WHITE PAPER

Why Security Teams are Replacing IDS with Network Detection and Response (NDR)

VECTRA®

TABLE OF CONTENTS

Introduction

With the increasing complexity of the network and the growing sophistication of attacks, organizations are reassessing their security strategy. It is becoming more difficult to distinguish attacker behavior and prevent serious breaches, data theft, and ransomware using standard network security tools. Intrusion detection systems (IDS), intrusion prevention systems (IPS), and the convergence of the two, known as intrusion detection and prevention system (IDPS), have been considered vital in uncovering and preventing unwanted and/or malicious activities in the network. Still, many breaches are unabated, highlighting how organizations need to address the protection of internal assets better and improve their ability to detect atypical threats born in the network and stop nefarious lateral movement.

IDPS offers in-line protection that enables security professionals to identify and block potential threats, intrusions and attacks on an organization's networks, applications or systems, automatically. IDPS uses various techniques to detect and block known attacks with high confidence, significantly assisting IT operations teams where patching cannot be executed in the same time scale as threat actors are operating.

But today, even when combined with other tools like XDR, EDR, SIEM, and firewalls — organizations using IDS can't easily discern unknown active threats and stop sophisticated attacks already inside.

In this white paper, you'll discover:

- The unique challenges of detecting today's advanced threats.
- Why the emergence of NDR is redefining IDPS.
- How NDR empowers security teams to detect and respond to threats across cloud, SaaS, identity and network.

The evolution of IDS

Historical usage

- The protection of confidential assets from internal users as external threats weren't a concern.
- Build rules to reveal suspicious behavior to identify deviations from normal baselines.

Today's usage

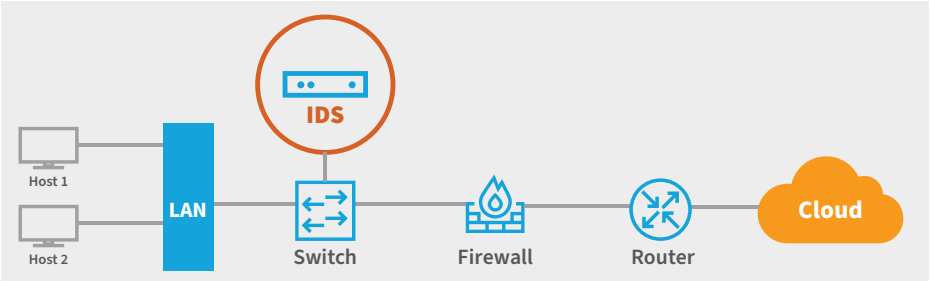
- Deployed on the host or network for single-host monitoring or monitoring of the entire network.
- Signature and anomaly-based detection models both require skilled analysts to interpret large volumes of data.

The shift from IDS to IPS

- As more outside threats emerged, focus shifted to detecting external threats.
- IDS changed direction to focus on perimeter detection and IPS was born.
- IPS overtakes IDS and its functionality, creating a new category known as IDPS.

Challenges of IDPS:

- Requires analyst expertise
- Data needs interpretation
- Adds to security alert noise
- Only relies on signatures and anomalies
- Lacks visibility across all surfaces



Modern threats require modern detection

Attackers today can easily evade and avoid perimeter and malware detection techniques. Detection avoidance may take on one of five characteristics, or a combination of all, including:

- Signature evasion
- Encrypted traffic
- Perimeter avoidance
- Internal movement
- Credential harvesting

Signature evasion

The most straightforward approach to evading signature-based IDPS is to use traffic that doesn't match known signatures. This can be trivial or highly complex. For example, signature detection is often based on "known" compromised IP addresses and URLs used by botnets and malware. For attackers, avoidance is as easy as registering a new domain.

At the other end of the spectrum, highly sophisticated attackers can find and exploit previously unknown vulnerabilities. Attacks on such "unknown" vulnerabilities naturally lack the type of signature that IDPS may be attempting to locate.

Encrypted traffic

Another way to avoid signatures is to obscure the traffic. This can be as simple as encrypting malicious network traffic. While SSL decryption at the perimeter is an option, it's costly by introducing performance penalties and has become complicated to operationalize.

Today's sophisticated attackers use customized encryption that cannot be decrypted, even under the best of circumstances. This leaves security teams to decide whether to block or allow unknown traffic at the perimeter.

Perimeter avoidance

Attackers have learned to avoid the perimeter, and its protections altogether. By infecting users' devices at home or outside the perimeter, threats can be carried in right through the front door.

