LMNTRIX

BE THE HUNTER | NOT THE PREY

WHITE PAPER

NETWORK DETECTION & RESPONSE

WITH LMNTRIX XDR

Cloud-delivered, full packet capture, real-time and retrospective threat detection and visualization.

2022

LMNTRIX USA.
333 City Blvd West, 17th Floor,
Suite 1700, Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65 3159 0639

LMNTRIX INDIA.
VR Bengaluru, Level 5, ITPL Main Rd,
Devasandra Industrial Estate,
Bengaluru, Karnataka 560048,
sales@lmntrix.com
+91-22-49712788

LMNTRIX Australia.
Level 32, 101 Miller Street,
North Sydney NSW 2060,
+61.288.805.198

lmntrix.com

EXECUTIVE SUMMARY

Network Detection and Response has evolved from network traffic analysis techniques to deliver total network coverage for security solutions. This technology category closes the gap in visibility that traditional network security solutions offer where they offer minimal visibility of attacks once the threat or attacker has breached these outer controls based on perimeter defenses such as firewalls coupled with intrusion protection systems, email and web security solutions. The sophistication of persistent network threats means that the traditional approach is no longer practical.

On-premises and remote, cloud and hybrid cloud, physical and virtual, the complexity of network infrastructure are increasing. Networks are also leveraging encryption techniques to protect internal messaging, making monitoring more challenging. The increased threat levels and sophistication add to this additional complexity, making them harder to secure. These factors are coupled with diversification in endpoints to include a broader range of connected equipment, including operational and manufacturing technology and internet-of-things devices. These factors create more complex network traffic for attackers to exploit for information gathering and hiding their presence.

Monitoring network logs and endpoint data does not provide a complete picture of network activity. A comprehensive network security solution will require access to all network traffic, open or encrypted, for all endpoint devices. Monitoring must also extend beyond looking for known threats, malicious code signatures, or sequences of commands known to indicate an attack. Instead, security needs to intelligently monitor traffic to identify unusual events or abnormal behavior that can mean a novel attack is in progress. It must also do this quickly enough to contain and respond to an attack before real damage occurs.

This challenging operating environment is where network detection and response fits into an integrated security solution. It provides complete visibility of all network traffic to all endpoints, analyzing behavior to spot the unusual in vast volumes of regular traffic. Alongside endpoint detection and response and security log analysis techniques, this provides comprehensive end-to-end security across an organization's entire infrastructure, regardless of technology, location, complexity, and scale.

A cloud-delivered Network Detection and Response (NDR) platform is the evolution of effective IT security. It reliably detects threats and sophisticated attacks, retains full-packet forensics for as long as necessary, and enables integrated response. Cloud-delivered Network Detection and Response (NDR) consolidates multiple security point products into a single platform that deploys rapidly. It provides continuous threat visibility as organizations move workloads from on-premises to the cloud or expand into other environments such as industrial networks. Network Detection and Response (NDR) also increases the efficiency of security teams to allow them to mitigate any impact of attacks rapidly.

As an added benefit, the network detection and response approach fits seamlessly with the zero-trust philosophy that is gaining traction for organizations looking for a step-change enhancement of their security posture. It not only delivers network security controls but also provides continuous validation of the zero-trust implementation.

CONTENTS

Executive Summary 2
An Overview of Network Detection and Response 7
Introduction 7
What is Network Detection and Response? 8
Detection Benefits of NDR 9
Response Benefits of NDR 10
History of NDR 12
The Role of NDR 13
NDR Market Trends 14
Terminology 16
Principles of NDR 18
Visibility 18
Threat Detection 18
Proactive Analysis 19
Retrospective Analysis 20
Investigation 20
Response 21
Recovery 22
Forensics 22
Cloud 23
Components of Enterprise NDR 24
MetaData Capture 24
Retrospection 25
Anomaly Detection 25
Threat Hunting 26
Implementing NDR 27
Strategy and Goals 27
MITRE ATT&CK Framework 26
The NDR/EDR/SIEM Triad 27
Integration Benefits 28
Deployment Strategy 29
Deployment Preparation 29
Objectives 29
Deployment 30
Sensor Deployment 30
Data Capture 30

Deployment Example – Single-Point 31
Deployment Example – Split Route 32
Deployment Example – Hierarchical 33
Data Center Deployment 35
Azure Deployment 36
AWS Deployment 36
GCP Deployment 37
Cognito Stream Deployment 37
Configuration 37
Monitoring 38
Measuring 38
Importance of NDR for Security Investigations 39
Overview 39
Investigation Playbooks 39
NDR Solutions 39
Investigation Benefits 40
Leveraging Network Telemetry for Forensics 41
Core Concepts 41
Logging 41
Analysis 42
NDR Case Studies 44
SolarWinds Case Study 44
Introduction 44
Terminology 44
Attack Profile 44
Detailed Analysis 45
Discovering the Breach 45
Recovery 47
MS Exchange Case Study 47
Introduction 47
Detailed Analysis 48
Exploitation 49
Server Vulnerability 50
Detection 50
Recovery 50

NDR Use Cases 51
Immediate time to value 51
Advanced forensics 51
Detections in depth 51
Early Detection 51
Integrated response 51
Cloud Monitoring 52
Encrypted Attacks 52
Infected Third-Party Devices 52
Phishing Attacks 53
Insider Threats 54
Compliance 55
Shadow IT 55
Frictionless scale 56
Organizations want proactive network security 56
How LMNTRIX XDR Benefits from NDR and Network Telemetry 57
LMNTRIX XDR 57
LMNTRIX Network Detection & Response (NDR) 58
Benefits 58
Cloud-based network memory 58
Intelligence from sensor-driven data 59
Retrospection 59
Intuitive data visualization 59
Technical requirements 60
About LMNTRIX 61

Figure 1 - How Network Security Fits In 7
Figure 2 – Visibility, Detection, Containment, and Response 8
Figure 3 – NDR and EDR Benefits 10
Figure 4 – The Attack Chain 11
Figure 5 – Threat Detection and Response Time 11
Figure 6 – NDR Pattern Scanning 12
Figure 7 – Biggest Perceived Threats 13
Figure 8 – SANS Survey Results 14
Figure 9 – NDR Solving SOC Priorities 15
Figure 10 – LMNTRIX NDR Sensor Feature List 25
Figure 11 – SOC Visibility Triad 28
Figure 12 – Single-Point NDR Deployment 31

Figure 13 – Multiple-Point NDR Deployment 32
Figure 14 – Hierarchical NDR Deployment 33
Figure 15 – Example Data Center Deployment 35
Figure 16 – Network Security and Forensics 43
Figure 17 – SolarWinds Attack Timeline 46
Figure 18 – Microsoft Exchange Static Keys 48
Figure 19 – Phishing Site Occurrence 53
Figure 20 – Insider Threat Detection Time 54
Figure 21 – Shadow IT Presence 56

AN OVERVIEW OF
NETWORK DETECTION AND RESPONSE

INTRODUCTION

Traditional security solutions have focused on protecting boundaries and endpoints, concentrating controls around the perimeter of systems and in connected devices. Unfortunately, this approach has allowed attackers to bypass the perimeter controls to loiter within networks undetected. By avoiding triggering endpoint agents, they can take their time exploring systems looking for ways to increase access and find information of value.

Network Detection and Response (NDR) is a valuable component of integrated security solutions. They provide your security team with visibility of activities inside networks where traditional security products such as Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) cannot see.

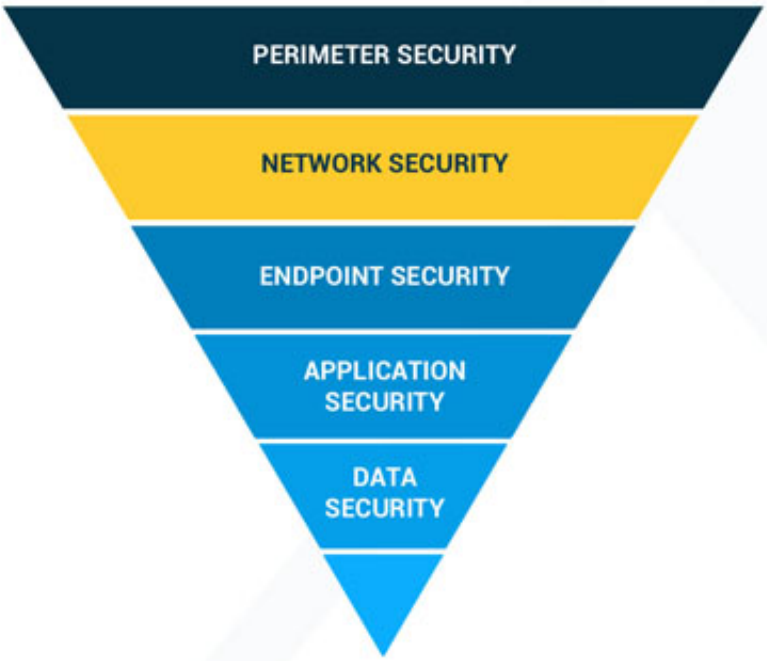


Figure 1 - How Network Security Fits In

NDR solutions build on network traffic analysis (NTA) and Network Analysis and Visibility (NAV) services that provide internal visibility and threat detection while offering intelligent response and enhanced investigation capabilities. This response capability is the critical differentiator for this technology solution. Monitoring and analyzing network data provide threat detection. However, traditionally network analysis throws up too many false-positive results, allowing genuine threats the chance to remain hidden in the noise. The automated response capabilities of NDR solutions analyze the detected threats to eliminate these false positives to enable focus on actual threats.

The network provides an incorruptible source of truth about how attackers breach defenses and what has been impacted. Previously, only organizations with large budgets could purchase the software and hardware needed to record and retain network traffic. However, those legacy products captured traffic from on-premises environments only, and complex deployments limited the rollout to a few network segments. Cloud-delivered Network Detection and Response levels the playing field by making what was once a luxury enterprise-wide packet capture retained for long time periods — available to all organizations. It does not need any specialized hardware and can be rapidly deployed in any segment of the modern network-enterprise, cloud, or industrial. The ability to capture traffic from any network is of tremendous importance, given that more and more business workloads are running on infrastructure that is not owned by the organization. By being able to record traffic from any network, this approach provides security teams with what they need most: visibility. Visibility is the key for detection, forensics, containment, and verification of threats.

WHAT IS NETWORK DETECTION AND RESPONSE?

NDR solutions implement network traffic analysis using non-signature-based behavioral monitoring techniques to detect unusual or suspicious traffic. Intelligent analytical techniques built around machine learning continuously analyze raw network traffic to compare with reference models of normal behavior. This includes analyzing encrypted content to identify any attempt by an attacker to conceal their activities. Compared to simple log analysis, this approach enables the detection of unusual data flows or message types that may be associated with a sophisticated ongoing attack that has evaded perimeter controls and intrusion detection solutions.

The critical advantage that an NDR solution brings to threat detection as part of an integrated security stack is monitoring all communications within networks. Traditional boundary-based defenses focus on tracking the north/south traffic that crosses perimeters. NDR solutions also analyze east/west communications within internal networks. The NDR solution must have visibility at all points across internal networks through strategically placed network sensors to be fully effective.

The second part of the NDR solution is the threat containment and response. Automated capabilities react to detected threats in two ways. First, threat containment activities look to halt suspicious network traffic to restrict and eradicate any ongoing attack. Second, information-gathering activities record comprehensive and forensically acceptable evidence to support recovery and intelligence sharing.

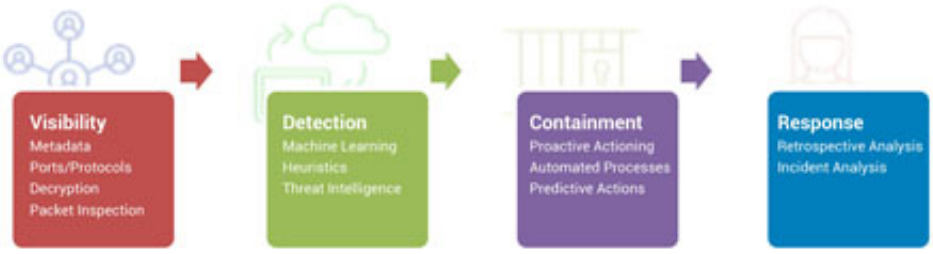


Figure 2 - Visibility, Detection, Containment, and Response

It's a known fact that it's not a matter of if but when cybersecurity defenses will be breached. Prevention-based network security approaches alone, which rely on the ability to control enterprise-owned resources, are no longer sufficient. Organizations are looking for proactive detection and response. Network Detection and Response complements prevention–only security technologies such as Intrusion Detection Systems (IDS) and Intrusion Detection and Prevention Systems (IDPS). It uses advanced methods (e.g., machine learning, anomaly detection, correlation) to augment detections by other products. Full-fidelity forensics allows security teams to actively threat hunt. When information about a new attack is announced, long–term forensics also allow security teams to search back in time to see if that attack has ever impacted the organization.

DETECTION BENEFITS OF NDR

NDR solutions deliver significant benefits for detecting threats across the entire footprint of an organization's infrastructure. They can see abnormal behavior of services irrespective of where that service is hosted, including microservices hosted on the cloud that typically may not be within the scope of security monitoring.

The monitoring can cover encrypted and unencrypted network traffic, eliminating the ability for attackers to hide their activities by hiding within encrypted data flows. This ability also allows the collection of comprehensive traffic information for use in forensic investigation processes, incident analysis, and triage, along with post-incident remediation.

They can detect abnormal behavior of endpoints or any other connected device without needing to deploy an agent on the device. This extends detection capabilities across the entire network real-estate to include devices that generally cannot support an agent, such as operational and manufacturing technology and internet-of-things (IoT) devices. To put this lack of IoT coverage into context:

- By 2024 there will be over 83 Billion IoT devices connections
- By 2025 over 150,000 IoT devices will connect every minute
- By 2025 IoT devices will generate around 70 zettabytes (That's 10 to the power 21)
- By 2026 the IoT device market will be worth more than $1 trillion

While most IoT devices cannot support endpoint agents, less than 2% of their message traffic uses encryption, and around 60% of organizations cannot identify insecure IoT devices.

Traditional Intrusion Detection Systems (IDS) are employed to monitor networks to detect possible attacks. More advanced Intrusion Detection and Prevention Systems (IDPS) introduce functions for preventive actions to contain attacks. NDR solutions incorporate automated response capabilities to supplement the monitoring and prevention functions, providing a comprehensive end-to-end network defense solution.

This capability progression is analogous with Antivirus (AV) software employed to monitor endpoints to detect possible attacks. More advanced Next-Generation Antivirus (NGAV) services introduce more comprehensive threat detection. EDR solutions incorporate automated response capabilities to supplement the threat detection functions, providing full-cycle endpoint defense.

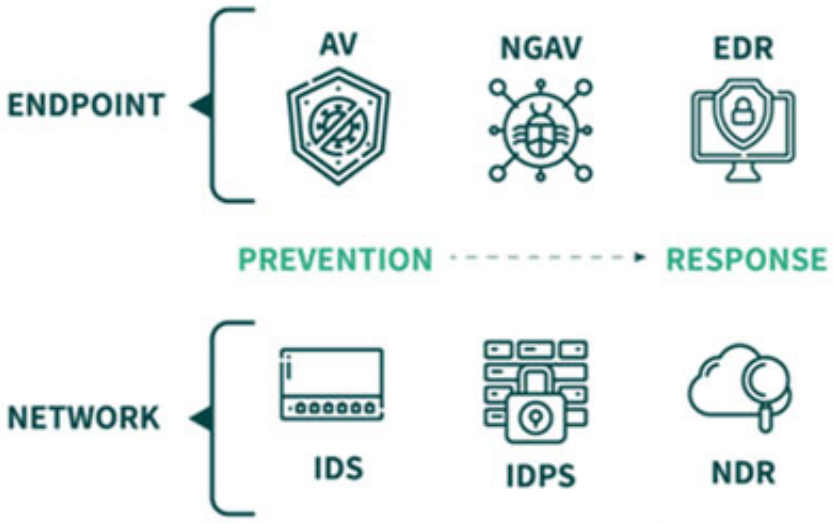


Figure 3 - NDR and EDR Benefits

They can operate seamlessly across on-premises and cloud-based systems, being platform-agnostic and infrastructure-independent.

