GATEWATCHER

NDR *Insight_*

The essential guide for CISO and CIO.

Why and how NDR can be an essential brick to strengthen your cyber resilience.

Table of content_

This section is part of the complete NDR Insights Guide

Download full report

01

ALL GOOD CYBERSECURITY should start with the network_

*Why yesterday's cybersecurity won't save you tomorrow_*

In a shifting threat landscape, cyber resilience comes from continuous evolution.

EVOLVING AND UNKNOWN THREATS THAT TRADITIONAL SOLUTIONS CAN'T ALWAYS KEEP UP WITH_

Traditional cybersecurity solutions, such as firewalls, antimalware software, and intrusion detection and prevention systems (IDS/IPS), play a **vital role in perimeter protection and managing known threats.** However, these systems primarily address well known attack vectors, rather than new sophisticated attack vectors or techniques, 0-day exploits and their variations, or new technologies adoption for weaponization, causing a slowness in defense and wrong estimate of the actual security posture. Once attackers penetrate the system, **the damage is already done, frequently irreversible and potentially detected days or months after.**

Given the rapidly evolving and complex nature of cyberattacks, these technologies have inherent limitations. Primarily **relying predominantly on signatures or predefined rules**, they often struggle to detect emerging threats or adapt to new attack techniques.

Network Detection and Response (NDR) solutions complement these traditional approaches **by introducing a proactive and behavioral dimension**. By monitoring, analyzing, and responding to network traffic behavior, structure and low signal in real-time, NDR provides enhanced visibility with a contextual mapping of network activity and the ability to detect and qualify suspicious activities at their earliest stages, thereby strengthening existing defenses.

THE LIMITS OF TRADITIONAL SYSTEMS IN A COMPLEX LANDSCAPE_

At first glance, **this might look like a seamless and secure IT environment**—a symbol of modern cybersecurity at work.

But **take a closer look.** Beneath the surface lies a hidden complexity of challenges and weaknesses that traditional systems struggle to address.

What appears calm and controlled masks the cracks that sophisticated attacks exploit daily.

Traditional perimeter-based solutions, while foundational, face significant limitations in addressing the evolving complexity of modern cyber threats and digital environments. As organizations expand their IT landscapes and face increasingly sophisticated attack techniques, **these challenges become starkly evident:**

> Complex and dynamic digital evolution_

With architectures, data flows, and applications growing more intricate, traditional tools struggle to maintain comprehensive oversight, generating substantial blind spots. The convergence of IT and OT environments demands constant monitoring that traditional solutions cannot provide.

> Inadequate threat detection and investigation capabilities_

The rapid evolution of attack techniques, including the daily emergence of sophisticated threats, outpaces traditional detection methods that rely on predefined rules or signatures. High false positive and negative rates and limited contextualization of incidents further weaken SOC teams' ability to identify and qualify alerts effectively amongst heavy prioritization alert process.

> Limited visibility across expanding attack surfaces_

Traditional solutions often focus on endpoints or high-level network information, leaving critical blind spots in the broader network and cloud interconnections.

As organizations increasingly rely on cloud-based services, the lack of insight into virtualized environments and third-party systems exacerbates threats and supply-chain attacks.

> Fragmentation and overlapping tools_

Organizations frequently layer multiple network analysis tools, leading to operational inefficiencies and higher maintenance costs. This fragmented approach hampers unified threat detection and response, leaving gaps that attackers can exploit leading to SOC analysts fatigue and downtimes in defense response.

What about EDR & SIEM ?

EDR *(Endpoint Detection and Response)*

Continuously monitors and analyzes endpoint activities to detect and mitigate threads. An agent is deployed on each compatible system. It tracks suspicious behaviors, active processes and system interactions to enforce incident response. However, EDR scopes are limited to endpoints where the agent is deployed (very often EDR are not deployed everywhere they should be for financial or technical limitations), leaving gaps in visibility across broader network activities and east-west traffic.

SIEM *(Security Information and Event Management)*

Historically collects logs and events from a wide range of IT components within a network. While it allows for correlation and holistic analysis, it lacks the granularity needed to understand the precise interactions and exchanges between IT components. Furthermore, SIEM relies essentially on collected logs. However, mainly for technical and cost reasons, logs from all components are not conveyed to the SIEM. This makes subtle or lateral threats detection less effective.