Notably, mobile devices provide logical and physical paths around the perimeter. Mobile devices with LTE or 5G data connectivity have easy paths to the internet and act as an invisible conduit that attackers love to use to get inside networks.

Internal movement

Given the almost exclusive focus of IDPS is on the perimeter, once around the initial defenses, attackers can move much more freely. This involves an ongoing process of internal reconnaissance, lateral movement, and the access and theft of key assets. Each area employs a wide variety of attacker techniques, and they all take place inside the network where visibility is typically low.

Taking this one step further, with the onset of hybrid and multicloud deployments, network visibility gaps often extend to connections between compute and storage instances. Cyber attackers love to make use of this visibility gap.

Credential harvesting

Once inside the network, savvy attackers don't need exploits and malware to extend their incursion. Instead, they simply harvest user credentials from compromised hosts to spread through the network.

Typically, they capture a username and login during the authentication process or steal credentials or hashes from memory. In either case, attackers can spread throughout the network using valid credentials without having to use exploits or malware.

Network Detection and Response: Redefining IDPS

Today's threat landscape consists of an ever-expanding attack surface, more evasive attack methods with more tools that ultimately lead to more alert noise. In this environment, not only are prevention solutions not enough to stop attacks, but they can also add to the overwhelming number of alerts that security teams have to prioritize. Detecting and responding to hidden attacks that progress across cloud, SaaS, identity and network data must be a top priority. This is where NDR now plays a critical role.

The right NDR understands the way attackers think so security teams know what is malicious and urgent — empowering security teams with the full context of an attack. They are easy to deploy, manage and use without requiring a full-time expert to keep them operational. NDRs also implement a method of noise reduction and incident prioritization that enables a security analyst to focus on the threats that pose the biggest risk.

The importance of cloud and network visibility

Attacks can be classified as one of three types: targeted, insider or opportunistic. Knowing one from the other requires a full understanding and context of what the attacker is doing inside the network.

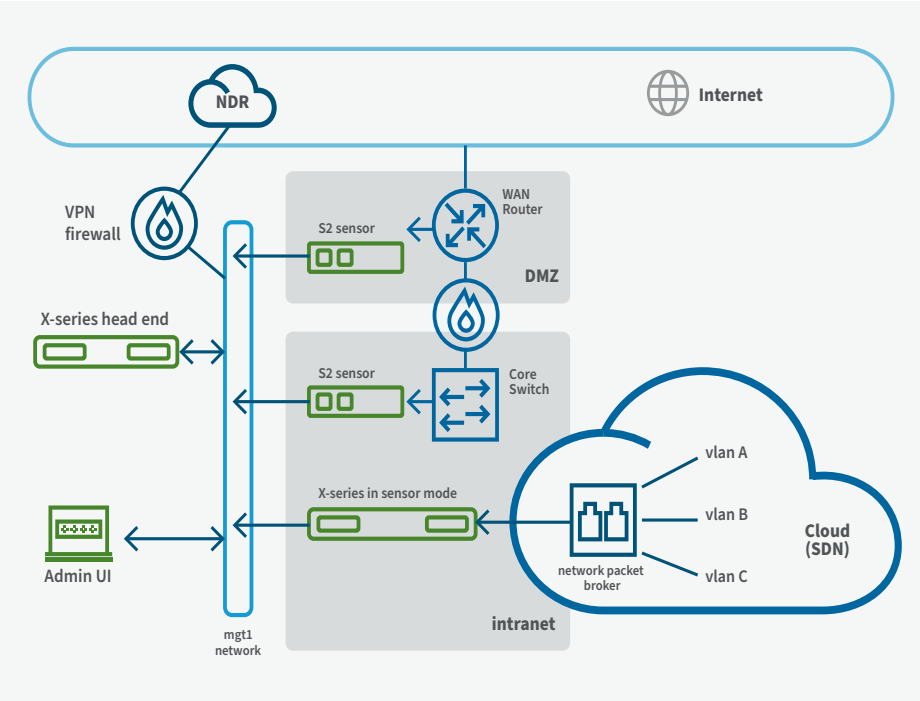
Without full traffic visibility, security teams are limited in their ability to see the entire attack lifecycle, which in turn limits the understanding and context of what is really happening.

Where IDPS solutions only monitor at ingress and egress points, NDRs can watch all user-to-user, user-to-server, server-to-server, and user-to-internet traffic. The goal is to monitor all traffic and behaviors across every asset in cloud, SaaS, identity and networks.

NDRs provide context and prioritize the behaviors they see, including options for responses relevant to specific threats.

