Coralogix

Cloud Security for AWS

The wide-spread adoption of cloud infrastructure has proven to be highly beneficial, but has also introduced new challenges and added costs - especially when it comes to security.

As organizations migrate to the cloud, they relinquish access to their servers and all information that flows between them and the outside world. This data is fundamental to both security and observability.

Cloud vendors such as AWS are attempting to compensate for this undesirable side effect by creating a selection of services which grant the user access to different parts of the metadata. Unfortunately, the disparate nature of these services only creates another problem. How do you bring it all together?

The Coralogix Cloud Security solution enables organizations to quickly centralize and improve their security posture, detect threats, and continuously analyze digital forensics without the complexity, long implementation cycles, and high costs of other solutions.

3-Click SIEM

Install the Security Traffic Analyzer (STA)

Directly deploy the Coralogix Security Traffic Analyzer (STA) in your own VPC using our in-app installation wizard.

Mirror Existing VPC Traffic

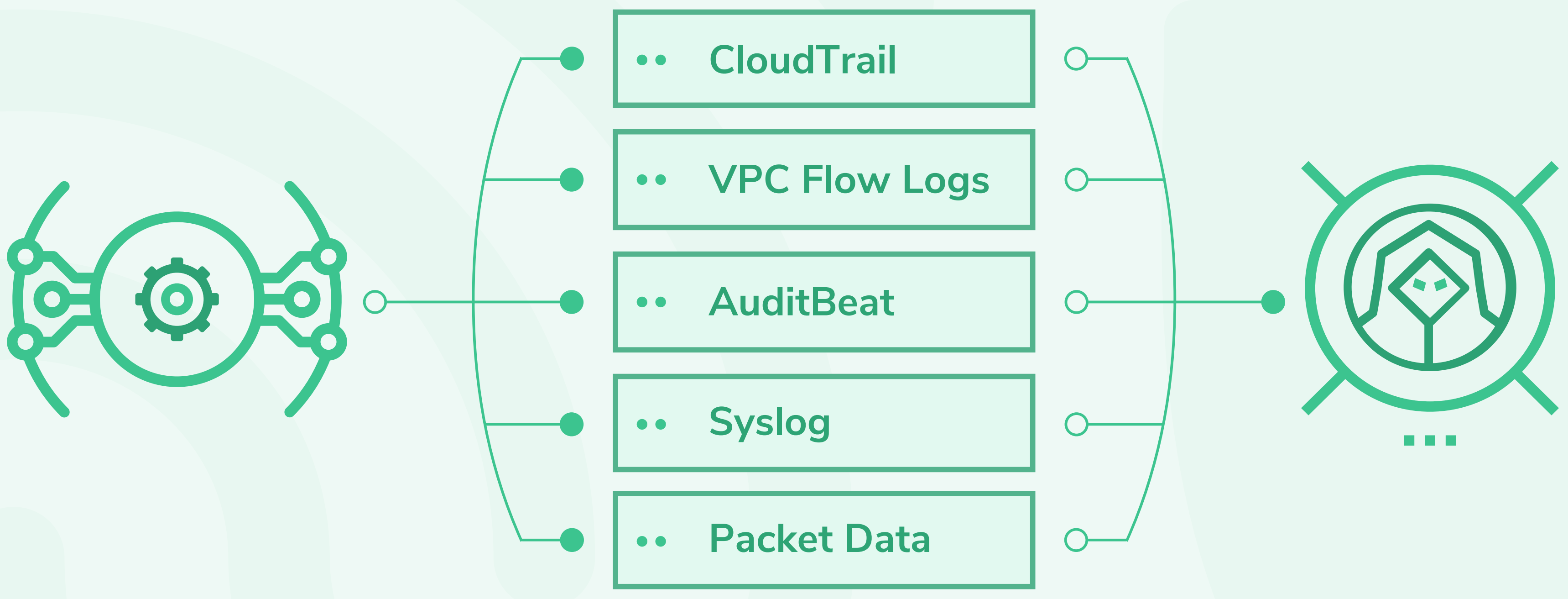
Quickly set up traffic mirroring in minutes, using the mirroring strategy of your choice, with our VPC Traffic Mirroring Configuration handler.