*How NDR solutions complement and enhance traditional security approaches*_

> *Detection* of unknown threats and zero-days_

NDR solutions leverage AI and Machine Learning to analyze abnormal behaviors, identifying threats before they reach their targets. Unlike traditional security methods that mainly relies on signatures, NDR threat detection based on behavior, enables the identification of unknown and zero-day threats.

> *Comprehensive and centralized* network visibility_

Unlike perimeter-based and endpoint solutions, NDR provides visibility across the entire network, including hybrid and multi-cloud environments. This detailed, centralized perspective enables security teams to detect suspicious activities and anomalies throughout the network and respond effectively.

> *Reduction* of false positives_

Behavioral analysis powered by AI and ML distinguishes critical anomalies from legitimate activities, significantly reducing false positives. This relieves SOC teams of unnecessary alerts, allowing them to focus on genuine threats.

> *Continuous adaptation* to more sophisticated emerging threats_

By continuously learning and evolving, NDR systems adapt to adversarial tactics, maintaining effectiveness even against polymorphic attacks and new threat vectors. This ensures that organizations are equipped to handle constantly changing threat landscapes.

> *Proactive and contextualized* threat hunting_

NDR solutions enable proactive threat investigation, identifying attack vectors and strengthening the organization's security posture. Unlike reactive traditional approaches, NDR facilitates preventive measures through real-time detection and contextual understanding.

> *Rapid and automated* detection and response_

NDR solutions deploy countermeasures in real time, drastically reducing response times. Automated actions, such as asset isolation, user account deactivation, blocking of malicious network flows, etc. help limit the impact of incidents and minimize data loss and damage.

> *Enhanced* incident response_

NDR systems assist security teams by providing relevant data and insights during incident response. Real-time analysis of network traffic and continuous anomaly monitoring allow teams to understand the scope, cause, and impact of an incident. This accelerates response times, minimizes damages, and speeds up the restoration of affected systems and services.

Additionally, **NDR systems offer rich forensic analysis capabilities based on metadata** collected from monitored network traffic, enabling security teams to reconstruct and investigate past attack attempts. This helps identify weaknesses and attack vectors, which can be mitigated to further strengthen network security.

By integrating these capabilities, **NDR solutions bridge the gaps left by traditional technologies**, offering a more dynamic, proactive, and comprehensive approach to cyber defense in an increasingly complex threat landscape.

Focus *Business benefits_*

CIOs - Better decision-making and alignment of security investments

> Business resilience

> Minimize breach impact

> Cybersecurity cost optimization

CISOs - Robust unified defenses that meet regulatory obligations

> Enhances organization's security posture

> Compliance support

SOCs - Reduced alert fatigue and improving operational efficiency

> Steamlines threat detection

> Automated response

> In-depth analysis and reporting

HOW EDR, SIEM, SOAR AND NDR COMPLEMENT EACH OTHER?_

Solutions like EDR, SIEM, SOAR and NDR work in tandem to create **a comprehensive cybersecurity ecosystem.**

