CySight

Predictive AI Cyber and Network Intelligence

Getting Started with CySight

CySight analyzes, segments, and learns from granular flow telemetry already supported by your network infrastructure in real-time using historical big-data for machine learning and threat intelligence correlation to identify cyber-threats and abnormal behavior and context otherwise undetectable. Revolutionary flow collection and automated diagnostics provide unprecedented multi-faceted network and cyber intelligence from the network, application, data, and perimeter layers with support for all flow capable devices strengthening “defense in depth” and providing complete end-to-end network visibility and east-west and north-south accountability accelerating incident response and reducing enterprise risk in even the most challenging environments.

Experience may differ from published result and depends on flow size, hardware performance, operating system settings and flow variance or other environmental conditions. Although every effort is made to document all aspects of the application, changes may occur from time to time that may provide additional or changed features and you are responsible to perform due-diligence to ensure the product or any changes thereto meet your requirements. Subject to IdeaData EULA terms and conditions.

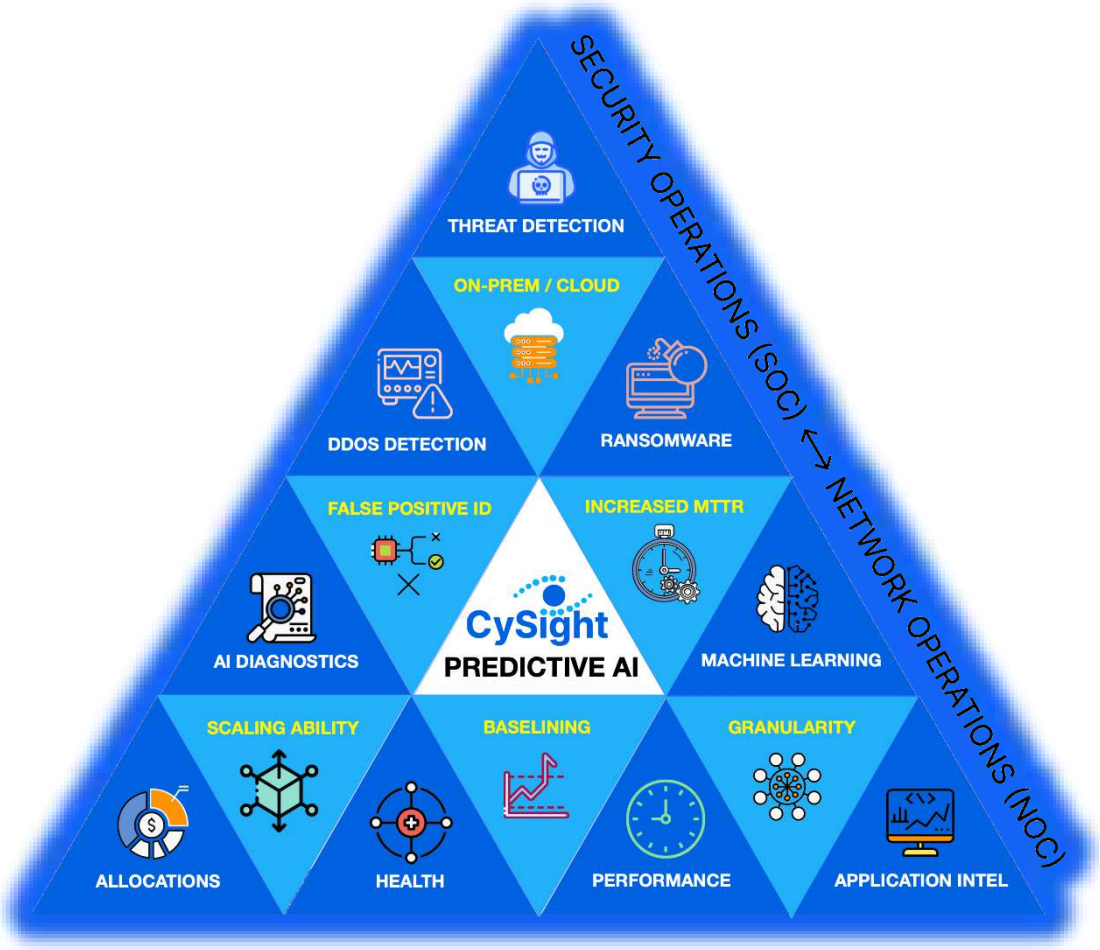
CySight.ai

Introducing CySight

CySight is an integrated network and cyber intelligence solution. It is a network super vision solution that provides, granular on-demand and actionable intelligence, about everything traversing your network, and is unique in its ability to retain and correlate context against high granularity telemetry.

