CySight

Predictive AI for Cyber Intelligence and Network Visibility

Delivering Actionable Insight, Business & Cyber Intelligence from every network flow

Provides NetOps and SecOps with predictive AI baselining detection and unrivaled visibility of on-premise and cloud networks with complete contextual big-data, small footprint forensics

We recognize that our customers require adaptable solutions that are flexible, scalable, and powerful enough to aid in network complexity control with significantly increased network visibility.

The major forces driving this market are a lack of visibility into all aspects of physical network and cloud network usage, rising compliance, service level management, regulatory mandates, rising cybercrime sophistication, and increasing server virtualization.

Determining the origin and the nature and assessing the impact are some of the major visibility issues that are encountered with maintaining service levels, understanding network slowdowns and outages, and detecting, DDoS, Ransomware and other cyber-attacks and risky traffic.

Multifunctional, affordable & feature-rich

- Intelligent Baselining, Threat Intelligence, Machine Learning, and A.I. Cyber Forensic Diagnostics.
- Deepest Retention Scalability of flow data globally.
- Network and cloud visibility and security.
- Vendor agnostic with broadest metadata support.
- Scalable dropless granular contextual analytics.
- Uncovers previously unknown threats.
- Identifies Ransomware, DDoS, ToR, and other outliers with real-time attack maps.
- Unprecedented Network and Cloud Visibility eliminates blindspots and improves Defense in Depth using powerful visualization, forensics, and alerting.

HIGHLIGHTS

CySight's innovative network flow auditing raises the bar for all-sized deployments seeking proactive multi-intelligence baselines that enable you to see, find, and manage outliers while also benefiting from deep contextual forensics.

SOLUTION FEATURES

Only full-featured monitoring solution that enables big data benefits in a small footprint at this price point

All baselines are preconfigured, learned and activated to make deployments fast and easy

Uses the same management user interface across all network and cloud devices to provide a consistent user and feature experience.

Correlation of endpoint detection and behavioral anomaly detection is provided through a single, intuitive open workflow interface.

Includes RESTful web-based API and powerful report automation for IPAM (chart of accounts) management and data extraction.

SOLUTION BENEFITS

Delivers actionable insight/business intelligence

Cost effective solution for all medium to huge locations

Simplified but flexible perpetual or subscription license configurations and ordering makes the product easy to buy or sell

Customer investment protection as CySight's collection and retention is combined with machine learning and predictive AI.

Every minute counts when resolving IT incidents and Security Risks and assessing the impact to the business. CySight's smart network predictive AI baselining solution continues to generate actionable insight by delivering the right monitoring information to the right teams at the right time.

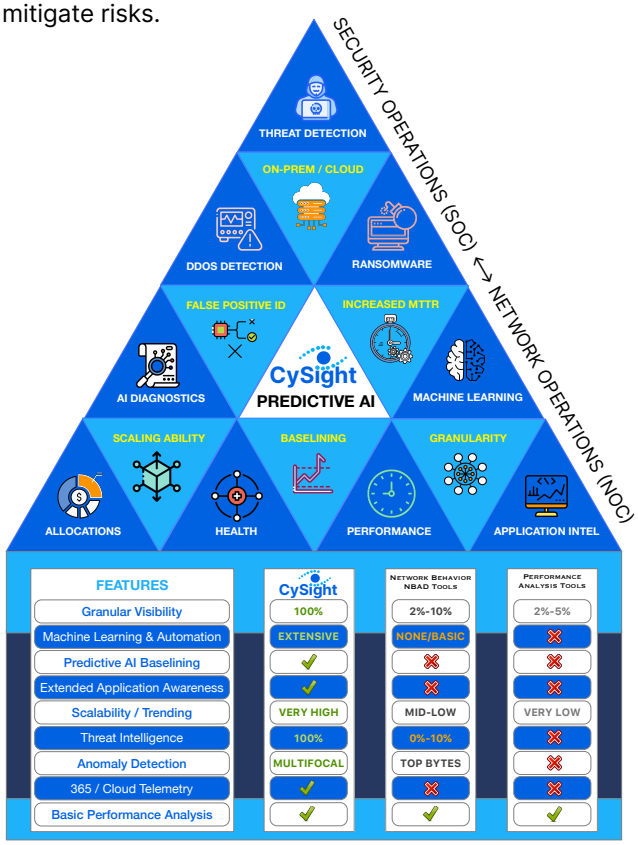
Existing network management and network security point solutions are facing a major challenge due to the increasing complexity of the IT infrastructure. Over 95% of network and cyber visibility technologies retain only 2% to 5% of all data acquired, resulting in significantly inaccurate analytics and risk!

