NetShield NDR

Agile approach for threat detection & protection

COSGrid NETWORKS

In today's ever - evolving cyber landscape, threats have become increasingly sophisticated, including **zero-day attacks, complex supply chain vulnerabilities, and advanced persistent threats (APTs)**. This presents a significant challenge as organizations struggle with an **overwhelming number of false positives (over 80%)** and an **excessive volume of alerts (10,000 per day)** that are **difficult for analysts to triage (only 10% addressed)**. Additionally, the expanding attack surface due to IoT, edge computing, BYOD, cloud, and 5G has made IoT/OT systems more vulnerable to volumetric attacks. In response to these complex challenges, **COSGrid Networks presents NetShield NDR** - a comprehensive NDR solution designed to proactively detect threats, prioritize alerts, and enable efficient incident response.

Gaps in Effectiveness

1. **Endpoint Detection and Response:**
   - Limited installation capabilities on all platforms/OS, including IoT/OT and BYOD, leaving critical areas exposed.
   - Vulnerability to attacker evasion and tampering of endpoint agents.
   - Difficulty in accurately mapping attacker movement.
   - Offers limited features and threat detection capabilities.

2. **Intrusion Detection System/Intrusion Prevention System:**
   - Reliance on signature-based detection, rendering them ineffective against zero-day attacks and sophisticated APTs.
   - Lack of device identification and classification leads to a lack of context for appropriate response and mitigation.

3. **Security Information and Event Management:**
   - Primarily focused on aggregating and correlating logs, lacking in behavior-based anomaly detection.
   - Rule-based approach limits its effectiveness in detecting emerging threats.
   - Insensitive to contextual information such as device class and specific use cases.
   - High false positive rates and prolonged mean time to detect (MTTD).

Highlights

- **Advanced Threat Detection:** Utilizes advanced techniques to proactively detect sophisticated threats that may bypass traditional security measures.
- **Comprehensive Visibility:** Provides deep network visibility and analytics for a holistic view of network traffic and behaviors, enabling informed security decisions.
- **Proactive Threat Hunting:** Empowers proactive threat hunting based on the MITRE ATT&CK framework to uncover hidden threats and respond swiftly to security incidents.
- **Streamlined Incident Response:** Facilitates efficient incident response with comprehensive investigation tools, visualization features, and automated response workflows.

NDR market continue to grow steadily at 22.5%, The steady growth of the NDR market is a sign that the reach of these tools includes enhanced analytical capabilities and response tactics.

Gartner

Filling the Gap: The Need for an Intelligent Security Platform

To bridge the existing gaps in cybersecurity effectiveness, there is a pressing requirement for:

Need solution that can
Baseline & Detect Anomalies
Deep Network visibility & analytics
TLS Fingerprinting
Encrypted Traffic Analytics
Micro-segmentation
Allow only well-known endpoints

Critical need is a platform that can be
Adaptive
Context based
Converged / Integrated / Correlating
Programmable
Scalable

How does NetShield NDR help here?

Network Detection and Response, is a comprehensive security solution designed to detect and contain post-breach activities within a network. It plays a crucial role in enhancing the effectiveness of cybersecurity measures by actively monitoring real-time traffic flows and comparing them against historical network connection metadata.