CySight analyzes, segments, and learns from granular flow telemetry already supported by a typical network infrastructure in real time. It uses historical big data for machine learning, and threat intelligence correlation to identify cyber threats and abnormal behavior and context otherwise undetectable.

Its revolutionary flow collection and automated diagnostics provides unprecedented and multi-faceted network and cyber intelligence from the network, application, data, and perimeter layers with support for all flow capable devices, strengthening “defense in depth” and providing complete end to end network visibility and east west and north south accountability. A CySight solution will substantially accelerate incident response and reduce enterprise risk in even the most challenging and complex environments.

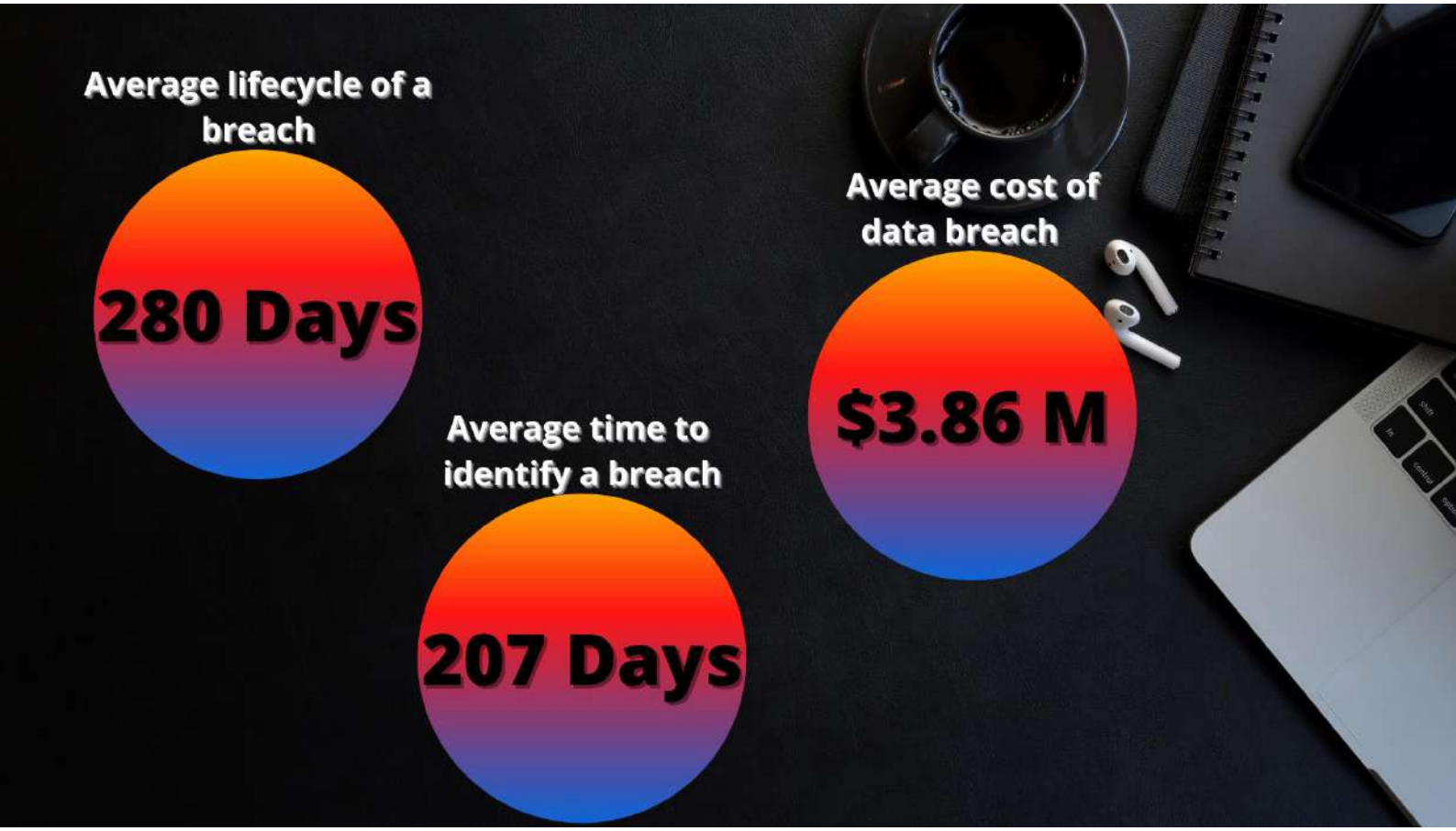


CONFIDENTIAL. NOT FOR REDISTRIBUTION WITHOUT IDEADATA PERMISSION
All rights reserved 2021

CySight's ability to scale in collection, retention and correlation goes well beyond any other flow tool in the market. The granularity benefits that are derived from our rich contextual data, coupled with a flexible toolset to analyze every aspect, allows for high-definition forensics.