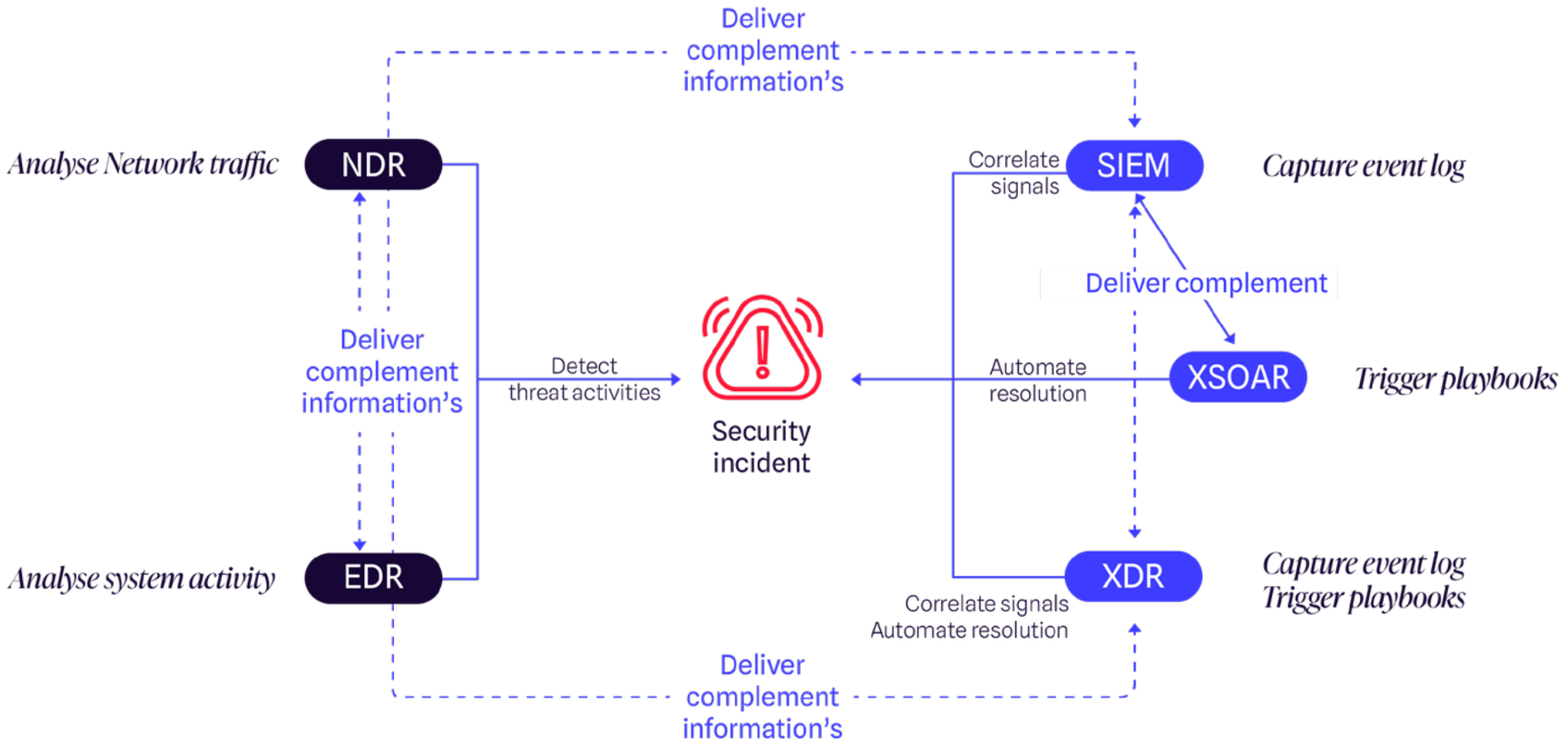
EDR focuses on analyzing system activity and endpoints, while **SIEM** captures and correlates event logs to provide contextual insights into potential threats. **SOAR** takes this a step further by automating responses with triggered playbooks, streamlining incident management. **NDR** complements these tools by focusing on network traffic, identifying threats in real-time, and delivering critical insights to enhance detection and response efforts.

Together, **they form a multi-layered defense strategy,** ensuring a seamless and effective approach to modern cyber threats.

> We have decided to approach our three projects - architecture, organization, and tooling - in an integrated manner. The idea is to combine several complementary solutions: EDR for individual protection, NDR for large-scale security, and leveraging the CERT in case of an emergency or a business continuity plan (BCP).

Bertrand Frémont - CISO Lynred

Zero Trust_



/!\ However, the most suitable NDR solution for a company depends on various factors, including security requirements, network infrastructure, budget, and more. It is, therefore, recommended to conduct thorough research on different NDR solutions and compare them to identify the one that best meets the company's specific needs

*Gatewatcher NDR Platform: Rethinking network security for tomorrow's challenge_*

Network Detection and Response (NDR) is a cybersecurity solution designed to protect networks from evolving threats by analyzing network traffic for abnormal behaviors. By applying advanced behavioral analytics, NDR detects anomalies and suspicious activities in real-time, focusing on both internal (east-west) and external (north-south) communication flows. Unlike traditional signature-based methods, NDR identifies both known and unknown (0-days), hidden and past threats, through continuous traffic analysis

NDR solutions integrate automated responses, either directly or through other cybersecurity tools. Deployed as a combination of hardware, software, or SaaS, they provide flexibility to fit various organizational needs. With comprehensive visibility and proactive detection, NDR strengthens network defenses, enabling organizations to respond faster and more effectively to more sophisticated emerging threats.

What if you prioritized NDR as your starting point in cybersecurity?

Focus *Business_*

> Strengthen cyber resilience: Ensure full visibility across on-prem, cloud, and hybrid environments to mitigate blind spots and reduce risk exposure.

> Ensure business continuity: Detect and neutralize threats in real time to minimize disruptions, reduce costs, and accelerate recovery.

> Leverage AI-driven automation to investigate threats faster, reduce response times, and minimize operational impact.

> Enhance decision-making: Make faster, smarter security decisions by reducing false positives and focusing on real threats.

