CySight

Predictive AI Cyber and Network Intelligence

Maximizing and Optimizing Flow Potential

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.

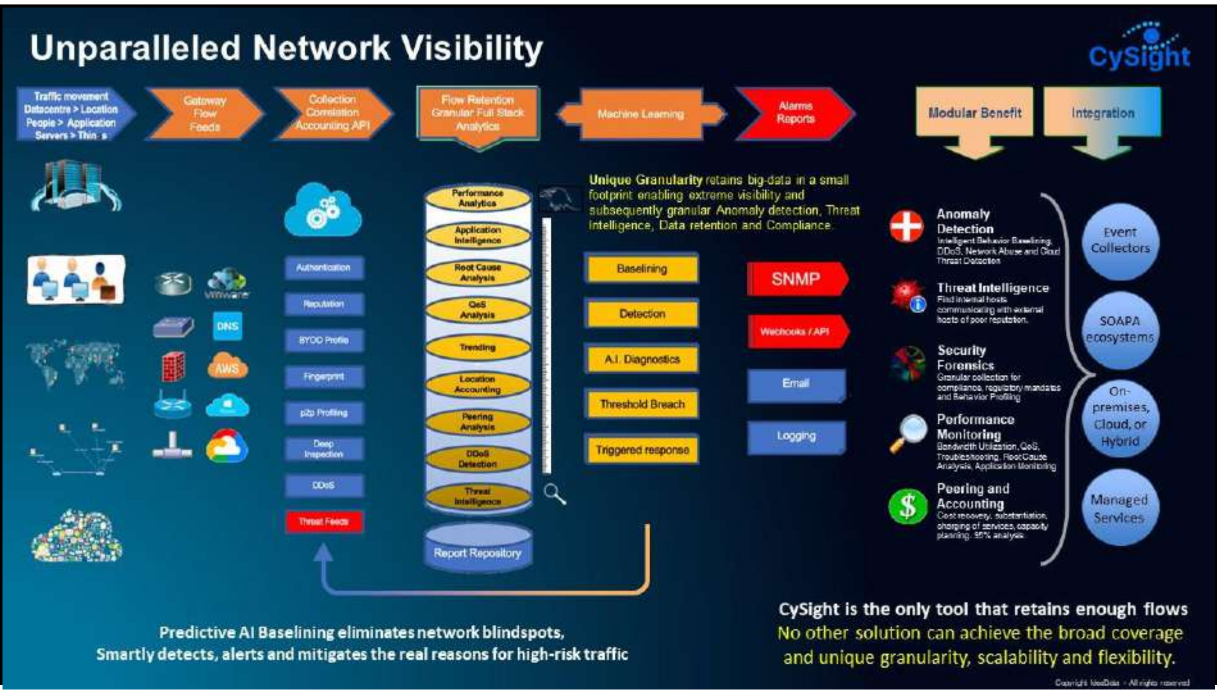
Experience may differ from published result and depends on flow size, hardware performance, operating system settings and flow variance or other environmental conditions. Although every effort is made to document all aspects of the application, changes may occur from time to time that may provide additional 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

CySight.ai

Not all Network Flow Analytics Tools were created equal

The potential that flow records provide is visibility of detailed traffic analytics and that is really the main benefit of flow. However, flows can be very profuse and a lot harder to manage than SNMP, RMON or Syslog data! Thousands and in some cases millions of flows can come across to a flow collector every minute. Therefore, it is important to have a flow solution that can scale to collect all the flows being sent.



Unparalleled Network Visibility

Unique Granularity retains big-data in a small footprint enabling extreme visibility and subsequently granular Anomaly detection, Threat Intelligence, Data retention and Compliance.

Predictive AI Baselining eliminates network blindspots,
Smartly detects, alerts and mitigates the real reasons for high-risk traffic

CySight is the only tool that retains enough flows
No other solution can achieve the broad coverage and unique granularity, scalability and flexibility.