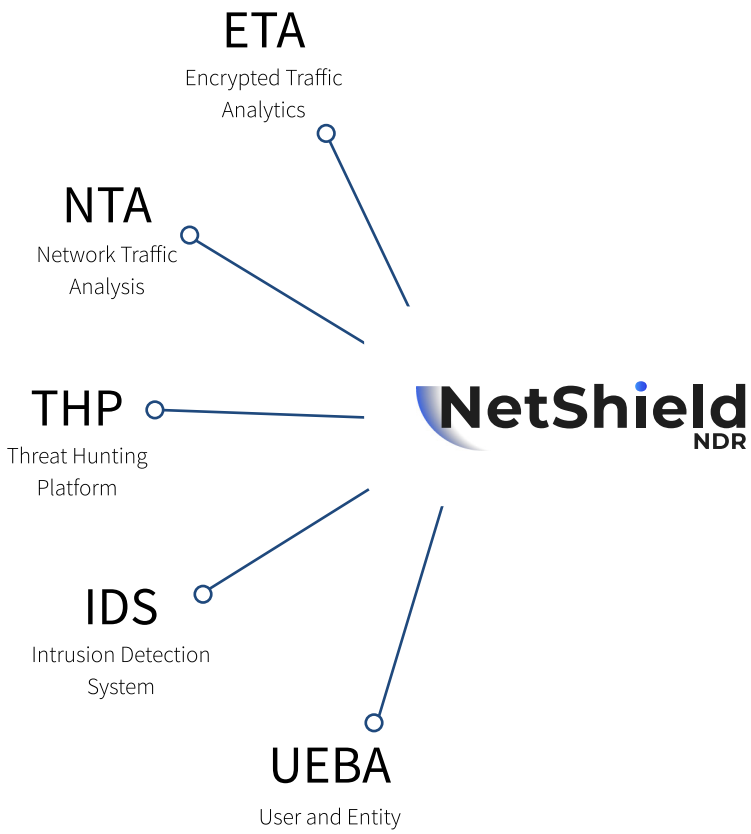
Key benefits of NetShield NDR include:

- **Detecting Post-Breach Activity:** NetShield NDR identifies and contains ransomware, insider threats, and lateral movements by analyzing real-time traffic against historical network data.
- **Rule-Based and Anomaly Detection:** NetShield NDR uses both rule-based detection and anomaly detection to identify known threats and spot deviations from normal network behavior.

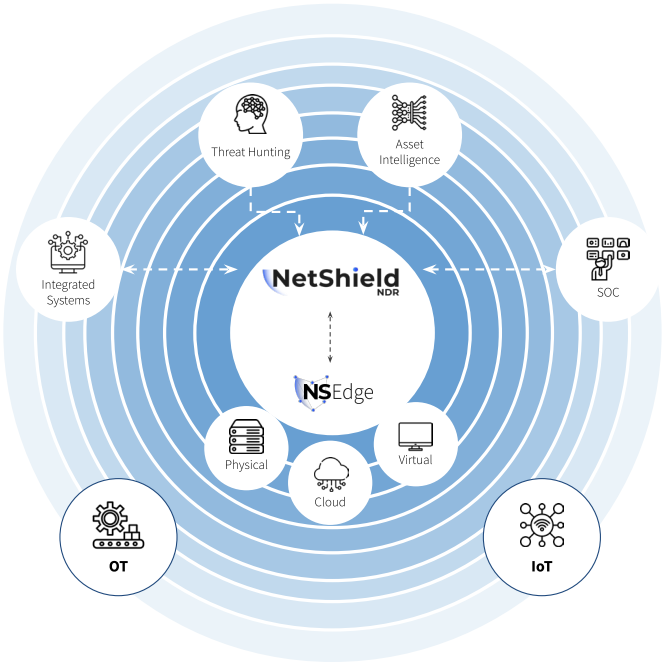
With NetShield NDR, organizations gain enhanced visibility into their network, enabling proactive response to threats and minimizing the impact of breaches.

NetShield NDR is also able to consolidate multiple security components into a single superset platform for both detection and response. NetShield NDR offers a unified and comprehensive approach to network security by integrating various technologies such as:

- **Network Traffic Analysis (NTA):** to analyze network traffic patterns and identify anomalies or suspicious activities.
- **Intrusion Detection System (IDS):** functionality helps detect known threats and signatures.
- **Endpoint Threat Analytics (ETA):** focuses on analyzing endpoint behavior to identify potential threats.
- **User and Entity Behavior Analytics (UEBA):** adds behavioral analytics to monitor user and entity activities for detecting insider threats or abnormal behaviors.
- **Threat Hunting Platform (TIP):** to leverage threat hunting feeds and enhance threat detection.



