CySight

Predictive AI Cyber and Network Intelligence

Network and Cyber Monitoring 101

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

Understanding strengths and weaknesses of network and security monitoring technologies collection strategies

It is important to have a basic understanding of the kinds of technology that various flow tools, network management and security tools use to source their network traffic behavior. Each tool in the market processes and value-adds various data sources.

This basic non-technical detail will be helpful in discerning the strengths and cost benefits of using flow records as the primary data source. It will also help you recognize why CySight's unique approach to flow collection and flow retention are revolutionary, along with the high-benefit of its innovative machine learning and the resulting flexible network and security intelligence.

There are 7 primary methods to collecting network knowledge:

1. **Collect and filter SNMP traps**
   The timeliness depends on the processing time of the trap event and will vary for each network element that is sending a trap.
2. **Walk SNMP RMON** structures to collect the top data provided by a network device. The timeliness of the data is usually around 5 minutes per poll.
3. **Collect and filter Syslog events**
   The timeliness depends on the processing time of the syslog event and will vary for each network element that is sending an event.
4. **Scrape device and build flow logs**
   The timeliness depends on the frequency of scraping. Prior to flow technology, CySight achieved this method of collection at high-granularity, scraping every minute.
5. **Analyze flow records**
   Timing of flows is usually set to send every minute, but for some of the low-end flow tools they set to 5-minute intervals to try to reduce flow pressure.
6. **Analyze packets**
   Packet analysis is usually a real-time process and is usually down to the second.
7. **Honeypots and Honey nets**
   Attack analytics use deception technology for intrusion detection. This is a near real-time process.

Each method has a value and should be used for its strengths, but network engineers and security engineers also need to be aware of their shortcomings.

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

Packet Analysis

Packet processing can provide high-detail because it is a stateful way of analyzing data. These tools are most helpful with analyzing short term performance issues but also can provide insight into application sessions. Firewalls, congestion management tools, packet brokers and taps read packets directly and use block and tackle techniques to prevent unauthorized intrusion or diagnostics. Network equipment such as routers and switches to some extent analyze what is “on-the-wire”, allowing traffic to be shunted into different paths or blackholes.

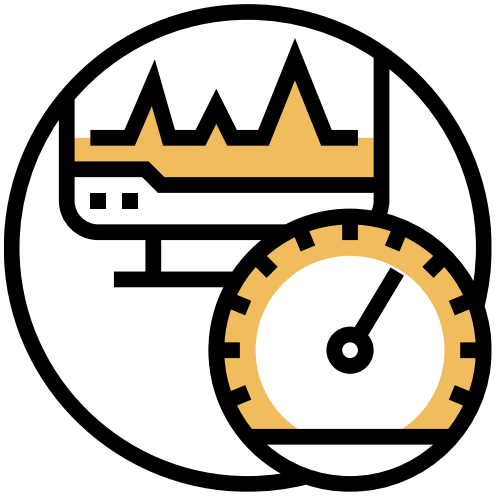
On the down-side, packet processing is usually extremely intrusive and exceedingly costly to deploy and maintain across an organization.

Today, most packet capturing solutions struggle to maintain both a heavy traffic load and deep packet inspection simultaneously, forcing customers to choose one or the other.

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

SNMP & RMON

Traditionally, network engineers relied almost exclusively on Simple Network Management Protocol (SNMP) to monitor bandwidth. Although SNMP facilitates capacity planning, it does little to characterize traffic applications and patterns, which are essential for understanding how well the network supports the business. A more granular understanding of how bandwidth is being used is extremely important in IP networks today.



The beauty of SNMP is that it is an open standard, and it has a unique ability to bring together multiple disparate systems alerts in a common and standardized way.

SNMP is useful for basic performance analytics as it can help guide you as to when you may need to purchase more bandwidth. If however, bandwidth is being abused then SNMP isn't going to help to qualify who used the bandwidth.

Remote Monitoring (RMON) is an extension of SNMP that provides some top-level bandwidth statistics but it is a polling technology, whereas NetFlow, sFlow and IPFIX push the data to CySight.

RMON is severely limited in visibility as it cannot provide the granularity that flow based network monitoring enables. Packet and byte interface counters are useful but understanding which IP addresses are involved as the source and destination of traffic and which applications are generating the traffic is invaluable.

The benefit of leveraging both the detail of flow and the use of traps that CySight can provide, means that CySight can be quickly integrated into a management framework based upon SNMP.

Both network and security professionals, can anticipate exceptional conditions by defining thresholds and alerts and respond to special situations identified by CySight's machine learning anomaly detection engine, threshold alerts or threat intelligence as soon as they occur, and to enable automatic responses. They can store and analyze the historical flow alert data that has been obtained through SNMP trap collection.

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

Syslog Servers

Syslog is another way for network devices to send event messages to a logging server, usually known as a Syslog server. The Syslog protocol is supported by a wide range of devices and can be used to log different types of events. Most network equipment, like firewalls, routers, and switches, can send Syslog messages. However, unlike SNMP, Syslog can't be used to "poll" devices to gather information. Syslog simply sends messages to a central location when specific events are triggered.

