radware

Case Study: **Ad Technology**

Radware's Cloud Native Protector Reduces Management and Operational Costs for Ad Tech Company

OVERVIEW

This multinational advertising technology company delivers data-driven ad and search solutions for brands and publishers. Founded in 2000, it is headquartered in the Middle East with additional locations throughout Europe and the U.S.

CHALLENGES

As organizations migrate computing workloads to publicly hosted clouds, IT and security administrators face new security challenges. Cloud environments make it easy to deploy new resources and grant wide-ranging permissions that can eventually be abused. Such misuse often leads to cloud-native risks, including data breaches, compromised accounts and resource exploitation, which can cause businesses to lose customers, reputations and revenues.

This ad tech company has a complex cloud environment comprised of a variety of services deployed in multiple Amazon Web Services (AWS) accounts. Managing these accounts was a challenge for several reasons. First of which was that permissions management was spread across different teams with constantly evolving account administrators and processes.

Second, managing accounts using multiple tools was labor-intensive, resulting in significant expense. Operational support costs were approximately $7,200 per month[1] since AWS management tools, such as GuardDuty, Config and CloudWatch, did not provide adequate capabilities to view and protect cloud assets and workloads across multiple environments. Engineers typically spent nine hours a day[2] to manually identify, prioritize and mitigate risks, including internet-exposed assets, excessive permissions, misconfigured assets and inactive users with high-level permissions.

Lastly, the cost of using these stand-alone AWS tools was greater than using a single comprehensive tool. A single AWS management tool such as GuardDuty cost this ad tech company approximately $14,700 per month,[3] bringing the customer's total cost across all AWS tools to $35,200 per month.[4]

Publicly exposed assets made the company vulnerable to sensitive data and intellectual property being compromised. Amazon's management tools are not integrated and did not provide a single 360-degree view of risks threatening the company's cloud environment. Since account management was manual, risks could easily be missed or prioritized incorrectly due to human error.

The ad tech company needed a new solution that would provide:

- Visibility into account updates and timely identification of dangerous misconfigurations across multiple AWS environments to prevent potential data loss
- The ability to track the usage of access permissions to services/data and reduce excessive permissions across multiple AWS environments to decrease the attack surface
- Accurate identification of attacks by recognizing active risks in a timely manner while improving SOC team efficiency by reducing the false positive ratio significantly
- An easily deployable and easy-to-operate solution to save the time and effort of the operations and security teams
- Assistance with prioritizing the high risks to allow the operations and security teams to focus on other priorities

SOLUTION

The ad tech customer evaluated several solutions, including Radware's Cloud Native Protector, a managed security information and event management (SIEM) service, several cloud misconfiguration detection tools and Amazon GuardDuty. The customer dismissed the SIEM service and the cloud-native security tools which satisfied only part of its requirements.

During the testing of attack detection capabilities, Radware's Cloud Native Protector detected all eight attack steps, while Amazon GuardDuty detected none. The Cloud Native Protector demonstrated that it could protect the ad tech company's workloads and data by identifying critical misconfigurations and excessive permissions, as well as detecting simulated cloud-native attacks in the company's environment.. To ensure Liberty had access to in-country vendor expertise and support, they took advantage of Radware's attack mitigation experts and purchased Radware's Emergency Response Team

[1] $40 per hour per engineer x 3 management tools x 3 hours daily for each tool x 5 days per week x 4 weeks per month

[2] 3 management tools x 3 hours per tool per day

[3] 60 million events x $4 (per 1 million events) + 500GB logs x $1 + 1,500GB VPC flow logs X $0.50 + 52,000GB VPC flow logs x $0.25

[4] $14,700 (cost of GuardDuty) + $20,500 (cost of Config and CloudWatch)

(ERT) service to keep the Liberty team apprised of what is happening with their environment and improvements they can make to their security posture.

BENEFITS

The Cloud Native Protector reduced the time needed by the operations team to manage accounts and the number and cost of the tools required. The total operational cloud workload protection cost decreased from approximately $42,400 per month to $12,400 per month.

Cloud Native Protector provides the ad tech company with a single automated tool that does the work of three tools, which satisfied all of the company's requirements for account visibility and management and data breach protection. The solution automates the monitoring of account updates and configuration changes for misconfigurations and excessive permissions, all from a single point of control and visibility. This aligns account management across teams, requiring fewer resources, so security and development and operations (DevOps) teams can focus on other priorities.

The service reduced the support effort required to identify, prioritize and mitigate risks from nine hours to only 30 minutes a day[5] and reduced the cost of support from $7,200 per month to $400 per month.[6] The customer significantly reduced its tool cost from $35,200 per month to $12,000 per month[7] while improving risk mitigation.

	OPS SUPPORT TIME/DAY	OPS SUPPORT COST/MONTH	TOOL COST/MONTH	TOTAL OPS COST
RADWARE CNP	30 minutes	$400	$12,000	$12,400
AWS MANAGEMENT TOOLS	9 hours	$7,200	$35,200	$42,400

> *"Radware's Cloud Native Protector has helped identify threats in real time without the noise of false alerts. It has been excellent in exposing misconfigurations and potential risks and, thus, very helpful in both detection and prevention."*
>
> **- Sr. Director of Engineering Operations at Ad Tech Company**

[5] 6 issues (20% of 30 cloud environments) x 5 minutes per issue

[6] $40 per hour per engineer x 1 tool x 30 minutes per day per tool x 5 days per week x 4 weeks per month

[7] CNP cost for 1,000 instances

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.