EASTWIND

Eastwind for Logs - 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
Logs

The Benefits:

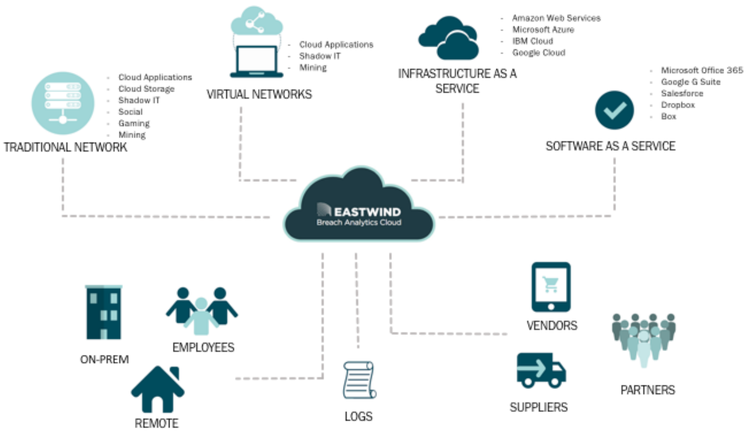
- Combine logs with telemetry from network sensors, SaaS, IaaS, and DNS.
- End to end cyber security and visibility of your infrastructure.
- Enhance your Breach Analytics with Eastwind for Logs telemetry.

Advanced Breach Analytics for Logs

Eastwind for Logs provides centralized visibility, threat analysis and user and entity behavioral analytics to identify malicious activity, insider threats and data leakage within your environment, whether it’s traditional or hybrid . Eastwind for Logs enables organizations to centralize logs from multiple sources quickly and easily.

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 logs, 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 Solution



Eastwind for Logs

Eastwind provides unified visibility of your entire cyber terrain. With this solution, security teams can reduce the overall impact from breaches, including costly fixes, disrupted business, stolen information, and damaged reputations.

Monitor the following types of events:

- Administrative and API access to cloud environments
- Network access control lists changes
- Authentication - failed/successful/brute force/directory harvest
- Security group changes
- IAM policy changes
- Cloud storage activity
- VPC / Compute instance changes
- Anomalous user behavior - geo/irregular hours

Eastwind for Logs Capabilities

The Eastwind for Logs product, collects, analyses and enriches telemetry from cloud environments and system logs into our breach analytics cloud.

Features include:

- Support for cloud infrastructure providers: Amazon Cloudtrail, Google Stackdriver and Microsoft Azure
- Support for Windows

Breach Analytics at Speed and Scale

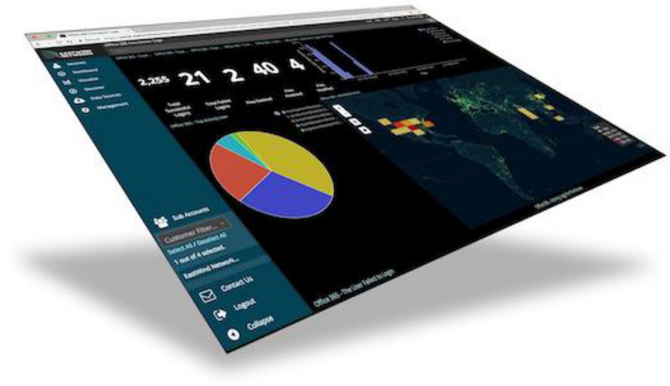
Combined with logs, fuse telemetry from Office 365, G Suite, Salesforce.com, cloud storage providers, cloud infrastructure, traditional networks and virtual environments all from within a single pane of glass.

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 Logs costs

Eastwind for Logs

—Metered or Contract offerings per GB ingested.

Remove friction from Log analysis

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

EASTWIND

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