> Stay ahead of emerging threats: Integrate real-time Cyber Threat Intelligence (CTI) to anticipate and counter evolving attack techniques.

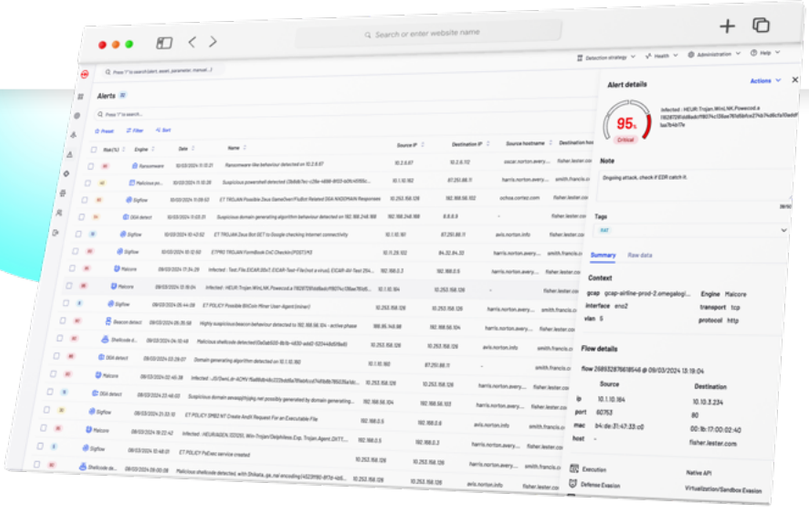
> Simplify security management: Unify detection, investigation, and response in a single platform for streamlined operations and reduced complexity.

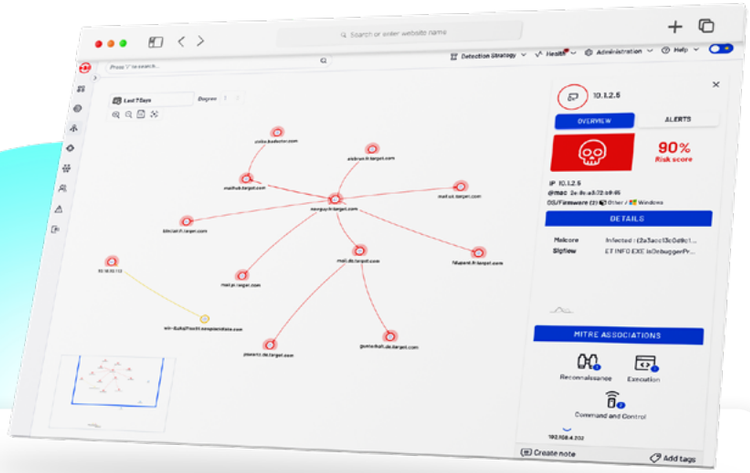
*Scope of action of Gatewatcher NDR Platform: detect, analyze, respond, anticipate_*

Data collection and acquisition_

NDR systems operate by continuously collecting data from network traffic, including packet data, flow information, and metadata. This comprehensive data acquisition provides an extensive view of the network, enabling detailed forensic analysis of security incidents. By capturing information before, during, and after an event, NDR systems offer the contextual insights necessary to reconstruct the timeline of an incident and identify attack vectors.

Gatewatcher NDR Platform is unique in its ability to operate entirely disconnected from cloud service providers, ensuring data sovereignty. Its outbound architecture guarantees zero impact on production environments, allowing seamless detection without interfering with business operations. Customers retain full ownership and control over their data and detection results, including sensitive Indicators of Compromise (IoCs) and hashes.





Real-time visualization and mapping_

NDR provides real-time mapping of your network, encompassing IT, OT, IoT, virtual machines, and cloud environments. Understanding your network's structure, assets, users and communications is essential for effective protection. Real-time visualization ensures that organizations can detect low signals at the early stage of a compromise, helping to identify potential threats, trace them back to patient zero, and initiate an active response before adversaries escalate into more significant attacks. This comprehensive mapping enables both a clearer infrastructure understanding and faster threat identification.

Gatewatcher NDR Platform further enhances this capability by offering seamless integration into increasingly complex and heterogeneous IT and OT environments, allowing rapid deployment and immediate results.