How it works



4D Traffic Analysis & Visualization

- Auto-discovers and classifies devices
- Multi-pronged traffic meta-data capture
- Adaptive Deep packet inspection, signature

Network Segmentation & Access Control

- Micro-segment and zero trust access using SDN
- Encrypted tunnels for channel protection

Monitor & Detect

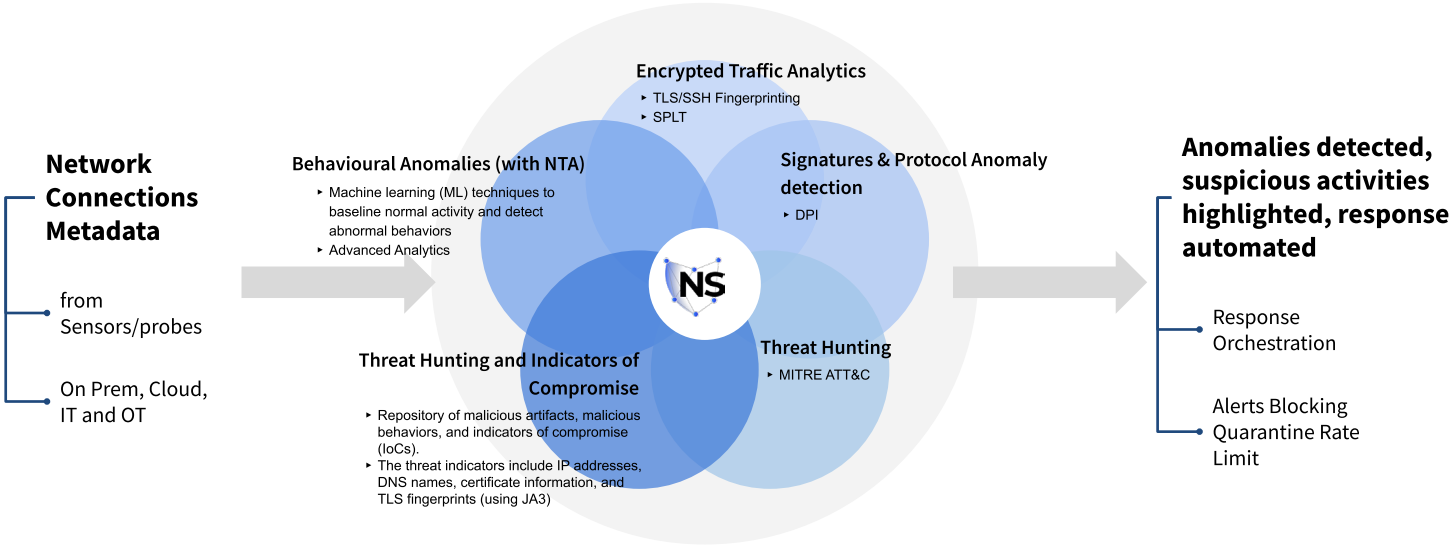
- Learns behavior and detect anomalies in real-time
- Threat hunting through intelligence and visualization with contexts

Adaptive Orchestration & Defend

- Edge/Distributed intelligence for quick remediation
- Security Orchestration and 3rd party integrations

Netshield NDR Capabilities

NetShield NDR is a holistic platform that takes an adaptive approach to threat detection. It combines various components to provide comprehensive network defense capabilities.



Behavioral Anomalies (with NTA):

- Uses machine learning (ML) techniques to baseline normal activity and detect abnormal behaviors.
- Employs advanced analytics to enhance the detection of potential attacks.

Encrypted Traffic Analytics:

- Incorporates TLS/SSH fingerprinting and other techniques to analyze encrypted traffic.
- Identifies potential threats hiding within encrypted communications.
- Examines protocol usage and traffic patterns to uncover malicious activities attempting to evade detection.

