prdeadlines

Radware extends cloud workload protection service for risk-based threat visibility, compliance and attack detection

SYDNEY, June 12, 2020 —Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, has enhanced its Cloud Workload Protection Service (CWP) to give enterprises a full-suite of visibility, compliance and reporting features, coupled with enhancements to its industry-leading attack detection engine. Radware has extended its comprehensive compliance engine to support multi cloud environments. The engine compares the organisation's cloud security posture against multiple industry compliance standards, including: PCI DSS, HIPAA, NIST CSF, SOC2, CIS AWS/Azure Foundation Benchmark. The service includes a new security posture dashboard that provides comprehensive visibility into both the overall cloud risks associated with workloads hosted on both AWS and Azure and the organisation's cloud security posture. This dashboard provides a detailed and comprehensive view of security risks across multiple accounts, regions, and public cloud vendors. Radware has enriched its existing, industry-leading attack detection engine to detect cloud native attack vectors and added a new attack simulation tool. The attack simulation tool allows organisations to proactively test their public cloud environments, harden security posture and improve their security teams' readiness using simulated attacks based on real-life cloud data breach events. The result is a comprehensive, end-to-end CSPM solution for identifying security risks, unintended public exposure, excessive permissions, and compliance breaches as well as detecting breach attempts and automatically remediating threats. "As companies increasingly turn to public cloud environments, they need unprecedented visibility into their environment that is based on real risk analysis," said David Aviv, Chief Technology Officer for Radware. "Too often, organisations use tools that struggle to distinguish between suspicious activity performed by legitimate entities and malicious activity conducted by threat actors." He added: "Radware's Cloud Workload Protection Service helps organisations to identify both scenarios by providing meaningful threat intelligence and advanced analytics with an unmatched ability to identify attack-kill-chain. Our CWP service empowers customers to take fast, accurate action to block attacks and shore up vulnerabilities in their cloud environments before it's too late." Companies have relied on Radware's Cloud Workload Protection Service for comprehensive visibility into complex environments. One example is ad-tech innovator Perion, whose employees managed multiple AWS instances. AWS provided only limited visibility into the multiple workloads and assets spread across numerous environments. Perion's operations did not have a window into dangerous misconfigurations, such as network configurations of assets exposed to the internet. "The Radware Cloud Workload Protection Service provided a single solution with enhanced visibility, immediately identifying dangerous misconfigurations," said Amir Arama, Vice President of Operations at Perion. "By combining those capabilities to CWP's continuous attack detection capabilities and compliance tools, Radware is continuing to add value to a product that already offered immense value." "We recently conducted a trial run with a cybersecurity startup that was quickly growing its customer base after receiving a large investment from a venture capital firm," said Nissim Pariente, Vice President of Security Analytics. "During the proof-of-concept period, we discovered that many of the identified public exposures were actually false positives, often reported by the company's partners. Additionally, we discovered that nearly every employee in the organisation's cloud environment had admin privileges. With CWP, this company was able to optimize permissions to the right level of access, with a level of granularity and control that was much appreciated by executives." Radware's CWP has also helped companies to monitor workloads and maintain productivity, as their workforce transitioned to remote and work-from-home arrangements. Radware worked closely with one particular client to monitor remote worker engagement and optimise permissions that align with the principle of least privilege. About Radware Radware® (NASDAQ: RDWR), is a global leader of cyber security and application delivery solutions for physical, cloud and software defined data centres. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application, and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com. Radware encourages you to join our community and follow us on: Facebook, LinkedIn, Radware Blog, Twitter, YouTube, Radware Mobile for iOS and Android, and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats. Media Contact: Deborah Szajngarten Radware 201-785-3206 deborah.szajngarten@radware.com ###

Contacts

David Frost
(02) 7903 9567
mailto: davidf@prdeadlines.com.au