Our cyber security additions turn on powerful, real time cyber intelligence tools, that use smart baselines to identify anomalous outliers and threat intelligence correlation for ultimate visibility of nefarious communications.

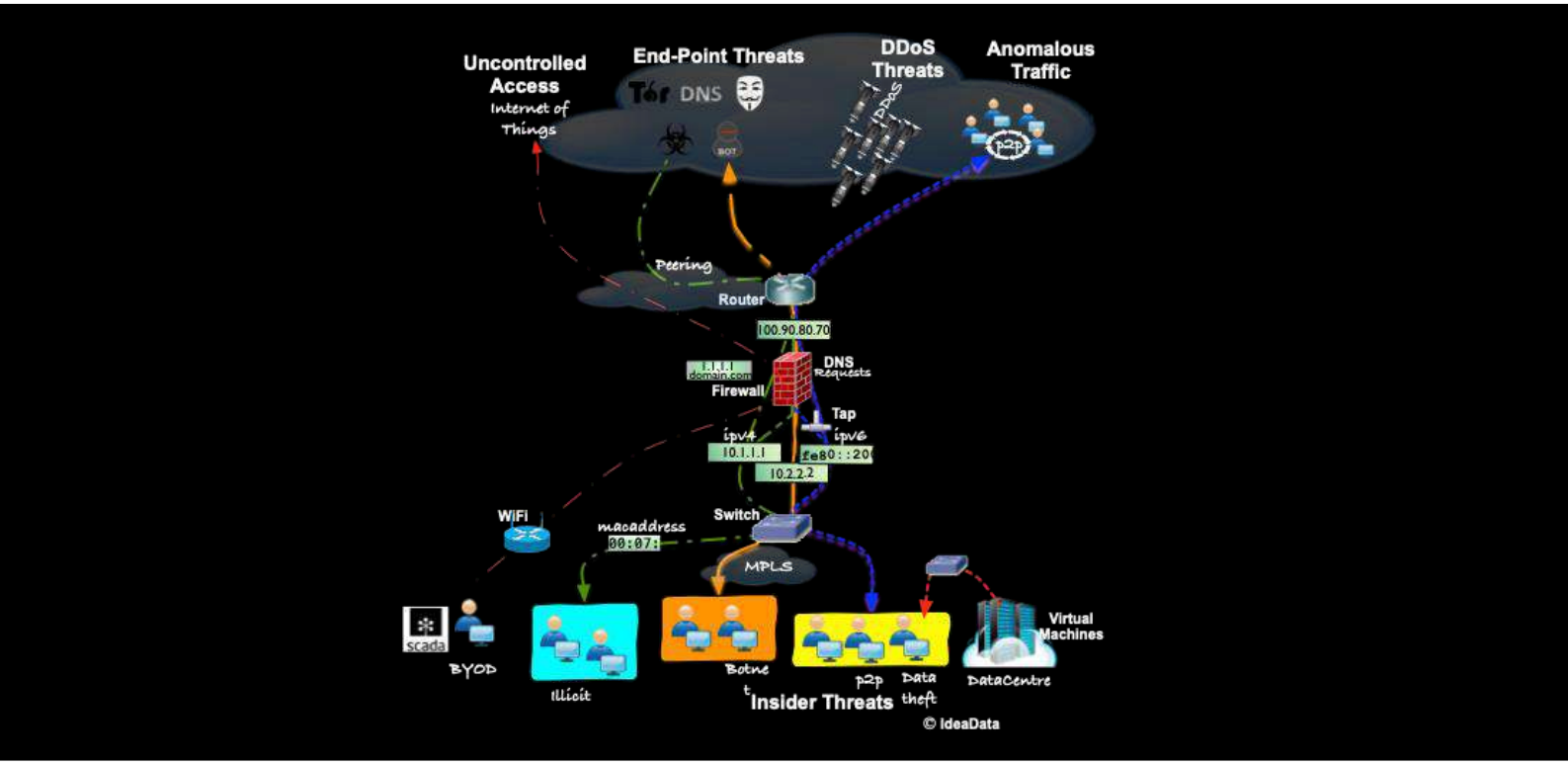
The confluence of analytics, detection, context and early warning substantially speeds up Mean Time To Resolution (MTTR), and eliminates network blindspots, giving you extreme visibility and control.



