intigrityShield

intigrityshield NDR Capabilities

AI-ML Powered Network Detection Resposne
intigrityshield NDR Capabilities

NDR Solutions in 2023

NDR (Network Detection and Response (NDR) solutions evolved out of the network traffic analysis market (NTA) and were enabled by the arrival of both “big data” and the highly scalable ability to analyze network traffic in real-time and the machine learning era where models were able to apply baseline and anomaly behaviors.

Gartner recognized NDR in 2020 and since that time, many point solutions have launched as well as established SIEM and XDR vendors have added NDR capabilities. The market quickly matured and SOAR solutions by the big SIEM vendors became big license options and some early point solutions appeared. NDR became part of the “SOC Visibility Triad” of SIEM, EDR and NDR.

With the recent growth of yet, another category of XDR (which a few vendors added NDR capabilities), the reality remains - each of these are often purchased, licensed and deployed as siloed point solutions, from multiple vendors with limited correlation and multiple gaps of coverage. And security teams are left with a complex security stack to manage and scale.

Many SOAR implementations failed due to their complexity and the number of integrations required to make them work seamlessly across attack surfaces, infrastructure and silod teams.

The best SOAR solutions are either native to a modern platform or easily and affordably configured and coordinates and automates tasks in response to threat indicators, incidents or alerts. It enables organizations to not only react swiftly to cyberattacks, but also monitor, analyse, and prevent future threats, thus enhancing their overall security posture.

intigrityshield’s NDR Capability Overview

intigrityshield’s NDR capabilities are based on ingesting flows and logs from across infrastructure that spans on-premises, cloud, IoT, OT and beyond. In real-time intigrityshield’s platform is applying AI/ML, threat intelligence feeds, and behavioral analysis with advanced algorithms and neural networks to learn from network, data and generate insights and predictions. comprehensive visibility into network activity, including endpoints, protocols, applications, users, cloud assets, and devices.

intigrityshield's fully integrated NDR capabilities enables faster and more effective incident response by automating threat containment, mitigation, and remediation actions across your networks via manual push-button or automated playbook responses.

intigrityshield NDR reduces the complexity and cost of network security by providing a single platform that integrates with your existing security tools and network infrastructure.

intigrityshield's NDR Solution Details

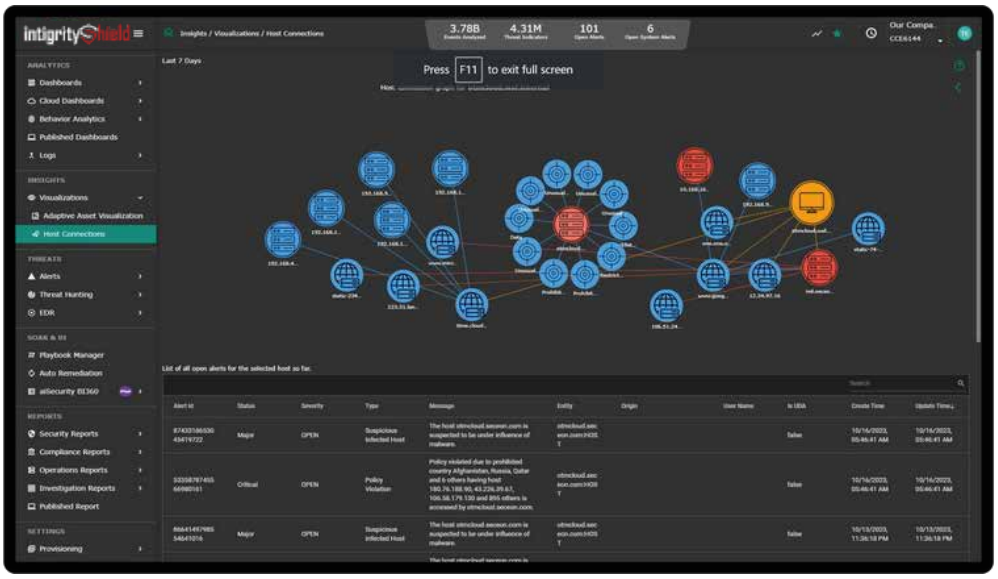
Contextual Network Visibility:

intigrityshield NDR relies on visibility as its core principle. You need to see everything that happens in your networks, whether they are on-premises, cloud-based, or hybrid, to detect and respond to threats in real-time. Visibility means having insight into all the entities, devices, and traffic that enter, exit, or move within your system. This kind of visibility is essential for NDR solutions, making it the most critical component of NDR.