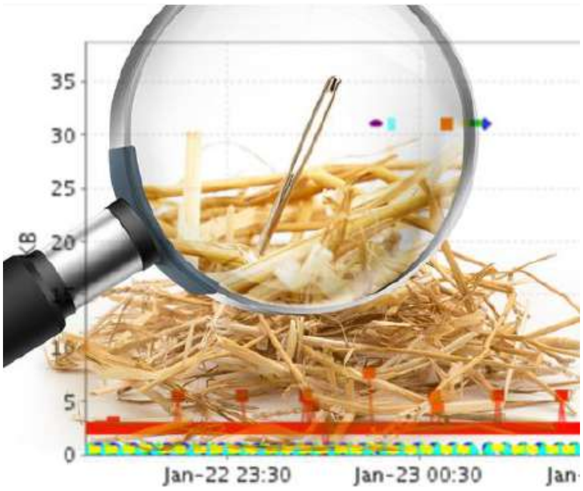
Flow data can be very diverse and can be exported out of a router, switch, firewall, wi-fi point, virtual machine, tap, or a cloud-based environment like Google, Azure or AWS. As data traverses through those pieces of equipment the call detail records are being sent to our collectors.

All flow collectors were not created equal! Collecting flows is only the first part of a flow solution. It is even more important to be able to scale to firstly, collect all the flows and secondly, retain sufficient granularity or be able to retain the important flows. In high compliancy cases the ability to retain all the flows is absolutely paramount.

As a point of distinction, CySight is unique in its ability to scale in collection as well as retaining the highest granularity and the ability to extend flows with a real-time tagging process that enhances the flow data with correlated value-adds. As you will appreciate as you progress with CySight, is its unique ability for granular flow retention is a good fit with packet processing tools like firewalls and packet brokers or dealing with many flow exporters.

The importance of Granularity

The ability to collect flow at a more granular level provides the ability to analyze new applications and their network impact. For example, you can identify new application network loads or remote site additions or see improvement from application-policy changes.



Deeper forensics of Netflow traffic can enable the detection of unauthorized traffic, which is useful for performance analytics to avoid costly upgrades and identifying the applications causing congestion. It is also needed for security compliance to quantify which IP addresses are involved in peer-to-peer file sharing (p2p), leaking intellectual property, or trying to access secured services. Granular Netflow can be used for anomaly detection to discover misconfiguration or security intelligence, identifying DDoS and worm diagnosis, and with appropriate correlation, which end-points have been blacklisted as malicious or risky. You can validate quality of service and confirm that appropriate bandwidth has been allocated to each class of service and that no Class-of-Service is over or under-subscribed.

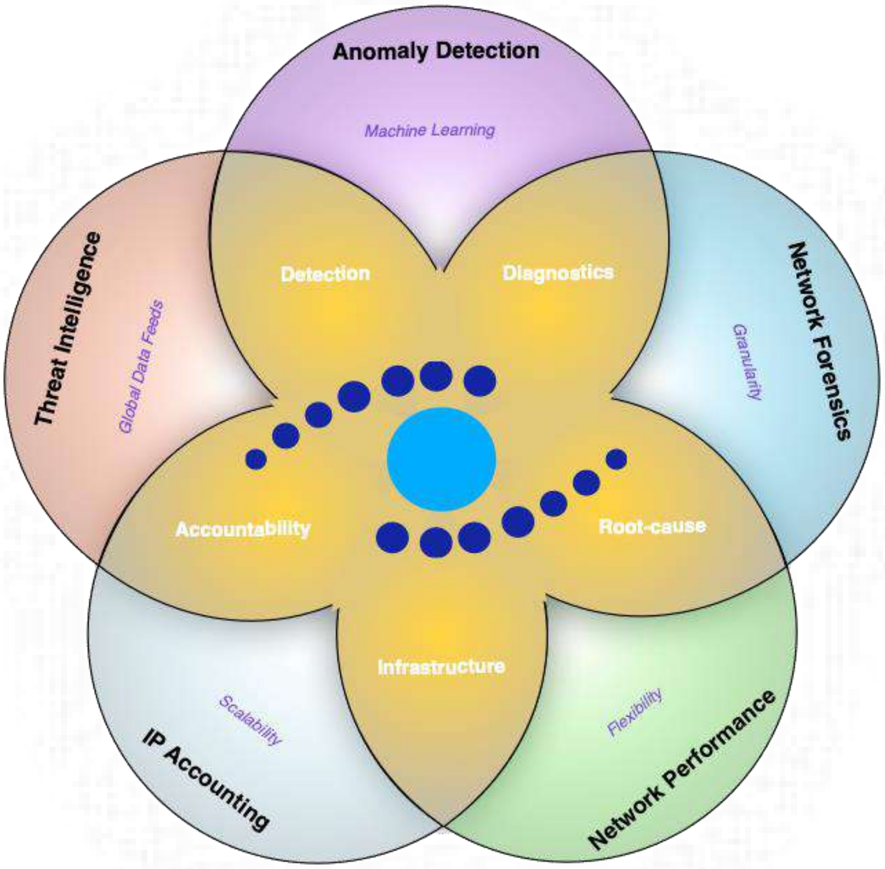
A lot of organizations still have only very basic, bandwidth orientated network visibility and little or no cyber intelligence! They're using SNMP, RMON or Syslog tools or similar kinds of very basic applications and so they don't have a good idea or understanding of the detail of traffic traversing their network. The flow detail provides the ability to see a depth of data from throughout their network that is otherwise unattainable through other methods of collection.

