EASTWIND

Eastwind for AWS - Datasheet

The Challenge:

Enterprises today fight a complicated battle: there is a global army of hackers who never sleep and who are looking for new and creative ways to break into networks, whether hosted or on-premise. Eastwind arms security teams with comprehensive visibility.

The Solution:

EASTWIND
AWS

The Benefits:

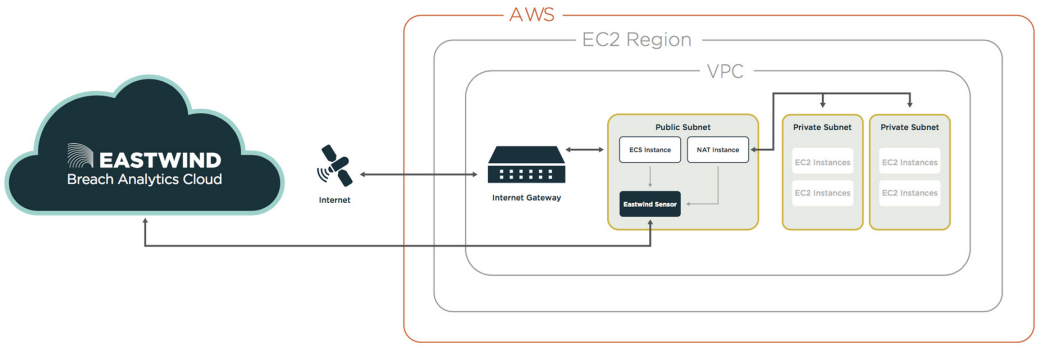
- Collect, analyze and enrich network and AWS Services telemetry via CloudTrail with your other network, IaaS, SaaS, DNS and application data.
- With Eastwind for AWS, fusing multiple intelligence sources, machine learning, signatures, and anomaly detection with a fast and powerful query engine allows you to interpret months or even years of data.
- The Breach Analytics Cloud performs continuous realtime and historical monitoring to identify threat factors, scope incidents, and reduce dwell time.

Advanced Breach Analytics for Amazon Web Services

Eastwind for AWS provides visibility, threat analysis and user and entity behavioral analytics to identify malicious activity, insider threats and data leakage within your AWS Services.

At its core, Eastwind is powered by the Breach Analytics Cloud. This powerful solution enables cyber defenders to hunt, analyze and visualize all activity relevant to your enterprise. Eastwind provides a comprehensive array of sensors and applications that gather, enrich and analyze telemetry from all areas of your cyber terrain, including SaaS, IaaS, DNS, hybrid networks and all users on and off premises. The result is breach analytics at speed and scale accelerating incident response and forensics.

Eastwind Networks AWS Solution Architecture



Eastwind for AWS

Eastwind and Amazon have partnered to provide a more comprehensive security solution. Eastwind for AWS provides complete visibility across your AWS network and leverages the AWS cloud to scale up or down as your needs change. With this solution, security teams can reduce overall impact from breaches, including costly fixes, disrupted business, stolen information, and damaged reputations.

Eastwind Sensor Capabilities

The Eastwind Sensor collects, analyzes and enriches network telemetry from traditional physical and virtual infrastructures on-campus, in remote offices and datacenters. Features of the sensor include:

- deep application inspection of 2700+ applications, creating 5000+ network attributes
- MD5 hash of all files flowing through the network
- deception services to detect east/west and lateral movement
- intrusion signatures

Breach Analytics at Speed and Scale

Analyze telemetry from Office 365, G Suite, Salesforce.com, cloud storage providers, cloud infrastructure, traditional networks and virtual environments all from within a SINGLE pane of glass.

Eastwind offers the only breach analytics cloud that provides complete visibility of your key cyber terrain. We help analyze the flight data flowing across your corporate networks, virtual networks, cloud provider networks, cloud application networks, and your mobile workforce—with speed and precision. Always watching, our automated hunters enable you to identify malicious activity that evades all other security solutions.

Our breach analytics technology searches, automatically and on-demand, through months of information to accelerate incident response and forensics. Serving as the system of record, Eastwind Networks provides the critical context you need to make intelligent decisions quickly.

Power of the Portal

The Eastwind Portal displays areas of interest quickly and easily using the breadth and depth of metadata using our customizable dashboards. It not only provides security event information but cyber situational awareness and context of your cyber key terrain. Eastwind provides the necessary context for security teams to respond and recover with bolstered threat intelligence and multiple detection techniques built upon complete visibility of your hybrid network. With the Eastwind Portal you can pivot rapidly, find complex relationships, and visualize patterns using the Breach Analytics Cloud.

Eastwind for AWS costs

Eastwind AMI instances:
—varies by instance type.

Data transmission from AMI to Eastwind Cloud:
—varies by region but typically $0.01 per GB.

Remove friction from AWS security

Pay for visibility and cyber security of your AWS deployment directly through your Amazon account. Streamline your procurement; no POs required.

EASTWIND

For more information on Eastwind for AWS,
please see eastwindnetworks.com