need to know where all ingress and egress points are, who has access to them and have the ability to proactively respond to any potential attack vectors like misconfigurations.

Organizations also need to work to embed strong security practices within their devops processes, and ensure that all teams with responsibility for cloud security understand how policy enforcement differs between on-prem networks and clouds.

The Importance of Visibility

In the face of the regular and inevitable changes taking place in cloud infrastructure, organizations need to test their security and make sure that it is properly safeguarded. Nothing is static, and this is especially true when it comes to dynamic cloud environments. This is why it is vital for organizations to continuously monitor their environments and engage in thorough reporting — in order to manage their exposure to risks in the cloud, they need to have full visibility of their entire hybrid environment.

Organizations should start all monitoring activities by creating an attack surface model which shows all the ways in which they are susceptible to attacks. By modeling a network infrastructure that is inclusive of vulnerabilities and threat intelligence, enterprises will have an accurate view of how susceptible they are to attacks. Other information, such as app usage, as well as the type of data being uploaded and shared should also be incorporated into reports.

With this context-driven insight and visibility, actions can be accurately prioritized, moving security programs away from constant firefighting and towards developing more strategic and mature processes. With rich content classification, organizations can define and enforce granular policies that help automate data governance. Security teams should also plan a collection of roles to fill both shared and consumer-specific responsibilities. These roles should ensure that no one person can adversely affect the entire virtual environment. It is also possible to block specific unwanted behavior within cloud apps or encrypt specific types of information, leaving all the benefits of the cloud intact and still maintaining healthy security and compliance policies.

Best Practices for Strengthening Cloud Network Security

Each type of cloud needs to be evaluated based on the access and control you have to implement security measures: for example, in software as a service (SaaS) environments you may not have any access to implement security, whereas in infrastructure as a service (IaaS), you have a great deal of control. Cloud environments should also be evaluated for detection capabilities; in the case of a breach, it's important to know who's responsible for discovery and notification.

For standard IaaS, improper configurations of access controls and key management are common drivers behind cloud attacks. To avoid these risky misconfigurations:

- Don't assume that the cloud incarnation of a program will behave in the same way as the local version — follow the provider's guidance for development and deployment to avoid preventable pitfalls
- Enforce strict multi–factor authentication and be stringent with the authorization of managed policies
- Make sure to have backup policies in place and manage them properly — if you have too many, you're exposed to leakage; too few, and you're exposed to loss
- Continuously and thoroughly test your cloud infrastructure; model the network infrastructure and incorporate vulnerabilities and threat intelligence to gain an accurate view of how susceptible you are to attacks

CONCLUSION

Instead of focusing on cloud vulnerabilities, enterprises would be wise to concentrate on improving the security which surrounds the deployment of their cloud services. Investing in the cloud is never as simple as it looks on the surface: this is highly dynamic technology that is running a number of hosts that are as vulnerable as those which exist in on-premise environments. Unlike their on-premise counterparts, however, cloud services are often lacking the necessary security diligence to ensure effective network segmentation, access to resources and rigor in risk and vulnerability management.

The processes which many companies currently have in place to secure their cloud projects simply don't go far enough to guarantee proper testing both before, during and after the technology has been implemented. In order to make misconfigurations and similar issues a thing of the past, security — and security management — needs to be baked into any new cloud initiative from the very beginning.

Additionally, the CISO needs to ensure that they are able to influence security decisions around strategic initiatives like investments in cloud services. They need to make sure their team is seen to support and drive innovation, that they can provide visibility of increasingly fragmented security environments and work to become a true partner to operations teams. If they are able to achieve those feats, they will be well on their way to ensuring better cloud security — and business agility — within their organizations.

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 130 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060