ACCEDIAN

Guide

Next-Gen Intrusion Detection

Complementing perimeter protection to secure the virtual attack surface

Table of Contents

1. The Need for Next-Gen Network Intrusion Detection Systems

1.1 Protecting the network perimeter

The last 30 years have seen some amazing network computing advances. Computing power is now a commodity and networks span the globe. Mobile smartphones let users do nearly all the things they could only do on PCs and they can now access the Internet from their wristwatch. Soon, a wide range of new innovative Internet of Things (IoT) devices will make universal Internet access and digital connectivity ubiquitous.

Despite all these advances, information security is still a serious problem and could limit or slow future digital expansion. Exponential connectivity growth has led to equally exponential growth in security vulnerabilities. The move to the cloud, for increased IT elasticity and scale, has exacerbated these vulnerabilities due to a lack of cloud server and network visibility. The current virtual technology evolution from virtual machines to less secure containers and microservices has created even more chance for attack.

Throughout these technological advances, information security technology, of course, hasn't stood still. It has improved significantly, especially over the past decade, but the improvements have not been substantive enough to avert the increasing pace of IT security breaches, malware, IoT attacks, and so on.

Many of these security improvements have come in the form of perimeter security enhancements, which includes firewalls, border routers, screen subnets, and endpoint technology. Perimeter security provides a secured boundary barrier between internal IT networks, i.e. intranets, and public networks, such as the Internet. The goal of perimeter technology is to prevent malicious intruders from gaining access to intranets, and innovations, such as smart firewalls, have improved network perimeter protection.

With the advances in information security technology, Intrusion Detection System (IDS) technologies have also emerged. IDS solutions detect vulnerability exploits against a target network, computer, or application. Current generation IDS solutions use technologies such as network TAPs or SPAN ports to analyze a copy of the network traffic stream on a separate subnet to conduct threat analysis.

These technologies ensure that the IDS solution doesn't impact production network performance by sending security data over a production network. But, current generation legacy IDS solutions are limited by the large amount of data they need to analyze and their lack of viability in public infrastructure, such as the cloud.

However, security vulnerabilities persist. Malicious cyber criminals have become equally innovative, devising new security breach methods such as malware, ransomware, and phishing schemes to obtain access to the intranets they can't breach by other means.

These tactics enable intruders to obtain authorization using valid credentials through phishing emails and then using that access to hold data and systems hostage through ransomware. They also frequently install malware software that can impede access or damage IT assets.

Another risk is that with the rapid technology changes, IT teams are under constant pressure to update or install software or add new infrastructure. With these frequent updates and changes, it is easy to forget about backdoor access points into the networks that can create serious unknown security vulnerabilities. Cyber criminals use any and all methods to find and exploit any opportunity to steal information and assets, and to create mayhem.

Any and all exposed points in the network, from the edge to the core cloud or data center, define the virtual attack surface for today's enterprise IT environment. Any vulnerability within an enterprise network mesh can be exploited by cyber criminals. The attack surface is defined as virtual because of the vast use of virtual and container processes in the cloud, as well as in the data center.

2. Securing the Virtual Attack Surface

2.1 Why perimeter protection alone isn't enough

Securing the virtual attack surface requires a multi-faceted approach to achieve the strongest security protection possible. As previously stated, firewalls and endpoint protection are effective at providing access control for networks and systems, but don't provide any insight into what occurs once a cybercriminal is inside the network.

Passwords, tokens, Kerberos, and other access controls provide casual to strong breach protection, dependent upon implementation, but they aren't immutable, and they don't protect against phishing schemes and unprotected backdoor access points.

In-depth security protection requires a new level of active intrusion and behavior monitoring. There is a crucial need to detect, alert, and then enable methods to protect against Tactics, Techniques, and Procedures (TTPs) that are used once an intruder is inside the reach and visibility of the perimeter protection. But, the current generations of legacy intrusion detection solutions are complex, resource intensive, and still leave visibility gaps.

2.2 Legacy Intrusion Detection Systems defined

Legacy IDS technology is typically comprised of a device or software application that monitors for malicious activity or policy violations on a network. Any malicious activity or violation is reported either to a SecOps administrator or is collected centrally by a Security Information and Event Management (SIEM) system. SIEM solutions combine inputs from multiple security sources to generate alarms for malicious activity.

A current generation IDS workflow consists of:

1. Gathering network metadata and log information
2. Centralizing that information in a SIEM solution
3. Receiving an alert from the SIEM
4. Gathering evidence about the alert
5. Logically connecting the events that lead to the alert
6. Responding to the attack

Each of these steps, using legacy technologies, is fraught with limitations. These limitations are illustrated in the diagram below.