NDR solutions can also be used for performance optimization by identifying misconfigured services or misdirected traffic that unnecessarily consumes network bandwidth.

RESPONSE BENEFITS OF NDR

The critical benefit of integrating NDR into a security solution is the faster detection and response to advanced persistent threats that have breached perimeter defenses. Without NDR, threat detection would typically occur when the attacker moves from a passive to an active attack posture. Passive lateral movement, privilege escalation, information gathering, and data exfiltration will pass unnoticed for sophisticated attackers with the skills to bypass security controls and keep activities hidden from routine scanning and logging. Detection is possible if the attack moves to aggressive and noticeable tactics such as disabling a service, data deletion, or ransomware deployment. If the attack remains passive, an organizations' first indication of compromise is when data stolen from its systems are observed on the dark web or used as part of a ransom.

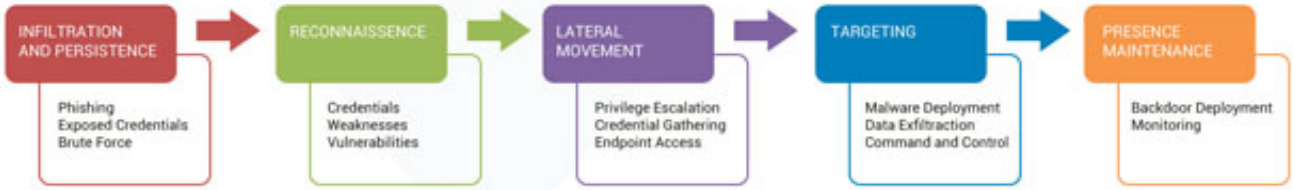


Figure 4 - The Attack Chain

Earlier detection of an attack will allow containment and response before the attacker has a chance to compromise systems and exfiltrate sensitive information. The goal is to minimize the attacker's dwell time. This is measured as the time from the initial system compromise to when the threat is contained.

Figure 5 - Threat Detection and Response Time

The temporal benefits of NDR solutions are:

- Detection time is significantly reduced by the capability of detecting abnormal behavior in network traffic that would not be spotted by pattern matching techniques or scanning for known threat signatures.
- Triage time is reduced by automated response functions eliminating false positive alerts, allowing the security team to focus on genuine incidents.
- Response time is reduced by providing comprehensive reporting information that enables informed decision-making for response actions and resourcing priorities.
- Containment time is reduced by automated response functions that integrate with perimeter controls to deny the attacker further access to networks.
- Remediation time is reduced thanks to comprehensive records of the attacker's actions giving the recovery processes complete and accessible visibility of where remediation actions are required. Additionally, this eliminates any requirements to deduce attacker actions based on potentially compromised log files.

HISTORY OF NDR

NDR is a very recent development in the cybersecurity field but has seen rapid growth as a service in its first years.

Initially, network security focused on using perimeter firewalls and intrusion prevention systems to screen traffic entering and leaving a network. However, this approach had the disadvantage that once a threat had evaded this screening, it was free to operate unconstrained within networks. As a result, NTA techniques were adopted to scan network traffic to look for known threats identified from recognizable patterns in the message content.

The problem with pattern scanning is that it will only detect the threats it is programmed to seek. Novel threats or threats that disguise themselves using encryption or other obfuscation techniques will evade signature-based (or) pattern scanning.

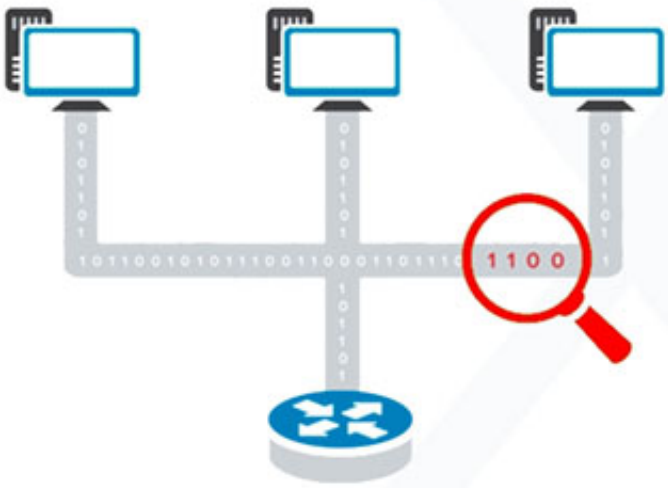


Figure 6 - NDR Pattern Scanning

NDR evolved from NTA technology to resolve the issues by using intelligent analysis techniques that look for abnormal behavior. This approach requires a machine learning or alternate analytical-based process for the NDR solution to determine expected behavior patterns to use as a reference. The critical advantage is that this technique does not rely on the threat being previously known. Instead, novel threats will be detected in precisely the same manner as known threats.

NDR solutions obtain traffic information from a diverse range of sources. For example, existing firewalls, intrusion detection systems, intrusion prevention systems, metadata, or other sources can be used as sources of traffic and dedicated NDR sensors located around the network.

An effective NDR solution will ensure comprehensive coverage of all network traffic across the entire network. This includes both north/south and east/west traffic in physical and virtual environments. The aggregated monitoring data can then be analytically processed, conscious of current threat intelligence information, to perform threat identification.

THE ROLE OF NDR

NDR fills the gap in defenses that perimeter-based controls leave unprotected, namely the presence of attackers on internal networks inside the shields. The two biggest perceived threats to organizations are those avoiding boundary controls by stealing credentials or misusing authenticated access credentials.

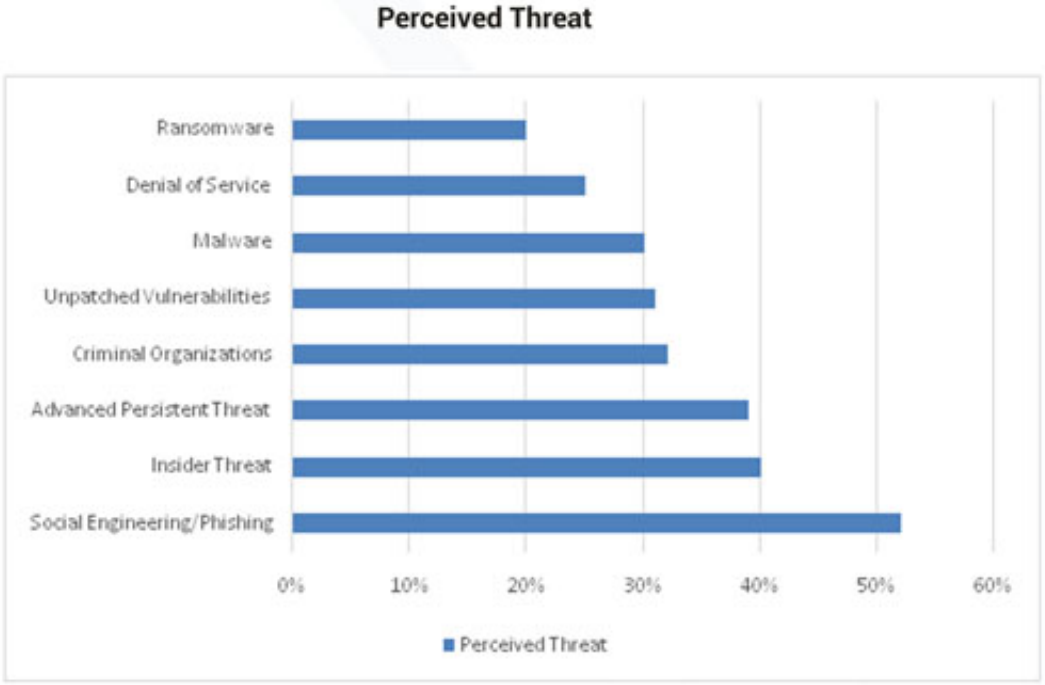


Figure 7 - Biggest Perceived Threats

Traditional network monitoring and detection strategies rely on a rule-based approach supporting log data for post-event analysis. Unfortunately, this has a severe weakness when dealing with novel and evolving threats that the rules won't recognize as security risks. For example, external attackers breaching undetected perimeter defenses or insider attacks with authorized access but malicious intent. NDR solutions combine rules-based checks with intelligent behavioral analysis to identify threats within the perimeter. The use of encryption on internal networks reduces the visibility of monitoring tools without an effective out-of-band decryption capability. NDR provides the ability to monitor all traffic and detect suspicious activity with full-fidelity packet capture.

The adoption of cloud-based solutions has created an often unrecognized need for NDR solutions. Organizations are often unaware that the service provider is only responsible for securing the cloud infrastructure under the Shared Responsibility Model for cloud security. The organization itself has responsibility for the protection of its cloud-based systems and infrastructure. NDR provides the capability to secure services and information within the cloud.

For post-incident analysis, an NDR solution can quickly generate a coherent and fully accessible dataset of forensically acceptable evidence. Automated workflows can significantly reduce resource requirements and speed up incident validation and triage processes. Detection information combined with real-time network data provides valuable evidence for impact assessment and remediation strategies. Additionally, the detailed information allows a comprehensive analysis of attacker actions, a capability not available with traditional log files that are vulnerable to alteration or deletion as part of an ongoing attack.

NDR MARKET TRENDS

In recent SANS survey results, only 38% of respondents had high or very high confidence levels in their ability to discover all the devices connecting to their networks. Furthermore, while around 52% of respondents believe they have high visibility of north-south traffic passing through perimeter controls, not surprisingly, a mere 17% thought they have the same east-west traffic visibility within their networks. This lack of internal visibility emphasizes the need for NDR solutions.

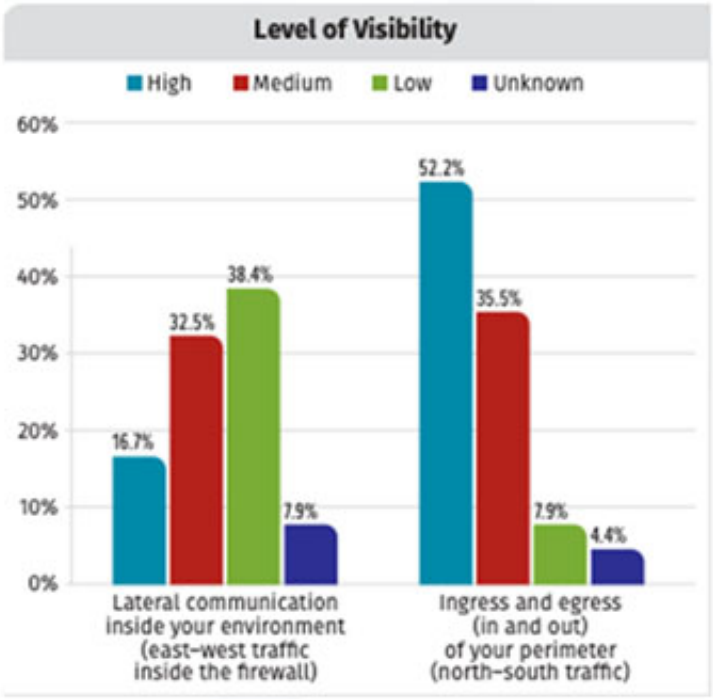


Figure 8 - SANS Survey Results

Perimeter controls continue to develop, with next-generation firewalls offering advanced threat detection and containment facilities and the capability for secure sockets layer (SSL) inspection. While these devices provide integrated intrusion detection and prevention, they predominantly rely on pattern matching techniques to detect known threats. This has created a market for NDR solutions that detect novel threats.

The focus on current NDR development is integration with other security controls to provide end-to-end protection of the information processing environment.

- Application of machine learning techniques to analyze network traffic, improving detection of suspicious traffic that other security methods cannot see.
- Integration with firewalls will enable the automatic dropping of suspicious network traffic as a containment strategy.
- Integration with network access controls (NAC) and Endpoint Detection and Response (EDR) solutions will enable automatic isolation of endpoints observed to be the source of unusual traffic patterns.
- Capabilities to decrypt, analyze, and, where necessary, terminate TLS traffic.
- Integration with Security Operations Automation Response (SOAR) solutions will enable automatic response actions using appropriate playbooks.

The potential importance of NDR solutions can be seen in a survey of the top areas of threat detection that organizations prioritize. All the following priorities can be addressed by implementing an NDR solution:

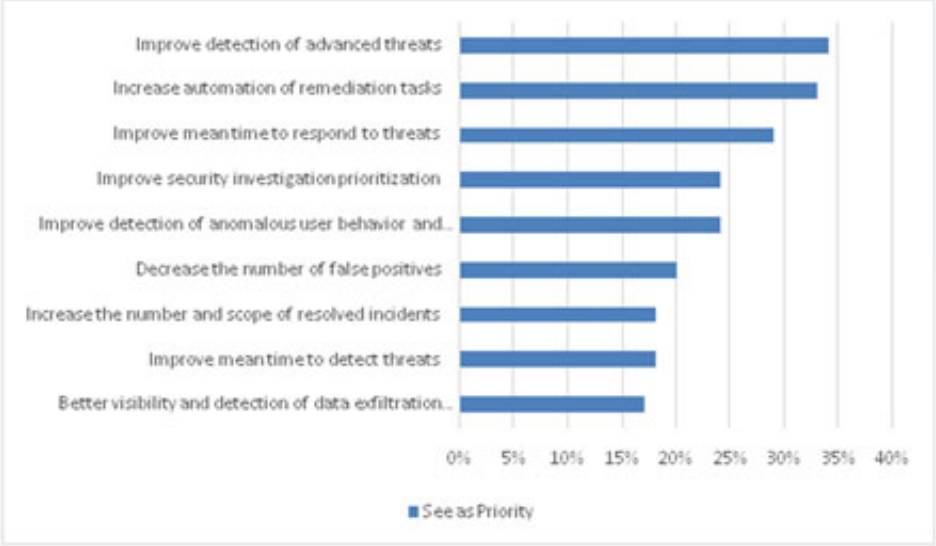


Figure 9 - NDR Solving SOC Priorities

While the NDR market is still nascent / evolving, it has become crowded with vendors providing network analytical monitoring. However, not all offer comprehensive network coverage, intelligent behavioral tracking, and integrated automated response solutions. Therefore, when choosing an NDR solution, the service must include:

- An analysis of raw network packet traffic or traffic flows in real-time or near real-time
- The monitoring and analyzing both north/south network traffic as it crosses perimeters and internal east/west network traffic
- The modeling of regular network traffic to detect and report abnormal traffic
- The use of behavioral, heuristic, and signature-based techniques to detect abnormal network traffic
- The minimization of false-positive security incident alerting
- Automatic response capabilities for validated security incidents
- A standalone solution that does not mandate any prerequisite security products or technologies to operate
- The provision of a forensic facility in addition to detection and response services

TERMINOLOGY

East-West Traffic refers to data packets transmitted between two or more endpoints within a network.

North-South Traffic refers to data packets that pass across the boundary of a network, transmitted between any external sources to one or more endpoints within a network.

Data packets are the electronic packages of information sent over a network in a format determined by the transmission protocols used by the network.

Endpoint Detection and Response (EDR) refers to security solutions that monitor and protect network-connected equipment. A software agent deployed on each endpoint records all activity on the endpoint for analysis. The analysis can be performed on the endpoint by the agent. Alternatively, data is transferred to a central or cloud location for analysis. The assessment inspects the data to detect the presence of an attacker. Detection techniques range from simple pattern matching to artificial intelligence based on a search for indicators of compromise (IOCs), behavioral analysis, and use of threat intelligence. Response capabilities include alerting, generating forensic data, suspect endpoint isolation for threat containment, and rolling a compromised endpoint to its last known safe state. The effectiveness of EDR relies on the deployment of agents on all endpoints, which may not be possible for internet-of-things (IoT) devices, operational technology, or network-enabled manufacturing equipment.