ML-Powered Threat Analysis

The Coralogix STA automatically captures, analyzes and (optionally) stores your traffic, employing ML-powered algorithms to alert you to potential threats.

Mirror Traffic From Any Source

Connect any source of information to complete your security observability, including Audit logs, Cloudtrail, GuardDuty or any other source. Monitor your security data in one of 100+ pre-built dashboards or easily build your own using our variety of visualization tools and APIs.



Automated Data Enrichment

Automatically enrich the data passing through it such as domain names, certificate names, and much more by using data from several other data sources. This allows you to create more meaningful alerts and reduce false-positives without missing anything.

Customizable Alerts & Visualizations

The Coralogix Cloud Security solution comes with a predefined set of alerts, dashboards and Snort rules. Unlike many other solutions on the market today, you maintain the ability to change any or all of them to tailor them to your organization's needs.

One of the most painful issues that usually deters people from using an IDS solution is that they are notorious for their high false-positive rate, but Coralogix makes it unbelievably easy to solve these kinds of issues. Dynamic ML-powered alerts, dashboards, and Snort rules are just a matter of 2-3 clicks and you're done.

Automated Incident Response

Although Coralogix focuses on detection rather than prevention, it is still possible to achieve both detection and better prevention by integrating Coralogix with any orchestration platform such as Cortex XSOAR and others.

Optimized Storage Costs

Security logs need to be correlated with packet data in order to provide needed context to perform deep enough investigations. Setting up, processing, and storing packet data can be laborious and cost-prohibitive.

With the Coralogix Optimizer, you can reduce up to 70% of storage costs without sacrificing full security coverage and real-time monitoring. This new model enables you to get all of the benefits of an ML-powered logging solution at only a third of the cost and with more real-time analysis and alerting capabilities than before.

Here's a full comparison between the STA and all the other methods in AWS:

Feature	Coralogix STA	CloudWatch Metrics	CloudTrail Logs[2]	VPC Flow Logs	GuardDuty	VPC Traffic Mirroring	VPC Firewall
Provides a set of metrics that are calculated based on the traffic	✗ [1]	✓	✗	✗	✗	✗	✗
Provides auditing information about AWS activities	✗	✗	✓	✗	✗	✗	✗
Allows the user to create new metrics and modify existing ones	✓	✗	✗	✗	✗	✗	✓ [6]
Provides Layer 4 Context Data (IPs, Port Numbers)	✓	✗	✗	✓	✗	✓	✗
Provides Layer 7 Context Data (HTTP URI's and methods, SSL Certificates, DNS Queries, FTP commands, files, etc)	✓	✗	✗	✗	✗	✓	✓ [4]
Detects threats or malicious content	✓	✗	✗	✗	✓	✗	✓ [5]
Detects potentially malicious behaviors	✓	✗	✗	✗	✓	✗	✗
Allows the user to understand, modify, disable and create new detection rules	✓	✗	✗	✗	✗	✗	✗ [3]
Allows the user to access and store the captured traffic	✓	✗	✗	✗	✗	✓	✗
Enriches the data (for example by adding domain creation dates to domain names)	✓	✗	✗	✗	✗	✗	✗
Allows integration with OSSEC/Wazuh or similar agents for the purpose of collection of instance specific data such as processes running on each instance	✓	✗	✗	✗	✗	✗	✗
Comes with predefined set of alerts, including ML powered ones	✓	✗	✗	✗	✓	✗	✗
Allows the user to customize the set of alerts and to create new ones	✓	✗	✗	✗	✗	✗	✓
Comes with predefined dashboards for each type of protocol	✓	✗	✗	✗	✗	✗	✗
Can be used to detect lateral movements	✓	✗	✗	✓	✓	✗	✗ [7]
Allows the user to customize the predefined dashboards to his needs	✓	✗	✗	✗	✗	✗	✗