If you don’t collect and retain the context of granular network data flows, the systems providing alerting will naturally be limited to the event and not what occurred before or after. Consequently, having depth and granularity that you can properly analyze what occurred is critical. It is therefore especially important that you have network and cyber auditing tools that can allow you to analyze the network layers from all perspectives and to enable you to completely eliminate the blind spots, without you getting lost in a data forest, or drowning in a data lake.

Why CySight?

Scalable, Granular and Flexible flow analytics are needed by corporates, ISP's and managed service providers, government and university networks, data centers, global distributed networks and large corporate campuses who require varying degrees of visibility to manage their network environments and to dramatically improve their security posture.

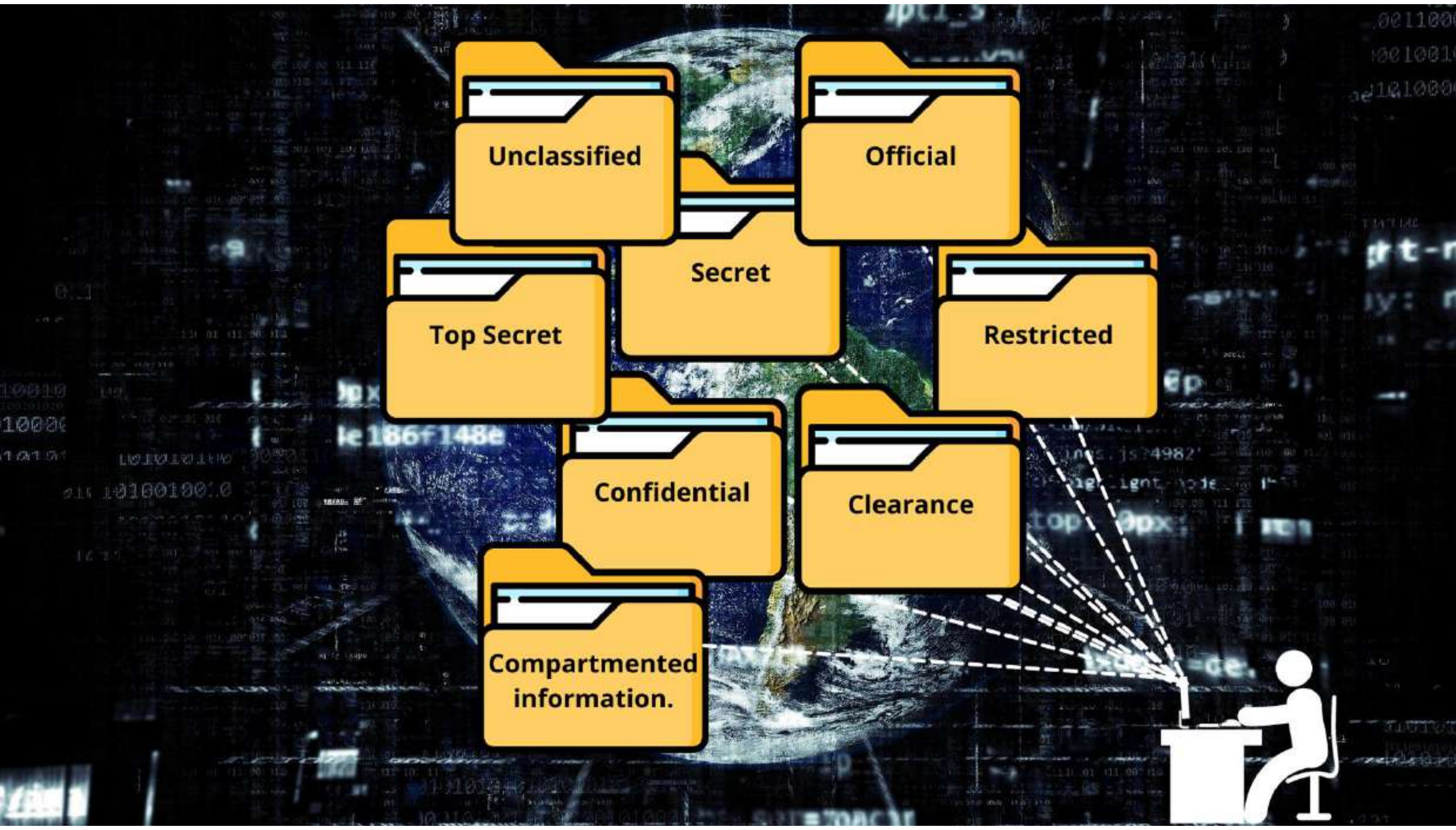
It is, important to properly understand your current and future needs along with the importance of granularity and how it impacts the ability to fully fulfill the following benefits: Performance Analytics, Anomaly Detection, Threat Intelligence, Forensics, Root-Cause Analysis, Baselining, Compliance, Billing, Peering and Cloud visibility.



