

Threat Exposure Management for Amazon Web Services (AWS)

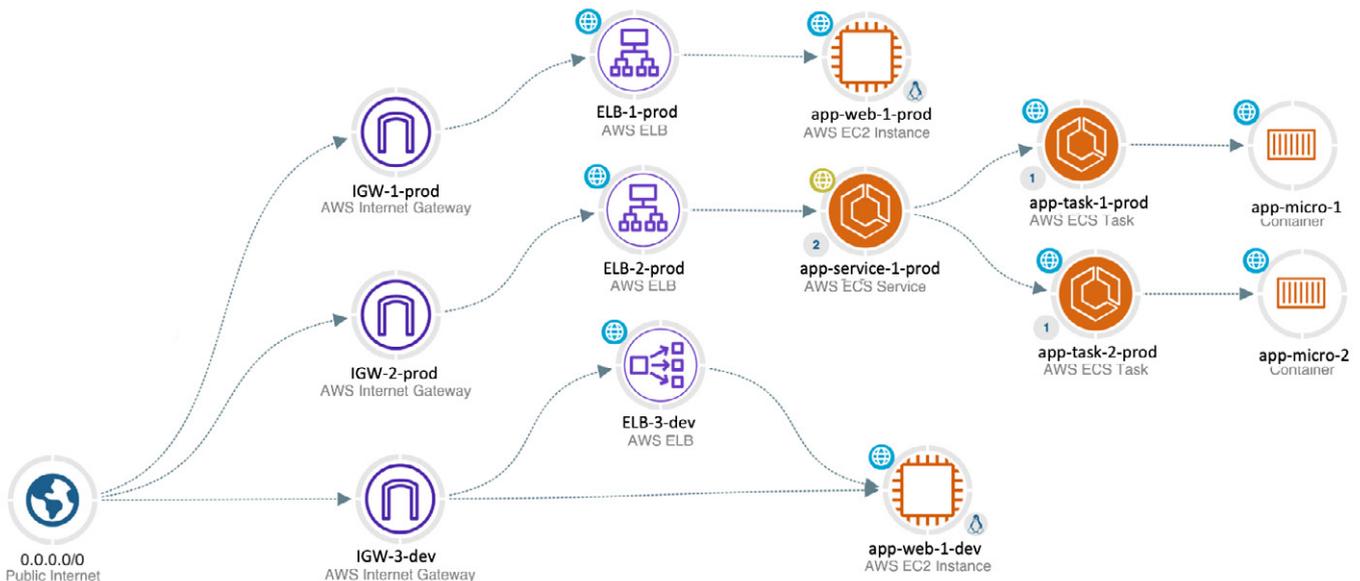
Observer Sentry lets you see your environment from the attacker’s perspective

The Challenge

In an effort to continuously improve and expand service delivery and fully leverage technology advancements, cloud-based service delivery architectures are constantly changing. Business and competitive pressures force many organizations to react quickly — frequently implementing changes as fast as possible. The consequences? Overly permissive cloud identities, third-party container applications with security vulnerabilities, and critical assets that are externally exposed. These widespread issues have resulted in dramatic growth in cloud exploitation cases and data breaches.

The Solution

VIAVI Solutions’ Observer Sentry provides software-as-a-service-based Threat Exposure Management, giving SecOps, DevOps, and Cloud Architects the much-needed threat visibility into ever-changing AWS environments. By discovering and combining internal attack paths with focused external attack surface scanning, Observer Sentry identifies security exposures, analyzes the business impact, and helps prioritize remediation activities.



“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”
John Lambert – Microsoft Threat Intelligence Center

