REVSOC

REVOLUTIONIZING SECURITY OPERATIONS

Cloud Security and Monitoring

Cloud Posture, Workload, and Entitlement Security

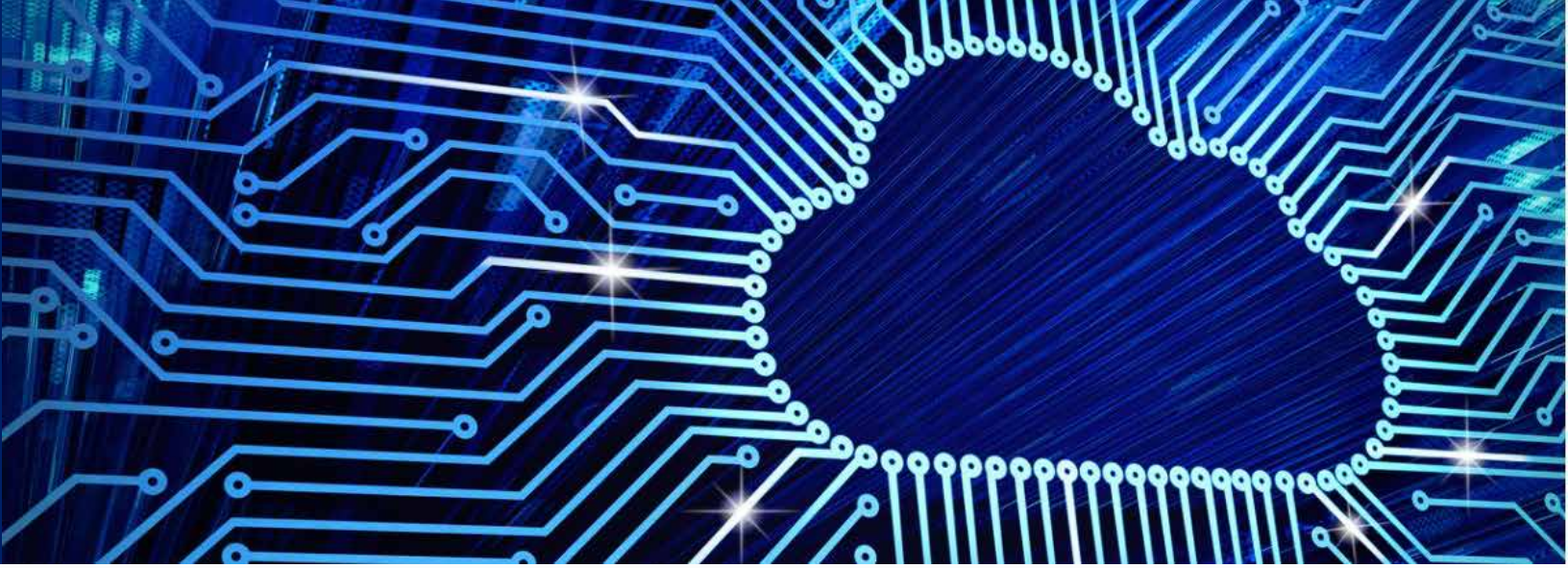
www.revsoc.ai | info@revsoc.ai | 586-789-9878

Background

Infrastructure as Code is becoming a staple across platforms like AWS, Azure, and GCP to improve efficiency and reliability. SOC understanding of this emerging threat landscape, however, has not maintained pace. Gartner has reported that 75% of cloud breaches will be due to misconfigurations. Recently, we have seen cloud breaches from the case of 540M Facebook profiles exposed to the 1.8M voter records exposed in Chicago due to an unsecure S3 bucket and misconfiguration, respectively. One of the biggest challenges in understanding this threat vector is the lack of visibility into possible access control drift and misconfigurations for critical cloud applications. With a lack of structure around security posture management, these misconfigurations can unintentionally expose sensitive data. At RevSoc, we have seen this vulnerability either viewed as an afterthought or not even accounted for so we approached the problem from a foundation of knowledge-based detection engineering to ultimately automate security monitoring as it pertains to cloud detections.