Network Traffic Analyzer

intigrityshield' s Traffic Analyzer provides a comprehensive platform for network traffic analysis with focus on security monitoring at scale. It is a passive raw network traffic analyzer off network tap/SPAN or MIRROR ports, to inspect and monitor for security events. The analyzer performs port-independent analysis of application layer protocol. It supports analysis of many application layer protocols such as DNS, HTTP, FTP, IRC, SMTP, SSH, SMB, SSL etc. The Traffic analyzer not only identifies the protocols but also performs extensive sanity checks of these protocols. Additionally, it does the analysis of the file content for Regex pattern and malware fingerprinting. It also supports IDS-style emerging threats pattern matching and Netflow generation for further analysis.

The traffic analyzer's Protocol Analysis Engine performs deep packet inspection and performs a port-independent analysis of the protocol. In addition, it performs extensive sanity checks for every protocol. The traffic analyzer's Event Engine module is able to extract metadata from L2/L3/L4 and L7 headers.



intigrityshield Network Visualization

Wide-ranging Network Data Visibility and Analysis:

intigrityshield makes it easy to obtain a complete picture of the network activity and detect any malicious behavior. To achieve this, intigrityshield NDR uses a combination of various sources of data, such as raw packets, NGFW and IDS logs, Sysmon data, Netflow, and IPFix. This metadata provides rich information about the network traffic, the devices involved, the protocols used, and the events triggered. By analyzing the metadata from these sources, we can identify potential threats across various environments, such as physical and virtual networks, containers, on-premises servers, and public clouds.

AI and Automation Driven Prioritization:

intigrityshield NDR scores and ranks events based on urgency and expertise enabling your team to focus on the most critical and major threats in real time. And intigrityshield provides automatic correlation across networks, infrastructure, endpoints, users, and threat intelligence feeds.

AI- Automation Powered Detection:

intigrityshield NDR uses advanced analytics and deep learning to automate threat detection and analyzes complex behaviors and attacker methods to identify incidents from billions of data points. It helps teams find threats and attributions related to attacks and malicious network activities including duplicate or asymmetric traffic and encapsulations to verify weak indicators, and evasive and unknown patterns. intigrityshield covers up to 90% of attacker tactics and techniques in the MITRE ATT&CK framework.

Network Policy and Governance Engine:

Apply network policies and auto-remediate and/or alert when policy violatations occur, for example specific micro segmentation rules.

Built-In Response Measures:

Apply MITRE D3FEND countermeasures to respond to cyberattacks. intigrityshield's playbooks can be configured to investigate, contain, quarantine, and remediate compromised networks, endpoints, applications and systems

About intigrityshield

IntegrityShield reduces cyber threat risks and security stack complexity while significantly improving the ability to detect and block threats and breaches at scale. IntegrityShield's Open Threat Management (OTM) platform enhances and automates security with our AI and ML-powered aiSIEM and aiXDR solutions. The platform provides comprehensive coverage by collecting telemetry from logs, identity management systems, networks, endpoints, clouds, and applications. This data is enriched and analyzed in real-time using threat intelligence, AI and ML models based on behavioral analysis, and correlation engines to generate reliable and transparent detections and alerts. IntegrityShield supports over 8,000 clients by delivering high-margin, efficient security services with automated cyber threat remediation and continuous compliance.

Learn more about Intigrityshield NDR

Schedule a Demo