Investigations and *analysis*_

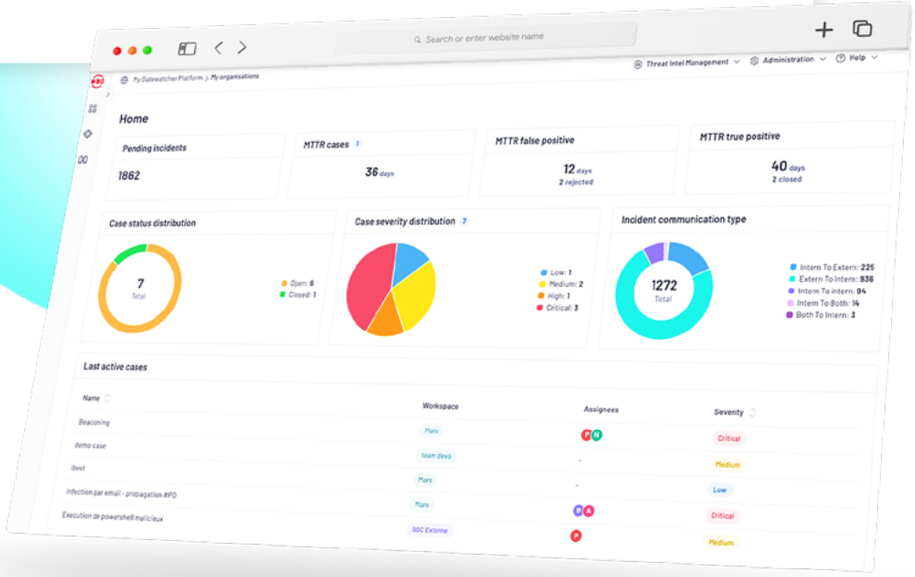
NDR systems empower security / SOC teams to investigate incidents comprehensively by:

> Building timelines and uncovering connections between events to better understand attack progression and causal chains.

> Analyzing behavioral patterns and malicious activity indicators to identify attackers' TTPs'.

> Enhancing forensic investigations to uncover vulnerabilities in security architecture and prevent future incidents.

Gatewatcher NDR platform's relational and behavioral analysis capabilities between users and IT assets provide an unparalleled depth of understanding, enabling faster identification of root causes and attack vectors.



*Detection*_

Using advanced AI and Machine Learning (ML) algorithms, NDR systems detect and analyze threats at every stage of the kill chain, from initial compromise to lateral movement. By processing large volumes of data, NDR systems can identify threats even on encrypted traffic.

Key capabilities include:

> Identifying known, unknown (zero-day), hidden (encrypted traffic), obfuscated and even past threats through retro-hunting.

> Detecting attacks from internal or external sources.

> Reducing Mean Time to Detect (MTTD) and minimizing false positives.

> Dynamic detection rules that adapt to the evolving threat landscape.

> Immediate detection without requiring baseline data (plug-and-detect).

Gatewatcher NDR Platform distinguishes itself by combining multiple engines to target the most relevant attack techniques. Its multi-layered detection approach ensures rapid identification of weak signals, providing actionable intelligence faster than conventional methods.

*Enrichment_*

NDR systems automatically enrich analysis by integrating contextual data through Gatewatcher Cyber Threat Intelligence (CTI) and metadata. Enhanced forensic capabilities, such as mapping threats to the MITRE ATT&CK framework, allow teams to react more effectively. By providing actionable insights, NDR systems ensure rapid and precise incident response, improving overall security operations. Key features include Active Hunt and Retro Hunt engines powered by CTI, enabling both proactive and retrospective threat hunting. Additionally, built-in external exposure detection leverages AI and CTI to monitor assets, users, and brands for vulnerabilities. Native incident enrichment further enhances the understanding of suspicious activities, empowering teams with comprehensive and actionable intelligence.

Gatewatcher NDR Platform's independence from cloud constraints ensures that all enriched analysis is conducted within fully controlled environments, preserving both technical, integrity and ownership.

*Response_*

After an incident, or even worse a compromise, has been recognized, NDR systems can facilitate incident responses by preparing additional information about the threat. This enables incident response teams to react more quickly and effectively. NDR systems offer intelligent alert aggregation, which provides a comprehensive view of attack scenarios. Alerts are scored and prioritized in real time based on their business impact, ensuring the most critical threats are addressed first.

With a global response capability that integrates APIs and third-party tools into a unified product, NDR systems enable orchestrated and automated one-click remediation, all under the control of a SOC. These solutions ensure integrated responses leveraging your existing ecosystem without disrupting business operations. By drastically reducing the Mean Time to Respond (MTTR), they enhance the speed and efficiency of incident management.

