Security Analysis of Cloud Security

Team Members

Alac Springer
Corban Sy
Epifanio Solano
Erik Ziegler
Jamison Stalter

Abstract

This paper will examine security practices and mechanisms of cloud services with example testing from ARP spoofing and vulnerability scanning via NMAP scripts. Analysis of security features and tools offered by the two leading providers, Amazon Web Services (AWS) Google Cloud Platform (GCP), aims to show the strengths and weaknesses of these platforms and what consumers can expect in protecting their applications from threats while also being made aware of their shared responsibility for security.

Intro

Cloud computing and services has become an integral and revolutionary part of modern business operations as scale and efficiency is more necessary than ever. Understandably, consumers can have some reservations about putting their data and applications in the hands of seemingly random servers elsewhere and how they are protected from threats. Two of the leading providers of these services, Amazon Web Services (AWS) Google Cloud Platform (GCP), offer many tools and features to combat data breaches and other security threats. While the services offered by both AWS and GCP are similar, these features have been refined over many years through serious certification and rigorous design.

This paper will focus on testing the AWS services via ARP spoofing and NMAP vulnerability scanning with the aim of showing the consumer how they are part of the solution to protect the cloud systems. Additional focus will be on examining the additional tools offered by AWS and GCP in how to combat these two scenarios and additional resources for protecting against other threats. These outcomes aim to help everyone involved in the use of cloud services better understand how to be smart, effective, and informed users in how to protect their applications while on cloud services.

Related Work

The purpose of our assignment was to find out the security features that Cloud Providers have and use a few well known tools to see what information they can get out of these servers. We used ARP Spoofing and NMAP as the tools to see what information can be taken from our cloud servers or how the providers repel against these attacks. It will be reiterated later in its own section but Cloud Security is a Shared Model, where Providers will ensure the machines are physically secured and that no VM can affect other VMs on the same box, but Users must also ensure that their applications are secure on a programmatic level.

Other works found that would be similar to our project's goal would be *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. This book was written during the beginning of the Cloud as a service (around 2010) but has the same goal of going over all the security features that are available to secure your applications. Whatever vulnerabilities that existed at the time the book was written may have been fixed but the book provides methods and strategies to help you stay secure when using a Cloud Environment that are still very relevant even today. The book also provides a comprehensive exploration of Cloud computing, starting with an introductory overview of its foundational concepts and then delves into various aspects, including service delivery approaches. Additionally, it tackles complex issues surrounding data ownership, privacy protections, bandwidth costs, and data protection strategies. The book thoroughly examines risk management in Cloud computing, discussing compliance, legal responsibilities, life cycle management, and disaster recovery planning both from the user's and the Cloud provider's perspectives. It also covers incident handling, remediation, application security, encryption, storage, virtualization, and access control, offering a comprehensive understanding of the intricacies and vulnerabilities of Cloud environments.

This book is written by cybersecurity professionals to help developers considering a move to the Cloud when it was a newer and emerging technology. In comparing this massive piece of work to ours, we try to provide some information on current day tools that can be used to test for vulnerabilities. When using Cloud Environments, one of the most important parts in making that decision is understanding the security capabilities and features that each provider has, as well as testing your applications security using extra tools as well.

Another piece of work that would be related to our assignment's objective is *A Comprehensive Guide to Cloud Security (Risks, Best Practices, Certifications)*. This is a great article that provides simple principles to secure and dangers to avoid when building your applications. This information is paired with the benefits of moving your project to Cloud Environments. This article, just like the book, is a great source of benefits of moving to the Cloud and a summary of security features that the providers give to Cloud Users. A unique piece of information this article gives, is a list of recommended Cloud Certifications that developers can pursue if they feel the description would be applicable to their project's needs.

ARP Spoofing

ARP Spoofing, also known as ARP Cache Poisoning, is a technique used by attackers to intercept network traffic between two hosts. To understand ARP Spoofing, it's important to know about the Address Resolution Protocol (ARP), which is responsible for mapping IP addresses to MAC addresses on a local network. When a device needs to communicate with another device on the same network, it uses ARP to find the MAC address associated with the IP address of the destination device.

ARP Spoofing works by sending fake ARP messages to a network, tricking other devices into associating the attacker's MAC address with the IP address of the victim. This allows the attacker to intercept, modify, or block traffic between the victim and other legitimate devices on the network.