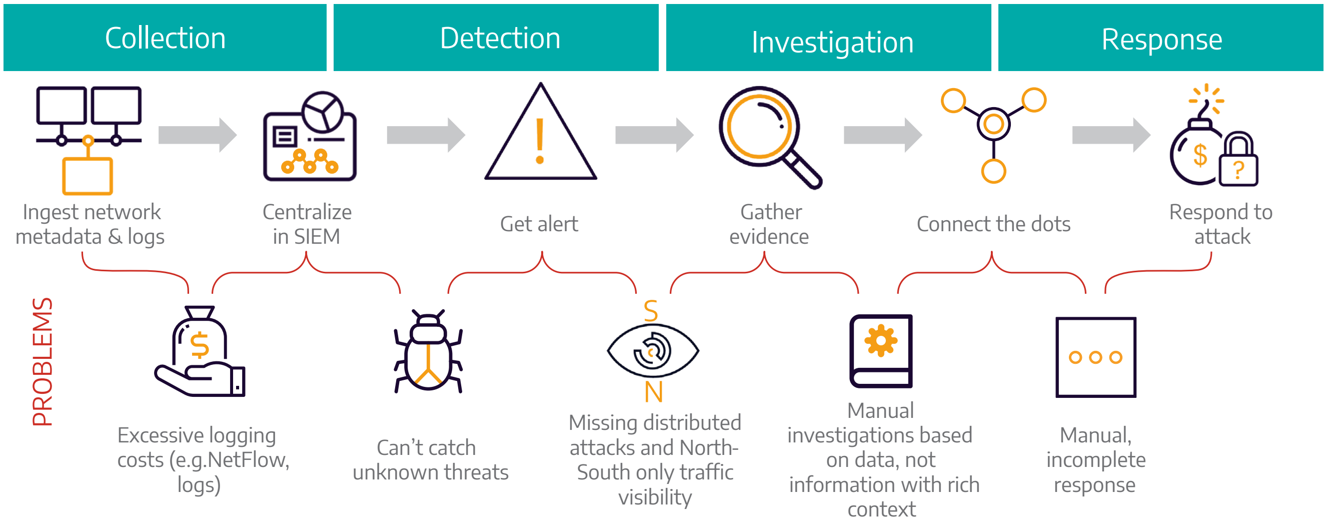

Collection
Detection
Investigation
Response
Ingest network metadata & logs
Centralize in SIEM
Get alert
Gather evidence
Connect the dots
Respond to attack
PROBLEMS
Excessive logging costs (e.g.NetFlow, logs)
Can't catch unknown threats
S
N
Missing distributed attacks and North-South only traffic visibility
Manual investigations based on data, not information with rich context
Manual, incomplete response

Figure 1: Limitations in current generation IDS systems outlined

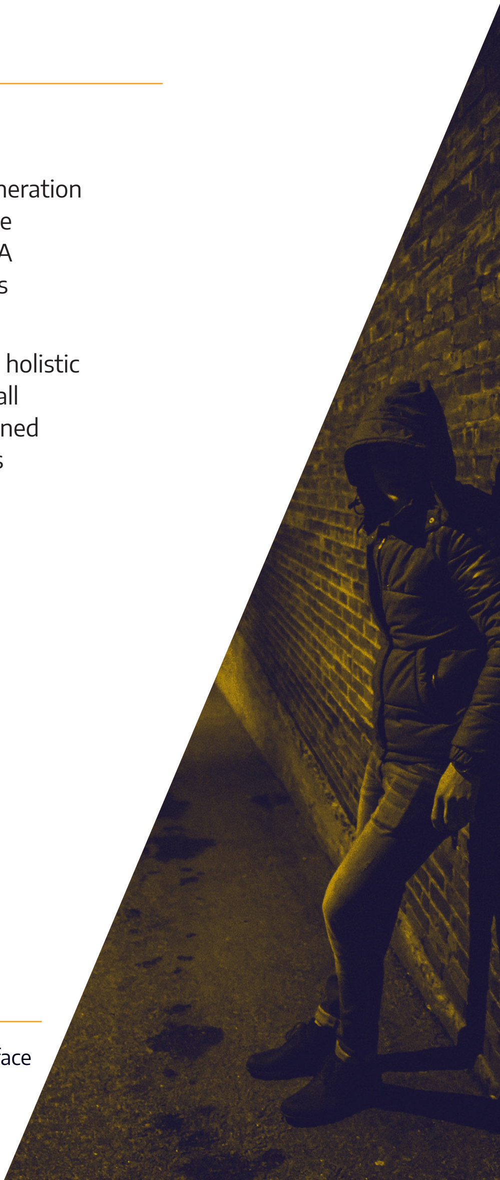
As shown on the previous page, there are many issues with legacy IDS workflows, including the excessive costs of legacy IDS data capture methods. This is further compounded by the significant manual efforts required to evaluate the large data volume captured. Also, despite all of this data legacy IDS technologies don't provide the complete data set needed to identify all of the potential threats, which leaves numerous, exploitable gaps in coverage.

What's needed is a new approach to network intrusion detection that is highly integrated and automated, is able to examine both illicit threats and behaviors, and is designed from the ground up to provide complete coverage for cloud, data center, and the network edge. To make next-gen IDS solutions viable for the cloud and network edge, they need to be easy to install, deploy and scale in a highly elastic infrastructure. They also need to be cost-effective so as to not overwhelm these environments with high volume and expensive raw data transfers.

3. What Constitutes a Next-Gen IDS?

Next generation IDS solutions will be designed to address the limitations of the current generation IDS implementations. They use less 'raw data' and manual investigation and instead feature intelligent data and machine learning to implement full Network Traffic Analysis (NTA). NTA facilitates comprehensive coverage and visibility into any untoward activities and behaviors occurring within the network.

NTA-based IDS solutions will complement network perimeter protection to provide a more holistic approach to network security that each approach alone can't completely provide. The overall goal is to provide strong access controls in order to prevent unauthorized access. It's combined with active, 24x7 activity monitoring using network traffic anaytics to detect illicit activities and behaviors from an intruder that found a way through the perimeter defenses.



4. Elements of a Next-Gen Network IDS

4.1 Data

When it comes to increasing IT security protection, it's all about the data. Next-gen IDS solutions require complete and precise data, not partial, sampled data. The single source of truth for any IT environment is network traffic. Any access occurs through the network or any malicious behavior takes place over the network, and it can be found or shown in the traffic and data.

This means that to provide strong threat and illicit behavior detection all network traffic and 100% of the transactions traversing the network must be analyzed to provide complete visibility. Within that scope, all of the pertinent network layers, from Layer 2 to 7 must be examined to achieve that goal.

The key data capture capabilities of a next-gen IDS include:

- Rule-less data capture
- Ability to capture 100% of the transactions
- Ability to handle 10+ GB network links
- Capture from network levels Layer 2-7
- Lightweight deployment and a focus on ease-of-use once deployed
- No Quality of Service (QoS) impact when deployed
- Economically viable and operationally feasible

The above IDS capabilities lead to the requirement for network traffic analysis that can acquire critical information from full traffic packets but store and transfer this information in the form of intelligent metadata. The use of metadata make traffic capture and retention much more lightweight and does not impact infrastructure performance or cost.

Full network traffic capture is not economical or manageable for a large, geographically dispersed network or organization, and it is especially unsuited for cloud environments. Partial capture of selected full traffic does not provide full visibility of all transactions and network activities. Network traffic analysis that represents the full packet information as highly condensed metadata does provide transaction and network activity visibility in order to satisfy the requirement.

4.2 Platform

The manner in which a next-gen IDS is deployed is also important. The platform needs to be viable for all IT environments; cloud, on-premises data centers, and hybrid, as well as IaaS, PaaS, and SaaS implementations. A SaaS next-gen IDS delivery model supports all of those environments and provides the elasticity and cost benefits that cloud-based environments offer.

An open architecture that allows for third party data integration, as well as for third party applications to be able to access data gathered by the IDS, is also a key next-gen IDS capability. Many enterprises may prefer to continue using tools that they already use and the ability to integrate with and complement those tools enables those enterprises to have all the capabilities that meet their needs.

The key platform requirements for a next-gen IDS include:

- SaaS delivered
- Open for integrations
- Enforcement with 3rd party APIs and orchestrators
- Integration of 3rd party threat intel
- Integrated active directory for enriched incident context