CySight acts as a glue between network, security, risk, architecture, applications and billing teams, allowing these multiple teams to analyze and share information from the same rich common data source. Network and security teams don't always work closely with each other. Having a tool that provides a means to communicate issues from the same deep analytics we have found has been considerably beneficial for many customers.

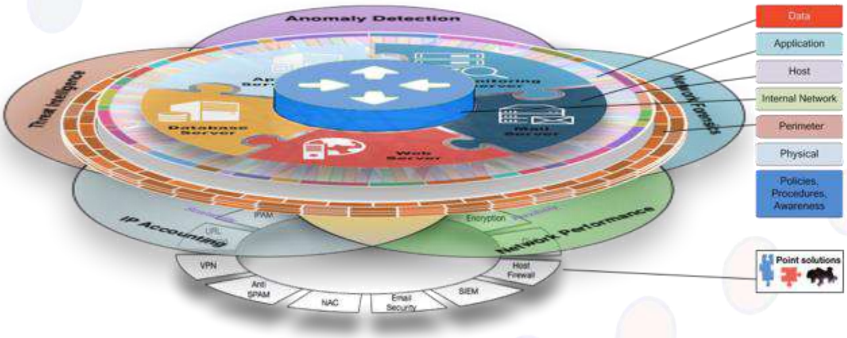
With flow you are dealing with a lot of different perspectives at the same time. In some cases, you need to analyze servers and other times your physical infrastructure and occasionally, it's about the applications. If you have only dealt with simple netflow analytics tools you will quickly appreciate CySight's power as you are now able to analyze multiple perspectives of related data and can easily quantify the complete use of the physical infrastructure delving into the application use, quality of service, host behavior, risky traffic and tracking and tracing complex issues.

Where CySight differs from other solutions is that it broadly analyzes and provides granular network and cyber intelligence completely across the networks information layers as opposed to analyzing limited information from syslog or SNMP or being limited to one specific point within the network. Point Solutions do not cover enough ground as there are multiple risks and is cumbersome to maintain multiple products and to integrate a suite of products. Point solutions tend to be dedicated and orientated to providing information around a specific use case. What tends to get lost in a point solution is context. Once an issue arises in your network, context becomes you best friend.



Retaining Contextual Data

Provides a broad and strategic "Base Layer" modules for Predictive AI network and cyber intelligence enhancing Network management, Defense in Depth visibility and Context to existing tools.
The growing complexity of the IT infrastructure and multiple issues and risks means Point Solutions can't cover enough ground. No other solution can achieve the broad coverage and unique granularity, scalability, flexibility and intuitive forensics and cyber features at the same low cost, low impact and easy deployment.



Eliminating network blindspots, Detect reasons for high-risk traffic, Reduce Mean Time To Know (MTTK)
CySight is the glue between network, security, risk, architecture, and applications taking data feeds from the widest range of devices and functions to enable network and security professionals and existing tools to benefit from a single intelligent data source.

It is also important to understand that where the data is being exported from is going to provide a different context. It also may be for a completely different value proposition.

Analyzing data from wireless network devices or from firewalls, you're going to get a different context of network traffic information versus collecting from a router or switch. For example:

- Firewalls are generally edge points. They may also provide more stateful information and additional information that will allow you to analyze their access lists performance.

- Analyzing a wi-fi point is generally orientated to laptops, mobile phones, tablets, wireless and various "internet of things", and provides the ability to track mac addresses of devices that travel between wi-fi points.