Moving from payloads to behaviors

Best-in-class NDR solutions move beyond the realm of solely relying on signatures and simple anomalous behavior detection. This approach can be quite powerful. Although attackers can easily put on a new coat of paint to avoid signatures, they can ultimately be exposed by their malicious behaviors.



Attackers usually perform the same tell-tale actions and behaviors to carry out an attack. By learning to recognize the unique characteristics of these malicious behaviors, NDRs arm security teams to reliably identify network intrusions, even if the tools, malware or attack style are completely unknown.

Leveraging ML in your NDR to enhance signal clarity

Proactively detecting threats requires two types of high-level experiences. The first is a global set of experiences that understands how threats differ from normal or benign traffic. Second is a local set of experiences that reveals unusual or anomalous behaviors in a unique environment.

The first approach reveals behaviors that are always bad, and the second reveals threats based on local context. Both are essential to detecting threats, and they must work cooperatively.

- **Supervised machine learning** analyzes known malware, threats and attack techniques.
- **Unsupervised machine learning** recognizes what is normal for a particular environment and when behaviors deviate from that norm.

Both styles support detection algorithms based on information that is observed over extended periods of time. Instead of detecting in a few milliseconds based on a single packet or flow of data, models should learn and detect based on times ranging from seconds to weeks.

Signature-based detection isn't lost

While effective NDR solutions utilize AI to detect, triage and prioritize threats — this doesn't mean signature-based detection capabilities are obsolete. In fact, signature-based detection focuses on known exploits that still need to be stopped. When coupled with NDR, IDPS capabilities allow teams to ingest intrusion detection signature context for more efficient and effective threat investigations and hunting while remaining aligned with compliance regulations. When done this way, security teams have access to rich context of every incident for a more proficient investigation beyond just relying on standalone IDPS — together enabling analysts with AI-driven and signature-based detection capabilities.

This scenario enables teams with:

- Access to signature-based context for enhanced AI-driven detections.
- More attack coverage across the entire network when coupled with NDR.
- Consolidated security tooling with signature-based context in one NDR solution.

Fighting fire with fire: Vectra NDR's answer to modern threat detection

To address attacks prevalent across today's landscape, Vectra NDR leverages Security AI-driven Attack Signal Intelligence™ to automatically detect, triage and prioritize threats — arming teams to effectively investigate, hunt and respond to attacks across cloud and datacenter networks. Vectra NDR is capable of advanced detections for attacker obfuscations and activities such as:

- Encrypted traffic
- Command-and-control
- Internal reconnaissance
- Lateral movement
- Data acquisition and exfiltration

Encrypted traffic

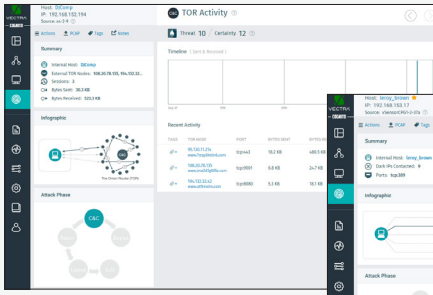
SSL/TLS and other types of encryption pose a challenge for most security products. However, by focusing on malicious actions instead of malicious payloads, Vectra NDR identifies active threats in encrypted traffic without decrypting it. Furthermore, by analyzing tiny fluctuations in protocols like HTTPS, HTTP and DNS, Vectra NDR can reveal when additional layers of communication are hidden within.

Command-and-control

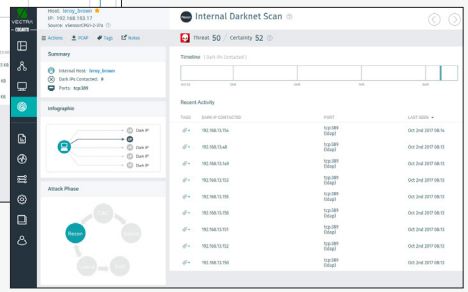
While command and-control signatures work well for large, well-known botnets, they are easily evaded by attackers who customize their command-and-control infrastructure for only one target organization.

