

Ne2ition

Advanced Network Detection and Response Helps You Detect & Respond To Critical Threats Faster and More Effectively



Helping detect critical threats to the environment

Threat actors continue to advance in their tactics, techniques and procedures (TTPs). One of the more sophisticated types of attacks is advanced persistent threats (APTs). They often target specific industries or even companies, taking interest in the long haul of data exfiltration.

Due to their level of expertise and abilities, they may be able to remain hidden in your network. The recent Verizon Data Breach Investigation Report (DBIR) shows that 81% of breaches took days or less to contain in 2022, which is an improvement over the months it took for 56% of the companies to detect a breach in 2021, according to the prior Verizon DBIR.

One of the biggest challenges with cybersecurity tools is that security teams become inundated with a multitude of alerts that hinders the visibility of the true threats. Tickets generated from the front-line are routed to the more seasoned operators who hold the deeper expertise and know-how to be able to look into a variety of different alerts. It is no surprise that a huge burden is placed on very few analysts, thus resulting in bottlenecks, burnout and a high turnover.

According to recent research, security teams receive up to 1,000 alerts daily and have to switch between 12 systems, on average, to address the alerts. This current model takes up no less than 20% of the analyst's day in non-value-added activities. Another significant percentage of time is used for redundant activities (redundant true positives - such a when a security tool is alerting on every packet (out of thousands) of a communication with a command and the control server is p alert generated - not to mention working on the false positives). This keeps the analyst from addressing the actual attacks that threaten the organization.

To make things worse, three out of four newly hired security team members will be replaced or will resign within just one year. The reason for the high turnover is a large amount of pressure, increasing workload caused by chasing too many alerts, tedious tasks of "gluing back" pieces of the puzzle, and an overall frustration of not being in a position to actually protect the organization.

Clearly, security teams today need a more efficient way to deal with alerts that is conducive to identifying the attack and effectively responding to it.

Visibility is a key factor

Complex networks are defined by elaborate topologies that make the inference of the connections between clients, applications and other network components difficult. Complexity promotes the degradation of network visibility. Without visibility, awareness of data flows and network activity disappear and malicious events and indicators go undetected and unmitigated. Threat detection and response is, after all, entirely dependent on access to visible, actionable data.

In addition, this complexity yields a larger attack surface, more opportunities for misconfigurations and human error, and an environment tailor-made for APTs. IBM research has discovered that a breach persists, on average, for 209 days before detection and requires an additional 76 days for containment. This finding emphasizes the consequences of complexity without visibility.

Visibility is essential, but you will need actionable data and a system that is doing the heavy lifting of the analysis automatically so you can focus on the most important aspect – decision-making.

In order to achieve true visibility, network tools must provide an analysis of the payload packets. If only metadata is decoded, then application layer visibility will not be available. If you are seeking HTTP protocol fields, SMB file information (including the file itself), DB transactions, URL and DNS data, or TLS certificate data, then high-level flow data collection like NetFlow will be insufficient. Metadata pertains to information about the network traffic and not the packet payloads themselves, so it is similar to getting mail only to find out you have the person's name and address but the entire mail itself is not included.

Application layer visibility and access to transmitted content become possible when network packets are reassembled into sessions. Full packet capture can be expensive and hard to work with. It is no surprise that Gartner reported that rich metadata that looks at network payloads is the new way to go, as full packet capture is not able to provide long enough history and is typically limited to only a few days. More and more organizations today are adopting network detection and response technologies, as the immense value of network data – with its ability to reveal a clear picture of systems communication – can no longer be ignored. It can be expected that the value of network data will only increase as methods of easily exploring the data, without needing to write complicated regular expressions, become the norm.

One of the biggest problems when monitoring alerts is not only the false positives, but also a high volume of duplicate true positives. Alerting is great when it directs you to an actual issue. However, knowing what is truly malicious behavior takes a deep knowledge of the environment, the ability to set a baseline of normal activities and the capabilities to dig deeper to discern the actual nature of the threat. Perimeter defenses are necessary but will not protect against a user clicking on a malicious email or an insider sending data out through steganography. Moreover, they don't tell you what is going on inside; as an example, east-west traversing continues to be a blind spot in many enterprises.

