White Paper:

Next-Gen Network Traffic Analysis (NTA) Log-based NTA vs. Packet-based NTA

ALEX VAYSTIKH, SecBI CTO & Co-Founder

Executive Summary

Network Traffic Analysis (NTA) is a critical component in the war against cyberattacks, allowing corporations to detect and resolve IT infrastructure and network issues. NTA also provides the advantage of ubiquitous monitoring across all platforms and systems, without the limitations found in localized software-based solutions.

The massive amount of information obtained from network traffic using NTA provides analysts the ability to detect malicious activity, and to respond proactively to protect the cybersecurity of their organization.

Traditional NTA solutions based on packet capture require large investments of time and money to get up and running, and demand significant efforts for their daily operation to achieve useful results. Alternatively, NTA solutions that use log analysis and metadata eliminate this overhead, while providing equal insight into potential cyberattacks.

When discussing the various types of NTA solutions, it is important to consider the following:

- The data's value for cybersecurity
- How SSL/TLS encrypted data is handled
- How the solution is deployed in large multi-location organizations
- The storage, processing and hardware requirements

SecBI's solution is based on field-proven technology that detects the types of cyberattacks that are growing in number and sophistication. This paper will explain how SecBI's "Autonomous Investigation" technology, based on cluster-wide detection, provides a faster and more effective solution than hunting through individual logs. As SecBI is deployed on top of Level 7 gateways, SSL termination is already completed eliminating the challenge of encrypted data. Encryption makes looking at the tiny variances in nuances of communication, distribution, frequency, and many other features that differentiate between encrypted malicious traffic and legitimate benign traffic impossible, limiting the effectiveness of packet-based NTA.

This white paper describes the differences among three types of NTA solutions. It explains how the SecBI metadata solution, using unsupervised machine learning, is more scalable, provides the same if not better data quality, is implemented and operated in an extremely short turnaround, and comes with a lower total cost of ownership than any other NTA product on the market.

The Value of Data in Cybersecurity

The amount of network data that is generated in an organization presents many challenges and establishing the value of the data used in analysis is equally as important in evaluating an NTA approach. The three approaches to NTA implementation discussed here are: Event-based packet capture, Layer-7 (L7) metadata, and Flow analysis.

Event-based packet capture utilizes extensive amounts of data for detection and investigation, continuously scanning the local network in real time. L7 metadata provides the same level of detail as packet capture, except for the actual data payload, as seen in Appendix A. The payload is often encrypted by the malicious actor, making it inaccessible for analysis and eliminating the main advantage of event-based packet capture.

Flow data, on the other hand, contains significantly less information that is useful in cybersecurity investigation. Cisco standard NetFlow defines a flow as the following seven values:

1. Ingress interface
2. Source IP address
3. Destination IP address
4. IP protocol
5. Source port for UDP or TCP, 0 for other protocols
6. Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
7. IP Type of Service

Therefore, it is clear from the limited type of information that is captured in Flow analysis that it has little use beyond general network debugging and is rarely helpful for any type of cybersecurity investigation or threat hunting effort.

Event-based packet capture and L7 metadata are the only approaches that can analyze network traffic data thoroughly enough to be effective. Next, we will compare these two in regard to the handling of SSL/TLS encrypted data, deployment in multi-location organizations, and storage, processing and hardware requirements.

Handling SSL/TLS encrypted data

Over 50% of the web's traffic is now encrypted, and the level of corporate data encryption is generally even greater. Analysis of this data requires a SSL/TLS termination/decryption processing system on the organization's network. Deploying a packet capture solution with SSL/TLS termination requires as much as three times the processing resources as that of the basic system, which already requires a great deal of processing capacity, as explained previously. Furthermore, since SSL/TLS is terminated at the gateway, there is clearly additional overhead when deploying this duplicate functionality in the packet capture appliance. Encryption renders packet capture solutions blind to well over 50% of the network traffic, which defeats the purpose of NTA. Encryption makes looking at the tiny variances in nuances of communication, distribution, frequency, and many other features that differentiate between encrypted malicious traffic and legitimate benign traffic impossible.

In contrast to event-based packet capture, most gateway solutions are deployed with SSL/TLS termination (decryption), so this critical information is always available in L7 metadata NTA solutions.

Deployment in large organizations

Packet capture appliances, typically deployed out-of-band via the span port, require additional hardware at each network "choke-point" to accurately capture network data. For larger organizations, this creates significant overhead, as this hardware must be deployed in each of the synchronized multiple network locations.