A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts communication between two parties without their knowledge. ARP Spoofing is commonly used in MITM attacks because it allows the attacker to position themselves between the victim and the gateway (such as a router), effectively becoming the middleman.

Once the attacker successfully spoofs the ARP cache of the victim and the gateway, they can intercept all traffic passing between them. This enables the attacker to eavesdrop on sensitive information, such as passwords, credit card numbers, or any data transmitted over the network. Additionally, the attacker can modify the intercepted traffic before forwarding it to the intended recipient, allowing for various malicious activities.

To execute ARP Spoofing, the attacker typically follows a specific technique. Firstly, the attacker identifies the IP address of the gateway using the **arp -a** command, which displays the ARP cache table. From this table, the attacker can determine the MAC address associated with the gateway IP.

Once the gateway's MAC address is obtained, the attacker then uses the **arp -i eth0** command to spoof the ARP cache of the victim's IP address, replacing the legitimate MAC address with their own. This makes the victim believe that the attacker's MAC address is the correct one associated with the gateway.

As ARP Spoofing progresses, observable changes occur in the network. For instance, network administrators may notice the MAC address associated with the gateway suddenly changing to that of the attacker's device. Moreover, when inspecting ARP replies, they may see unexpected MAC address associations, such as "MAC address x talking to IP y," where x represents the attacker's MAC address and y the victim's IP. These observations indicate that ARP Spoofing is taking place, and network traffic is being redirected through the attacker's machine.

With the ARP cache poisoned, the attacker effectively intercepts all traffic intended for the gateway. By relaying this traffic through their own machine, they can inspect or modify it as desired before forwarding it to the legitimate gateway, and vice versa. This allows the attacker to

remain undetected while monitoring or altering the communication between the victim and the network.

In conclusion, ARP Spoofing is a powerful technique commonly used in Man-in-the-Middle attacks to intercept and manipulate network traffic. By exploiting vulnerabilities in the ARP protocol, attackers can deceive devices on a local network into sending data through the attacker's machine, giving them unauthorized access to sensitive information. Understanding the workings of ARP Spoofing is crucial for implementing effective security measures to protect against such attacks. Regularly monitoring network traffic and implementing techniques like ARP spoofing detection can help mitigate the risks associated with this type of attack, ultimately safeguarding the integrity and confidentiality of network communications.

Testing with NMAP

This research looks into the intricacies of cloud security, with a specific focus on using AWS Server in the free tier with Ubuntu and Linux platforms. We investigated several security techniques, including key pair security, TCP server scans, operating system scans, aggressive server scans, obscuration commands, and scripting engines. Despite hurdles such as AWS security features that prevent scans, our investigation highlights potential vulnerabilities and mitigation strategies that are critical for protecting cloud infrastructures.

To investigate cloud security, we used several different approaches, beginning with key pair security to prevent unauthorized server access. Following that, we ran TCP server scans with nmap, using techniques like full open scans and half-open scans to examine port status and potential vulnerabilities. In order to identify any risks and learn more about connected hosts, aggressive server and operating system scans were employed. Moreover, network filters and firewalls were circumvented by using obscuration instructions, and vulnerabilities were found using scripting engines.

Our experimentation yielded valuable insights into the security landscape of AWS Servers. Despite encountering limitations imposed by AWS security features, we identified potential vulnerabilities and highlighted the importance of robust security measures. The scans provided detailed information on open ports, operating systems, and potential vulnerabilities, empowering users to proactively mitigate security risks.

A Man-in-the-Middle (MITM) attack scenario, such as the infamous P00dle assault, demonstrates cloud infrastructures' vulnerability to sophisticated cyber threats. In such an assault, an adversary intercepts communication between two parties, potentially obtaining sensitive information. Using flaws in SSL/TLS protocols, attackers can decrypt encrypted data, posing serious security threats. Our experiment emphasizes the need for strong encryption techniques and ongoing monitoring to reduce the risk of MITM attacks and protect data integrity in cloud environments.

Throughout the project, we encountered challenges, particularly in bypassing AWS security features to conduct comprehensive scans. We adapted our approach, focusing on alternative scanning techniques. Despite these hurdles, our project serves as an outlook to the importance of adaptability, and security in the face of evolving security threats.

In conclusion, our experiment emphasizes the importance of cloud security and the need for ongoing detection in protecting cloud infrastructures. Moving forward, more study is needed to address the problems given by AWS security features and improve the effectiveness of security measures.