Signatures & Protocol Anomaly Detection:

- Utilizes Deep Packet Inspection (DPI) techniques to detect signatures and anomalies in network protocols.
- Identifies known threat signatures and deviations from expected protocol behavior.
- Enables proactive identification and mitigation of network-based attacks.

Threat Hunting:

- Includes threat hunting capabilities based on the MITRE ATT&CK framework.
- Proactively searches for indicators of compromise (IoCs) to identify potential threats.
- Assists in early detection and response to advanced attacks.

Threat Hunting and Indicators of Compromise:

- Maintains a repository of malicious artifacts, behaviors, and IoCs.
- Collects and analyzes information such as IP addresses, DNS names, certificates, and TLS fingerprints.
- Enhances detection and response capabilities by correlating network activity with known malicious entities.

Netshield Components

To provide comprehensive network detection and response capabilities, NetShield by COSGrid Networks comprises two main components:

IOT/OT NetShield Edge

HW appliance Models

- E-Series: Max 500 IoT devices; 100 Mbps BW
- B-Series: Max 1000 IoT devices, 500 Mbps BW
- D-Series: Max 5000 IoT devices, 1 Gbps BW

Virtual Appliance Model Options

- Vmware: vmdk & ova image
- KVM: qcow2 image
- Bare metal: iso image

Security Analytics & Responder (SAR)

Cloud SAR

- Multi-tenant infrastructure hosted in public cloud and ready on customer signup

On-Prem SAR

- Vmware: vmdk & ova image
- KVM: qcow2 image
- Container: docker compose (PoCs)
- Kubernetes: Helm

Security Analyzer and Responder (SAR): is the heart of the NetShield NDR architecture and encompasses several advanced technologies to provide comprehensive security analytics, detection, and response capabilities such as:

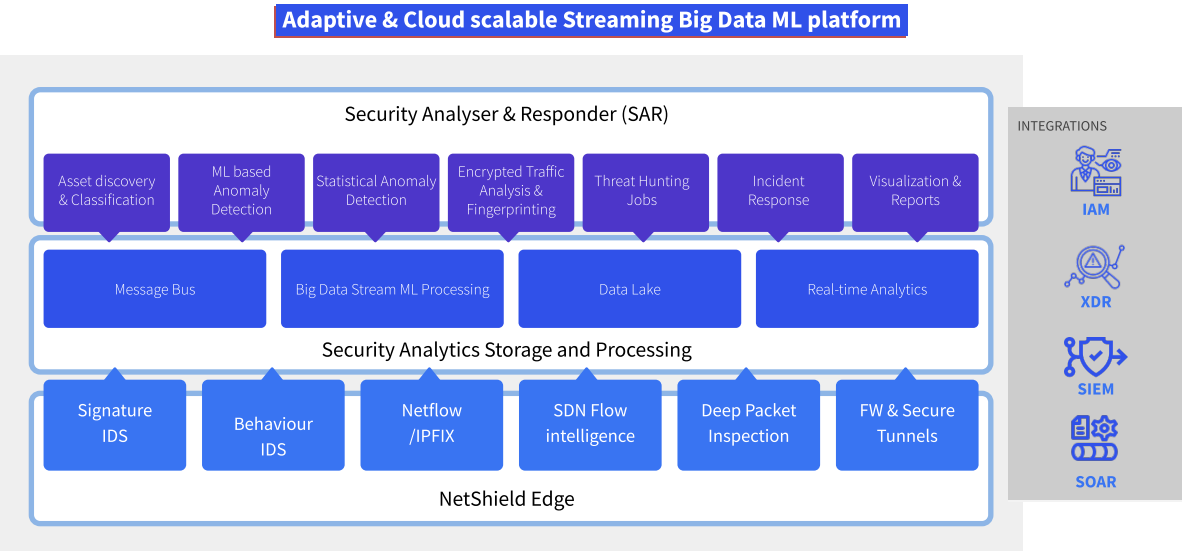
- **Asset discovery and classification:** SAR automatically discovers and classifies all assets within the network, including devices, applications, and users.
- **ML-based anomaly detection:** SAR uses machine learning algorithms to identify and detect anomalous network behaviors that may indicate a security threat.
- **Statistical anomaly detection:** In addition to ML-based detection, SAR also leverages statistical models to detect anomalies in the network traffic.
- **Encrypted traffic analysis and fingerprinting:** SAR can identify and analyze encrypted traffic, even without the decryption key. It uses fingerprinting techniques to identify the type of encryption and determine if it is legitimate or malicious.
- **Threat hunting jobs:** SAR can be configured to perform threat hunting jobs, which proactively search for known and unknown threats within the network.
- **Incident response:** SAR provides a centralized incident response platform that allows security teams to quickly investigate and respond to security incidents.
- **Visualization and reports:** SAR provides a comprehensive set of visualizations and reports that allow security teams to monitor the network health and security posture in real-time.