Vectra NDR understands a wide range of command-and-control behaviors, such as:

- Attempts to imitate browser behavior
- Use of hidden tunnels
- Peer-to-peer communication
- Malware updating
- Broad varieties of anonymization techniques like TOR
- Use of external remote access tools



Command-and-control detection of TOR anonymization activity



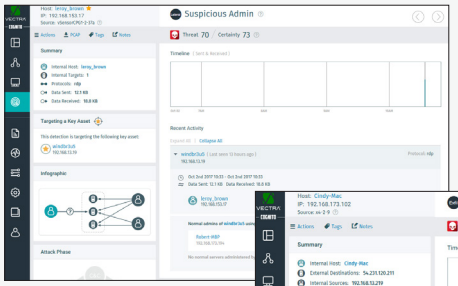
Reconnaissance detection of an internal darknet scan

Internal reconnaissance

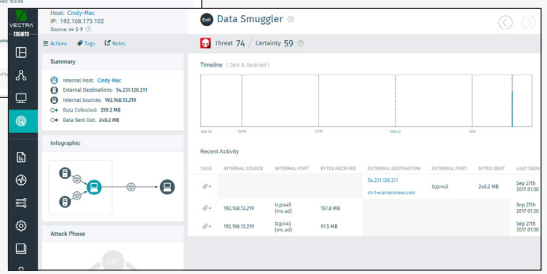
The initial victim machine usually doesn't contain the most valuable data in the network. As a result, attackers will learn the local network environment and identify other hosts and segments to exploit. Vectra NDR can pinpoint reconnaissance behaviors, even if attackers take a low-and-slow approach.

Lateral movement

The most crucial phase of a cyberattack involves lateral movement. The ability to move laterally inside the network provides attackers with places to maintain persistence and enables them to dive deeper as they progress toward key assets.



Lateral movement detection of suspicious admin activity



Exfiltration detection showing a data smuggler

Lateral movement typically takes on one of two forms, both of which Vectra can detect:

- **Spreading malware host to host**: By monitoring all standard internal traffic, Vectra NDR can detect an anomaly in the patterns of the host, thus preventing it from continuing to spread malicious payloads.
- **Stealing credentials from victims**: Vectra NDR constantly monitors the internal Kerberos infrastructure to identify signs of theft or credential re-use. This capability reveals very subtle attacks, even when no malware is involved.

Data acquisition and exfiltration

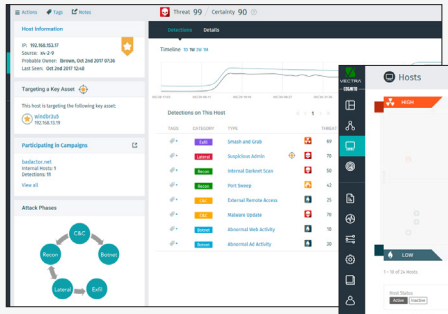
The final phase of an attack often involves the acquisition of data to send back to the remote attacker. Vectra NDR monitors the network for devices that are acquiring and sending data at an abnormal rate. Additionally, the exfiltration process requires attackers to stage data for aggregation. The data is typically moved to areas of the network where uploading draws less suspicion. Automatically and in real time, Vectra NDR connects the dots and recognizes when data is being staged and prepared for transfer.

NDR detects what others miss

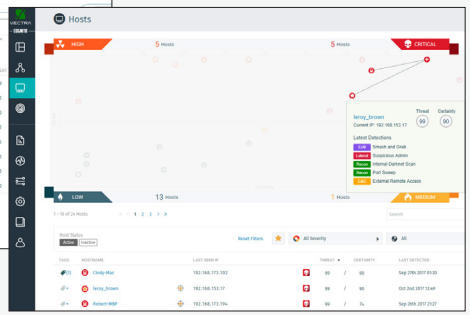
Traditional security solutions continue to lose their edge as modern cyberattackers gain momentum using more evasive and sophisticated methods to spread rapidly throughout the network. This leaves security teams without the means or visibility to identify threats that pose tremendous risk to their organizations.

Vectra NDR, powered by Attack Signal Intelligence™, is the ideal solution to provide threat coverage, signal clarity and intelligent control when other solutions reach their limits in stopping today's attacks.

It's time to concentrate on detecting and mitigating active threats inside the network — from cloud, SaaS, identity and network data centers — before attackers have a chance to spy, spread and steal.



A view of host details shows the progression of attacks over time



The Vectra Threat Certainty Index

Vectra NDR harnesses Security AI-driven Attack Signal Intelligence™ to ensure early visibility with clarity, precision and context to erase unknowns and surface threats, attacks and malicious activities across a full chain of suspicious events.

Learn more: https://www.vectra.ai/products/ndr

Request an NDR demo: https://www.vectra.ai/demo

About Vectra Vectra® is the leader in Security AI-driven cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence™ detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Vectra Network Detection and Response (NDR) is the industry's most advanced AI-driven attack defense for identifying and stopping malicious tactics in your network without noise or the need for decryption. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai