Perion Protects Its Amazon Web Services Assets with Radware Cloud Workload Protection

THE CHALLENGES

Perion lacked the ability to track and tighten access permissions to services and data and automatically detect malicious activity inside its AWS accounts.

THE SOLUTION

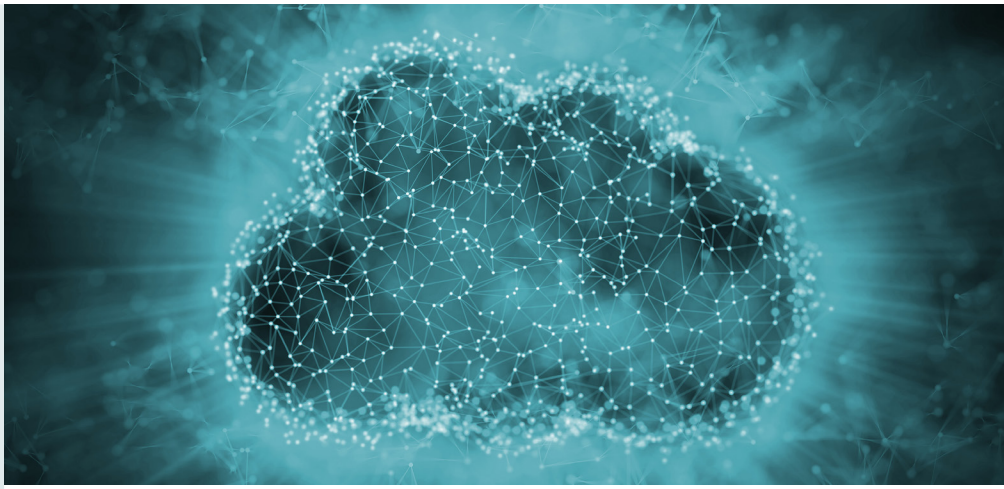
Radware's Cloud Workload Protection Service is an agentless, cloud-native solution for comprehensive protection of cloud assets.

WHY RADWARE

It identifies misconfigurations and reduces excessive permissions while detecting breaches, providing superior breach detection capabilities than those of Amazon GuardDuty.

BENEFITS

Perion's operations and security teams now have an automated breach detection tool that continuously monitors its cloud accounts for malicious activity while avoiding alert fatigue and helps Perion comply with current regulations.



Perion Network is a multinational ad tech company that delivers data-driven ad and search solution for brands and publishers. Founded in 2000, it is headquartered in Israel, with additional locations throughout Europe and the United States.

THE 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 to public cloud services, namely data breaches, account compromise and resource exploitation.

Perion 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. Various teams/employees at Perion had access to different AWS accounts. In addition, processes for managing accounts and the people managing them are in a constant state of flux.

Unfortunately, AWS does not provide sufficient capabilities to view and protect cloud assets and workloads across multiple environments. Perion's operations and security teams had limited visibility of account updates and dangerous misconfigurations, such as network configurations exposing servers to the internet. Perion lacked the ability to track and tighten access permissions to services and data and automatically detect malicious activity inside its AWS accounts.

Perion needed a solution that could provide:

- Visibility into account updates and timely identification of dangerous misconfigurations across multiple AWS environments
- The ability to track the usage of access permissions to services/data and reduce excessive permissions across multiple AWS environments
- Protection from data breaches, account takeovers and other threats, without generating false positives
- An unobtrusive and easy-to-deploy solution
- Assistance with managing and securing cloud accounts, so Perion's operations and security teams can focus on other priorities

THE SOLUTION

Perion Network evaluated several solutions, including Radware's Cloud Workload Protection Service, a managed SIEM service, several cloud misconfiguration detection tools and Amazon GuardDuty. They dismissed the SIEM service because it couldn't identify misconfigurations and had weak breach detection. They also eliminated the cloud misconfiguration tools, which did not provide breach detection. During testing of attack detection capabilities, Radware's Cloud Workload Protection detected all eight attack scenarios, while Amazon GuardDuty detected none.

> "Radware's Cloud Workload Protection service has helped Perion to 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."
>
> *— Amir Arama, Sr. Director of Engineering Operations at Perion*

During testing, Perion experienced firsthand how Radware would protect its workloads and data, including identification of dangerous misconfigurations and excessive permissions, as well as detection of simulated cloud-native attacks conducted in Perion's environment.

Cloud Workload Protection Service provided a single solution for Perion's requirements, verses other offerings that would only solve one or two of their issues.

Radware's service takes an innovative approach compared to traditional workload defenses. To reduce attack surfaces, Radware's Cloud Workload Protection Service addresses the core problem of excessive permissions and exposed assets. It analyzes the gap between granted and used permissions, applying the "principle of least privilege" to offer smart hardening recommendations, thereby reducing the organization's attack surface.

Radware provides a robust detection engine based on advanced machine learning algorithms that identify malicious activity within cloud accounts. Radware then correlates individual alerts into streamlined attack storylines, which show the step-by-step attack progression. This maps a hacker's attack kill chain and helps block data theft before it results in a breach.

Perion implemented Cloud Workload Protection Service for several reasons:

- It identifies misconfigurations and reduces excessive permissions while detecting breaches, providing superior breach detection capabilities than those of Amazon GuardDuty.
- Delivers breach alerts without generating false positives. Although Radware detected many anomalies during testing, it only alerted the Perion security team when it garnered enough evidence for a possible breach.
- It provides actionable misconfiguration alerts. The Cloud Workload Protection Service only alerts when an actual configuration issue is detected that risks exposing workloads.
- Radware provided exceptional support during testing and implementation.
- The Cloud Workload Protection Service was an easy-to-deploy, nonintrusive cloud security solution with quick onboarding and no need to install additional software or appliances in customer AWS accounts.

BENEFITS

Cloud Workload Protection provides Perion with several security and business benefits. Operations and security teams have an automated breach detection tool that continuously monitors their cloud accounts for malicious activity while avoiding alert fatigue and helps Perion comply with current regulations.

In addition, the solution automates monitoring account updates and configuration changes for misconfigurations and excessive permissions. This aligns account management across teams, requiring fewer resources, so security and DevOps teams can focus on other priorities.