- Packet brokers with new metadata fields like URL may provide additional visibility relating to the end-point of an HTTP request but, also shift the traditional flow visibility value propositions.

Collecting data from the core of a network is different than collecting from the network edges. The flow pressure at the core will require a different configuration and architecture than collecting from the edges.

Where is the Value?

Even if you choose to not currently turn on our security modules, CySight's unique scalability, granularity, automation, and flexibility, will ensure you are going to gain significant benefits when you swap out an existing tool with CySight’s base performance analytics module. As our baselining and security modules are professional extensions to our base tools, they can be easily extended as required.

All flow tools were not created equal. You need to use the right tool for the job. CySight goes well beyond other solutions. We can start by providing an equivalent, but better, retention level at a comparable price point and then allow you to scale up the granularity retention rate, to provide an unprecedented level of visibility.

Your control of your investment into a flow technology will benefit by understanding each of the vendors technical offerings and being able to discriminate between their actual performance capabilities versus their marketing.

Where is the Value?

The ease of a flow tools ability to collect, archive, report, baseline, diagnose and alert beyond a basic bandwidth performance analytic is critical for you to be aware of. Otherwise, you will likely land up having to do a lot of heavy lifting later when you try to get the reports you need – if at all. Many customers that have swapped to CySight, reported to us that they were unaware when they first purchased another tool, that the information that they were able to analyze was exceedingly limited. They were understandably upset, once they understood just how severely misleading the information was, because of their collection and retention limitations.

One major reason these tools are so handicapped is because they do not have the technical capability to scale to retain flows at sufficient granularity, therefore, creating serious detection problems. The data they have retained, can only be orientated around bandwidth performance analytics value propositions, to track the top 10 IP addresses that are consuming the most bandwidth. The level of granularity these tools provide is not that much better than deploying SMTP RMON technologies. many tools have invested more in displaying results in pretty looking screens than having focused on the data collection and automation function necessary to provide real value.

Some of these tools provide what they suggest are security functions. However, without retaining sufficient granular depth or performing baselining and machine learning, the kind of alerts and analytics they provide can only be within the top bandwidth-oriented data they have retained. Even if they allow you the ability to see different perspectives of what they have retained, they still leave you with basically the same blind spots they claimed in their marketing they could solve. Seeing as they cannot scale or flex in their flow collection and retention, ultimately handicapping your visibility and impacting your business, you have to ask, “where is the value in deploying a traffic analytics solution?”.

Some flow tools have orientated their offering towards security and intrusion detection. However, to remain functional they collect additional granularity only when they identify outliers. Many of these tools also fail to provide overall granularity as they are also not built to scale in high retention. This also causes critical data loss that impacts on the ability to analyze other systems that may have been party to the identified issue.

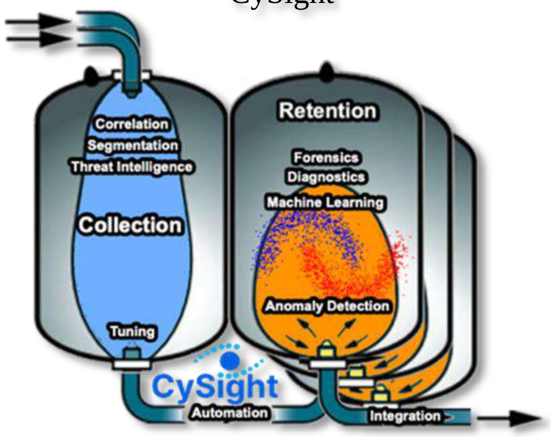
Learn how to identify the right tool

As the level of visibility and security analysis is being extremely misrepresented, engineers need to be careful not to be, “led down the garden path”, and buy into statistically flawed systems with bandwidth biased data and alerts. It is advisable to properly bake-off solutions. Compare the tools side by side to properly understand each tool’s limitations and strengths and ensure they fully meet your current and future requirements.