Threat Detection and Response (TDR) refers to a type of EDR service that limits the volume of endpoint data records by focusing on critical functions or recording data for analysis once a threat is detected.

Extended Detection and Response (XDR) is a security solution that integrates an EDR service with an NDR service to provide a more comprehensive detection capability. A single service collects and correlates endpoint agent data, network-level information, and log data. The service applies analysis techniques to this single dataset to maximize detection effectiveness.

Managed Detection and Response (MDR) is a specialist threat detection and response capability that uses an outcome-based approach to identify and limit the impact of security incidents rapidly. The service relies on remote threat monitoring using host and network-layer technologies deployed on network chokepoints and endpoints. In addition, advanced analytics, threat intelligence, forensic data, and human expertise are leveraged for investigation, threat hunting, and response.

Security Information and Event Management (SIEM) are security solutions that collect, aggregate and analyze event data from endpoints and network logs. The data is analyzed to identify any abnormal events or patterns of behavior that could be caused by a threat actively exploiting, or attempting to exploit, a security weakness. The effectiveness of SIEM is directly dependent on the coverage and quality of the log data.

Security Operation Centers (SOC) are staffed facilities that perform round-the-clock threat detection and response activities based on manual detection and response processes. The SOC requires physical and logical access to the systems being monitored.

PRINCIPLES OF **NDR**

VISIBILITY

The key principle of NDR is to provide visibility of all network activity, enabling analytical techniques to be applied to all data passing over the network. This includes all traffic for all ports, network endpoints, and other connected devices and services. NDR looks at both north/south traffic crossing boundaries and east/west traffic within the perimeters when analyzing network traffic for threats.

This includes message protocols and content, data files, scripts, executables, and any other traffic. Irrespective of how content is formatted, encapsulated, embedded, or encrypted, all content is analyzed. This prevents attackers from disguising or obfuscating data associated with these actions in a manner that could evade analysis. The challenge is to thoroughly inspect all network traffic without impacting network data integrity and business process efficiencies.

Networks now typically use encryption techniques across all traffic, inside and outside of the boundaries. This approach enhances the security of sensitive information, protects confidentiality, and ensures data integrity. The downside is that attackers can use encryption to hide their activities from traditional monitoring and logging-based controls. Behavioral monitoring of encrypted traffic can identify potential abnormal events, but the encrypted nature of the information makes investigation challenging. The decryption of all message traffic is an essential aspect of an NDR solution in removing this potential blind spot from the security controls.

THREAT DETECTION

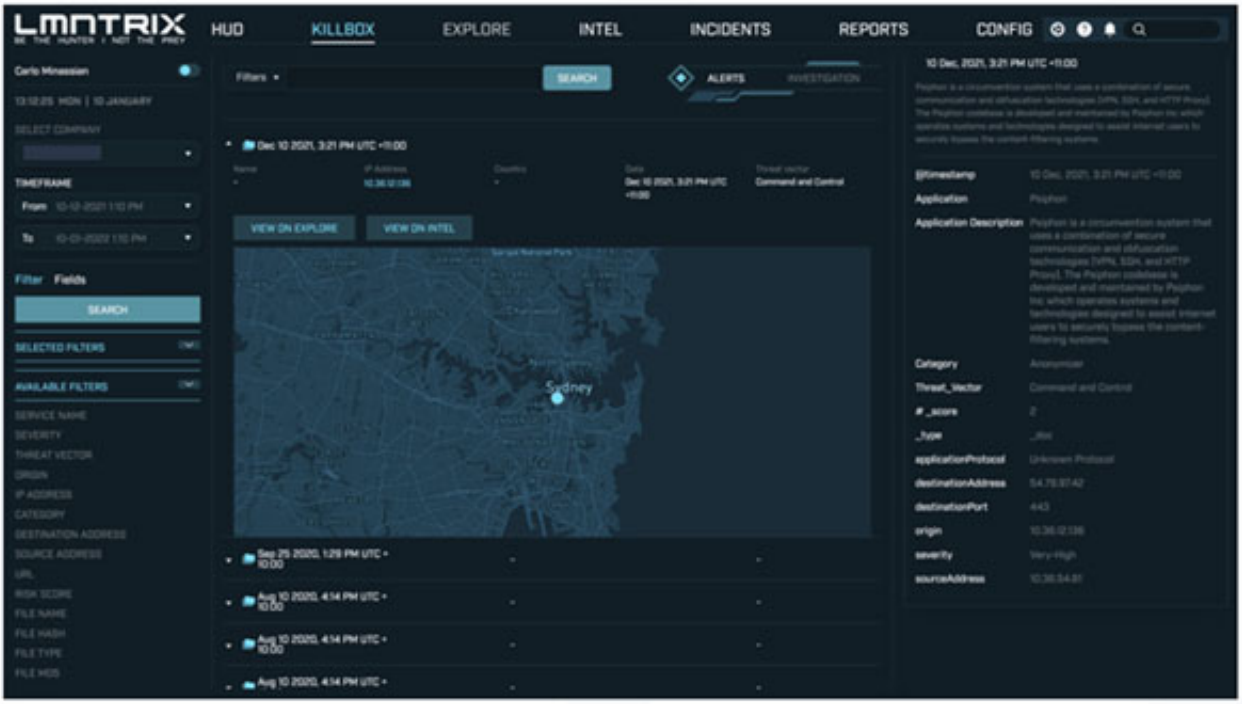
In the current threat environment, it's estimated that defenders have less than twenty minutes from the time of initial compromise to the attacker being able to alter records to hide their presence on a network. After this window closes, detecting activities attributable to an attack can be far more challenging. A sophisticated attacker can disguise their actions as normal user behavior, bypassing traditional network analysis techniques.

Automated threat detection processes offer the best opportunity of recognizing an attack during the initial stages, before the window of attack visibility closes. Automated processes will be presented with complex event information that drives decision-making. Strange events and anomalous behavior detected by machine learning processes deliver threat information derived from traffic analysis and data from perimeter defenses.

The process needs to distinguish between genuine threats and behavior due to changes to systems, users, or external resources. For example, threats may result from a malicious attack or be inadvertently created from system misconfiguration or service malfunction.

Traditional manual threat investigation processes consume significant resources to identify genuine threats amongst the noise of security alerts. In the face of overwhelming numbers of alerts, actual threats can be overlooked. Continuously alerting can lead analysts to assume that the warnings are false positives due to configuration issues or system faults. Capable attackers have the psychological knowledge to exploit weaknesses in analyst behavior to create false alerts and hide their actions.

NDR solutions following automated playbooks eliminate the time and resources required to analyze every alert. A thorough investigation of all alerts can enable the elimination of false alerts. The technique can identify and flag genuine attacks before the attacker has the chance to cover their tracks. Analysts, relieved of the burden of the initial alert investigation, can focus their efforts on resolving attacks.



PROACTIVE ANALYSIS

The network visibility available to NDR solutions enables the proactive analysis of an organization'si nformation systems real estate to identify weaknesses and vulnerabilities before exploitation.

One of the key capabilities of NDR solutions is the automated identification and classification of network assets, from endpoints to network-enabled sensors and firewalls to gateways. This feature enables NDR solutions to detect and react to changes, from a device going off-line to the connection of a new appliance. Processes can be initiated to respond to such changes, from beginning maintenance actions to raising a security alert depending on the nature of the detected change. This feature also allows automation of asset management processes as necessary.

The network asset register can, in turn, drive system risk assessments based on known vulnerabilities and weaknesses of assets based on their configuration status, patching state, and operating profile. As threat intelligence reveals new exploits, intelligent asset management can automatically highlight those vulnerable network assets to initiate a risk-based decision process to update, replace, or retain affected devices.

The information available from network asset registers can also be applied for attack simulation exercises, including blue-team and red-team analysis of the network. The results can help identify security gaps and exploitable weaknesses for further impact assessment and a cost-benefit analysis for remediation. In addition, this process enables a continuous proactive security improvement process that preempts attacks rather than relying on a reactive post-incident lesson learned approach.

RETROSPECTIVE ANALYSIS

NDR solutions' visibility across the entire infrastructure allows the extraction and analysis of network metadata to enable a retrospective analysis of past events to support behavioral analysis techniques. In addition, correlations between past and present can provide indications of abnormal events.

Shared threat intelligence can provide new insights into attack patterns that allow previously undetected abnormal events to be retrospectively identified. Thus, a previously undetected attack can be deduced, and a response initiated based on this examination of old data with new knowledge.

NDR solutions require access to complete metadata records extending back over significant periods. Records should include complete network metadata for all traffic, potentially a large volume of information but manageable. Typically records should also cover at least three months to accommodate typical dwell times for persistent threats. This places a manageable data retention requirement on systems. Alternative solutions relying on full package capture to provide the same visibility would be prohibitively expensive to implement. Realistically analyzing such a large data set can only be undertaken by the automated processes that NDR solutions offer.

The benefit of committing to storing this comprehensive set of records is the ability to use shared threat intelligence to identify novel persistent threats sophisticated enough to evade behavioral analysis.

INVESTIGATION

NDR solutions encompass the network analysis functions developed by NTA and NAV services to provide practical data analysis. Leveraging advances in data science that are implemented using advanced analytical methods allow efficient data analysis of the high volumes of available data.

The nature of behavioral analysis generated large volumes of indicators that require investigation to distinguish genuine threats from expected behaviors and abnormal events of a non-malicious cause. For example, software bugs, hardware failures, and legitimate user actions can create events requiring analysis. NDR provides the capability to analyze all incidents to identify those of malicious intent that need a response.

The key to efficient investigation is to present the analyst team with credible attack indicators supported with sufficient information for the alert to be triaged and a response initiated. Traditionally this required a detailed review of log files and other difficult to interpret data. NDR solutions present information in a clear and accessible format that can be quickly and efficiently interpreted, minimizing the chances of attacker actions being missed due to incomprehensible data.

Efficient resourcing and prompt response require intelligence to minimize the number of attack indicators miscategorized as false positive events and the false positives presented as confirmed attacks. Refinement of models should recognize this behavior going forward.

RESPONSE

A key advantage of NDR solutions over traditional perimeter security is the minimization of false-positive alerts. This benefit allows smaller, more agile security teams to focus on response activities to contain and eliminate threats quickly and efficiently.

The first phase of any response is containment and prevention. NDR can prevent attacks proceeding with automated protective measures including:

- Firewall actions
- Packet dropping
- Session dropping
- TCP resets
- Email quarantine
- URL filtering and page blocking
- IP blocking
- Compromised account disable

Then, where the attacker is seen to alter systems, automated system rollback or restoration of files can counter their actions.

The security team will have complete visibility of the automated response, focusing on assuring the response processes instead of manually performing the response actions. This automation allows significant savings in resource requirements while minimizing attacker dwell times.

Integration with a SOAR service can accelerate and automate security workflows using predefined playbooks. SOAR technology coordinates, execute and automates security response tasks across an organization's entire infrastructure. In addition, intelligence capabilities enable flexible and adaptable responses to meet complex multi-faceted attack profiles.

RECOVERY

A crucial part of incident recovery is the availability of information that supports efficient and informed decision-making by the security team. Precisely knowing what network components need to be isolated and restored and the impact of these actions on the network will minimize business impact during the recovery phase. NDR solutions provide this required information that can inform the business's incident recovery strategy.

NDR solutions also ensure that the security team has access to sufficiently detailed and easily accessible information for the thorough restoration of compromised systems to their pre-attack state. This will enable the security team to quickly restore business operations with confidence that the attacker leaves behind undetected vulnerabilities such as backdoor functionality or dormant malware.

Post-incident NDR operations on the recovered network will confirm that the malicious activity associated with the incident is no longer present on the network. Collected network data can also be compared to known normal pre-incident baselines to confirm proper network operations.

FORENSICS

Each attack on a network will leave traces of what actions the attacker took, what information was accessed, and if data was exfiltrated, what data was uploaded into the system. Post-incident analysis of these traces serves two purposes.

First, it enables faster response and recovery actions. Second, it supports forensic analysis for information gathering purposes. This gathered information provides intelligence on attacker behavior that is invaluable for the security community. It also allows the security team to identify any previously unknown weaknesses and vulnerabilities in their systems. Thirdly, the data gathered can be used to prosecute perpetrators should the affected organization launch civil or criminal proceedings if the attacker is identified and located in a cooperative legal jurisdiction.

The forensic analysis focuses on the aftermath of a security incident. In essence, it's a structured investigation that aims to determine exactly who did what and how. There are specific processes for collecting, preserving, and using evidence. NDR solutions support these with their comprehensive automated data capture and retention capabilities. The critical requirements for forensic information gathering are:

- Acquisition of evidence without altering or damaging the original data
- Authentication of recorded evidence as being identical to the original data
- Analysis of the data using techniques those guarantee not to modify the recovered evidence

Suppose the data captured by your NDR solution is to be used for civil or criminal actions, including internal disciplinary procedures in the case of an insider attack. In that case, the data-gathering processes must conform to these three critical requirements.

CLOUD

Monitoring network traffic in the cloud traditionally was problematic to be effective, with security solutions relying on deployment of agents and log monitoring to provide attack detection capability. NDR solutions have changed this by allowing virtual taps to collect and analyze manageable and scalable cloud-based network traffic.

Cloud service providers such as Microsoft Azure and Amazon Web Services (AWS) have robust security controls for their infrastructure. However, under the principles of the shared responsibility model, organizations that use cloud services are responsible for the security controls of their deployed systems. Estimates are that around 95% of security breaches in cloud-based systems are due to weaknesses in cloud customer security controls. Furthermore, where cloud services offer security controls as part of the service offering, these predominantly rely on log file analysis rather than the more comprehensive behavioral analysis offered by NDR solutions.

However, not all NDR solutions are fully effective across cloud-based environments. Therefore, the NDR must offer a cloud-native solution able to conduct cloud-scale machine learning for threat detection and response across multiple ecosystems, including on-premises and data center services, in addition to any cloud-based infrastructure. The solution must also be cloud-agnostic to support multi-cloud deployments and migrations.

COMPONENTS OF ENTERPRISE **NDR**

METADATA CAPTURE

Metadata is the fundamental building block upon which threat detection processes operate. Therefore, capturing and analyzing traffic across all network points is a key component of an effective NDR solution.

LMNTRIX NDR sensors should be deployed using network test access points (TAP) and port mirroring (SPAN) configurations to capture and analyze traffic. The coverage should include any network-connected industrial or manufacturing control systems, operational technology, IoT devices, and other network-enabled endpoints not covered by an EDR solution. Coverage is also required for all physical and cloud-based networks, on-premises, across data centers, or other locations.

The role of the LMNTRIX NDR sensors is to conduct deep network analysis by parsing all possible supported protocols and processes, including performing encrypted traffic analysis where possible. The collated information profiles devices, users, and applications autonomously while preserving network traffic for historical forensic analysis.

The key features for LMNTRIX NDR sensors include:

- Continuous monitoring of all devices, users, and applications.
- Behavioral learning that is based on past activities and current security knowledge to identify and profile all the devices, users, and applications.
- Behavioral and attribute classification to detect significant changes that can be recognized as resulting from abnormal events.
- Discovery, characterization, and tracking network relationships over time to create behavioral fingerprinting that can be used to detect potentially malicious actions.
- Using machine learning processes for behavioral profiling of all network-connected devices.
- Use of autonomous modeling to detect malicious intent based on known attacker tactics, techniques, and procedures.
- Available as a technology-agnostic solution, implemented as a lightweight network software sensor, deployed as a virtual machine (VM), docker image, or a physical LMNTRIX NDR Sensor.