CONFIDENTIAL. NOT FOR REDISTRIBUTION WITHOUT IDEADATA PERMISSION
All rights reserved 2021

CySight

Advanced Granular Flow-Based Network Analytics



The growing complexity of the IT infrastructure is the major challenge faced by existing network management and network security point solutions. The major forces driving this market are lack of visibility of all aspects of the physical network and cloud network usage, growing compliance, service level management, regulatory mandates, rising level of sophistication of cybercrimes and growing virtualization of servers.

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 cyber-attacks and risky traffic. Every minute counts when resolving IT incidents and Security Risks and assessing the business impact. The key objective of Network Forensics is to improve visibility of Network Traffic by eliminating network blindspots and qualifying sources and reasons for high-impact traffic

Using an integrated cyber and network intelligence approach offers, a superior and cost-effective way to significantly reduce the Mean Time To Know (MTTK) for a wide range of network issues or risky traffic, thereby dramatically reducing wasted effort and associated direct and indirect costs.

CONFIDENTIAL. NOT FOR REDISTRIBUTION WITHOUT IDEADATA PERMISSION
All rights reserved 2021

IdeaData

In today's connected world, every incident response action includes a communications component. An incident may need to be analyzed post-mortem and you need to be able to analyze historical behaviors, investigate intrusion scenarios and potential data breaches and qualify internal threats from employee misuse and quantify external threats from bad actors.

External Threats can come from many sources. These could be from new kinds of crawlers or botnets. Ransomware attacks are still on the rise and are finding new ways to infiltrate organizations. Denial of Service (DoS) and distributed denial of service attacks (DDoS) continue unabated and are a high risk to business.

Insider Threats can also occur in a number of ways. Your network may be used to download or host illicit materials or be used in whole or in part to attack. Your intellectual property could be slowly being leaked by negligence, hacking or compromised by disgruntled employees.

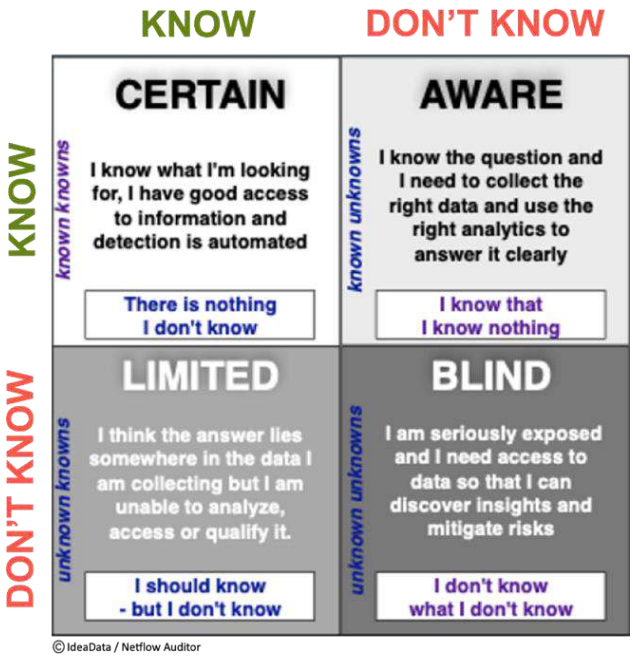
Networks are becoming increasingly complex. Many inadvertent threats can open the door to malicious outsiders because of negligence, failing to update and patch security holes.

60% of enterprise information security budgets by 2020, will be allocated for rapid detection and response approaches which is up from less than 10% in 2013.[1]

According to Gartner, advanced targeted attacks are set to render prevention-centric security strategies obsolete.

Industry analysts predict that by 2020, securing enterprise IT will require a shift to information and end-user centric security strategies focused on an infrastructure's endpoints.

- **It will lose control**
- **Continuous compromise**
- **Financially motivated attacks**



Network Matrix of Knowledge

[1] Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence". Gartner

CONFIDENTIAL. NOT FOR REDISTRIBUTION WITHOUT IDEADATA PERMISSION
All rights reserved 2021

Understanding the essentials

So, if prevention is failing, what is left that IT can actually still directly control?

IT increasingly will not directly own the user's device or the services they consume, limiting its ability to place invasive controls. In most cases, information must become the focal point for our information security strategies.

When breached, how are enterprises able to get visibility as to what happened?

Detailed monitoring and recording of interactions with content and systems. Granular Forensics, Anomaly Detection and Threat Intelligence ability is needed to Identify what other users were targeted, what systems were potentially compromised and what information was exfiltrated.

As you will learn in more detail in this session, there are only two methods available, packet or flow collection, to perform this kind of recording and monitoring.

So, how do you identify attacks without signature-based mechanisms?