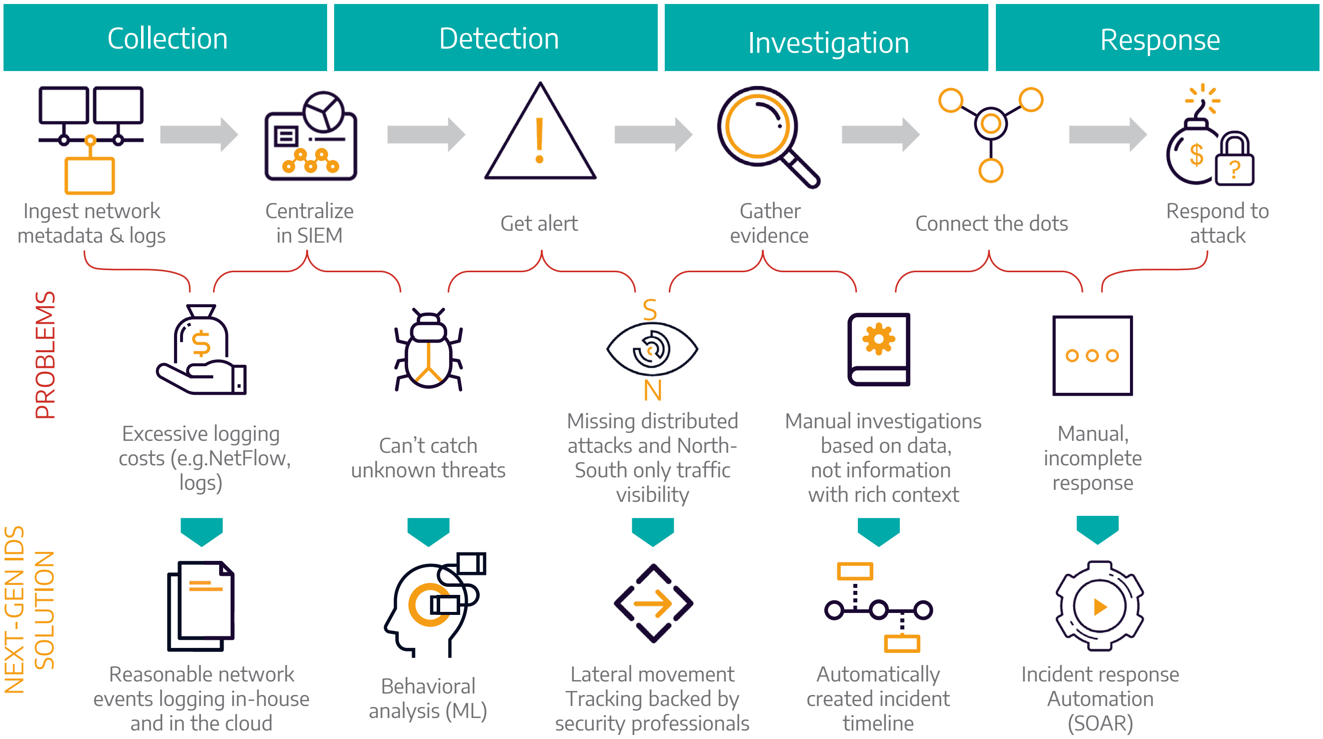

Collection
Detection
Investigation
Response
Ingest network metadata & logs
Centralize in SIEM
Get alert
Gather evidence
Connect the dots
Respond to attack
PROBLEMS
Excessive logging costs (e.g.NetFlow, logs)
Can't catch unknown threats
S
N
Missing distributed attacks and North-South only traffic visibility
Manual investigations based on data, not information with rich context
Manual, incomplete response
NEXT-GEN IDS SOLUTION
Reasonable network events logging in-house and in the cloud
Behavioral analysis (ML)
Lateral movement Tracking backed by security professionals
Automatically created incident timeline
Incident response Automation (SOAR)

Figure 2: Next-generation Intrusion Detection Systems alleviate the challenges associated with legacy IDS solutions

The next-gen IDS capability that ties the data and platform together is advanced analytics using machine learning to provide statistical, signature, and anomaly threat and behavior detection. These analytics will support threat and behavior detection, investigation and hunting, and produce alerts and alert management to provide guidance for what has been detected and where to investigate further. This will enable expedient drill-down and accelerated time to identify any issues.
It will also combine real-time data together with historical data to support advanced forensics.

The key analytics capabilities of a next-gen IDS solution include:

- Use of statistical, signature and anomaly detections
- Detection, investigation, hunting, and alert management
- Early cyber kill chain warning signals for threats, Indicators of Compromise (IoCs), attacks, etc.
- High fidelity forensic source data

5. How Next-Gen IDS Solutions Will Protect the Network

5.1 Cloud

Cloud infrastructure, whether IaaS, PaaS or SaaS, is driving the requirement for new ways to monitor and provide threat and behavior detection. With cloud infrastructure, Ops teams still can see the traffic between the endpoint connections and the cloud access points, but they lose visibility between server tiers and external services provided by third parties.

This lack of visibility creates a serious security risk because if a cybercriminal is able to breach the perimeter protection, they can cause damage to the organization from within the perimeter and it would not be detected, potentially, until it was too late to be stopped.