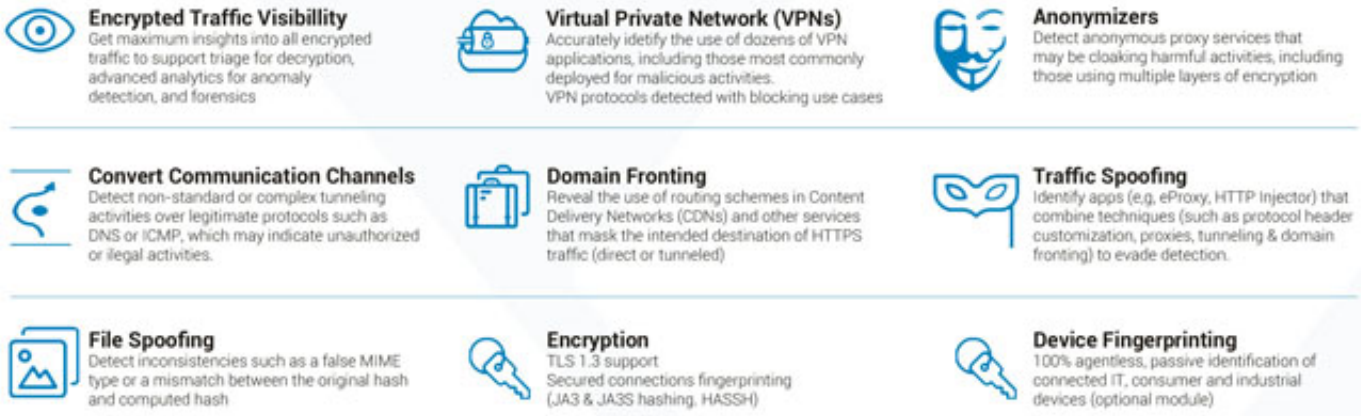


Figure 10 - LMNTRIX NDR Sensor Feature List

RETROSPECTION

The network activity data available from the LMNTRIX NDR sensors are used to uncover malicious intent using detection models. Advanced machine learning processes provide accurate alerting with minimum false positives than more simplistic anomaly detection techniques. In addition, an Adversarial Modeling capability uncovers the most complex and obfuscated attacker tactics, techniques, and procedures (TTP). Events of interest found across different entities, times, protocols, and attack stages merge into a single coherent picture of attacker activity.

Intelligence sharing across the security community allows participating organizations visibility of new TPPs when they emerge. Security best practice for organizations with a good security posture is to use the details of any emerging TPP to retrospectively examine network data records to see if this novel attack technique has been used against the organization without being recognized as an attack.

This capability can uncover previously undetected persistent threats to a network to contain the attack, followed by the response and recovery actions. No security solution is perfect 100% of the time. The resources available to nation-states will always mean they can invest time and resources uncovering weaknesses in security controls for exploitation. The ability to cross-check systems against emerging threats provides a mechanism to compensate for this inherent imperfection.

ANOMALY DETECTION

Anomaly detection capabilities should leverage machine learning techniques to analyze collected data and identify unusual or abnormal behaviors for further analysis. Autonomous network traffic analysis should identify, assess, and process threats, generating actionable intelligence for effective response.

Analysis techniques should use a building-block approach to express complex attack vectors, tactics, methods, and processes in a manageable and maintainable manner. In addition, examination of the abstract and inferred environment information, event-oriented activity records, low-level raw packets, and other collated information requires an unparalleled interactive language to implement effectively. Next, multi-dimensional modeling is needed to collate and integrate data, including protocols and behaviors across time. These features will enable automated detection at all stages of the kill chain. Finally, deep forensics and investigation automation will allow the analysis to deliver a quick and effective response.

THREAT HUNTING

Threat detection should be undertaken using a combination of techniques to ensure complete coverage and to maximize detection rates by reducing the probability those threats can remain hidden by exploiting weaknesses in each method.

- Signature-based detection to seek known threats integrated with threat intelligence
- Non-signature-based detections methods to seek novel threats
- Deep packet inspection using a protocol decoder

The extracted and analyzed activity data from LMNTRIX NDR sensors should integrate with an EDR solution to provide integrated threat detection. A combination of detection models will be needed to uncover malicious intent. Using an ensemble of machine learning approaches will avoid reliance on simplistic and noisy anomaly detection and unsupervised learning. In addition, an adversarial modeling capability will enable the most complex attacker tactics, techniques, and procedures to be uncovered.

IMPLEMENTING **NDR**

STRATEGY AND GOALS

The escalating sophistication and persistence of security threats mean that no single security solution will provide comprehensive protection. Traditionally security controls focus on prevention as the primary defense. As exemplified by the White House announcement in September 2021, the promotion of a Zero Trust philosophy is based on prevention to combat increasingly advanced and persistent security threats. The solution is a comprehensive, integrated approach that pulls together protection, detection, and response.

MITRE ATT&CK FRAMEWORK

SOC teams leverage the MITRE ATT&CK framework for analyzing attacks. The framework is built upon the categorization of attacks based on tactics and techniques. This approach results in a comprehensive matrix for each attack stage from initial access to exfiltration and impact. This framework has become the main driver for SOC teams when looking to detect an attackers' TTP.

Threat detection and response currently focus on endpoints and the network. While the NDR solution covers network threat detection, it does not eliminate the need for endpoint protection. Endpoint breaches are the primary mechanism for attackers seeking to obtain authentication credentials for lateral movement and privilege escalation. Implementing NDR in isolation will not provide a complete solution. It requires integration with other techniques to provide visibility across the entire infrastructure.

THE NDR/EDR/SIEM TRIAD

This approach is best seen in the SOC visibility triad. This is a network-centric approach to threat detection and response that maximizes threat visibility across an organization's entire operating environment. As the name suggests, there are three core elements whose goals are to detect, contain, investigate, and remediate threats.

- An EDR solution with agents deployed on all endpoints
- An NDR with visibility to all network data
- A SIEM solution with visibility to all log data

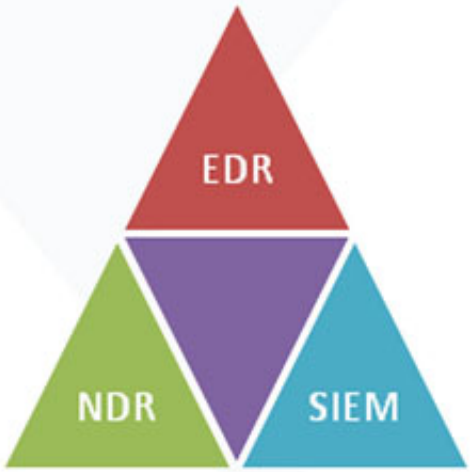


Figure 11 - SOC Visibility Triad

INTEGRATION BENEFITS

A fully integrated NDR/EDR/SIEM solution delivers significant benefits:

- Maximizes visibility of activity across network communications, endpoints, and events with access to all relevant data for behavioral analysis and threat detection
- Fast threat detection of anomalous behavior on endpoints and networks improves discovery with the EDR/SIEM rule and signature-based discovery supplemented with the NDR real-time behavioral discovery
- Enhance forensic capability from data-gathering capabilities for the NDR solution collecting network data packets, the EDR agents collecting usage and performance data, and the SIEM solution collecting logged event information

Automation for investigation, containment, and remediation processes using artificial intelligence techniques to provide fast threat detection and response with minimum security team resources

DEPLOYMENT **STRATEGY**

DEPLOYMENT PREPARATION

Successfully deploying NDR technology requires a clear definition of its objectives if it is to provide sufficient coverage to be effective. Then, the deployment can be implemented with the understanding of what the NDR solution is required to achieve and at which points on the network the traffic data needs to be collected and analyzed.

Objectives

The questions that need answering are:

- Where is the critical network traffic that an attacker will target?
- What are the ingress and egress points that an attacker would use?
- What user to Internet traffic must be monitored to detect an attacker's command and control connections, data exfiltration, or other interactions with the outside world? This can include the use of compromised systems for automated click fraud and botnet monetization.
- What user to data center traffic must be monitored to detect any reconnaissance, data acquisition, or exfiltration an attacker performs?
- What user to user traffic must be monitored to detect any reconnaissance, lateral movement, data acquisition, or exfiltration an attacker performs?
- What user to authentication server traffic must be monitored to detect brute force access attempts or lateral movement?
- What Dynamic Host Configuration Protocol (DHCP) traffic must be monitored to detect any surveillance performed by an attacker?
- What network traffic do I need to collect to provide a complete record of an attacker's actions?
- What network traffic do I need to collect to provide sufficient intelligence about an attack profile?

With the objectives of the network detection and response-based solution defined, the solution can be deployed.

DEPLOYMENT

Sensor Deployment

The location of physical and virtual network sensors determines what data is collected and what information is available to the NDR's behavioral analysis algorithms. Each endpoint and user on a network has a distinctive pattern of behavior that describes their normal operations. Sufficient information must be gathered to allow modeling of this behavior for every endpoint and user to ensure complete coverage for protective systems.

- Physical LMNTRIX NDR Sensors use port mirroring and network tap techniques to provide monitoring capabilities on physical infrastructure. Coverage requirements will govern their location, and peak packet transmission rates will drive the number needed. Network placement of the SPAN and TAP points across a network is critical to ensure sufficient coverage of network traffic to detect attacks of all phases quickly and efficiently.

- Virtual sensors in the form of lightweight agents provide metadata capture capabilities for virtual infrastructure.

- Cloud sensors in the form of lightweight agents provide full packet capture capabilities for cloud-based infrastructure and for situations where access is unavailable for the placement of physical LMNTRIX NDR sensors.

- Application sensors provide connection monitoring for third-party Security-as-a-Service (SaaS) solutions outside the reach of other sensor types.

Caution should be observed when implementing port mirroring due to the additional loading on switching devices that can adversely impact network performance and affect business services. Capacity planning and loading assessments are a necessary part of the planning process for LMNTRIX NDR sensor deployment planning.

Data Capture

Different segments of the network provide access to the different traffic types considered by the objectives of the deployment. Monitoring points should be placed at strategic locations across the internal network within the perimeter controls to collect as a minimum:

- DNS resolution traffic
- Authentication traffic
- Direct traffic to and from the Internet
- Indirect traffic to and from the Internet via a proxy or sequence of proxies
- DHCP traffic
- Internal traffic to server application services, including file services, print servers, web portals, and others handling sensitive information

- Traffic to and from cloud-based systems and services
- Traffic between internal endpoints

Deployment Example – Single-Point

Single-point monitoring can provide the necessary coverage for simple topographies where all communications pass through a central network device. For example, where clients, DHCP, and proxy servers exist on separate subnets, the common switch provides a single capture point for all traffic.

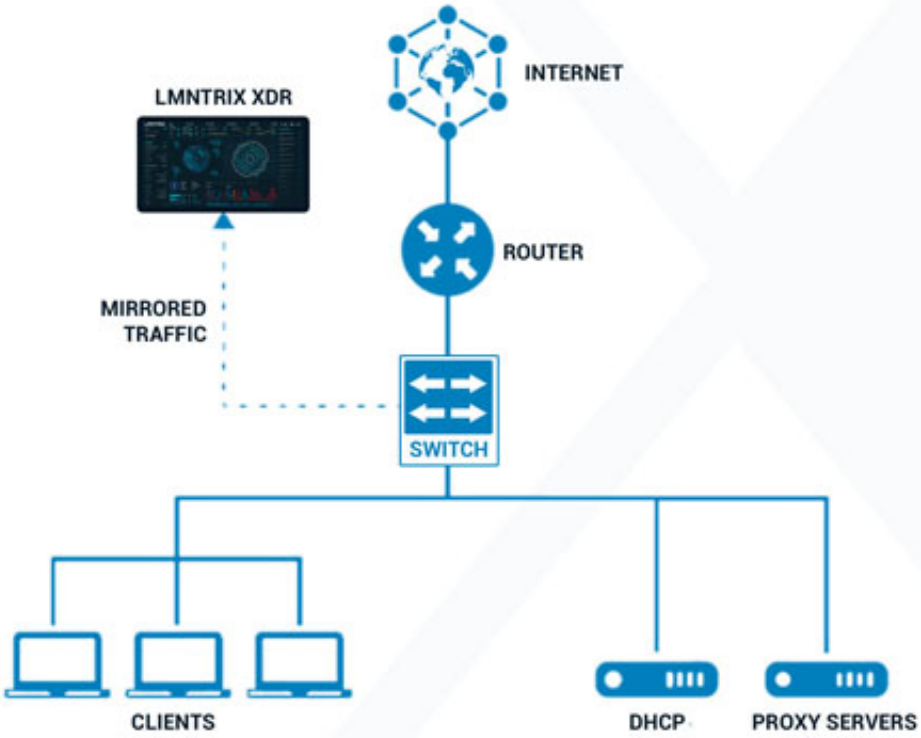


Figure 12 - Single-Point NDR Deployment

Deployment Example – Split Route

For topographies where split routing techniques are used, particularly for load balancing and redundancy, communications may pass through multiple devices. Therefore, capturing all network traffic will require monitoring at multiple capture points to provide full coverage

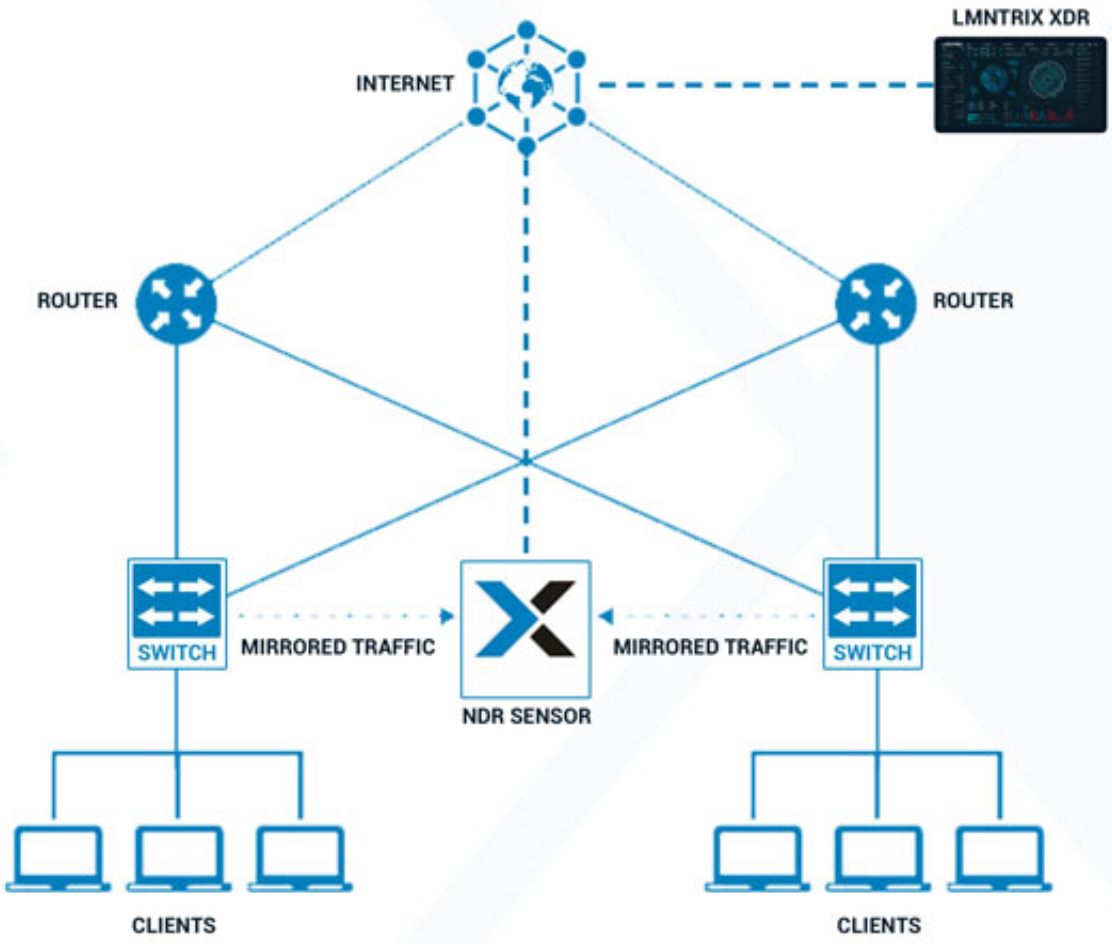


Figure 13 - Multiple-Point NDR Deployment

Deployment Example – Hierarchical

The following network topology provides an indication of the factors that are considered when deploying an NDR solution on networks with hierarchical topologies. In this example, multiple access switches link to a core switch.