This is because other vendors' products are designed to capture the surface level of network communication flow records orientated to a single value proposition and are not constructed to retain the critical flow records present in a typical medium to large enterprise, campus, or ISP.

Take Control of your Network

The key objective of Predictive AI Baselining and Machine Learning coupled with deep Forensics is to significantly improve visibility of Network Traffic eliminating network blindspots and providing qualified sources and reasons of communications that impact business continuity.

The ability to collect flow at a more granular level provides the ability to analyze new applications and mitigate risks.



CySight's advanced netflow auditing is available for on-premise and cloud deployments. Multi-tenancy collection, portal, and automated reporting provide the ability to automate data mining which can be integrated with upstream services and suits Managed Service providers (MSP's) and Internet Service Providers and Telco (ISP's) who are seeking to deliver advanced threat intelligence, network analytics and managed services.

It is comprised of multiple modules and can run standalone, clustered hierarchical and use multi-threaded collection to provide flexible architectural options enabling cost-effective high compliance network traffic transaction logging with forensic analysis tools to perform data mining and baselining on any aspect of flow data and can orientate from simple performance analytics to complex cyber-security profiling.

CySight scales in architecture and licensing and is therefore suitable for enterprises of any size.

Machine Learning-based Anomaly Detection and Automated AI Diagnostics consists of a comprehensive Intrusion Detection System (IDS) comprised of machine learning, detection and artificial intelligence diagnostic engines that work together to find network behavior anomalies with automated problem-solving processes to pinpoint, mitigate and qualify the reason(s) for an anomaly.

Threat Intelligence based on global threat knowledge powers an advanced threat intelligence engine correlating, identifying, and detailing communications with nefarious endpoints in real-time that are known to be risky such as Ransomware, ToR, Botnets, Malware and illicit p2p traffic.

Integrated Cyber and Network Visibility

- Recognize and baseline actual use of all key business services across cost centers.
- Automatically be alerted to the impact of outliers pro-actively manage and troubleshoot security and network application issues.
- Gain visibility of end-point and behavioral based threats such as viruses, hacking, multicast, DDoS, Ransomware, peer-to-peer (P2P) and worms.
- Account for all traffic to key business services on even the largest of environments on-prem or in the cloud.
- Identify unauthorized and inappropriate access.
- Identify network gateway bottlenecks.
- Reduce costs by substantially speeding up Mean Time To Repair (MTTR) and recovery using Automated Diagnostics and Comprehensive Traffic Accounting.
- Validate WAN Optimization schemes with pre-post deployment assessments.
- Analyze Peering traffic analysis
- Archive information for regulatory and compliance requirements. Retain full definition retention for compliance (sox, basel2, iso9000, ASGAR, Data Retention Compliance, Insurance) with long-term historical track and trace capabilities of all traffic to and from your key business systems.
- Monitor and managing service level agreements and ensure usage policies are enforced.
- Capacity Plan and forecast capacity requirements. Plan for expansion of your company's key business servers, data centers or whole of network needs.
- Accurately plan network changes and new application rollouts.
- Monitor and alert on Service Levels with customized QoS values.
- Identify network performance issues with comprehensive root cause analysis and forensics monitoring.
- Justify bandwidth upgrades.