There are general shortfalls identified in other tools that CySight can easily outperform:

Compare CySight’s ability to scale in collection and archival

CySight



- Machine Learning, A.I. Diagnostics, Baselining, Anomaly Detection and End-Point Threat Detection
- Unique ability to scale in collection and retention with the deepest granularity and historical retention in the market
- Ability to enhance flow context with a real-time correlation process
- Multi-scaling with granular collection
- Multiple devices and interfaces, bursts, high sustained flows, high variability in flows
- Multi-vendor + cloud support + unique flow templates
- Flexible Netflow, IPFIX, sFlow and NBAR
- Strong Integration to 3rd Party

Competitor

Collection
analytics
Lost Forensics
Lost Anomalies
Lost DDoS Detection
Lost Threat Intelligence
Lost Security Visibility
Lost Application Intelligence
Lost Compliance
Lost Context
Lost Billing
Lost QoS
Retention
Limited Top
Bandwidth Orientated
Performance
Analytics

- Cannot scale in retention
- Produces misleading information
- Analytics limited to retained data which is bandwidth-oriented
- Visibility severely impacted resulting in extreme and risky blind spots
- The data presented in reports and a front-end interface can only analyze what has been retained!

The Top 5 Flow Challenges

1. Collection Capacity.

Collection capability is currently expressed in flows-per-second, and many vendors would make you believe this is the main method to ascertain the strength of a flow tool and its ability to scale. This is misleading, as rate of collection has no relation to rate of retention.

It's common for flow tools to hype their flow-per-second rates without revealing how they are scaling in retention and their use of leaky bucket algorithms that sort the incoming flows by top bytes discarding the balance. In fact, they drop most of the flows (95%), losing critical context and content.

High-flow-variance and change capacity to handle sudden-bursts or managing when big flows occur can suddenly cripple and slow down inefficient flow collection.

2. Retention Capacity or Flow retention rate.

The real strength of a flow tool is in its ability to retain flows at scale and to archive flow records in a data warehouse. This is a critical function as granularity retained per minute is impacted by the mix of high flows-per-second and high flow-variance and the overall design of a flow collector application.

Tools lacking the technical capability to retain flows at sufficient granularity are severely handicapped limited to using minimal data that can only be orientated around bandwidth performance analytics.

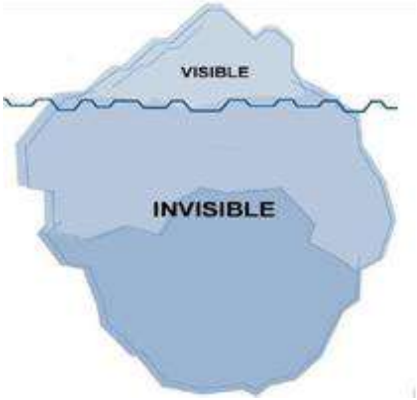
As you can only report on what has been retained, it follows that intelligence and security capability claims that make use of data derived from a limited data set are overstating, misrepresenting, and misleading.

3. Forensic depth and Anomaly Detection

Sufficient data is required to enable high-definition root cause analysis and the deeper the forensic ability, enables more accurate anomaly detection.

A common strategy with flow analytics tools is to rollup data into various intervals after certain limited periods. This repudiates the ability to perform forensics beyond rollup points. Detailed historical collections are critical in identifying issues that occur over a long-term period. You simply cannot report on what you have not stored.

4. Telemetry and Diagnostics ability



A tool can only highlight potential issues based only on data that has been stored.

There are many other telemetry points beyond bytes that can be counted to provide important visibility from conversations and latency to tcp flags, drops and threat counters.

Over simplistic bandwidth orientated collection and retention mechanisms keep you from monitoring critical network information increasing risk and loss.

5. Speed, number of monitored elements and flexibility

The speed, flexibility of alerting and reporting, ease of deployment and special field flow support can have further impact:

The number of monitored elements

The more devices, interfaces, applications, or other aspects monitored has been found to severely impact the performance of other tools.

The speed of reporting over time

Some tools appear useful when first deploying. However, performance may degrade over time.

Flexible architectural and hierarchical deployment

It doesn’t make financial sense, when the only way to scale a tool is by adding more collectors turning what you thought was going to be the cheap option into a cost nightmare that in the end just doesn’t, can’t and could never provide an effective return on investment.

CySight employs a unique methodology of retaining high granularity in small footprints at scale, overcoming the serious limitations that impact other tools.

Conclusion

The core and most vital aspect of network security and network monitoring is the ability to remain consistent and capture all traffic that traverses a network. Today, tools that cannot collect and retain at scale will soon be seen as legacy tools due to the rising advancements and complexity in the cyber market and especially after experiencing Covid-19.

CySight's **Dropless Collection** and **Retention** coupled with **Actionable Intelligence**, enables organizations with the most cost efficient and secure network at any scale. Collection and retention are the first step to permit any kind of network or security ability, as simple as it can be said, Collection and retention are the first steps to permit any kind of network or security ability, as you simply cannot inspect what you were unable to retain.