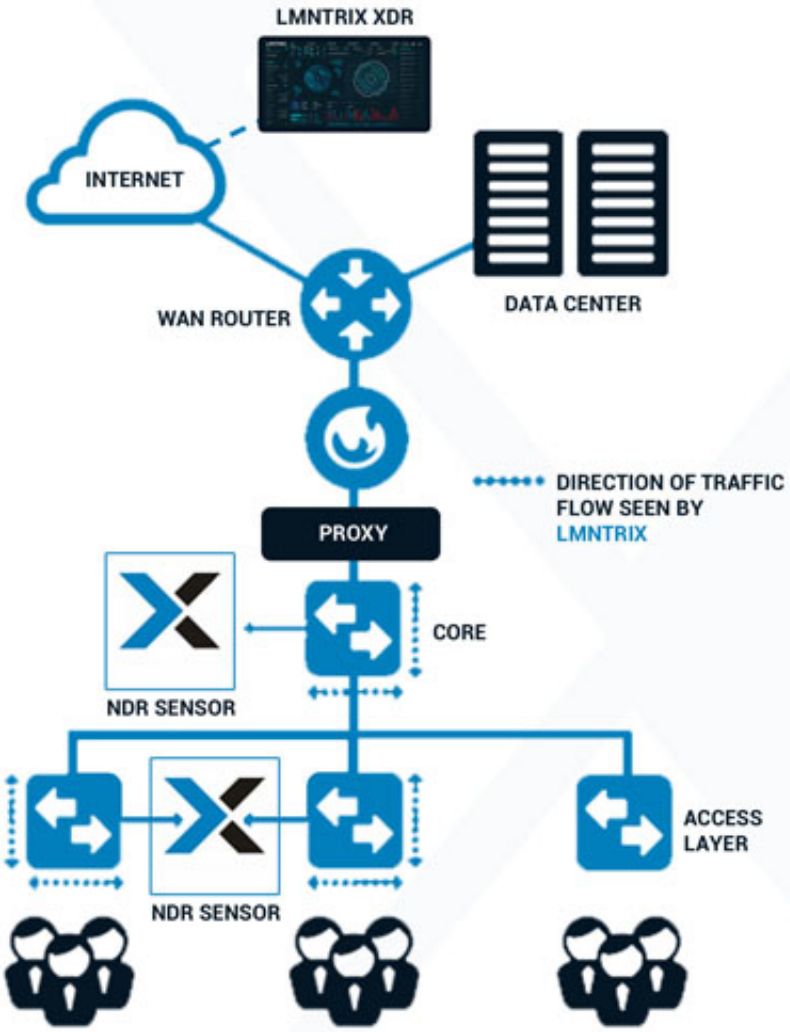


Figure 14 - Hierarchical NDR Deployment

In this example, monitoring at the core switch will allow access to:

- All user-to-server network traffic
- All endpoint-to-server network traffic
- All user-to-user network traffic that crosses the switch
- All user-to-endpoint network traffic that crosses the switch
- All endpoint-to-endpoint network traffic that crosses the switch
- All user-to-Internet network traffic
- All endpoint-to-Internet network traffic

Monitoring at the core switch will not provide visibility to network traffic within access groups that do not cross the core switch.

Monitoring at an access switch as shown will allow access to:

- User-to-Internet network traffic for those users connected to the access switch
- Endpoint-to-Internet network traffic for those endpoints connected to the access switch
- All user-to-user network traffic within the switch
- All user-to-endpoint network traffic within the switch
- All endpoint-to-endpoint network traffic within the switch
- User-to-server network traffic for those users connected to the access switch
- Endpoint-to-server network traffic for those endpoints connected to the access switch

Monitoring at each access switch will provide visibility to all network traffic within and between access groups. However, network traffic cross between access groups will be duplicated in the packet capture leading to additional resource usage for storage and processing.

It should be noted that every network is unique and will require specialist advice to ensure complete coverage according to the deployment objectives.

Data Center Deployment

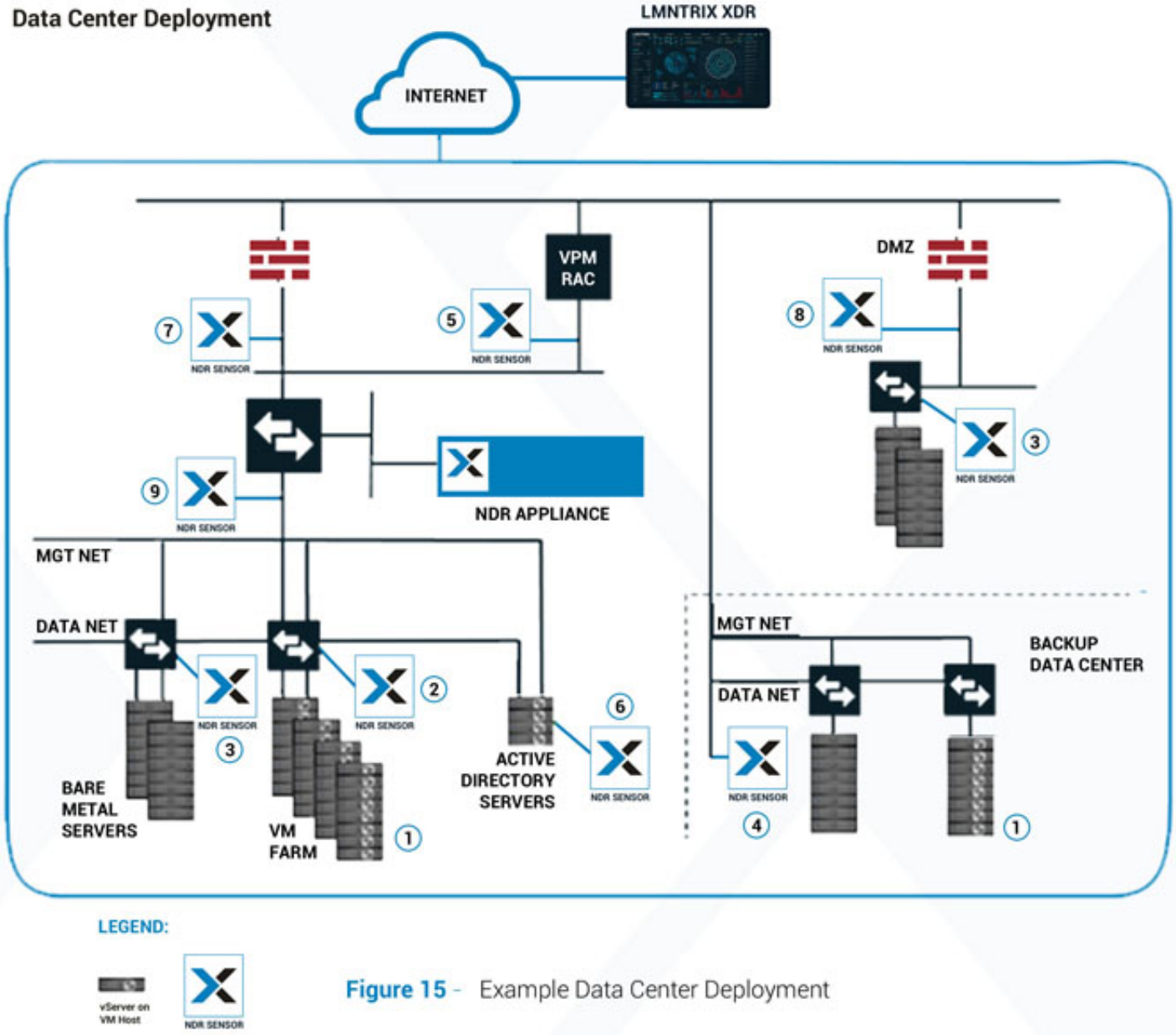


Figure 15 - Example Data Center Deployment

Virtual private network (VPN) hosts provide a valuable point of ingress for capable attackers looking to gain remote access to a system. Monitoring at Remote Access Concentrators (RAC) will provide visibility of all remote connections. Authentication server monitoring is also a key component of attack detection.

Monitoring within the Data Center (DC) Host perimeter defenses will provide detection capabilities for command and control communications with compromised endpoints and attempts to exfiltrate data. LMNTRIX NDR sensors should be positioned at all ingress and egress points along the perimeter to provide the required coverage.

Where a DC includes a demilitarized zone (DMZ) to provide additional access controls for external communications, further monitoring of traffic will be necessary between the perimeter defenses of the DC Host and perimeter defenses of the DMZ. This positioning provides monitoring capabilities for services and endpoints within the DMZ, including Simple Mail Transfer Protocol (SMTP) gateways and web servers.

Management subnets are often used to manage infrastructure separately from the information systems. Therefore, supervisory systems' configuration, management, and monitoring on the management subnet are attractive targets for advanced persistent threats and require NDR coverage.

The recommended deployment locations for LMNTRIX NDR sensors are:

- Hypervisor virtual switch monitoring using a virtual sensor provides visibility of all virtual machines, intra-hypervisor connections, and DC Host traffic.
- Virtual machine switch monitoring using a physical sensor provides visibility of all virtual machine traffic crossing the physical host and DC Host traffic boundary.
- Server switch monitoring using a physical sensor provides visibility of all server traffic crossing the physical host and DC Host traffic boundary.
- External DC traffic monitoring using a physical or virtual sensor provides visibility of all traffic to other DCs, including backup and recovery sites.
- Remote access VPN monitoring using a physical or virtual sensor provides visibility of all remote user access to DC Host.
- Authentication server monitoring using a physical or virtual sensor provides visibility of all authentication connections for the DC Host.
- Perimeter firewall monitoring using a physical or virtual sensor provides visibility of all DC Host to Internet traffic.
- DMZ border monitoring using a physical or virtual sensor provides visibility of all DC Host to DMZ traffic. Management subnet monitoring using a physical or virtual sensor provides visibility of all traffic to infrastructure equipment.

In this example data center deployment, monitoring will allow access to:

- DC Host to Internet traffic
- DC Host to DC Host traffic
- DC Host to/from User/Endpoint/VPN traffic
- DC Host to/from DMZ Host traffic
- DC Host/Users/Endpoints to Authentication Server traffic

Azure Deployment

Deployment in an Azure environment can be achieved using a virtual NDR sensor to monitor the Infrastructure-as-a-Service (IaaS) environment. These sensors collect data from Microsoft virtual network taps (VTAP) or compatible third-party packet brokers.

AWS Deployment

Deployment in an AWS environment can be achieved using a virtual NDR sensor to monitor the IaaS environment. Virtual sensors collect data from Amazon VPC traffic mirroring using an Amazon elastic network interface or compatible third-party packet broker.

One thing to watch is that actionable alerts need to be tied to the host being monitored. By default, mirroring is connected to a generic host identity. Therefore, the monitoring will require configuration to ensure the correct host identity is extracted and available.

GCP Deployment

Deploying virtual sensors in a Google Cloud Platform (GCP) environment is implemented using sensor templates that define the sensor's executable image and Google's command-line tool to facilitate deployment. GCP sensors collect data from GCP packet mirroring or compatible third-party packet brokers.

GCP packet mirroring is a native function that provides traffic cloning for analysis purposes. This mirroring is restricted to traffic on virtual machines rather than the network and can have a performance impact on the monitored virtual machines.

The solution will require an RSA SSH key pair to provide the LMNTRIX NDR solution with authenticated access to the sensors.

Cognito Stream Deployment

Cognito streams provide visibility of data stored in Amazon Cognito by providing security-enriched network metadata that can be imported directly into the NDR solution. The stream is deployed as a virtual machine on a hypervisor or IaaS cloud. The stream uses standard TCP protocols using SSH or HTTPS for both data extraction and monitoring purposes.

Cognito stream is available for Azure, AWS, and GCP deployment or using VMware, Hyper-V, KVM, or vCenter/vSphere via the command line.

High data throughput puts constraints on processing requirements and any use of data storage which needs to be considered part of deployment planning.

CONFIGURATION

Before the NDR solution is deployed, it will require configuration to ensure necessary coverage, including:

- IP addresses, network masks, and default gateways for the NDR solution
- DNS server addresses for domain name resolution
- NTP server hostnames or IP addresses for event synchronization
- SMTP server hostnames or IP addresses for alerting
- Syslog server hostname or IP address for alerting
- Public IP addresses for NDR monitoring
- Firewall rules for NDR monitoring

These details are captured during service onboarding in a Starter Pack that is used by the LMNTRIX CDC to pre-configure sensors ready for deployment by clients in their respective networks. In addition, deployed SPAN and TAP devices require configuration to integrate with the NDR service. The purpose of the SPAN is to copy traffic from a port or VLAN to another port that the NDR service accesses to perform the required network monitoring.

Switches may impose limits on SPAN ports that need to be observed to avoid dropped packets due to oversubscription, compromising NDR coverage. Therefore, TAP devices should be considered if a switch cannot support the required SPAN usage.

All traffic monitoring must be bidirectional, either using a single port capturing transmitted and received packets or two ports to capture traffic in each direction separately. The capture of bidirectional traffic is preferable to prevent duplication of recorded traffic that can negatively impact processing and storage requirements for captured packets and switch loading. This point also applies to VLAN monitoring.

MONITORING

An implemented and deployed NDR solution provides the means for detecting in-network threats to inform the response and recovery processes and allow post-incident forensic analysis and threat intelligence gathering. The implemented solution will therefore need to record the information necessary to achieve these goals.

The monitoring requirements form part of maintaining the NDR solution and ensuring it provides the required coverage. In addition, operational experience and post-incident lesson learned exercises would allow the placement of SPAN and TAP to be refined as part of the standard improvement processes.

MEASURING

NDR solutions provide a mechanism to measure the effectiveness of perimeter security controls for crucial performance indications and metrics generation. For example, the efficacy and reliability of existing security controls can be quantified using information gathered from tracing an attacker's ingress path and actions. The results from this stage can both drive perimeter control improvements and refine the incident response playbooks as part of the continuous improvement process.

IMPORTANCE OF **NDR** FOR **SECURITY INVESTIGATIONS**

OVERVIEW

Detection of a security incident requires rapid investigation if the threat is to be contained and removed. Studies reveal that the time between an attack being detected and the attacker disguising the attack as an indistinguishable event is measured in minutes. Failure to react quickly is the difference between stopping an attack and allowing a persistent threat to become established within a network. Here, they can monitor normal behavior for that organization and emulate this to remain hidden for dwell times that can be measured in months.

Automated prevention processes provide the ability to halt and rectify attacks for most cases, but this approach is not always possible. For example, a novel threat may not have a response playbook defined that will resolve it automatically. Or the nature of the attack may mean that automated containment may result in disabling or isolating business-critical systems or services that may cause more significant disruption than if the attack is allowed to proceed in the short term. In these cases, investigation rather than reaction is the more appropriate response.

INVESTIGATION PLAYBOOKS

Playbooks play a crucial role in automating the investigation process, collating, and presenting evidence for the security team to evaluate. This enables the team to focus their efforts on their value-added contribution to the investigation, namely the informed decision-making processes.