SNMP and Syslog completely lack the information such as who is doing what, where, when and with whom.

The ability to characterize IP traffic and understand how and where it flows is critical for network availability, performance, and troubleshooting. SNMP and RMON polling can be particularly noisy on the network and can impact the device being polled. Syslog can be extremely large with much irrelevant data and is event based only.

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

Honeypots and Data Scraping

Behavior analysis using deception technologies is particularly useful for discovering attempts to steal data, but it is awfully expensive to maintain, and limited information is captured.

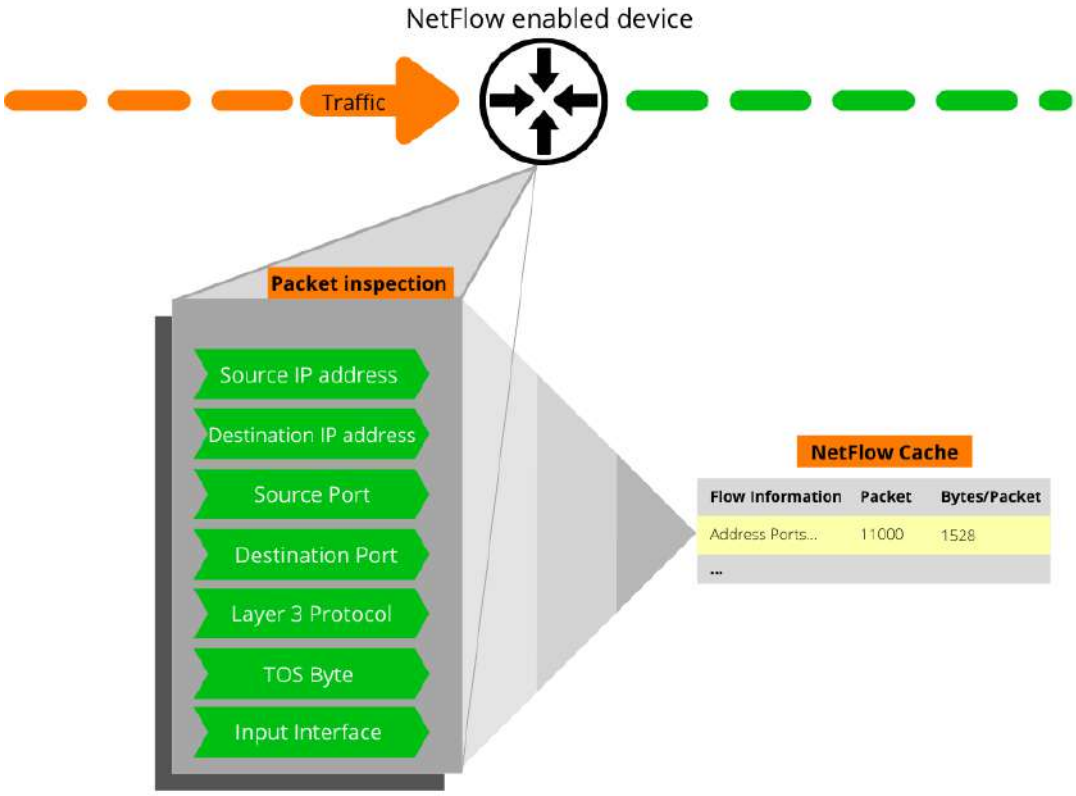
Coupled with CySight's outlier and threat intelligence correlation would provide a high-value analysis of an intruder's behavior pre and post attack. However, the value for identifying network issues or DDoS attacks with deception technologies is basically, nil.

Data scraping is mostly known to be a "specific problem solver", meaning it is used when there is no other option available for data interchange. In simple terms, data scraping is the process of scraping data off a website and putting it in a spreadsheet for dissection and analysis. Once organized on the spreadsheet, the data can be used for whatever purpose it was collected for, typically gathering business intelligence, or holding website data in a simple understandable format.

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

Flow Record Analysis

Flow is a real-time push technology that provides a continual stream of traffic data movement to a collector. It is generally down to one-minute granularity, although, at the expense of accuracy, flow pressure can be partially controlled by means of sampling and flow export timing. Flow analyzers can facilitate solutions to many common problems encountered by IT professionals. It allows a network admin to characterize traffic based on parameters such as protocol, application, source IP address, destination IP, quality of service and other aspects.



