WHITEPAPER

Is NDR the right security tool for you?

Plixer

Introduction

In a digital world, your network is everything. When running SecOps for your organization, you're expected to keep a reliable and secure network that enables day-to-day function and supports business growth. If your network is not safe or dependable, it can seriously compromise your ability to do business—and your job. Too often, though, companies will delay investing and implementing the right tools to protect their network.

No longer can we purely hope to avoid a cyberattack. Threat actors are finding ways to monetize every type of data and, in turn, have become industry agnostic. Hackers will attempt to infiltrate your network, whether you're at an international bank or a department store. While most people know that hackers look for financial data, they also can steal Personal Identifiable Information (PII), proprietary information, and trade secrets. If there is a potential market for the data or you're willing to pay to get the data back, hackers will try to find it.

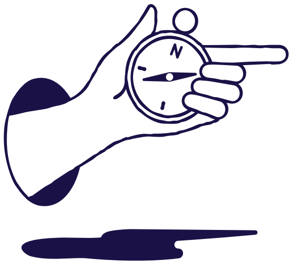
Additionally, the cost of a data breach has gone up. Verizon's Data Breach Investigations Report revealed that the average financial **impact of a ransomware attack was $1.2 million**. And a 2021 report from IBM and the Ponemon Institute found that the global **average cost of a data breach is $4.24 million**, up 10% from 2020. The longer it takes to recognize a breach, the more costly it becomes. Breaches that took longer than 200 days to be identified and contained cost about $1.2 million more.

Reducing dwell time—the length of time between a compromise on your network and its discovery—is essential to keeping your network secure. The goal of any team responsible for network reliability and security should be to see a threat as soon as it arrives. Imagine a radar for your network: a tool scanning all network traffic and alerting you to any potential threats. A network radar is essentially what network detection and response (NDR) solutions provide. The best NDR solutions out there will give you pervasive network visibility and flag unusual behavior for investigation.

When notified of a potential threat in the network, you can act quickly to intercept and eliminate the threat. NDR solutions help you detect threats, reduce dwell time, and protect your network from a serious data breach. An NDR solution is an essential part of your security stack.

What is NDR and how does it work?

NDR is a cybersecurity solution that analyzes network traffic for suspicious behavior. Think back to our radar example. The radar scans the area (your network) and alerts you of any approaching danger (threats). How the traffic is monitored and analyzed varies between each tool on the market. In general, though, NDR solutions either analyze information from network flow data or packet capture.



Most NDR providers use packet capture infrastructure to track and analyze network security. Packet capture works by inserting probes or other collection agents that monitor traffic on your network. Once packet data is captured—referred to as the payload—that data is then analyzed to determine normal and abnormal behavior.

This method has its shortcomings, though, as it requires a lot of resources. Inserting probes and collections agents across your entire network is very often cost-prohibitive and requires an untenable amount of storage capacity. Because of these issues, most companies must limit the number of probes and collection agents to a few key areas on a network. Using a packet-based NDR solution then means that your radar has blind spots. So, despite the ambitious promise of complete visibility from NDR vendors that rely on packet capture data, the reality is that most of their customers are only able to fully monitor segments of their network data.

Another way NDR solutions analyze network security is by using network flow data. This type of NDR solution analyzes communication data traveling across the switches, routers, and all other devices on your network. Unlike packet-capture data, network flow data provides an affordable and resource-light way of seeing all network conversations, as it taps into your existing network infrastructure, and eliminates any blind spots because it can monitor north/south and east/west traffic without relying on packet capture infrastructure.

Regardless of how the network is monitored, NDR solutions use artificial intelligence (AI) and machine learning (ML) to collect and analyze data (from either packet capture or network flow data).

The AI/ML engines ingest the data and analyze all activity—i.e., who was talking to whom, when the conversations occurred, and how much data moved across the network.

However, when using an NDR solution that is packet-based, the AI/ML engines will be limited to the data collected where packet capture is present. For instance, when you have packet capture only at one ingress/egress point of your network, the AI/ML engines only ingest data captured from that area. The engine will not process the other areas of your network.

Unlike solutions that rely on packets, when an NDR processes network flow data, the AI/ML engine can ingest data from across the entire network. Because network flow data is pervasive, the AI/ML engines that ingest network flow data tend to be more prolific and sophisticated with their threat detection capabilities. Network flow data casts a wider net than when using packet capture and, as a result, is more accurate at determining normal versus suspicious behavior.

As mentioned, a primary difference between NDR solutions is how they analyze data. But this is not the only difference that matters. Another key differentiator between NDR products is how the tool responds to threats. Most NDR vendors have integration capabilities that help teams orchestrate threat response with existing security infrastructure—like a SIEM/SOAR or workflow manager. Knowing if the solution you're exploring integrates with your other tools is critical to getting the right NDR solution for your organization.

Additionally, some NDR solutions have native capabilities that help respond to threats. For instance, an NDR solution may be able to send commands to a firewall to drop suspicious traffic. Or the tool could help enforce a zero-trust model when new devices or cloud services attempt to enter the network.

While there are many other differences between each NDR solution, the best products share the following key features:

- Has pervasive network visibility
- Uses AI/ML to provide sophisticated alerts about suspicious behavior
- Integrates with other tools in your security stack and responds to threats with native capabilities

An NDR solution is not the only security solution you'll need, just like having a firewall or antimalware is no longer enough to prevent and detect potential threats. In an ever-evolving threat landscape, though, an NDR solution is critical to ensure your organization is not at the mercy of bad actors.

Is network flow data enough?

You may be wondering, is it enough to capture network flow data? Will I have all I need to understand the threat from network flow data alone? To answer this, let's use phone records as an analogy.

A phone record will give you data like who called whom, how long they talked for, how often they talked, and maybe a few other high-level pieces of information. To an untrained eye, this may not seem like important investigative data, but say Person A is talking to Person B in a series of conversations that are under a minute in length. That looks a little funky, as Person A does not often have a series of short calls like this. It could just be a connection problem. Or maybe Person A is trying to coordinate something with Person B. As you begin to investigate Person A, you see that they are having many short conversations with several numbers associated with burner phones. Suddenly, Person A looks highly suspect. Though richer in content, network flow data is akin to phone records in this example.

In some instances, though, you may want to dig even deeper. Suppose a data breach has occurred, and you could not catch it before the hacker stole data. You may want to know the exact data exfiltrated during the breach. Assuming the traffic was not encrypted or could be decrypted, this is where packet capture has great value. If you have packet capture in the breach area, you can see packet details beyond what the network flow data offers. In the case of our phone record analogy, using packet capture and examining the payload would be more like having the call record and a recording of the conversation. While this is helpful for a forensic case, it is more than you need to spot suspicious behavior. As shown above, you can detect suspicious behavior from just the call records alone. Moreover, the recording might be encrypted, preventing you from getting any details about the call. At this point, you're in the same place as if you only had a call record but have wasted money on a recording that you cannot listen to.

Because of the resource strains and the prevalence of encrypted traffic, packet-based solutions often compress packet capture data to something akin to network flow data. But that's a lot of effort and money to essentially end up with network flow data already available from your existing infrastructure. Security teams know the struggles to secure budget and justify spend. By using an NDR solution that uses network flow data, you're able to tap into infrastructure you've already invested in and do not have to worry about gaps in visibility.

How does an NDR solution use network flow data to determine a threat? To answer this, we need to look at how hackers behave. In most cases, they gain access to your network through a device—be it a laptop or a peripheral server. Once on the network, they start moving around, looking for valuable data. Take the call record example above; suspicious behavior—like a series of short phone calls or calls to burner phones—can be spotted by paying close attention to the data. Rather than hunting for indications of a hack, the best approach is to proactively search for the tactics, techniques, and procedures a bad actor must take.

Distinct patterns will emerge when an AI/ML engine ingests network flow data. When digested and analyzed, network flow data shows you when devices access servers they've never accessed before, when new devices come onto the network, when the data volume exceeds an expected range, or when data moves from critical infrastructure to a device. A hacker will invariably act unusual and leave a data trail that an NDR solution will flag as anomalous.

Like a call record, network flow data provides an NDR solution with enough data to detect threats. Packets can help dig deeper for a more forensic look, but it is not necessary for threat detection and investigation.

The ROI of NDR

Security teams are often in a tough spot. You must fully secure the organization's IT infrastructure with a precarious budget. When no incidents occur, you may get questions like: why pay for all these tools if we're safe? Or is the risk/cost-benefit *really* worth it? From this perspective, adding another tool to your security stack is a lot to ask.

Unfortunately, the threat landscape is at an all-time high. For ransomware attacks alone, the FBI found a yearly increase of 62% from 2020 to 2021. The goal has switched from preventing a hack to limiting the impact of a breach. Limiting the impact is incredibly important, as the cost of a breach is also increasing.

The 2021 IBM and Ponemon study mentioned earlier revealed that the **average cost per record was $161**. That's $161 per compromised piece of information. When you think about the amount of data on your network, even a relatively minor breach can cost you hundreds of thousands of dollars. That same study found that businesses that experienced **a breach lost about 38% of their overall value**. Customer turnover, lost revenue due to system downtime, and the increased cost of acquiring new business after the blow to their reputations contributed to the loss of business value.

An NDR solution is the right type of tool to include in your toolkit for a few reasons. NDR solutions that use network flow data provide pervasive visibility to **all the activity** on your network, which in turn gives you a source of truth for normal and abnormal behavior. A sophisticated AI/ML engine will help clear the noise from the critical anomalies worth investigating. An NDR provider that uses network flow data is also very cost-effective. As mentioned above, packet capture data is very resource-heavy and requires much more investment to capture segments of your network traffic. Unlike packet-based solutions, an NDR that processes network flow data can use existing infrastructure to provide a much more holistic analysis of suspicious activity.

The reality is that you need tools to keep your network and data safe. We're beyond the days of relying solely on antivirus and firewalls. Though these tools are still important, we now need a suite of tools to quickly detect, respond to, and remediate threats. But you don't have to empty the coffers to achieve a sophisticated security posture.

The Plixer NDR platform

The Plixer NDR platform consumes the network flow data already available from the network and security devices deployed throughout your network. Using network flow data as a raw data source, with advanced detection algorithms and machine learning, Plixer quickly identifies anomalous behavior. This process makes it easy to spot the bad actors before they can compromise your critical resources.

When running our NDR solution in concert with a SIEM/SOAR, you can be quickly alerted of suspicious behavior. Once alerted, our platform allows you to thoroughly investigate the activity and begin your response. We also integrate with ServiceNow to help automate workflows and streamline problem isolation and incident response. The Plixer NDR platform gives you all the information needed to contain the situation and stop the attacker in their tracks.

Enterprises looking to lower their exposure to—and costs from—breaches need a best-in-class NDR. The Plixer NDR platform is an innovative and intelligent NDR solution that helps identify suspicious behavior, reduces dwell time, and is cost-effective. We leverage the most powerful detection sensor available to you. A resource you've already invested in: Your network.

About Plixer

Plixer provides a single platform for network security and monitoring, delivering the insight and analytics needed to manage the immense opportunities and risks of a digital business. As a leader in the Network Detection and Response & the Network Performance Monitoring and Diagnostics markets, Plixer provides the comprehensive intelligence and visibility needed to analyze, evaluate, and visualize the millions of conversations that cross networks every second.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.