Cloud Security Features overview offered by AWS and GCP

As the leading providers for cloud services both AWS and GCP offer a robust amount of tools and features users can leverage to better safeguard their applications and data. While nothing can fully mitigate risk, better informed consumers will help both themselves and the service providers. This section provides a high level overview of some important tools provided by these service providers and ways to implement in your pipelines for better security.

AWS Security Features

AWS has a fully comprehensive and exhaustive security system that spans many levels of the service from the physical to the network. At the network level, AWS makes extensive use of the Virtual Private Cloud (VPC). This lets users isolate their products and applications fully within their own network, subnets, and security groups. By isolating user networks, users are better protected from data breaches and other security vulnerabilities introduced from other users. For example, if a user network is fully compromised and spreads to their full VPC, a different VPC will not be compromised. Security groups within the VPC also serve as a type of virtual firewall to help control traffic in and out of the instances. With full control of traffic, consumers can be confident that their products will only be accessible to certain individuals. This does come at the cost of necessary advanced knowledge and training for the consumer to make sure they are handling their security groups correctly.

Encryption at rest and in transit is another vital tool for securing data which is heavily used by AWS. By using the Key Management Service (KMS) users can expect to have their data encrypted at rest while within services such as S3 buckets, Elastic Block Store (EBS), or Relational Database (RDS). In transit data is protected via enforced TLS encryption protocols. KMS supports customer managed keys and adheres to strict regulatory requirements.

Monitoring and logging tools are additional services provided by AWS that can help users identify potential threats or ongoing security events. CloudTrail logs account activity and API usage giving an audit trail of action taken on the customer services. CloudWatch gives real-time

monitoring dashboards of consumers' resources. Users can see the health of these services and identify any issues easily. GuardDuty provides continuous monitoring for threat detection and checks for errant behavior.

An additional suite of features are being implemented that leverage AI-enhanced services. Macie helps to identify Personally Identifiable Information (PII). It uses machine learning and pattern recognition and gives a risk assessment on how to better fix the issue. For example, an S3 bucket may receive a bad score for unencrypted data or public access while containing potentially sensitive data. AWS Detective helps rebuild the sequence of events that led to a security issue by using machine learning and statistical analysis. By getting the logs and audit trails from other services such as CloudTrail and GuardDuty, Detective aggregates the data into a visual representation for easy auditing.

GCP Security Features

Google's security model is very similar to Amazon's by making sure users have access to strong access management, data security and encryption, and network security. GCP implements their own version of VPC with subnetting, traffic routing, and security policies to control access to resources. GCP's Identity and Access Management (IAM) service allows granular control over how services and resources are used and accessed. Security definitions can be as granular as needed to the extent that individuals can be restricted from specific actions on certain resources.

GCP also ensures data encryption at rest and in transit through similar means as AWS. Users can encrypt data through Google managed keys, consumer managed keys, or even consumer supplied keys. This flexibility allows users to expand their security management potentially even further with their own strong keys.

Data Loss Prevention API which is similar to AWS' Macie helps identify at-risk resources and data, Cloud Audit Logs give extensive details to the actions taken with the system, and Cloud Monitoring gives users exhaustive tools to monitor their services for threats and security events. GCP also leverages several other services to ensure customer resources are compliant such as Security Health Analytics to identify additional vulnerabilities and offer suggestions to fix them. Foresti is another tool that can be used to monitor services and ensure best security practices are being used.

Cloud Security Features to combat vulnerability scanning

Today's cybersecurity landscape has to face significant vulnerability scanning challenges as it can expose potential weaknesses in cloud infrastructures. We took a deep dive into the comprehensive set of security tools specifically designed to counteract such scanning activities and reinforce the robustness of cloud environments. Network Access Control Lists (NACLs), Virtual Private Cloud (VPC), AWS Web Application Firewall(WAF), and AWS Shield-each are tailored to mitigate the risks associated with unauthorized scans and probing activities. NACLs act as the first line of defense at the subnet level, allowing granular control over inbound and outbound traffic to prevent malicious data packets from scanning network resources. The VPC enhances this protection by enabling the creation of isolated network segments, where resource visibility and accessibility can be tightly controlled, reducing the attack surface visible to scanners. AWS WAF extends these defenses to the application layer, detecting and locking sophisticated scanning techniques that target web applications. Lastly, AWS Shield provides specialized protection against DDoS attacks, which are often preceded by scanning activities to identify exploitable vulnerabilities. Find our findings regarding the AWS tools, we can declare that the safeguards for AWS deployment are in good hands and are equipped with an integrated defensive strategy.

The NACLs are indispensable when it comes to security within AWS. The stateless firewalls control inbound and outbound traffic based off a set of rules processed in ascending order. The IP protocol, address range, and port number are all taken into account when battling unauthorized scans or potential intrusions. Using NACLs allows segmentation of the network so configurations are able to be customizable. A good example of this is public-facing subnets versus a backend database subnet both need to be configured drastically different from each other. The segmentation of these subnets reduces attack surfaces. This AWS security feature also has to ability to reject traffic from known malicious IP addresses or high-risk ports. NACLs work best with another tool like AWS CloudWatch which enhances visibility toward unusual traffic patterns. This pivotal role taken by NACLs is considered the first line of defense in the AWS infrastructure.

Building on the foundational security provided by NACLs, the Virtual Private Cloud (VPC) serves as a critical component when securing the AWS environment. The creation of segregated virtual networks that mimic a traditional data center empowers users to take control of the virtual network environment. Tasks like management of IP address ranges, configurations of subnets, and setups of route tables and network gateways are now put in the user's hands. VPC enhances security through the isolation of resources within distinct subnets which means it varies the levels of exposure to external traffic. This limiting exposure reduces risks of unauthorized access and vulnerability scanning. The subnets can be configured to be private of public which also can be beneficial against MITM attacks. VPC customization includes Internet Gateways (IGW) and NAT devices. This helps with the flexibility of network configurations to allow efficient communication between instances in the VPC and the internet. NAT devices safeguard instances on private subnets by keeping them unexposed to incoming internet traffic which is essential for a database server to remain shielded while maintaining necessary external connectivity. These additional layers of security allow more fine-grained access control

at the subnet and instance level while also applying strict rules that govern traffic flow. This control is vital for protecting against vulnerability scans cementing VPC as a cornerstone in secure cloud deployments by safeguarding data integrity and system availability.

Transitioning from network-level security measures with VPCs, AWS WAF (Web Application Firewall) plays a pivotal role in protecting web applications from sophisticated exploits that target the application layer. As a robust layer of defense, AWS WAF scrutinizes HTTP and HTTPS requests directed at applications, employing a comprehensive rule-based security system to filter and block potentially harmful traffic. This functionality is vital in preventing the exploitation of vulnerabilities within applications and operating systems hosted on AWS servers, safeguarding them against common threats like SQL injection and cross-site scripting (XSS). AWS WAF operates by allowing administrators to define customizable rules that dictate which requests should be allowed or blocked, enhancing the security granularity. These rules can target specific IP addresses, HTTP headers, or patterns in the HTTP body, making AWS WAF highly effective at identifying and mitigating attacks based on their signatures or anomalous behavior patterns. For example, blocking requests that do not contain expected tokens or identifiers can prevent unauthorized access, while rate-based rules help mitigate potential Distributed Denial-of-Service (DDoS) attacks by limiting requests from IPs exceeding certain thresholds. Moreover, AWS WAF's flexibility extends to its integration capabilities, notably with AWS Lambda for automating defensive responses and Amazon CloudWatch for continuous monitoring and alerting. This integration enables real-time security adjustments and insights, which are crucial for maintaining the integrity and availability of web applications. By setting up AWS WAF to work in conjunction with AWS Lambda, automated scripts can instantly update security rules in response to detected threats, thereby enhancing the reactive capabilities of the security infrastructure. The strategic deployment of AWS WAF is crucial for any security-sensitive project leveraging AWS. It not only blocks known attack vectors through managed rule sets but also offers the adaptability to customize protections to address new or evolving threats. This dynamic adaptability is essential for maintaining a robust defense against the ever-changing landscape of cybersecurity threats, particularly those that exploit application-level vulnerabilities. AWS WAF adds critical protections at the application layer that complement the previously mentioned subnet and network-level safeguards. Filtering and monitoring web traffic ensures the maintenance of both performance and reliability.