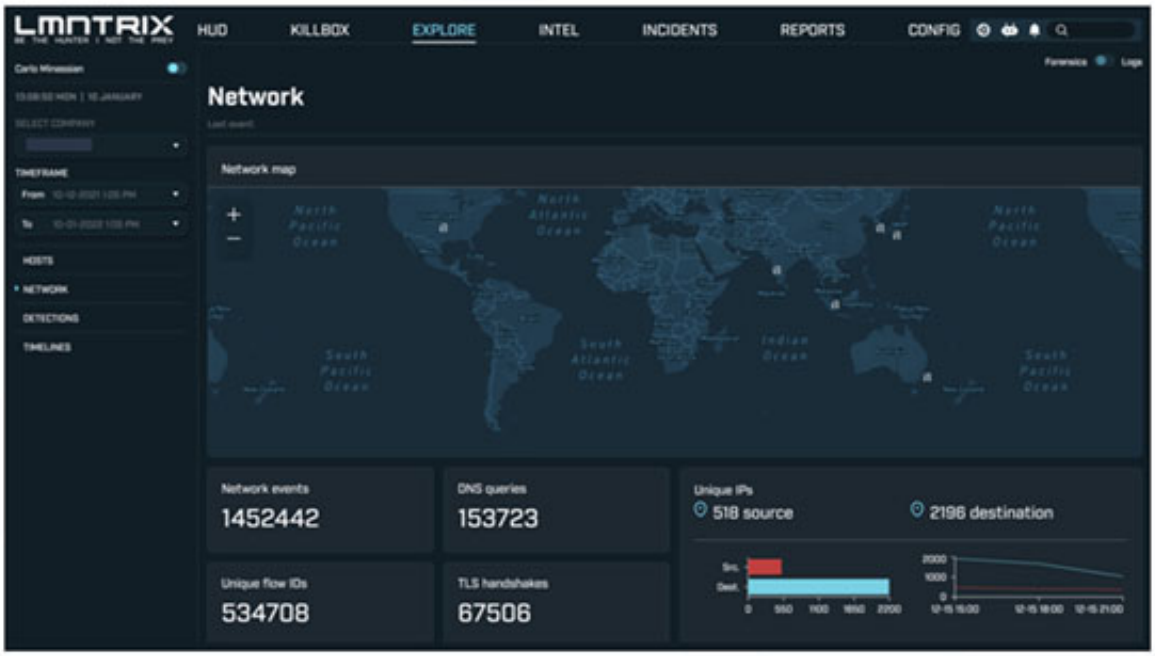
The detection of abnormal behavior initiates the investigation playbooks. Machine learning processes using artificial intelligence methodologies offer details of possible attacks, with the supporting evidence for each event. Often, abnormal behavior can be attributed to legitimate changes in services or users or inadvertent changes such as configuration errors or equipment failures. Intelligent investigation processes can filter out most issues. Behavioral models can be updated to reflect the levitate changes. Maintenance requests can be generated to resolve errors and failures. This leaves the subset of events that are either unexplained or probably an attack.

NDR SOLUTIONS

The benefit of NDR solutions is their visibility of all vital network information that enables thorough behavioral analysis and advanced threat detection. The downside for post-event investigations is the vast volume of data that an analyst may potentially need to sift through to uncover the actual cause of the detected event.

A typical investigation will require analysis of relevant network traffic as well as information from endpoints. In addition, data from perimeter defenses, including firewalls and intrusion prevention systems, need to be gathered and correlated against network traffic. Add in event logs and other data from security controls, and the volume of data quickly becomes impractical for manual interrogation practices.

However, the automation that NDR solutions bring to the correlation of data and identification of abnormal events can also be leveraged for investigations, speeding up the investigation process by identifying and presenting the critical data of interest.



INVESTIGATION BENEFITS

The automated collection and correlation of large volumes of data into manageable packages of single event-related contextual information dramatically speed up investigation times. Automated processes and workflows enable the security team to validate, triage, and investigate events quickly and effortlessly using a single interface that provides all the supporting information they require in an easy-to-access form.

Where the event's cause is an attack, this has direct benefits in reducing the attacker's dwell time and limiting the harm they can inflict on the compromised system before response and recovery processes remove the threat.

If the event's cause is an error or failure, detailed information can pinpoint the cause and recommend the best remediation. Fast identification and resolution reduce the period of potential business disruption and can reduce the effort needed to manage the IT infrastructure. Identifying and resolving configuration issues will also enhance the robustness of the organization's security by finding and fixing weaknesses before they are exploited. As a side effect, maintaining robust systems will help support security compliance and governance processes.

LEVERAGING NETWORK TELEMETRY FOR FORENSICS

CORE CONCEPTS

Network telemetry offers comprehensive detection capabilities that collect, trend, and correlate observed network activity for diagnostic and security monitoring purposes. In addition, forensic analysis of network telemetry can be instrumental in investigating network leakage, data exfiltration, and abnormal network traffic.

For some organizations, regulatory and legislative requirements necessitate systems that support forensic capabilities. For example, forensic analysis for post-incident investigations relies on information gathered from endpoint and network logs. The logs from network telemetry are essential to provide a complete picture, covering agentless information gathering where endpoint agents cannot be deployed and adding additional context to the endpoint logs.

Whether cloud-based or physical, remote or on-premises, comprehensive network telemetry is vital for effective forensic discovery and investigation activities. However, ensuring that sufficient data is captured and retained for adequate periods to allow practical analysis is challenging. In addition, the integrity of the data must be assured to prevent an attack altering data to hide its actions.

However, capturing and securely storing network telemetry is only part of the challenge. The organization must also retrieve and correlate the data as part of investigations quickly and painlessly. Automated processes that facilitate information retrieval and analysis will significantly reduce resource requirements while ensuring results are available sufficiently fast to contain any ongoing attack, remediate any compromised systems, and resolve exploited vulnerabilities.

LOGGING

A fundamental requirement for all network telemetry logging is to establish a coherent date and time source to ensure that every event uses a consistent temporal marker to correlate events in different locations correctly. Any inaccuracy or inconsistency will render the data unsuitable for forensic analysis. Therefore, access to an authenticated Network Time Protocol (NTP) is essential.

Local device statistics provide the most basic telemetry providing throughput and bandwidth statistics for each interface and protocol-based traffic statistics. In addition, device-based monitoring such as processor loading and memory usage can support this monitoring to provide a rough indication of possible abnormal behavior.

Network log files provide invaluable information about network activities, including events associated with Internet Protocol (IP) addresses, Transmission Control Protocol (TCP) traffic, and Domain Name Services (DNS). This allows investigations to trace the source and destination pairs to recognize suspicious traffic amongst legitimate messages. Network telemetry logs also cover the range of message types, including the following.

- Connection Logs record each connection to a network, detailing the ports, protocols, connection start and end times, IP address, and the packet count for each.
- Simple Network Management Protocol (SNMP) logs record information detailing the status of managed devices on IP networks.
- Hypertext Transfer Protocol (HTTP) logs record transactional details for all HTTP traffic, including connection information, request methods, header information, mime types, and Uniform Resource Locator (URL).
- Secure Shell (SSH) logs record transactional details for all SSH traffic, including connection information, authentication information, along with all inbound, outbound, lateral, and failed movements.
- Secure Sockets Layer (SSL) logs record transactional details for all SSL traffic, including connection information, encryption and certificate information, and server name indication (SNI).

In addition to higher-level traffic logging, packet capture can provide definitive information. Still, the volume of data involved typically limits this option for investigating a specific event at limited points on a network. Typically packet capture is limited to bidirectional traffic recorded at key topological points such as switch meshes and distribution gateways. In complex topographies, care is required to prevent duplicate package capture overwhelming storage and processing capabilities.

An issue to bear in mind with routine full packet capture is that the stored data is an attractive target for attackers. Therefore, protecting this information from unauthorized access itself creates an additional security burden.

ANALYSIS

Forensic analysis of network telemetry is challenged by the large data volumes from which abnormal instances must be identified and the data's volatility. In addition, copies of data flows are needed to provide a static image upon which retrospective analysis can be performed. This contributes to the enormous volumes of data that must be collected, stored, and assessed.

NDR solutions automate the correlation of data and identification of abnormal events for investigation, speeding up forensic analysis by focusing on the data of interest.

Network forensic analysis can identify suspicious traffic patterns, including behavioral patterns indicative of attempted breaches and malware infection. Additionally, real-time monitoring with historical records analysis can identify ongoing attacks while still in the reconnaissance phase and trace the attacker's actions back to the initial breach event.

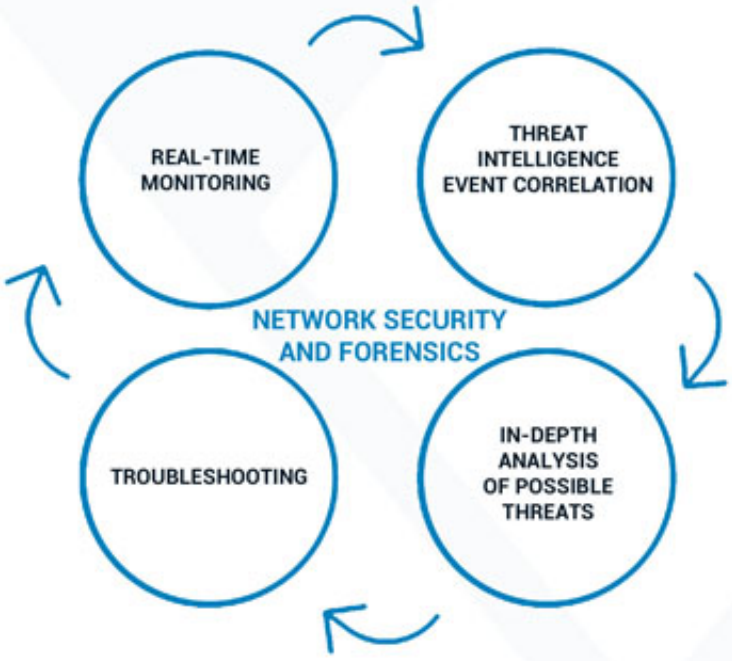


Figure 16 - Network Security and Forensics

Network forensic analysis can also be beneficial in monitoring the availability and performance of services for optimization or diagnostic purposes.

NDR CASE STUDIES

SOLARWINDS CASE STUDY

Introduction

The American IT services company SolarWinds Inc specializes in producing IT infrastructure and network management solutions. Their Orion Network Management System (NMS) is a centralized performance monitoring and network administration solution. It is designed to oversee and maintain networks, including configuration management, installing software updates, and deploying critical security patches.

In December 2020, the SolarWinds Orion product was found to have been infected with malicious code, with the infection originating around March of that year. Subsequent investigations deduced that the state-backed attackers responsible would have required a significant dwell time before this initial infection for their actions to have evaded the security controls in place.

The attack's complex nature resulted in undetected propagation of the attack to the clients of SolarWinds Inc, causing one of the most damaging supply chain cyber-attacks to date.

Terminology

Several different labels describe the SolarWinds attack, SUNBURST, SUPERNOVA, SUNSPOT, TEARDROP, and RAINDROP.

The state-sponsored actors that successfully attacked the SolarWinds systems and inserted malicious code into the Orion product used a process labeled SUNBURST. This process created a vulnerability that the attackers could exploit once the infected Orion software was installed on customer systems.

The SUNBURST vulnerability was then used to download malware code labeled SUPERNOVA onto infected systems. The process for injecting the SUNBURST backdoor during the Orion Platform build process is marked as SUNSPOT.

The SUNBURST vulnerability uses malware loaders labeled TEARDROP and RAINDROP as part of its operation.

Attack Profile

The attack started when sophisticated state-backed actors gained access to the SolarWinds systems. They achieved this in a manner that allowed their presence to remain undetected while enabling them to access the update servers. This allowed them to add malicious code into the software that the Orion product pulled down into the client's systems as part of the update process. The clever part was that this malicious code remained inactive while the update software was verified on development systems. It only became active once it was deployed into a production environment.

Once operational, the malicious code would then communicate back to the attacker's systems to download additional resources to give the attackers control over the infected systems. Communications were routed through IP addresses located in the victim's own country to reduce the chance of detection. This was implemented as a multi-layer attack using a range of different attack vectors to maximize the probability of success when attacking robustly protected networks. The key to success was exploiting successful infections without detection, allowing the malware to spread and extract as much information as possible.

The malicious code exploited the software patching mechanism as the attack vector. This allowed the code to automatically access a process with the highest privileges and the most significant reach in the affected networks.

Detailed Analysis

The malicious code was inserted in the SolarWinds.Orion.Core.BusinessLayer.dll plugin component of the SolarWinds Orion software. The code contained a backdoor function that used HTTP to communicate with attacker-controlled servers. This code was sufficiently obfuscated to avoid detection. After an initial dormancy period and verifying that the code was on a live network by checking for server connectivity, the code became active. It accessed the remote servers to download commands to fulfill a range of functions. These included identifying anti-virus and forensic tools, disabling system services, profiling the infected system, transferring data, and executing files. These functions were designed to mimic legitimate operations performed by the SolarWinds Orion software to avoid detection. Of particular use was the Orion Improvement Program (OIP) protocol that collects evaluation, performance, and usage data from users. It does this to enable SolarWinds to monitor software performance and aid fault diagnostic processes. The SUNBURST malware collected data and reported it back to its servers by emulating this protocol without raising suspicions.

Another technique employed was to hijack a legitimate process and replace the functionality of the standard operating system process with a malware function, executing the malware and then replacing the malware code with the original legitimate code. Again, this prevented any forensic analysis from identifying that the malware code has been run, with log files only recording the legitimate code's execution.

The benefit of using an NDR solution is this behavior would be recognized as unusual and flagged for investigation. Network records would identify both the occurrence of a code switch and provide sufficient detail to enable forensic analysis of the malicious code to determine what actions it had performed.

Discovering the Breach

The breach was uncovered when the US cybersecurity company FireEye identified that its systems had been breached and traced the attack vector back to the SolarWinds Orion product. They dubbed the malware SUNBURST and produced a set of signatures to enable organizations to scan their systems to determine if they had been infected. This set off a chain of events where thousands of Orion product users were alerted to the breach.

It was estimated that around 18,000 out of the 33,000 SolarWinds Orion users had installed the infected software, representing approximately 6% of the total SolarWinds customer base.

Most infected users were non-governmental organizations. However, this customer base included organizations across the US that handles some of the most sensitive national security information, including:

- The Office of the President of the United States
- The National Security Agency (NSA)
- The Pentagon and all five branches of the Military
- The State Department
- The Department of Homeland Security
- The Department of Justice
- The Federal Reserve
- The National Aeronautics and Space Administration (NASA)
- Major US telecommunications companies

Overall, it is estimated that more than 250 US federal agencies were affected by the security breach. It also affected governmental organizations worldwide and critical worldwide corporations, including Microsoft, Cisco, Intel, Visa, and AT&T.

Evidence suggests that the Russian Foreign Intelligence Service operating under the guise of Advanced Persistent Threat group 29 (APT29), also known by the slang name "Cozy Bear," was responsible.

The main concern was how the malware could be present in many supposedly secure systems for around nine months without detection. If the specialized cybersecurity firm FireEye hadn't been one of those companies, would the infection have been detected?