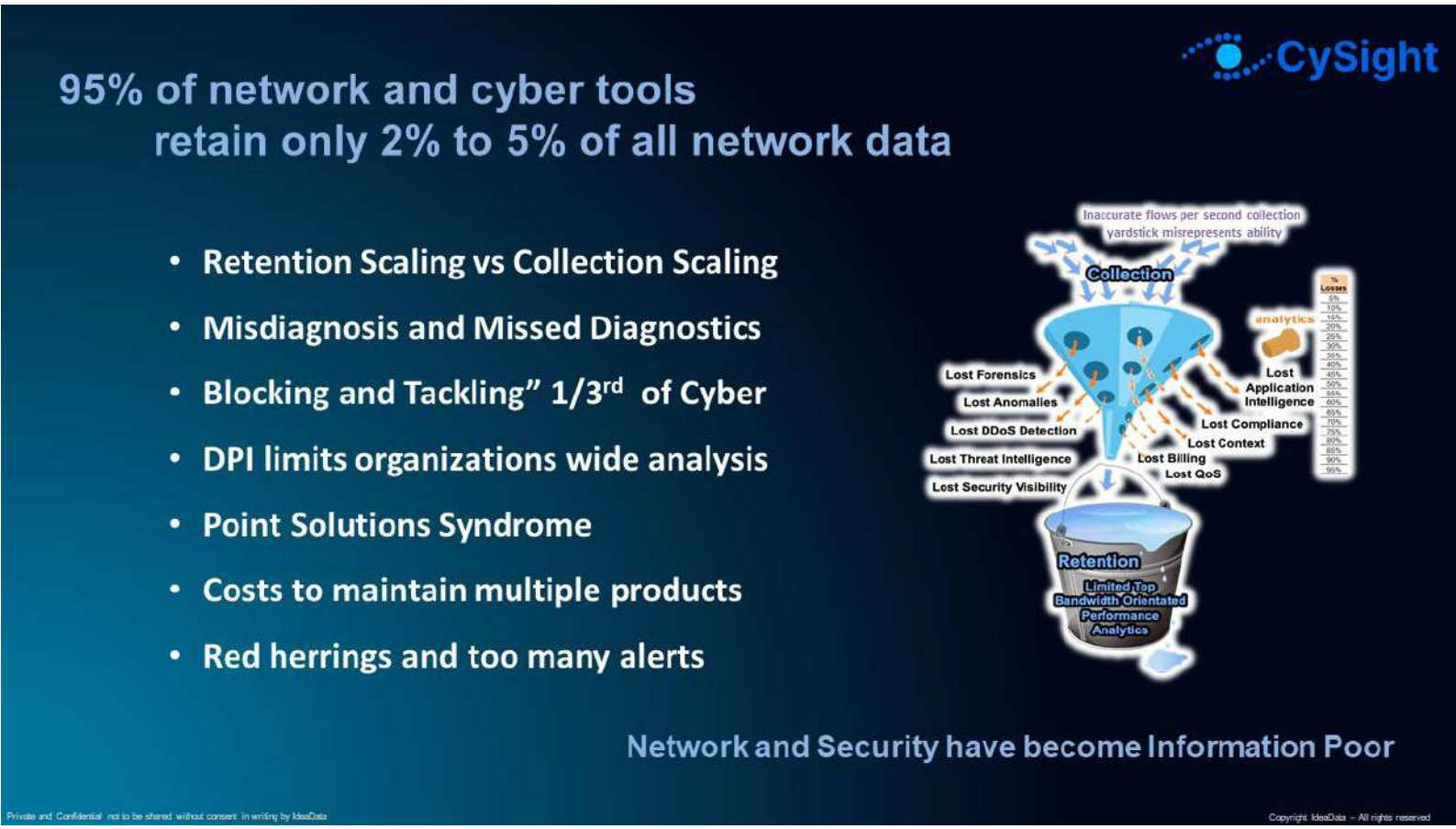
You will appreciate the potential of flow data does not mean that every flow tool can provide all the anticipated benefits. Although flows are exported as granular records, poorly designed flow analyzers cannot scale in flow collection.

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

Unscalable flow analyzers, ***due to minimum retention capacity***, tend to focus predominantly on surface-level collection providing basic performance analytics, allowing you to only understand the bandwidth hogs who are most utilizing the network but they do not necessarily help you diagnose slow network performance.

It is becoming more and more important for Packet processing devices to hand-off reporting and alerting to a flow collector as the task of both collecting and analytics reporting concurrently have proven to be untenable. Packet inspection devices are well suited to providing flow metadata in the form of flow. However, if a flow tool cannot scale in retention ability then it will not be able to provide the level of detail needed to appropriately value-add a packet processors flow export.

Monitoring IP traffic flows with CySight facilitates more accurate capacity planning and ensures that resources are used appropriately in support of organizational goals. It helps IT determine where to apply Quality of Service, optimize resource usage, and it plays a vital role in network security to detect Denial-of-Service attacks, network-propagated worms, and other undesirable network events.



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

Conclusion

Successful network analysis is all about optimization and efficiency, using less and doing more. Adding more tools that will only increase alerts and reports defeats the purpose of a productive IT department, leading the market to find smarter and more **Intelligent** ways of gathering data efficiently.

CySight delivers a complete **Predictive AI** and **Dropless Collection and Retention** method, with unsurpassed granularity to gain in-depth understanding of contextual data, scalability that empowers organizations of all sizes to monitor at various levels of granularity from simple visibility to full compliance, and extreme flexibility to create intelligent alerting and reporting.

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