Secureworks®

Network Detection and Response (NDR) Buyer's Guide

The Current State of Vulnerabilities

Network security remains a foundational element to any organization's overall risk management strategy. While most organizations recognize its importance, many still don't have the right network security tools to stay protected from modern cyber threats. As remote work has become widely accepted and more applications are based in the cloud, network flow is high and threat actors can easily mask behavior in the sheer volume of traffic, up 21.4% overall in 2024 versus 2023. The result has been a mass volume of alerts, overwhelmed security teams, and exhausted executives looking to maximize their resources as their organizations struggle to keep up.

Connected devices represent an opportunity for cyber criminals, as few organizations have the central governance and strong policies to ensure 100% up-to-date coverage at the endpoint. With advances in Business Email Compromise (BEC), phishing and identity theft combined with ransomware dwell times sitting under 24 hours, known vulnerabilities are prime targets to exploit for threat actors to enter and then move laterally across the network. And it can all start from a single compromised device.

The average cost of a data breach reached an all-time high of $4.45 million in 2023 (Source: IBM, Cost of a Data Breach 2023), many of these breaches could have been prevented at the network level. Organizations need to respond proactively through blocking and prevention of network-based attacks to prevent further exploitation. Prevention is the best defense

> **There can be no Zero Trust without visibility into what's happening inside networks**
>
> *Senior Analyst Heath Mullins, Forrester*

The average cost of a data breach reached an all-time high of

$4.45 million

in 2023

against network security threats, and while network blocking may sound basic, it still requires time and effort to be performed accurately and monitored effectively. With any strong defense-in-depth security strategy, the network prevention and detection of malicious traffic is a paramount method to improving any organization's security posture.

Why the Old Approach to Network Security Does Not Solve the Problem

To address network security, organizations have small network security teams as part of network operations or rely on broader cybersecurity teams tasked with monitoring across multiple domains beyond security, such as endpoint, cloud, identity, and email. As a result, there is typically limited in-house network security expertise, and those overwhelmed teams are also tasked with the ongoing maintenance and manual intervention that traditional network security tools require.

To further protect themselves, organizations need to not only prevent as much malicious traffic as possible at the network edge, but also detect and respond to malicious threats within their internal network traffic. Unfortunately, traditional network security solutions focus on perimeter defenses, and are noisy and cause too many alerts for security personnel to react to. Of the tens of thousands of third-party network security alerts that Secureworks processes every day, 99.999% are identified as false positives. And by overly relying on signature files based on simple watchlists, traditional tools such as firewalls and IPS are not able to keep up with modern threats hiding in the noise.

Of the tens of thousands of third-party network security alerts that Secureworks processes every day,

99.999%

are identified as false positives.

To counter these shortcomings, organizations often put too much reliance on EDR to prevent, detect, and respond to threats that made it through traditional network defenses. But few organizations have the resources and time to keep controls on all connected endpoint 100% up to date. All it takes is one compromised endpoint to open the floodgates, especially if the existing network security control isn't able to properly monitor internal east-west traffic within the network.

A New Approach to Network Security: NDR

Network detection and response (NDR) has emerged as the next evolution of network security. NDR leverages artificial intelligence, machine learning, and behavior analytics to detect anomalies in network traffic that could indicate a compromise or an attack in progress.

Unlike their predecessors, NDR systems do not rely solely on known signatures; they continuously analyze network behavior to identify deviations that could

suggest a breach, such as unusual data flows or connections to suspicious domains. This shift from signature-based detection to behavior-based detection allows NDR to identify and respond to novel and sophisticated threats more effectively.

NDR solutions also provide greater visibility into network activity, enabling security teams to investigate and respond to incidents with more context and precision. This is especially true when coupled with a unified security operations platform like extended detection and response (XDR) to further reinforce security posture.

5 "MUST HAVES" FOR YOUR NDR SOLUTION

Network Visibility

Monitors both north-south (external) and east-west (internal) for more opportunities to detect and block threats

Network Prevention

Ability to prevent threats with in-line blocking to reduce response times, without impacting legitimate traffic flow

Network Response

Automated response actions to contain and mitigate network threats

Network Detection

Conducts deep packet inspection (DPI) for more comprehensive detection of network threats

No Device Management

Updates to countermeasures, rules and signatures managed for you, allowing resources to be deployed elsewhere

Questions to Ask a Vendor When Evaluating an NDR Solution

- Does your solution monitor both north-south (external) and east-west (internal) network traffic?
- Does your solution have the proven ability to block threats on the network without impacting legitimate traffic?
- Can your NDR be deployed physically or virtually depending on my needs?
- Does your solution perform deep packet inspection (DPI)?
- How does your NDR leverage artificial intelligence (AI) to help detect the latest threats?
- How much time will my team need to spend on updates, maintenance, and overall device management?
- What visibility would your solution provide across my network environments?

- What sorts of countermeasures are included with your NDR solution?
- Do you offer a centralized XDR platform that your NDR solution can be integrated with for broader data correlation and threat detection and response?
- Where can I go to monitor device health, updates, and other key data points related to the deployed solution?
- What percentage of malicious traffic on the network does your solution reliably block?

Introduction to Secureworks® Taegis™ NDR

Network threats are real. Secureworks curates and maintains over tens of thousands countermeasures that block one million* network threats each month across customer base. Secureworks has a deep history of tracking and preventing threat actor behavior with unique insights based on trillions of processed events, deep security research and adversarial testing, and thousands of real-world incident response (IR) engagements.

With continued evolution of threat actor tactics, techniques, and procedures, signatures alone are no longer sufficient to detect advanced threats. AI is used in the foundation of Taegis NDR to analyze network traffic for anomalous application and port usage in order to identify potential threats before they can cause harm.

Secureworks Taegis NDR monitors traffic entering, leaving, and within your network to reduce the risk of a breach by blocking 99%* of malicious activity. Through up-to-date countermeasures, AI-based detectors and automated response actions, the security burden on downstream systems and staff is greatly reduced. Seamless integration with the Taegis XDR platform provides central management and more holistic visibility and protection across the complete attack surface.

** as measured across Secureworks entire customer base*

Next Steps

Read the National 9/11 Memorial & Museum case study.

Read the NDR Datasheet

TRY US TODAY

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com