To truly understand your network, you need a real-time examination of packets; this is performed through the evolution of network traffic analysis (NTA) into actual network detection and response (NDR). As corporate environments expand beyond their traditional infrastructures to more virtualized and cloud environments, many blind spots are created.

The benefits of NDR (Network Detection and Response)

The primary function of NDR is to use real-time network traffic analysis to detect and investigate threats targeting your network and WireX Systems main focus is in its ability to empower your operators with forensic investigation capabilities and enable automatic collection, correlation analytics and visualization literally in seconds. Enabling these capabilities are powerful machine learning and analytics engines that leverage recent incident information to predict and prevent future attack patterns.

NDR provides an integrated, set of capabilities that greatly enhances detection, investigation, forensics and threat response capabilities for operators protecting the network. Network detection components gather data across environments and apply machine learning and AI algorithms to identify threats that have never even previously occurred. The investigation capability provides operators with near real-time insights and contextualized information that speed up and improve the results of forensics analyses. Furthermore, response capabilities automate the application of robust security workflows that prevent system breaches and mitigate damages before they occur.

A robust NDR takes the data from NTA and generates actionable data. The actionable data provides guidance for the next steps after a threat is identified, allowing for less-senior staff to choose a proper response to the incident.

To fully monitor the environment, NDR sees all communications taking place within the network and cloud infrastructures. NDR takes many steps to determine what is normal behavior for your network in relation to your applications and users as well as what is anomalous. It builds a profile of normal network behavior by examining raw data packets and alerts when abnormal activities are detected.

Data exfiltration does not have to take place in large chunks of data to be considered anomalous behavior; a sophisticated anomaly detection will factor many other dimensions. If a device is sending out lots of data or smaller chunks of data over a period of time, NDR can detect the threat, increasing the chances of detecting slow-moving threats. Regardless of what the threat is, NDR provides useful information about what is taking place.

What are the differences between the NDR and IDS systems?

NDR and IDS systems both monitor network traffic to detect malicious activities and provide immediate analytics to mitigate these threats. So what are the key differences? From a birds-eye view, the limitations inherent in IDS systems best define the differences between them and NDR.

Let's start with the most critical: IDS systems are heavily reliant on maintaining a database of common signatures and anomalies tied to attack patterns. While vendors do their best to keep these databases up to date with the latest threats, they often fail to keep up with the rapidly evolving pace of innovation and creativity from malicious actors.

In contrast, NDR systems use a robust suite of machine learning features and AI to create predictive behavior profiles capable of identifying and mitigating day-zero security threats that signature-based systems will likely miss (until they see the specific attack over and over again).

Another key differentiator between NDR and IDS is in investigation and forensics capability. IDS systems are primarily limited to malware and well-understood attack signatures.

NDR systems like WireX can leverage investigation and forensics features to protect against insider threats, prevent the abuse of credentials and permissions, and fully identify the scope of data exfiltration and breaches.

For a more specific example of the differences, IDS systems commonly rely on something akin to NetFlow to recognize patterns of behavior across the network. NetFlow inspects packets to provide metadata to determine information such as the source/destination IP addresses and source/destination ports. IDS systems compare this information to common attack patterns in the signature database to identify suspicious activity occurring at that moment.

When an IDS performs this comparison, it makes what is called a "point in time decision." If a threat pattern is detected, the specific session will be flagged, and in some cases, the network flow may be recorded. If the traffic appears legitimate, the IDS will not flag the session or record any information about the data transmitted. From a forensics perspective, this has a significant impact in scenarios where it is later determined that a system was compromised. The traffic data is lost to the follow-up investigation and forensics process unless the attack was detected in the first place.

In contrast, NDR applies a far more holistic and long-term approach to monitoring the same traffic. In addition to the metadata, NDR systems inspect the packet payload information, dissect protocols and provide insight into internal data exchanges between network-enabled applications. NDR systems are capable of storing this information for extended periods. The application of machine learning to this data allows NDR systems to determine the "patient zero" of infected systems well after an attack has taken place.

Automation as a first step in the right direction

SOAR (security orchestration, automation and response) provides predefined playbooks that run when an alert is generated. The purpose of these playbooks is to gain effectiveness and consistency, as much as to automate activities as appropriate. So, in general, it is a good starting point, BUT this still requires organizations to have the actual information to turn alerts into identified attacks. For the alerts that the playbook confirms as being problematic – we would still need to execute the investigation that identifies the threat. So, the value of the SOAR is that it can help focus on the more important alerts and it will support the automation of repetitive activities, but it doesn't replace the need for a deeper investigation – and this is where WireX comes into play.

Also, SOAR is still far from being broadly adopted by most security teams, which makes the problem even worse. The value of predefined playbooks is limited if the organization doesn't have the visibility to truly identify attacks (not alerts) and respond to them.

NDR complements EDR and SIEM

The old way of focusing resources on stopping an attack at the gate or being reactive in nature is not enough. More firewalls or intrusion detection systems (IDS) are simply not providing the answers for the more sophisticated threats. Reviewing aggregated logs from a security and event management (SIEM) device requires more man-hours than most companies have and is still insufficient as log data is not enough when needing to perform deep investigation or hunting activities. Other solutions, such as endpoint detection and response (EDR), provide rule-based automated responses and analyses based on what happens in the endpoint itself. As a result, subtle attacks cannot be detected, such as lateral movement. The attacker will tend to operate in “almost” stealth mode until they are ready to launch their attack. To successfully counter it, the security team must perform many actions such as scanning active directory log files, using EDR, enforcing least privilege, collecting logs and configuring alarms. No single piece can detect the attack on its own, which is what makes detection and identification an operational nightmare.

True NDR sees the complete picture by using traffic analysis to understand user/data interactions and taking it a step further. NDR also builds the baseline of “normal” behavior, can alert when abnormal behavior is seen and can even be specific on what such behavior is indeed malicious.

By visualizing the “tree”, all user/data interactions, and enabling to focus on the suspicious ones, the “leaves”, the operator can move instantly from receiving an alert that lacks context to understanding the full scope of the incident.

WireX Systems transforms novice operators into valuable analysts

Traditional security investigation tools overburden your enterprise security teams who are likely already resource-constrained and scrambling to contain a data breach. These methods force your highly experienced team members to spend their time manually examining days of network packets and sessions totaling hundreds of terabytes.

When the team completes their work, they have little visibility into the transactions of the impacted applications. Related sessions are uncorrelated. User actions that could provide the team and machine learning algorithms the information needed to diagnose and prevent a future attack remain buried in mountains of application logs soon to be pruned by retention policies.

With WireX's Contextual Capture™, analysis engines continuously identify impacted applications and reconstruct and correlate related sessions. They extract and store

application content for long-term use independent of application-layer logging configurations. This information takes on the user-action classification, which provides operators a view into the precise actions a user performed in an exposed system in a clean, simple user interface. A fast and intuitive search feature allows even inexperienced operators to easily analyze user activities across multiple applications.

WireX Systems takes this approach of orchestration and automation a few steps further and delivers simplified and actionable context into these alerts to reduce the workload placed on the responding team members. Currently, most of an analyst's time is spent on reviewing logs and alerts that can turn out to be false positives (or simply redundant true positives), which takes their focus off the actual attacks that impose a risk to the organization.

To fully monitor and understand the environment, WireX Systems leverages network detection and response (NDR) to see all communications taking place within the network. We also utilize our Contextual Capture™ technology to reconstruct the raw data into a human-readable format that the security personnel can act upon.

It is worth mentioning that NDR not only monitors all traffic across the network, but it also has the ability to decrypt the data for packet inspection and re-encrypt the data in a transparent manner. Even in cases where decryption is not enabled, it will point to the servers being used, the certificates, who signed them and their validity in order to provide the bigger picture.

According to Dark Reading, it takes new security team members about a year to become active contributors, and, on average, the security staff leaves after just two years. With WireX Systems, a security manager can train new employees and turn them into effective analysts in a manner of weeks. WireX Systems also provides an Incident Management that is also used as a knowledge sharing framework to guide teams when performing incident response, whether they have a SOAR tool in place or not. Teams can then automate various steps of the detection, identification or response process for further efficiencies and output. This enables even entry-level operators to become as effective as the tier three analysts while also enabling the experienced analysts to focus only on the most pressing threats and providing them with all the relevant insights automatically. With the ability to understand the context around a specific alert, security teams require less expertise, fewer senior analysts and less time to effectively respond to threats.