In the comprehensive defense against cybersecurity threats within the AWS ecosystem, AWS Shield stands as a critical component specifically engineered to combat Distributed Denial of Service (DDoS) attacks. This managed service is designed to protect applications on AWS by providing always-on detection and automatic mitigations that maintain application performance and minimize downtime during such attacks. AWS Shield is divided into two tiers: Standard and Advanced, offering a spectrum of protection that meets various operational needs and security demands. AWS Shield Standard provides basic DDoS protection automatically to all AWS customers at no extra cost, covering common network and transport layer attacks which frequently target web applications and services. This baseline protection is crucial for smaller applications, such as personal blogs or small business websites, where even minimal disruptions can lead to significant impacts. For environments where the risk or potential impact of DDoS attacks is greater, AWS Shield Advanced offers enhanced protective measures. This

premium tier includes additional detection capabilities to recognize and mitigate larger and more complex DDoS attacks. The integration of AWS Shield Advanced with AWS WAF provides a robust security posture that not only defends against volumetric attacks but also protects against application layer attacks, offering a dual layer of security that is essential for critical business applications. One of the hallmark features of AWS Shield Advanced is access to the DDoS Response Team (DRT), a group of dedicated security experts available around the clock to assist with the management of DDoS risks. The DRT works directly with customers to help tailor specific defensive strategies and respond to incidents in real time, ensuring that defenses are both proactive and reactive to the nature of the threat landscape. Moreover, AWS Shield Advanced supports businesses financially during an attack by offering cost protection, which shields organizations from scaling charges associated with traffic spikes during DDoS attacks. This feature not only helps maintain economic stability but also allows businesses to deploy necessary defenses without fear of unexpected financial burdens.

In conclusion, the strategic implementation of AWS's security features such as Network Access Control Lists (NACLs), Virtual Private Cloud (VPC), AWS Web Application Firewall (WAF), and AWS Shield provides a comprehensive defense mechanism against vulnerability scanning and other cyber threats. NACLs offer granular traffic control at the subnet level, effectively blocking unauthorized probes and scans. VPCs enhance this protection by isolating network segments, allowing for detailed control over traffic flow and reducing the exposure of critical resources. AWS WAF extends these capabilities to the application layer, safeguarding against sophisticated exploits that target web applications, while AWS Shield delivers robust DDoS protection, ensuring that services remain operational even under concerted attack efforts. Together, these tools form a layered security approach that not only defends against the immediate threats posed by vulnerability scanning but also adapts to the evolving landscape of cyber risks, ensuring that AWS environments are secure, resilient, and trustworthy. This multifaceted approach is essential for maintaining the integrity and performance of cloud-based services, highlighting AWS's commitment to providing advanced security measures that meet the needs of modern digital infrastructures.

Cloud Security Features to combat ARP Spoofing

Cloud providers offer features like Virtual Private Clouds (VPCs) or Virtual Networks, allowing users to create isolated network environments. These environments segment the network, restricting communication based on defined rules. By isolating resources within VPCs or Virtual Networks, the attack surface for ARP Spoofing is reduced. Even if an attacker successfully conducts ARP Spoofing within one segment, their impact is contained within that segment, limiting the overall damage to the network.

Network ACLs provide an additional layer of defense by filtering inbound and outbound traffic based on specified rules. Cloud users can configure ACLs to block ARP Spoofing attempts by denying traffic from unauthorized MAC addresses or preventing ARP replies from unauthorized sources. For example, administrators can create rules to allow only legitimate ARP responses

from authorized sources, effectively blocking any spoofed ARP packets. This helps prevent attackers from executing ARP Spoofing attacks within the cloud environment.

In cloud environments, Intrusion Detection and Protection Systems (IDPS) solutions play a crucial role in monitoring and safeguarding against malicious activities, including ARP Spoofing. These systems analyze network traffic in real-time, looking for patterns indicative of ARP Spoofing attacks. For instance, sudden changes in MAC address associations or unusual ARP reply behaviors can trigger alerts. Cloud-based IDPS solutions provide administrators with the ability to detect and respond to ARP Spoofing attempts promptly, thereby mitigating potential threats to the network.

Encrypting network traffic is essential for protecting against ARP Spoofing attacks in cloud environments. Cloud services often support encryption protocols like Transport Layer Security (TLS) or Virtual Private Network (VPN) tunnels for secure communication between instances or services. By encrypting data in transit, cloud environments prevent attackers from intercepting and tampering with sensitive information exchanged between hosts. Even if an attacker successfully conducts ARP Spoofing, the encrypted data remains unreadable, maintaining the confidentiality and integrity of the communication.