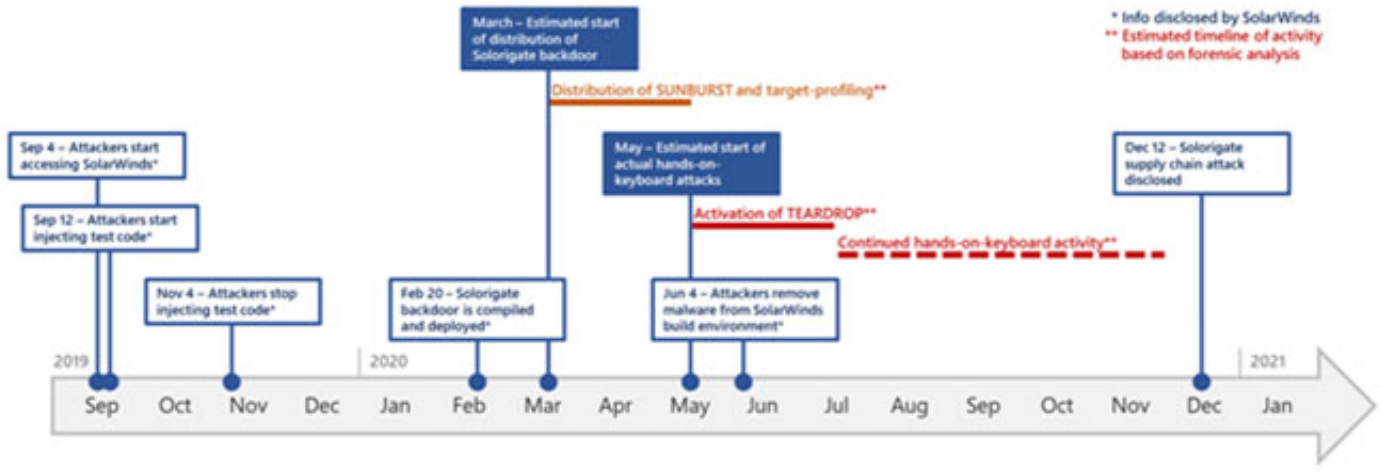


Figure 17 - SolarWinds Attack Timeline

Recovery

Tools were created to scan systems to look for Indicators of Compromise (IoCs). These include events recorded within log files, registry entries, and malware and backdoor code signatures. The tool uses passive monitoring and interrogation techniques, generating data that can be imported into a SIEM tool or similar application. The data can then be subject to further processing, investigation, and actions.

Detail investigation into the SUNBURST vulnerability and SUPERNOVA malware code has identified a range of markers and events of interest that reveal that infection has occurred. These include known observable indicators of lateral movement and certificate pull events. Lateral movement is a technique attackers use to move across systems and networks, gain privileges, and avoid detection. Certificate pulls allow an attacker to obtain authorized access to systems using digital certificates.

While the SUNBURST vulnerability is now known and understood, CISA has evidence of additional initial access vectors other than the SolarWinds Orion platform. However, these are still being investigated.

CISA has issued detailed guidance for detecting advanced persistent threat activity from known tactics, techniques, and procedures. The attacker has been observed where infected systems have been exploited to use the SUNBURST vulnerability to move laterally across multiple other systems, including Microsoft cloud environments. Additionally, they have employed difficult-to-detect persistence mechanisms that have targeted Microsoft Azure Active Directory and Microsoft 365 environments.

MS EXCHANGE CASE STUDY

Introduction

In early 2020, a patch was issued for a critical vulnerability in the popular and widely used Microsoft Exchange Server. Exploitation would allow an attacker to compromise corporate mailbox servers, launch phishing campaigns from inside the system boundaries, or act as an entry point for lateral movement across the affected network.

The vulnerability affecting all versions of the exchange server application meant that an attacker could carry out remote code execution by exploiting a .NET serialization vulnerability that existed on the Exchange Control Panel (ECP) web page.

Initially, Microsoft reported the vulnerability as being due to memory corruption, exploited when an email is received with specifically crafted content to cause the error. However, it was due to the incorrect creation of cryptographic keys during installation, affecting all clients. It was also initially reported that there were no credible reports of exploitation of this flaw in cryptographic protection.

Detailed Analysis

A code error causes the vulnerability in the ECP component that causes all installations to use identical validation and decryption keys instead of each using randomly generated keys. The keys are stored in the web.config file and are used to secure server-side data that ASP.NET web applications hold in serialized format on the client. The client sends this data back to the server via the __VIEWSTATE request parameter.

```
<system.web>
  <machineKey validationKey="CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF"
decryptionKey="E9D2490BD0075B51D1BA5288514514AF" validation="SHA1"
decryption="3DES" />
  <!--
```

Figure 18 - Microsoft Exchange Static Keys

As these keys are both static and publicly disclosed, an authenticated attacker can create ViewState data that will be accepted and deserialized by the server.

- Authentication with the exchange server can be achieved using a POST /owa/auth.owa request with a valid username and password
- The attacker needs the ViewStateUserKey and the __VIEWSTATEGENERATOR values from the authenticated session to exploit this vulnerability. A request to the /ecp/default.aspx page will return these values
- The __VIEWSTATEGENERATOR value for the authenticated session is stored in a hidden field, accessible using a browser's standard developer tools.
- The ViewStateUserKey can be readily obtained from the ASP.NET _SessionID cookie.
- The data obtained from parsing __VIEWSTATEGNERATOR will allow the attacker to craft a serialized payload containing malicious code
- The attacker then simply sends the serialized payload back to /ecp/default.aspx

These steps trick the YSoSerial.net module into executing the code as part of the Exchange Control Panel web application. The Windows Internet Information Services (IIS) worker process w3wp.exe will spawn the malicious code. As this code executes with SYSTEM privileges, the attacker now has complete access to the server.

As the affected validation key is statically defined in web.config, this exploit can be used for all the following webpages:

- /ecp/default.aspx
- /ecp/PersonalSettings/HomePage.aspx
- /ecp/PersonalSettings/HomePage.aspx4E
- /ecp/Organize/AutomaticReplies.slab
- /ecp/RulesEditor/InboxRules.slab

- /ecp/Organize/DeliveryReports.slab
- /ecp/MyGroups/PersonalGroups.aspx
- /ecp/MyGroups/ViewDistributionGroup.aspx
- /ecp/Customize/Messaging.aspx
- /ecp/Customize/General.aspx
- /ecp/Customize/Calendar.aspx
- /ecp/Customize/SentItems.aspx
- /ecp/PersonalSettings/Password.aspx
- /ecp/SMS/TextMessaging.slab
- /ecp/TroubleShooting/MobileDevices.slab
- /ecp/Customize/Regional.aspx
- /ecp/MyGroups/SearchAllGroups.slab
- /ecp/Security/BlockOrAllow.aspx

Exploitation

The vulnerability is a post-authentication flaw requiring the attacker to access an email account on the exchange server using valid credentials. However, a competent attacker can successfully gain credentials using social engineering techniques such as spear-phishing or password guessing techniques such as password spraying and credential stuffing.

Researchers claim that exploits for the vulnerability were not seen before the patch release on 11 February 2020. However, this vulnerability was present on the internet-facing Microsoft Exchange Server application in everyday use across governmental and commercial organizations. Nation-states employ technical specialists to examine such applications for zero-day exploits. The nature of the flaw suggests it would have been reasonably apparent to a capable specialist to identify. It cannot be ruled out that an advanced persistent threat would have known of the flaw and been able to exploit it without leaving evidence.

By 25 February, documentation on exploitation was publicly available, and evidence was seen that attackers were attempting to leverage the vulnerability in unpatched systems. Proof of Concept code that could scan for vulnerable servers and initiate an attack was seen shortly afterward, and by early March, a Metasploit module was publicly available.

A vital element of the vulnerability was that exploitation would provide an attacker with rapid lateral movement, making exploitation attractive to organized and sophisticated attackers, including nation-states and ransomware-as-a-service providers. In March 2020, security agencies released reports of nation-state actors using the vulnerability to deploy backdoors for continued access and execute in-memory post-exploitation frameworks. Additionally, evidence suggests that Russian and Chinese nation-state actors, including Berserk Bear and Ocean Lotus, have used the vulnerability to target US government, aviation, and defense organizations.

A secondary element was that the vulnerability gave attackers the ability to create and send internal emails for phishing purposes to collect additional credentials and other nefarious purposes.

Server Vulnerability

Microsoft categorized the patch with an Exploit Index of 1, indicating they expected exploits within 30 days of the patch release. This severity should have prompted administrators to install the patch as a priority. However, the reality is that a survey conducted in September 2020, seven months after patch deployment, found that over 60% of Exchange 2010, 2013, 2016, and 2019 servers examined were still vulnerable. This figure equates to around a quarter of a million vulnerable exchange servers.

Detection

The exploitation of this vulnerability will generate an SYSMON Event ID 4 in the server's application logs. The error message includes the attacker's serialized payload. Therefore, detection and remediation are straightforward if the attack is contained immediately. However, any response delay will allow the attacker to alter log files and hide their presence on the system.

The benefit of an NDR solution is that even if the attacker could hide their exploit of the vulnerability, the unusual behavior of the compromised email account used to authenticate their exploit would be detected and flagged for investigation. Additionally, network records would provide evidence of the execution of the malicious payload, irrespective of the availability and integrity of the application logs.

Recovery

Securing affected Exchange servers from this vulnerability simply requires installation of the available update for CVE-2020-0688. The affected servers are those with the ECP enabled, typically seen in servers with a Client Access Server (CAS) role that allows a user access to the Outlook Web App (OWA).

NDR USE CASES

IMMEDIATE TIME TO VALUE

A key design tenet of Network Detection and Response is rapid deployment, enabled by lightweight software sensors that can ingest network traffic from any environment. Free of any hardware, sensors can be installed in even the most resource-constrained network segments, such as industrial environments. For cloud environments where there is no network tap, the platform provides software forwarding agents that directly copy network traffic from the cloud instance and deliver it to the appropriate sensor. Rapid deployment makes it easy to get pervasive visibility. In addition to the visibility into threats on the enterprise network, Network Detection and Response also provides information about threats introduced by unmanaged personal devices accessing corporate resources and vulnerabilities in workloads running in the public cloud infrastructure.

ADVANCED FORENSICS

The limitless storage of the cloud enables a rapidly searchable network memory at a significantly lower cost than legacy products. Affordable forensics at your fingertips with results in seconds enable game-changing incident response and threat hunting. The platform provides controls for the fidelity and amount of data stored. An optimized index of stored data enables rapid search, which is a valuable feature for threat hunters trying to validate complex hypotheses quickly. An API enables secure access to data for use in other analytic systems.

DETECTIONS IN DEPTH

The platform performs detections at a scale not previously possible because of the elastic compute of the cloud. Machine learning, behavioral analysis, statistical modeling, and heuristics are some of the techniques used. These are augmented by threat intelligence curated by Network Detection and Response, from third party and open-source feeds, and in some cases from customers to capture the uniqueness of their environments.

EARLY DETECTION

Capable and sophisticated attackers can gain unauthorized access to systems protected by traditional perimeter defenses with relative ease if the system has discoverable vulnerabilities. If attackers have access to stolen or disclosed access credentials, then their task is made simple. And then, there are internal attacks, where an authorized user misuses their permitted access for malicious purposes. In all these cases, detecting the attacker's presence within the system inside the perimeter of the security controls is challenging.

INTEGRATED RESPONSE

Network Detection and Response enables rapid detection-triage-response workflows. Correlation of the suspicious actions with the corresponding incident, unique visualizations that allow analysts to make sense of massive amounts of security data intuitively, and policy-based enforcement and workflows facilitate rapid incident response and remediation. Integrations with existing security products—firewalls, endpoint, web security, and automation and orchestration products—and a robust API that enables additional integrations delivers a comprehensive response.

CLOUD MONITORING

Logging and flow data information provided by cloud service providers (CSP) do not provide sufficient detail and granularity to provide usable alerts and post-event analysis. Triage and analysis processes are, as a result, lengthy and complex activities that consume significant resources. This hinders the identification and prioritization of genuine attacks, slowing response times.

NDR solutions automatically collect comprehensive cloud asset information, network metadata, and actionable evidence in a form that facilitates analysis. Automated analysis processes triage cloud incidents and initiate response measures. In addition, information retention supports investigative traceback for advanced persistent threat hunting and intelligence gathering for threat attribution.

NDR solutions also provide proactive security control analysis to support vulnerability discovery and support regulatory reporting.

ENCRYPTED ATTACKS

The use of encryption to protect network traffic is now the norm. This feature offers confidentiality protection against eavesdropping and integrity protection against a man-in-the-middle attack. However, encrypted messages also allow attackers to hide their actions on a network by using the same encryption techniques to prevent monitoring commands and data sent across systems. Furthermore, as NDR solutions use behavioral analysis of metadata from message packets, the machine learning processes can detect hidden and unknown traffic attributable to an attack in real-time irrespective of if the traffic is encrypted.

INFECTED THIRD-PARTY DEVICES

NDR solutions provide protection against threats that egress networks through connected devices that cannot support the use of deployed agents for endpoint security. This can include network-enabled industrial and manufacturing equipment, devices under the Internet of Things category, and users' devices operating under the auspices of Bring You Own Device schemes. Crucially it can also include third-party devices from connected clients and suppliers across the supply chain and service providers such as maintainers, administrators, and other support providers.

This diversity of connected equipment outside of the reach of EDR solutions creates a significant security risk for businesses. Providing traditional boundary protective controls can reduce the risk, but it will not eliminate all threats. This approach also does not protect against the connection of a device directly to the network within the defensive perimeters if the only barrier is procedural controls.

NDR solutions protect against threats from all connected devices, whether inside or outside the perimeter. Any device hosting malicious services or acting as a gateway for an external attacker will be subject to the same behavioral monitoring as the rest of the network-connected devices.

This capability not only protects against attack but acts as a control against the unauthorized connection of devices and authorized connection of devices whose behavior subsequently causes adverse consequences on network performance. In addition, any impact on network operations can be quickly identified, and the device responsible isolated and investigated to rectify any misconfiguration or erroneous operation before business operations are affected.

PHISHING ATTACKS

Phishing attacks remain one of the most common techniques for gaining unauthorized access to a network. A successful phishing email will typically provide an attacker with a legitimate user's authentication details that allow the attacker to bypass all authentication-based access controls.

- 75% of organizations worldwide faced phishing attacks in 2020
- 43% of breaches in 2020 involved phishing or pretexting
- Phishing incidents increased from 114,702 in 2019 to 241,324 in 2020
- The FBI recorded phishing as the most common type of cybercrime in 2020
- Phishing websites have dramatically overtaken malware websites

Figure 19 - Phishing Site Occurrence

The advantage of NDR solutions is that as soon as the attacker leverages the credentials for an unusual or suspicious purpose, the behavioral change will be detected and the access for that account suspended for further investigation. This automated response will halt any exploitation of the stolen credentials in its tracks.

The network data collected by the NDR solution can then be used to determine how the breach occurred, leading to the identification of the phishing attack vector and identification of other user accounts that were similarly compromised.

INSIDER THREATS

Insiders remain critical security threats thanks to their authorized access to networks which negate perimeter-based security controls. Traditionally insider threats were detected when their actions triggered endpoint alerts. However, trends show insider threats are becoming more common and sophisticated, causing more significant damage and increasing costs.

In 2020, significant insider attacks included:

- Twitter suffered a very public attack when hackers stole credentials for employees to gain access to high-profile user accounts and post messages related to cryptocurrency transactions, resulting in other users losing around $0.18 million.
- A senior employee at Amazon leaked sensitive financial information that enabled family members to make nearly $1.5 million from insider dealing of stock.
- Members of the Shopify support team stole customer records associated with nearly 200 merchants for personal gain.

Another attempted attack involved a Tesla employee being offered $1 million to install malware on the company's systems. This attack was unsuccessful thanks to the employee reporting the attempt to the FBI. However, it demonstrates the lengths attackers will go to leverage insider attacks.

