EASTWIND

The Challenge:

As organizations digitally transform, their attack surface increases while their visibility and defenses do not keep pace. Defenses become fragmented with multiple solutions providing visibility and cyber security. Eastwind arms security teams with comprehensive visibility in an integrated cyber security solution.

Solution:

- Eastwind for SaaS
- Eastwind for IaaS
- Eastwind for DNS
- Eastwind for IaaS
- Eastwind for Networks

EASTWIND

Eastwind Benefits:

- Collect, analyze and enrich network and cloud monitoring APIs with your other network, IaaS, SaaS, DNS and application data.

- With Eastwind, 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 actors, scope incidents, and reduce dwell time.

Enterprise Breach Analytics at Scale and Speed

As you undergo digital transformation, Eastwind offers the only breach analytics cloud that provides complete visibility of your key cyber terrain. We analyze data flowing across hybrid networks and telemetry from cloud providers, hosted applications and mobile workforces – with speed and precision to identify malicious activity, anomalous behavior, insider threats and data leakage. Eastwind enables organizations to embrace emerging technologies such as SaaS and IaaS allowing them to grow with a security first approach.

Eastwind provides a comprehensive array of sensors and applications that gather telemetry which is enriched and analyzed by the Eastwind Breach Analytics Cloud. This powerful solution reduces analyst response time and keeps them in their mental workflow. Acting as a force multiplier, our automated hunters provide hindsight to identify malicious activity that has evaded other security solutions. Cyber defenders can quickly hunt, analyze and visualize all activity relevant to your enterprise, rapidly finding complex relationships, and visualize patterns using the Breach Analytics Cloud. The result is breach analytics at scale and speed, accelerating incident response and providing critical intelligence for network forensics.

Hunt
Search and pivot on indicators to identify threat actors and scope incidents with a fast and powerful query engine

Analyze
Fusing multiple sources, machine learning, signatures, and anomaly detection to interpret months of data

Visualize
Empowers analysts to build and navigate complex relationships revealing previously unknown patterns

Beyone the Traditional Network

Today, the IT footprint of most organizations has expanded beyond traditional networks and campuses into virtual networks, cloud providers and a mobile workforce; often times at breakneck. With this transition, companies often lack the visibility needed to reduce risk as they take advantage of these business-enabling technologies. When an organization is breached, only complete visibility of all the digital footprint can provide the context you need to identify and respond. Gain complete visibility across your entire attack surface by collecting telemetry from the following environments:

Eastwind for SaaS

Our SaaS integrations gather API and log data from cloud application providers such as G Suite, Office365, Dropbox, Box, Salesforce and others to detect breaches and enable cloud forensics.

Eastwind for DNS

Our DNS security services provides advanced threat protection and intelligence to block malicious attacks, while providing a single platform to analyze the data. Eastwind uses 20+ sources of threat intelligence data to monitor domains and machine learning to score and assess suspicious domains to guard your network's internet traffic.

Eastwind Compromised Credentials

Our compromised credentials service alerts you to data breaches that contain email addresses matching your organizational domain names reducing your window of exposure to attack or insider threats.

Eastwind for IaaS

Our cloud sensors are deployed directly into your cloud service provider's infrastructure collect network telemetry from AWS, Azure, Google Cloud, IBM Cloud and others. Coupled with native logging capabilities and APIs, gain critical visibility into your cloud infrastructure.

Eastwind for Networks

Our hybrid-network sensors collect telemetry utilizing our high-speed deep application inspection and enrichment engines utilizing both hardware and software appliances to provide visibility for your on-premises and datacenter networks. Our network sensors extract metadata from over 3,000 network-based applications providing analysts deep context of network and user behavior.

Eastwind 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.

Eastwind Deception

Our deception services enable defenders to rapidly deploy deception proxies to alter the attacker's situational awareness. An engagement with a deception service is either a misconfiguration or an attacker. Create uncertainty, increase the cost to the attacker, detect lateral movement and protect critical assets.

With the combined solution, security teams can reduce the overall impact from breaches, including costly fixes, disrupted business, stolen information, and damaged reputations.

Breach Analytics Built On Limitless Visibility

About Eastwind Networks

Dell for Entrepreneurs
Founders 50

Eastwind Networks recognizes that today's business and government organizations have a critical need to secure their IT networks and hybrid environments against an expanding number of increasingly sophisticated threats both internally and externally. To answer this demand, we are continually developing the best-of-breed solutions in enterprise breach analytics and detection technology.

The Eastwind Networks team consists of seasoned and knowledgeable professionals with over 40 years of combined experience in IT security. We have a passion for innovating powerful cyber security platforms that deliver on network security and breach analytics. Founded in 2014 and led by a team of Internet security veterans, Eastwind Networks was named a Founders 50 member by Dell.

EASTWIND

For more information on Eastwind, please see eastwindnetworks.com