VIAVI Solutions

Brochure

Threat Exposure Management for Amazon Web Services (AWS)

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

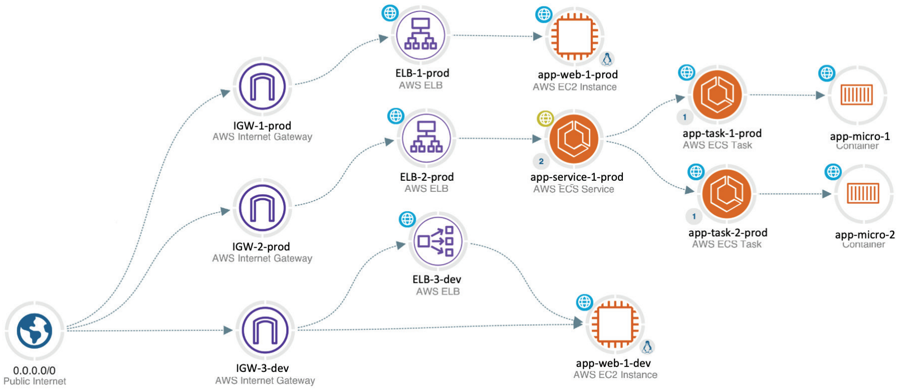
The Challenge

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. Through the integration of AWS --provided configuration details and traffic data, users can see can two critically important perspectives; what the configuration will allow (what’s possible) and what is actually happening. This reveals whether bad actors have compromised exposed resources or exploited known vulnerabilities.

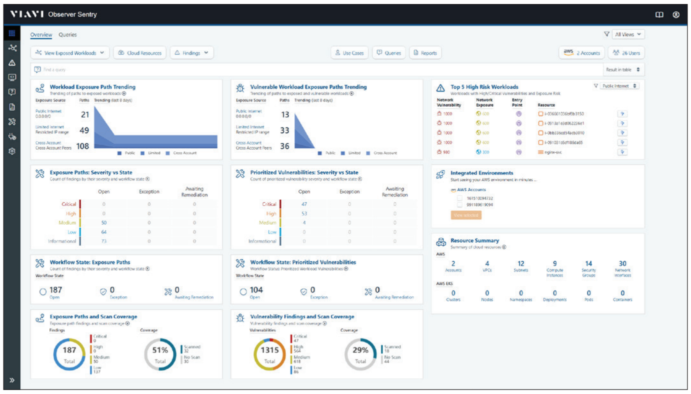


“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”
John Lambert – Microsoft Threat Intelligence Center

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.

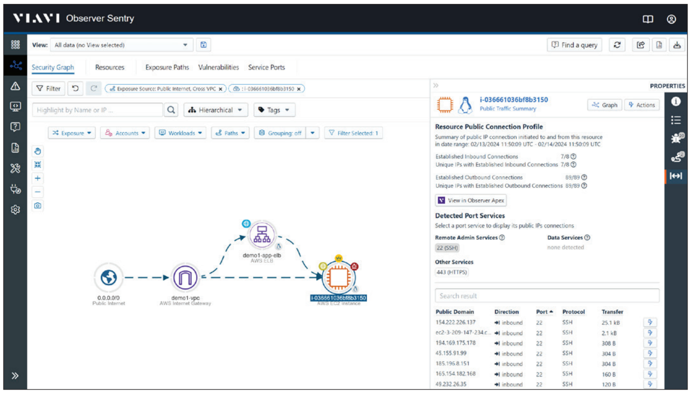
Attack Paths are the dangerous combination of exposure, exploitable network vulnerabilities and risky configurations that provide the paths of least resistance to high-value resources within your environment. Attack Path Management provides actionable context for your most critical issues, so your teams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


VIAVI Observer Sentry
Overview
Queries
Workload Exposure Path Trending
Vulnerable Workload Exposure Paths Trending
Top 5 High Risk Workloads
Exposure Paths: Severity vs State
Prioritized Vulnerabilities: Severity vs State
Integrated Environments
Resource Summary
Workflow State: Exposure Paths
Workflow State: Prioritized Vulnerabilities
Exposure Paths and Scan Coverage
Vulnerability Findings and Scan Coverage
21
49
108
13
33
36
187
104
187
51%
1315
29%

Identify unintended exposures and prioritize high-risk workloads at a glance

Traffic Data Integration

When unintentional exposures or unpatched vulnerabilities are identified, it isn't enough to understand what could happen, or what might have already happened — you need to know what actually happened. Through the integration of traffic data provided by AWS VPC Flow Logs, Sentry users gain visibility into inbound and outbound connection attempts and established connections by port and protocol along with the volume of data associated with a connection. Users can then pivot from Observer Sentry to Observer Apex in order to perform a detailed forensic traffic analysis of any conversations of interest or concern.



Security teams gain necessary insights into high-priority exposures by integrating detailed traffic and conversation history

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?
Where any exposed resources compromised?
Where any known vulnerabilities exploited?

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/en-us/sentry

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

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

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