As discussed, gateway prevention appliances such as web proxies are part of networks' existing infrastructure, often deployed to comply with corporate policies requiring organizations to deploy gateway solutions for prevention and monitoring. Since these gateway web proxies are widely available, analyzing gateway output, Layer-7 metadata, is now as simple as streaming it anywhere in the network or the cloud.

Storage, processing and hardware requirements

Packet capture requires tremendous amounts of storage, processing resources, and additional hardware. As an example, a simple 1 Gbps network that is utilized at 75% capacity will generate 8.1 TB of data every 24 hours. To store 90 days' worth of packet data, which is the minimum needed for the useful detection of advanced threats, will require a whopping 729 TB of disk space. However, storing that much data isn't the only issue, but packet capture also requires tremendous processing power. Each packet needs to be inspected to extract meaningful information to be used in analysis – the metadata.

In contrast, gateway prevention appliances, such as web proxies that are already deployed in most organizations, perform the metadata extraction themselves, thereby eliminating the processing resources required by packet capture solutions. Furthermore, metadata is several orders of magnitude smaller than the packet capture data, consequently requiring significantly less storage space. In sum, NTA solutions that use L7 metadata for analysis eliminate the requirements for large storage capacity, extensive processing power, and additional hardware appliances.

Conclusions

Network traffic analysis is critical in the detection of cyberattacks, but traditional solutions can be costly for the organization in terms of additional storage, processing and hardware appliance requirements and is handicapped by the growing use of encryption.

Using web gateway metadata and log analysis, such as the SecBI NTA solution, provides more value than that found in event-based packet capture. Additionally, the cost of implementing the SecBI solution is a fraction of the price of packet capture solutions. Furthermore, there are other cost reductions when using web gateway metadata and log analysis due to reduced complexity as the required gateway/web proxy infrastructure already exists.

When using an NTA solution based on logs, enterprises and organizations benefit from better visibility into its network behavior, due to SSL/TLS encryption issues, allowing for the detection of all malicious activity from external attackers. This type of next-generation NTA solution includes valued data of traditional NTA solutions, without any of the additional software or hardware requirements and time lags to implementation. In conclusion, SecBI's Autonomous Investigation technology using log-based Level 7 metadata enables NTA-as-a-software to provide the market's most effective, and affordable NTA solution.

About SecBI

SecBI is a disruptive player in automated cyber threat detection and network traffic analysis. The company's Autonomous Investigation™ technology uses unsupervised machine learning to uncover the full scope of cyberattacks, including all affected entities and malicious activities. SecBI detects advanced threats that other systems miss, creates a comprehensive incident storyline, and enables rapid and accurate mitigation. SecBI's technology is currently used by financial institutions, telecoms, retailers, and manufacturing enterprises worldwide.
For more information, please visit: www.secbi.com or write info@secbi.com

Appendix A: Packet network data vs. Log-based data in NTA

Packet	Packet metadata	Layer-7 gateway metadata
GET / HTTP/1.1 **Host**: example.com **Connection**: keep-alive **User-Agent**: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.59 Safari/537.36 **Upgrade-Insecure-Requests**: 1 **Accept**: text/html,application/xhtml+xml, application/xml; q=0.9,image/webp,image/apng,*/*;q=0.8 **Accept-Encoding**: gzip, deflate **Accept-Language**: en-US,en;q=0.9,he;q=0.8 **Cookie**: gsScrollPos-432=0 **HTTP/1.1 200 OK** **Content-Encoding**: gzip **Accept-Ranges**: bytes **Cache-Control**: max-age=604800 **Content-Type**: text/html **Date**: Mon, 27 Nov 2017 15:04:04 GMT **Etag**: "359670651+gzip"/ **Expires**: Mon, 04 Dec 2017 15:04:04 GMT **Last-Modified**: Fri, 09 Aug 2013 23:54:35 GMT **Server**: ECS (lga/131A) **Vary**: Accept-Encoding **X-Cache**: HIT **Content-Length**: 606 <Payload>	**GET**	cs-method
	Host	Cs-host, cs-url, cs(Referer)
	User-Agent	cs(User-Agent)
	Upgrade-Insecure-Requests	cs(Vary)
	Accept-Encoding	cs(Accept-Encoding)
	Accept-Language	cs(Accep-tLanguage)
	Cookie	cs(Cookie)
	HTTP/1.1 200 OK	sc-status
	Content-Encoding	sc(Content-Encoding)
	Cache-Control	rs(Cache-Control)
	Date	Date, time, time-taken
	Etag	cs(Etag)
	Server	rs(Server)
	Vary	rs(Vary)
	X-Cache	x-cache-info
	Content-Length	rs(Content-Length)
	<Payload>	*Not Available*

For more information visit: http://www.secbi.com/ or write info@secbi.com