VIAVI Solutions

Brochure

# Threat Exposure Management for Amazon Web Services (AWS)

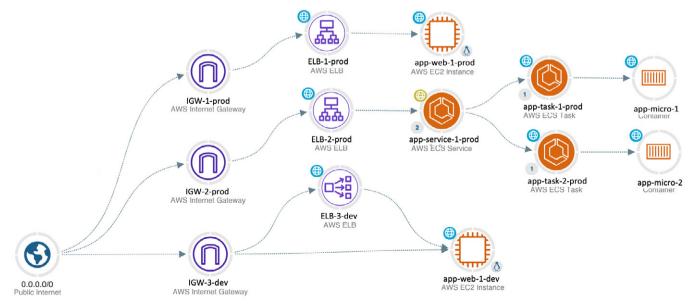
Observer Sentry lets you see your environment from the attacker's perspective

### 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.



#### **Attack Surface and Attack Path Management**

Observer Sentry creates a detailed inventory of your cloud assets and then performs an analysis to determine their attack surface, exposure and risk. This analysis can also be applied collectively to logical groupings of assets that make up specific applications or workloads. These groupings can be tracked in risk scorecards and visualized in attack surface maps.

Attack Paths are the dangerous combination of exposure, exploitable network vulnerabilities and risky configurations that provide the paths of least resistance to high-value resources within your environment. Attack Path Management provides actionable context for your most critical issues, so your teams can proactively and continuously improve your cloud security posture.



#### **Observer Sentry Answers:**

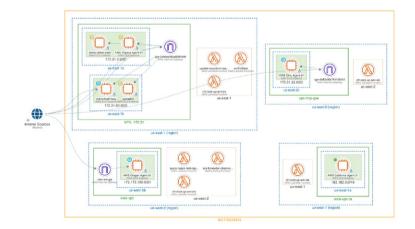
How do attackers see my AWS environment? Where do I have misconfigurations? Which paths can attackers exploit? Where are my cloud assets at risk?
Where do I have overly permissive settings?
How do I prioritize risk mitigation?

## AWS Observability and Risk-based Prioritization

Connect to your AWS environment, Elastic Kubernetes Services (EKS), and Elastic Container Service (ECS) clusters in minutes. Observer Sentry continuously scans your AWS environments and generates highly-intuitive cross-environment diagrams that help you quickly identify misconfigurations, overly permissive settings, and unintended exposures.

Observer Sentry prioritizes critical risks based on the analysis of misconfigurations, network exposure, vulnerabilities, and other factors to provide a prioritized view of risk for your cloud environment.

Learn more: viavisolutions.com/sentry



Try the Observer Sentry service, risk free, in your environment.
Typical account activation and initial setup takes less than 15 minutes.



Contact Us

**+1844 GO VIAVI** (+1844 468 4284)

To reach the VIAVI office nearest you, visit viavisolutions.com/contact

© 2023 VIAVI Solutions Inc.
Product specifications and descriptions in this document are subject to change without notice.
Patented as described at viavisolutions.com/patents observer-sentry-br-ec-ae 30193849 900 0923