Pervasive monitoring enables you to identify meaningful deviations from normal behavior to infer malicious intent. Nefarious traffic can be identified by correlating real-time threat feeds with current flows. Machine learning can be used to discover outliers and repeat offenders.

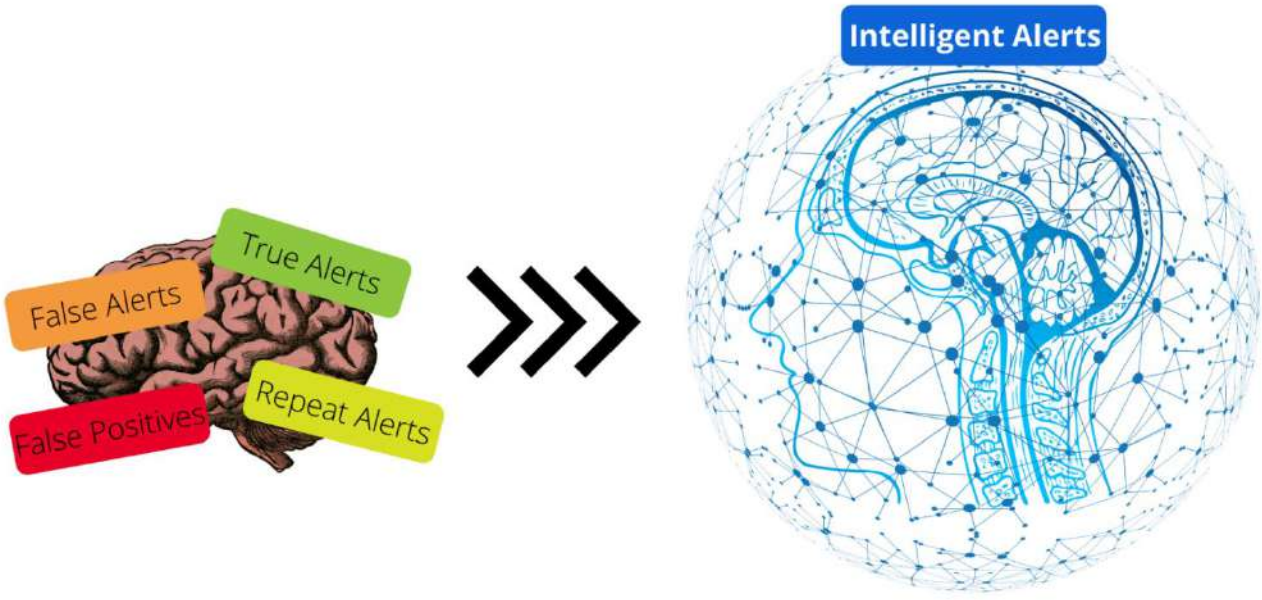
CONFIDENTIAL. NOT FOR REDISTRIBUTION WITHOUT IDEADATA PERMISSION
All rights reserved 2021

CySight

Understanding The shift towards Flow-Based Metadata for Network and Cloud Cyber-Intelligence

- The IT infrastructure is continually growing in complexity.
- Deploying packet capture across an organization is costly and prohibitive especially when distributed or per segment.
- “Blocking & tackling” (Prevention) has become the least effective measure.
- Advanced targeted attacks are rendering prevention-centric security strategies obsolete.
- There is a Trend towards information and end-user centric security strategies focused on an infrastructure’s end-points.
- Without making use of collective sharing of threat and attacker intelligence you will not be able to defend your business.

The ability to perform network forensics at a granular level enables an organization to discover issues and high-risk communications happening in real-time, or those that occur over a prolonged period such as data leaks. While standard security devices such as firewalls, intrusion detection systems, packet brokers or packet recorders may already be in place, they lack the ability to record and report on every network traffic transfer over a long-term.



CONFIDENTIAL. NOT FOR REDISTRIBUTION WITHOUT IDEADATA PERMISSION
All rights reserved 2021

IdeaData

Conclusion

Network security and network monitoring have gone a long way and jumped through all kinds of hoops to reach the point they have today. Unfortunately, through the years, cyber marketing has surpassed cyber solutions and we now have misconceptions that can do considerable damage to an organization.

The biggest threat is always the one you cannot see and hits you the hardest once it has established itself slowly and comfortably in a network undetected. Complete visibility can only be accessed through 100% collection and retention of all data traversing a network, otherwise even a single blindspot will affect the entire organization as if it were never protected to begin with. Just like a single weak link in a chain, cyber criminals will find the perfect access point for penetration.

CONFIDENTIAL. NOT FOR REDISTRIBUTION WITHOUT IDEADATA PERMISSION
All rights reserved 2021