RevSoc has built its products around three core principles/methodologies to be relevant and effective against cloud-native vulnerabilities: Cloud Infrastructure Entitlement Management (CIEM), Cloud Workload Protection, and Cloud Posture Management. With these concepts in mind, RevSoc created an extensive library of models allowing for unparalleled threat detection and visibility. In a cloud-native environment, security platforms are at a disadvantage when it comes to identity permissions. More users require permissions and privileges at a scale beyond what is easy to manage with traditional access control lists. With the RevSoc Autonomous Incident Responder (AIR), we monitor user access level to provide high-efficacy detections for any anomalous behavior on your cloud infrastructure. The RevSoc Cloud solution can be described in these three parts:

[@]Gartner Research. Mezzera, P. (2020). Managing Privileged Access in Cloud Infrastructure 1



1. Cloud Workload Protection (CWP)

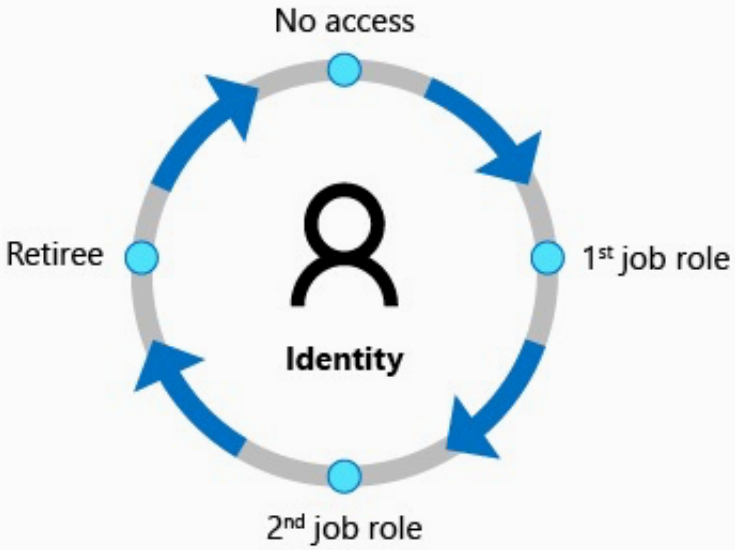
CWP can best be described as the security surrounding the compute, transport, and storage of data that is required to deliver an application. With the widespread adoption of public multi-cloud or hybrid compute infrastructure, the surface area of vulnerabilities has drastically increased for modern business. Workloads can be broken down into the application itself, the utilized data for the application as well as network resources used for the application. A standard cloud workload can span cross-platform and each of the three parts mentioned above entails properly configuring data stores, hosts, and serverless templates. A misconfiguration for any of these can open the door for a breach. Palo Alto Networks observed that of the security incidents with the greatest increase during COVID, workload related incidents saw a huge spike. Policies allowing all traffic:

- to a Kubernetes cluster increased by 122%
- over uncommonly used ports (like 445, 30 and 3389) increased by an average of 60%
- to databases (like MySQL or Postgres) increased by 58%.

Any of these vulnerabilities can provide an attacker access to sensitive data to encrypt and hold as ransom. The RevSoc AIR responds to this challenge by analyzing all the touch points of a workload through a centralized dashboard view. This enables SecOps to monitor hosts, containers, images, and serverless functions. Through this visibility, analysts are able to quickly understand behavior and respond to detected threats in a timely, scalable and customizable manner.

2. Cloud Infrastructure Entitlement Management (CIEM)

CIEM is the management of privileged identities to monitor, detect, and alert on excessive privileges that could potentially lead to a breach. As businesses favor Cloud infrastructure due to its reliable and scalable nature, there needs to be awareness on what level of access all users have. As we observed in the example above, the slightest of oversights can result in a breach which is why the RevSoc AIR ensures that any change in access is thoroughly monitored. With our rarity based detection models, we are able to tie user identity to their level of access to determine if a change in access can be exploited. If an entitlement is deemed risky, the Digital Investigator will create an incident for the analyst to evaluate and mitigate based on risk tolerance.



[@]Gartner Research. Mezzera, P. (2020). Managing Privileged Access in Cloud Infrastructure. 1

3. Cloud Security Posture Management (CSPM)

CSPM is the ongoing process of improving and building more complex detections in the cloud as well as increasing visibility on all critical assets in the cloud. Due to the spread out nature of cloud systems, the security model that may have been acceptable for on-premise infrastructure does not translate over to the public cloud. In multi-cloud environments the foundation for detections required in identifying misconfigurations is to have a deep understanding of the different access and audit logs these platforms provide. The RevSoc Brain is a collection of models built on this fundamental understanding of this data to ensure that misconfigurations are identified promptly. Once the Threat Hunter triggers an alert the Digital Investigator helps your SOC prevent and remediate threats with the power of machine learning to protect data at scale.

Conclusion

This product was built as a result of first-hand experience by analysts expressing their challenges and frustrations regarding securing the modern stack. We believe that by building a product that resolves the problems we have seen across various Fortune 500 companies, we will hopefully resolve any similar challenges you may also be facing in your security environment. Through our first-hand experience of working through the complexity of cloud configurations and access control, we have made complete visibility the top priority of this product. Our dedication to detection engineering gives analysts insight across computing workloads, data stores, containers, and more. We want to provide analysts not only the information they need to investigate, but also automated detection and response capabilities that further allow them to work smarter not harder and use their mind for more strategic analysis.