Cloud security platforms and network monitoring tools offer specialized features for detecting ARP Spoofing attacks. These tools analyze ARP traffic patterns and compare them against known behaviors to identify anomalies indicative of ARP Spoofing. For example, if a device suddenly starts using a different MAC address to respond to ARP requests, it may trigger an alert. By deploying ARP Spoofing detection tools, cloud environments can proactively identify and respond to potential attacks, thereby minimizing the risk of data breaches or service disruptions.

Regular security audits and updates are essential for maintaining the integrity and security of cloud environments. Cloud providers frequently release security patches and updates to address vulnerabilities, including those related to ARP Spoofing. By staying up-to-date with security patches and conducting regular audits, cloud users can ensure that their environments are protected against emerging threats. Additionally, periodic security assessments help identify any misconfigurations or weaknesses in the network infrastructure that could be exploited by attackers. By implementing a comprehensive security strategy that includes regular audits and updates, organizations can effectively defend against ARP Spoofing and other cyber threats in the cloud.

Shared Responsibility

While cloud service providers do much to secure their resources and systems, by the very nature of the service there is also a certain degree of responsibility that falls onto the user. The Shared Responsibility Model is a common model used by both AWS and GCP to illustrate the necessary relationship between the provider and user and how both have a duty to protect the

whole system. There tends to be a clear delineation in these models between the provider and user to clearly demonstrate what is the role of each entity.

Within this model the provider of the service is responsible for the infrastructure that the cloud runs on. This can include but is not limited to the hardware such as server, software, and facilities. They are responsible for making sure there is no unauthorized access to the hardware and facilities and fulfilling their requirements within the Service Level Agreement (SLA) that often defines uptime and availability. These uptimes can be stated to be 99.9 percent uptime with varying levels of credit back to the user for excessive downtime.

The provider is responsible for many areas of security but they can only do so much to secure the system until a user and their code is in the system. After this point responsibility now comes onto the user to adhere to best security practices. A user is expected to utilize proper configuration of security tools and access management to best ensure data privacy. Users are also expected to develop and maintain applications that are secure and any vulnerabilities introduced through their software is solely their responsibility.

Cloud services also provide differing models in Infrastructure (IaaS), Platform (PaaS), or Software as a Service (SaaS). Within IaaS, the provider is minimally responsible as they strictly ensure the security of the servers and facilities with the user responsible for operating systems, applications, data and much more. Moving to PaaS shifts more responsibility to the provider for them to maintain the operating systems and IT resources necessary to support the users. SaaS comes at the most responsibility for the provider responsible for nearly the entire model. This model requires only responsibility from the user to manage secure user access of their credentials.

The Shared Responsibility Model helps to show how utilizing the cloud services is two sides to a coin and is the responsibility of both the provider and the user. By working together, both parties can take advantage of an amazingly scalable and powerful system to better serve their customers. Both parties can be diligent in their agreed upon responsibilities within the model and together make a secure environment for everyone.

Summary / Conclusion

Through this paper we have shown a security analysis of cloud services with a focus on Amazon Web Services and Google Cloud Platform. The goal was to test how effective these systems were with ARP spoofing and NMAP vulnerability scanning while also documenting the importance for users to be well informed in best security practices.

The importance of network isolation with Virtual Private Clouds are critical for protecting against ARP spoofing while Access Control lists and detection systems work to prevent these attacks in the first place. Services such as CloudTrail, CloudWatch, and audit logs demonstrate the

necessity for vigilance against attack such as NMAP vulnerability scanning. Providing real-time health checks for services helps users identify and mitigate events before they can become worse.

Despite these robust tools offered by providers it is paramount for users to recognize the importance of the shared responsibility model and the role they play in making sure that their data is secure and safe. Future work should focus on testing new and emerging services such as AI and machine learning tools. Considering the rapid growth of that sector in everything today, it is another tool in the toolbelt of informed users but must be thoroughly and rigorously validated.

References

- *What is AWS Security?* (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/security/
- *AWS service level agreements*. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/legal/service-level-agreements/
- *Cybersecurity solutions: SecOps, intelligence, and cloud security*. (n.d.). Google Cloud. https://cloud.google.com/security/
- Krutz, Ronald, and Vines, Russel. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley. 2010. ISBN 9780470589878.
- Jones, Edward. *A Comprehensive Guide to Cloud Security (Risks, Best Practices, Certifications)*. Kinsta. December 7, 2023. A Comprehensive Guide to Cloud Security (kinsta.com)