NetShield Edge: is a network device that provides real-time threat detection and prevention capabilities at the network edge that include

- **Signature IDS:** NetShield Edge uses signature-based intrusion detection to identify known security threats.
- **Network security IDS:** NetShield Edge also includes network-based intrusion detection to detect and prevent unauthorized network access.
- **Netflow/IPFIX:** NetShield Edge can collect and analyze Netflow and IPFIX data to detect and prevent network-based attacks.
- **SDN flow intelligence:** For environments with Software-Defined Networking (SDN), NetShield Edge can integrate with the SDN controller to provide advanced threat hunting.
- **Deep packet inspection:** NetShield Edge uses deep packet inspection (DPI) to analyze the network traffic and identify any malicious packets.
- **Encrypted tunnels:** NetShield Edge can detect and prevent threats that use encrypted tunnels, such as VPNs.

Netshield NDR Architecture

To provide comprehensive network detection and response capabilities, NetShield by COSGrid Networks comprises two main components:



NetShield utilizes a distributed architecture to provide comprehensive network detection and response capabilities:

- Various applications deployed on NetShield Edge devices generate network connection metadata related to network traffic, security events, and anomalies.
- This metadata generated by the applications on NetShield Edge are sent to the SAR, which resides in the cloud.
- The network connection metadata received by SAR are first stored in the Message Bus, which serves as a data buffer for efficient communication between different components within the Security Analytics Storage and Processing unit of SAR.
- The metadata stored in the Message Bus are classified, processed, and analyzed in real-time using Big Data Stream ML Processing techniques. This step involves applying various algorithms and models to identify different types of threats and anomalies.
- The output metadata, after being processed and analyzed, are stored in the Data Lake. The Data Lake serves as a scalable and centralized storage repository for storing the security-related data.
- The stored metadata in the Data Lake can be further utilized for Real-Time Analytics, enabling security teams to gain actionable insights, identify trends, and make informed decisions to respond effectively to security incidents.
- By leveraging this architecture, NetShield enables efficient processing, classification, and analysis of network connection metadata, facilitating the timely detection and response to threats within the network environment.

NetShield NDR Use Cases

Netshield offers a range of Network Detection and Response (NDR) use cases for businesses looking to protect their network environments. These use cases include:

- **Advanced threat detection:** The use of advanced algorithms and machine learning techniques can help to identify and isolate suspicious activity, allowing security teams to take quick action to prevent any potential damage.
- **Deep network visibility & Analytics:** By analyzing network traffic patterns and identifying anomalies, organizations can gain a deeper understanding of their network environment and identify areas that may be susceptible to attacks.
- **Threat Hunting:** involves actively seeking out potential security threats before they can cause damage. This is accomplished by performing deep dives into network traffic and analyzing logs and other data sources to identify signs of suspicious activity.
- **Dependency mapping & micro-segmentation:** By understanding the dependencies between different systems and applications, organizations can create micro-segmented network environments that are more resilient to potential threats.
- **Forensic Investigation:** In the event of a security breach or other cyber incident, forensic analysis can help to identify the root cause of the problem and provide valuable insights into how to prevent similar incidents from occurring in the future.
- **Compliance & Audit:** By implementing NDR solutions that provide detailed logging and reporting capabilities, organizations can demonstrate compliance with industry standards and help to mitigate potential risks associated with non-compliance.