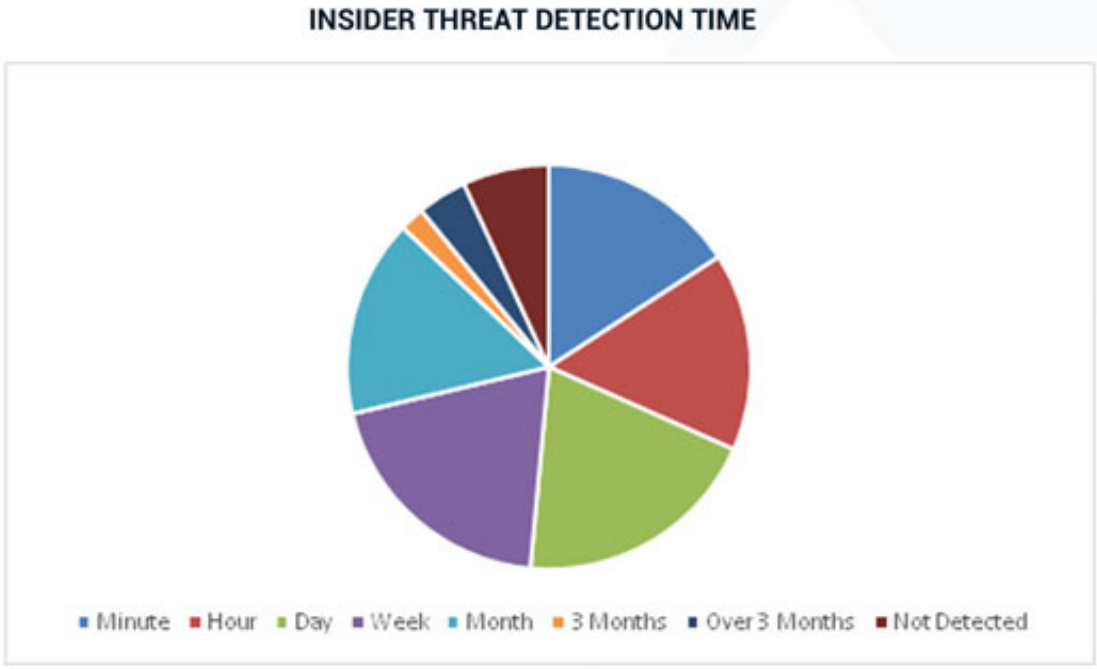


Figure 20 - Insider Threat Detection Time

According to studies conducted by the Ponemon Institute, the average cost of an insider attack rose from $8.76 million to $11.45 million from 2017 to 2019. At the same time, the average cost of investigating an insider threat incident (monitoring, investigation, escalation, incident response, containment, post-incident analysis, and remediation) rose from $513,000 to $756,760 over the same period. Thus, as the rate of insider attacks increases, the accumulated costs of investigating incidents will significantly increase.

The automated investigation and response capabilities of NDR solutions offer a solution to counter these costs with a step-change reduction in attack costs by detecting threats earlier and requiring fewer resources for investigation and remediation.

COMPLIANCE

The visibility afforded to NDR solutions provides a mechanism for leveraging automated processes for establishing and continuously monitoring compliance to policies and regulations. In addition, this capability allows evidence to develop compliance and support governance processes.

Detection of deviations can be alerted and reported in real-time, allowing prompt rectification. This ability is vital for zero trust architectures where variations from requirements can create exploitable vulnerabilities

SHADOW IT

Shadow IT represents a significant source of security vulnerabilities for organizations. IT equipment that is not under formal configuration and security control will often not be fully patched and will offer attackers a gateway into systems that the security team is unaware of. Additionally, for organizations relying on endpoint protection, an unknown endpoint creates a hole in the security coverage.

The immediate benefit of NDR solutions is the protection they provide across the entire infrastructure real-estate, including those endpoints that an agent cannot for whatever reason protect. The additional benefit is that the NDR solution will recognize its presence as an unknown device as soon as the shadow IT connects to the network. This detection will create an event for investigation, and automated response processes can, if necessary, isolate the rogue device from the network.

Of course, not all shadow IT is wrong. For example, where a legitimate business need requires users to add services, applications of devices to a network, playbooks can be created to adapt the NDR solution to accept the addition and consume it into the security coverage. In the case of added endpoints, the playbook may automatically install an endpoint agent and enroll the device into the pool of trusted equipment, with any issues with the configuration of patch status communicated to the owner rather than the IT department.

Figure 21 - Shadow IT Presence

FRICTIONLESS SCALE

Its cloud architecture enables Network Detection and Response to frictionlessly scale to secure even the largest enterprises. On a daily basis, the LMNTRIX platform analyses more than 500 terabytes of network data amassed from hundreds of deployments. Network Detection and Response analyses over 9 billion network connections per day to surface over 1 million potential threats. Those threats are distilled into 22,000 security events, with completely correlated context from network to endpoint–filtering data points to prioritize threats and reduce the noise for a more effective and efficient response.

ORGANIZATIONS WANT PROACTIVE NETWORK SECURITY

Organizations are looking for proactive detection and response at the network level. Prevention-based security approaches alone, which rely on the ability to control enterprise-owned resources, are no longer sufficient. A similar shift has already occurred at the endpoint, with organizations moving from antivirus (AV) and next-gen AV (NGAV) to Endpoint Detection and Response (EDR).

HOW **LMNTRIX XDR** BENEFITS FROM **NDR** AND NETWORK TELEMETRY

LMNTRIX XDR

LMNTRIX's Extended Detection and Response (XDR) platform is our cyber defense SaaS platform that provides a new utility model for enterprise security. It delivers pervasive visibility, threat hunting, validation, investigation, containment, remediation, and unlimited forensic exploration on-demand and entirely from the cloud. It is a single investigative platform for insights into threats on enterprise, cloud, hybrid, and Industrial Control System (ICS) networks.

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, Network Forensics, UEBA, and Deception Everywhere with completely automated attack validation, investigation, containment, and remediation on a single, intuitive platform.

LMNTRIX Detect & LMNTRIX Hunt provide the NDR, Network Forensics, and UEBA capabilities of the LMNTRIX XDR platform. Designed as separate NDR sensors that allow enterprises to deploy them at strategic choke points in their networks to achieve the desired security outcome.

The LMNTRIX XDR delivers unique advantages over current network security solutions. It is a holistic, multi-vector, hyper-converged cyber defense platform with an unlimited retention window of full-fidelity network traffic, innovative security visualizations, and the ease and cost-savings of an on-demand deployment model.

LMNTRIX NETWORK DETECTION & RESPONSE (NDR)

LMNTRIX XDR challenges the way organizations secure their networks with Network Detection and Response, a cloud-delivered security platform that is more intuitive, comprehensive, and immersive than legacy products that came before it. LMNTRIX Detect & LMNTRIX Hunt lightweight software sensors record complete traffic from any network segment from the DMZ to the core, on cloud networks, and even industrial environments to establish a high-fidelity memory of the network in the cloud. These sensors capture complete network data and send it to the LMNTRIX XDR for storage and analysis. The XDR platform acts as a cyber defense tool, allowing analysts to explore historical data retrospectively with the most up-to-date threat intelligence. Visualizations in Network Detection and Response can be used for real-time situational awareness or as a forensic workbench for incident response teams and threat hunters. It provides actionable intelligence, including a correlated view of threats and packet-level forensic capabilities to speed incident response and threat hunting

Benefits

- Delivers pervasive visibility across the network
- Provides an unlimited, full-fidelity forensic window
- Reduces detection noise and alert fatigue
- Replay network traffic against the latest threat intelligence to uncover previously unknown latent threats
- Simplifies security and frees up incident responders to hunt for threats
- Complements existing infrastructure through secure APIs
- SaaS model deploys rapidly

Cloud-based network memory

Record traffic from multiple networks into a single haystack for centralized analysis with unlimited, full-fidelity retention windows.

- Enables long-term retention and analysis of network traffic
  - Unlimited network packet capture, replay, and storage into a single haystack
- Choose to capture what matters to your risk profile.
  - Adaptive capture options for flows, metadata, or full packet capture (PCAP)
- Purpose-built for distributed networks
  - Can be deployed on any network segment for unlimited coverage models

Intelligence from sensor-driven data

Network data delivered in context.

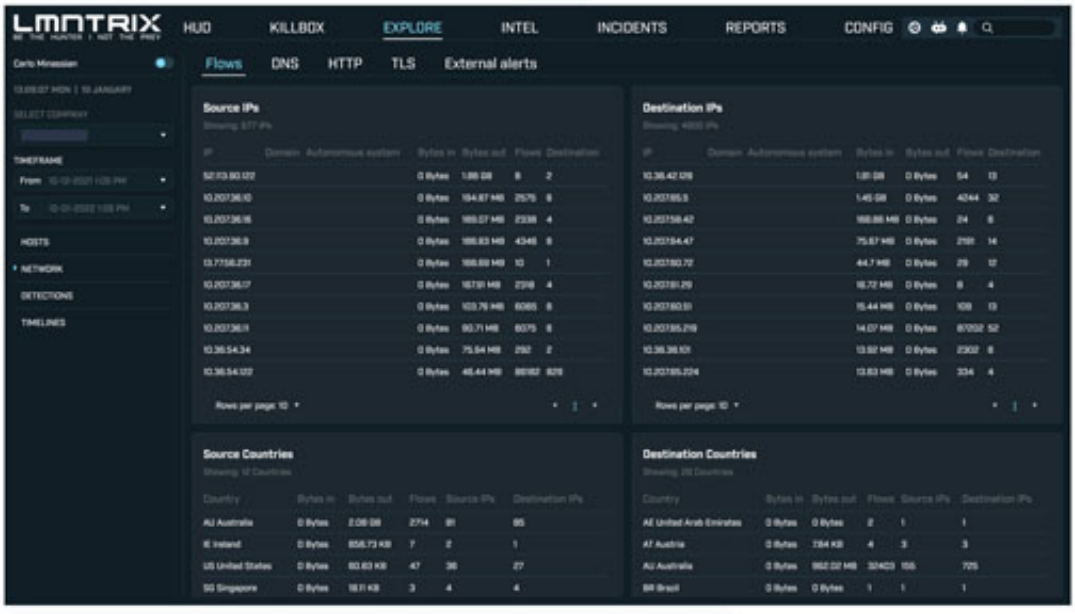
- Deep packet inspection of data from thousands of protocols and applications
- Network data compared with proprietary and third-party intelligence for the community – scaled detection
- Advanced traffic threat analysis performs correlation, heuristics, and machine learning

Retrospection

- Analysis engine powered by a centralized repository of full-fidelity network data allows for continuous detection and prioritization of threats
- New indicators of compromise from network intelligence make it possible to analyze past network behavior for newly discovered, latent threats

Intuitive data visualization

- Compresses dwell time and incident response with deep forensic exploration using cutting edge visualization tools
- Give security teams an easy-to-navigate system to more quickly act on threat intelligence
  - Advanced forensics visualization allows analysts to interact with data through kill-chain analysis, network connection graphics, and event timelines
- Powerful security console with customizable flexibility
  - Integration capabilities to feed threat data into custom SOC and forensics dashboards
  - Quick management of policies for sensor deployment, packet capture, user management, and alert notification

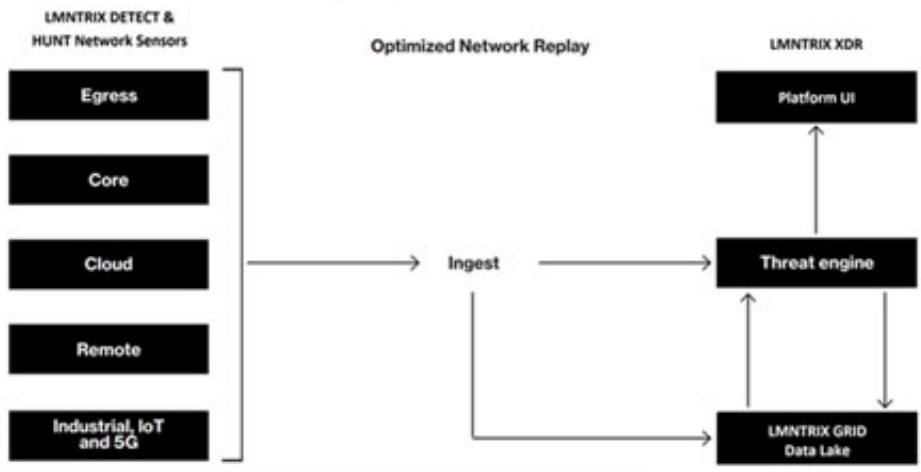


Technical requirements

- Recommended requirements for LMNTRIX Hunt sensor (physical or virtual):
  - CPU: Intel Xeon with 4+ Cores
  - Memory: 8GB or more free
  - Disk space: 100GB or more disk space (required for buffering)
  - Internet connectivity for the Relay and Management Interface
  - Two network interfaces
  - Monitoring NIC: 10/100/1000 Ethernet connected to a SPAN/Tap/Mirror port Relay and Management NIC: 10/100/1000 Ethernet for relaying optimized and encrypted data and sensor management

  Recommended requirements for LMNTRIX Detect sensor (physical or virtual):
  - CPU: Intel Xeon with
    - ✓ 2 Cores to support a 200 Mbps SPAN/Tap/Mirror port Relay
    - ✓ 4 Cores to support a 300 Mbps SPAN/Tap/Mirror port Relay
    - ✓ 8 Cores to support a 600 Mbps SPAN/Tap/Mirror port Relay
    - ✓ 12 Cores to support a 800 Mbps SPAN/Tap/Mirror port Relay
    - ✓ 16 Cores to support a 1Gbps SPAN/Tap/Mirror port Relay
    - ✓ 20 cores to support a 1.2Gbps SPAN/Tap/Mirror port Relay
    - ✓ 24 Cores to support a 1.4Gbps Gbps SPAN/Tap/Mirror port Relay
    - ✓ Contact LMNTRIX for higher port Relay needs
  - Memory: 8GB or more free
  - Disk space: 100GB or more disk space
  - Internet connectivity for Management Interface
  - Two network interfaces (NIC0 -MGMT, NIC1-SPAN)
  - Management NIC: 100/1000 Ethernet for relaying optimised and encrypted data to and from sensor to XDR platform and for updating IOC feeds from the Internet
  - Monitoring NIC: 100/1000 Ethernet connected to a SPAN/Tap/Mirror port for inspecting SPAN traffic

LMNTRIX NETWORK DETECTION & RESPONSE: HOW IT WORKS



LMNTRIX
BE THE HUNTER | NOT THE PREY

ABOUT **LMNTRIX**

LMNTRIX is the leader in intelligence led security-as-a-service. Working as a seamless, scalable extension of customer security operations, **LMNTRIX** offers a single MDR solution called Active Defense that blends our cyber defense platform called **LMNTRIX** XDR with innovative security technologies, nation-state grade threat intelligence and world-renowned Cyber Defence Centers. With this approach, **LMNTRIX** eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyberattacks. Our service differentiators include:

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, Network Forensics, UEBA and Deception Everywhere with completely automated attack validation, investigation, containment, and remediation on a single, intuitive platform.

LMNTRIX Tech Stack is a powerful proprietary threat detection stack that is deployed onsite, behind existing controls. It's made up of network sensors, endpoint agents and deceptions everywhere. It combines multiple threat detection systems, with machine learning, threat intel, correlation, static file analysis, heuristics, and behavior and anomaly detection techniques to find threats in real-time. It decreases alarm fatigue by automatically determining which alerts should be elevated to security events, and reduces false positives by requiring consensus across detection.

LMNTRIX Cyber Defense Centers - A global network of cyber defense centers that are complemented by our local partner SOCs, with highly trained and certified intrusion analysts who provide constant vigilance and on-demand analysis of your networks. Our intrusion analysts monitor your networks and endpoints 24x7, applying the latest intelligence and proprietary methodologies to look for signs of compromise. When a potential compromise is detected, the team performs an in- depth analysis on affected systems to confirm the breach. When data theft or lateral movement is imminent, our endpoint containment feature makes immediate reaction possible by quarantining affected hosts, whether they are on or off your corporate network while our automated network containment feature blocks the threat traversing your Firewalls or through our integration with cloud security solutions such as Zscaler, Netskope and Cisco Umbrella. This significantly reduces or eliminates the consequences of a breach.

TO LEARN MORE ABOUT **LMNTRIX** VISIT

https://lmntrix.com/

LMNTRIX USA.
333 City Blvd West, 17th Floor,
Suite 1700, Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65 3159 0639

LMNTRIX INDIA.
VR Bengaluru, Level 5, ITPL Main Rd,
Devasandra Industrial Estate,
Bengaluru, Karnataka 560048,
sales@lmntrix.com
+91-22-49712788

LMNTRIX Australia.
Level 32, 101 Miller Street,
North Sydney NSW 2060,
+61.288.805.198