A next-gen IDS solution will provide the critical capabilities necessary to protect cloud infrastructure. It provides complete visibility for all network connections – North-South (endpoint to cloud) and East-West (server to server). From that thorough visibility, it will detect threat signatures, anomalies, and behaviors in the cloud. It will also need to be cloud-native and designed specifically for cloud environments. Re-hosted, security hardware appliance implementations are too expensive and resource-intensive for cloud infrastructures.

5.2 On-premises data centers

A next-gen IDS solution will provide the same complete threat visibility for on-premises data centers as it does for cloud infrastructure. However, it will be much more economical than current generation full packet capture IDS solutions. Next-gen IDS will use metadata to reduce the amount of bulk and unnecessary historical data that needs to be retained for both detection and forensic investigation.

Next-gen IDS technology:

1. Reduces the amount of data that needs to be retained to provide full threat visibility
2. Reduces the amount and cost of storage required to retain the required information
3. Enables the capability to retain the data longer for forensic purposes

Intelligent metadata, combined with machine learning, makes it much easier to detect and evaluate threats. This is because it delivers much more precision and is much less labor-intensive than the manual steps required to parse through vast amounts of legacy IDS data and logs.

5.3 The network edge

The network edge provides the greatest challenge for IDS solutions. That's because it will be impossible to provide robust perimeter protection for many of the low capability and capacity devices that may be connected for IoT and IIoT, in particular. These devices may provide some perfunctory access protection, but most likely won't have enough capabilities to provide robust perimeter protection. This will leave threat vulnerabilities that could possibly be exploited by cyber criminals.

A next-gen IDS solution will support a range of monitoring capabilities for edge devices that are both economical and precise. These capabilities will also be integrated into the cloud and data center IDS instances to ensure they can provide complete threat surface visibility from the edge to the network core.

5.4 Open API and 3rd party tool integration

The last, critical next-gen IDS requirement is the ability to seamlessly integrate into an existing security infrastructure. This means it will be able to integrate data from existing tools. It will also allow sensor data from the next-gen IDS to be integrated into other tools using their APIs and integration points.

Next-gen IDS technology and network traffic analysis will provide threat and illicit behavior detection intended to supplement perimeter security measures, not replace them. Both are needed to provide strong holistic network mesh security. To accomplish that, it's critical that those systems work together effectively, just like it is for law enforcement agencies to work together and share information to solve a crime.

6. Summary

The scourge of IT security breaches hasn't been eliminated. In fact, they've only increased as every enterprise becomes fully digitized and as the deployment of public infrastructure such as the cloud and the network edge progresses.

Network perimeter protection has increased in sophistication to make it more difficult to breach the perimeter, but cyber criminals have also become more sophisticated in the methods they use to break into networks and then cover their tracks to mask their activities. This is why IT perimeter solutions alone are not enough.

Intrusion detection systems have existed for a while and have been used in on-premises data centers, but they haven't kept up with and adapted to be effective in public cloud infrastructure. Next-gen IDS technology that will use network traffic analysis will be purpose-built for public cloud infrastructure and the visibility problems and complexities these environments create.

Next-gen IDS solutions will also protect against threats and behaviors that occur once a cybercriminal is able to breach the perimeter. This will reduce the potential for far reaching damages, and use high performance machine learning to accurately identify threats rapidly. Combined with perimeter security, next-gen IDS technology will add another layer of protection to the enterprise SecOps arsenal to not only protect against illicit network intrusions and behaviors, but to implement active measures to catch cybercriminals in the act.

Next-Gen IDS comparison table

	Next-gen IDS	Legacy IDS	Smart firewalls
Cloud			
East-West traffic visibility	+	-	-
North-South traffic visibility	+	+	+
Data center			
East-West traffic	+	+	+
North-South traffic	+	+	+
Signature and pattern detection	+	+	+
Real time anomalous behaviors detection	+	-	-
L7 full stack protocol coverage	+	-	-

+ = Advantage & available
- = Not an advantage

Accedian is the leader in performance analytics, cybersecurity threat detection and end user experience solutions, dedicated to providing our customers with the ability to assure and secure their digital infrastructure, while helping them to unlock the full productivity of their users.

We are committed to empowering our customers with the ability to see far and wide across their IT and network infrastructure and a microscopic ability to dive deep and understand the experience and security of every user, helping them to delight and protect their own customers each and every time.

Accedian has been delivering solutions to high profile customers globally for over 15 years.

Learn more at accedian.com

2351 Blvd. Alfred Nobel, N-410
Saint-Laurent, QC H4S 2A9
1 866-685-8181
accedian.com