Outcomes

Netshield delivers various outcomes that are designed to provide better visibility into the security posture of the network. Below are some key outcomes of Netshield- NDR:

- Statistical Anomaly Detection using Device & User Traffic Profiling:
  - Detects Remote to Local (R2L) attacks by analyzing the statistical properties of network flows, such as mean, moving averages, and standard deviation.
  - Identifies anomalies related to Command and Control (C&C) communications and port scanning using features like bag of server ports and destination IP/domains.
- Detection of known Bad Behaviors (MITRE ATT&CK):
  - Detects SSH brute force attacks, identifying repeated failed login attempts.
  - Identifies port scans, both horizontal (scanning multiple hosts) and vertical (scanning multiple ports on a single host).
  - Queries blacklists to search for suspicious domains and hosts, alerting on potential malicious activities.
- Detection of Botnet & C2C using Analysis & Supervised ML:
  - Detects beacon behaviors commonly associated with botnet activities.
  - Searches for signs of DNS-based covert channels, which may indicate DNS tunneling.
  - Identifies Command and Control (C&C) activities, such as heartbeat, file download, and attacks.
  - Utilizes supervised machine learning techniques to detect patterns and signatures associated with known botnets like Mirai.
- Protocol Analysis / DPI-based Anomaly Detection:
  - Analyzes network protocols at a deep packet inspection (DPI) level to detect anomalies and deviations from expected behavior.
  - Man-in-the-Middle (MitM) attacks: Helps identify potential Man-in-the-Middle (MitM) attacks, where an attacker intercepts and modifies network communications.
- Data Exfiltration:
  - Monitors network traffic for suspicious patterns indicating unauthorized data transfer or exfiltration attempts.
- DoS/DDoS:
  - Detects and mitigates Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks by analyzing network traffic and identifying abnormal traffic patterns.

Technical Specifications

Complete and Deep Network Visibility	
1	Single dashboard providing a comprehensive view of network activities and alerts and mitigation functions.
Network Traffic Analysis	
2	Supports different formats of flows Netflow, IPFIX, IDS Logs and Correlation
3	Network Traffic Pattern Analysis based on IP addresses, groups of IP addresses, source/destination IP pairs, Flow Duration, Bandwidth Analysis etc.
4	Perform Layer 7 metadata analysis, providing application wise traffic categorization.
Threat Detection	
5	Real time monitoring of host behaviors and traffic analysis to identify threats and detect lateral movements
6	Performs real time and comprehensive threat identification by correlating the traffic with, including but not limited to FQDN, User-Agent, IP, Port, URL signatures etc.
7	Detects common events and anomalous behaviour like DDoS / DoS, port scanning, worms, unexpected application services including tunnelled protocols, backdoors and use of forbidden application Protocols, Policy violations, Command and Control communication, web shell traffic, botnet traffic etc.
Threat Mitigation & Response	
8	Automated response actions to mitigate the threats in real time using predefined and customizable playbooks
9	Integrations with SIEM/SOAR platform for the automated response
Threat Intelligence	
10	Integrates with multiple threat hunting feeds containing regularly updated threat hunting signatures for detecting, reporting and mitigating threats from malwares including but not limited to - Botnets, Ransomware, Trojans, Spyware, APT backdoors etc.
Integrated Response	
11	Integrates Firewalls, IPS, WAF, Routers, switches and other network and security products to orchestrate threat detection and mitigation from itself or via the common SOAR platform

+91 90227 64534 cosgrid-networks @cosgridnetworks2141 @CosgridNetworks

Ph: +91 90227 64534, +91 86101 44212 | **E-mail:** info@cosgrid.com
Address HQ: COSGrid Systems Private Limited - Velachery, Chennai - 600042
Address 2: COSGrid Networks Inc - New Castle, US, 19808