Gatewatcher NDR Platform can, for example, automatically isolate a host or user, deactivate user accounts, terminate communication sessions, close ports and send an alert to the security team.

Focus *Business_*

Your business gain with a unified NDR platform:

> Control through visibility: Gain a complete view of your network, identifying hidden threats before they escalate.

> Anticipate, don't just react: Use behavioral and generative AI to detect and neutralize threats early, reducing false positives and minimizing risks.

> Optimize SOC efficiency: Automate prioritization and streamline workflows to reduce alert fatigue and false positives while boosting operational performance.

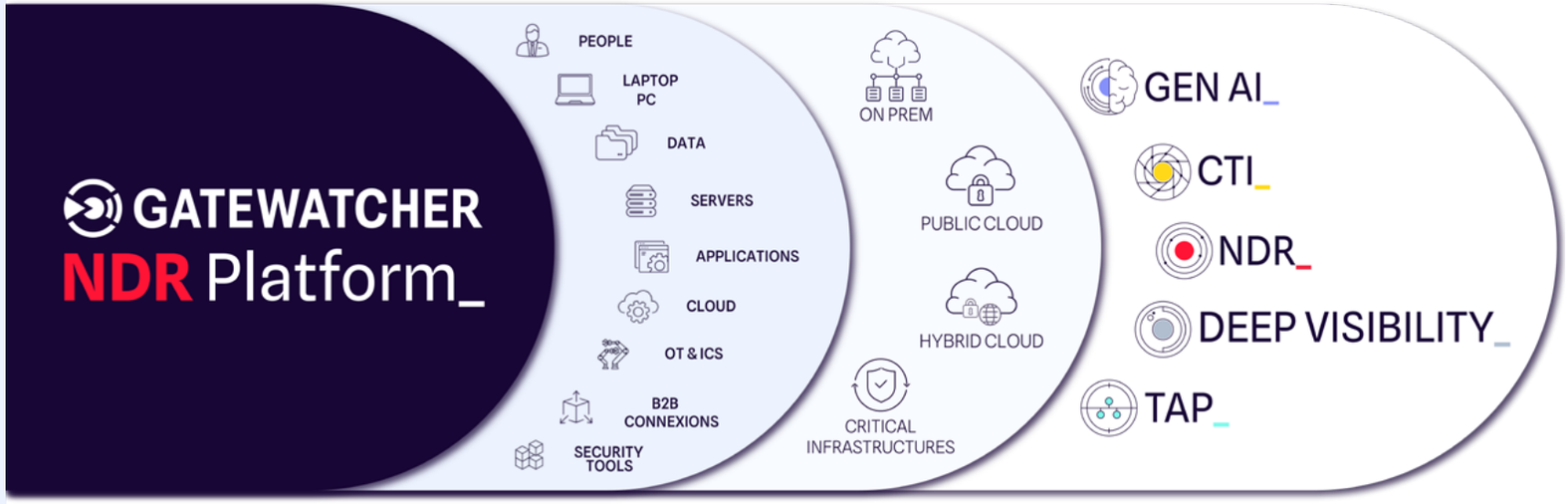
> Fast, targeted threat response: Accelerate remediation with tailored, automated response strategies that adapt to your business needs.

> Seamless & secure monitoring: Leverage non-intrusive TAPs for real-time visibility without disrupting critical operations.

*The unified power of Gatewatcher NDR Platform_*

Gatewatcher NDR platform is our industry-leading solution that combines cutting-edge technologies to deliver unmatched and convergent visibility, detection, and response capabilities.

At its core, Gatewatcher NDR® is strengthened Reflex®, Cockpit®, our Gatewatcher CTI, Generative AI Assistant, Deep visibility® and a full range of TAP solutions, seamlessly working together to ensure behavioral detection of cyber threats and rapid, comprehensive remediation.



Core products and *modules* driving the platform_

NDR_ AIONIQ

> *Gatewatcher NDR - AionIQ®_*

Gatewatcher NDR - AionIQ® - our NDR solution - leverages advanced artificial intelligence to monitor network activity in real-time, detecting behavioral anomalies that signal potential threats. Its precision ensures early detection and actionable insights.

NDR_ REFLEX

> *Reflex®_*

Reflex® automates and optimizes your response to cyber threats with precision. It offers comprehensive and targeted orchestration directly from your Gatewatcher NDR, ensuring rapid containment and resolution of incidents with minimal effort thanks to automated and personalized playbooks.

NDR_ COCKPIT

> *Cockpit®_*

Cockpit® intelligently aggregates, correlates and prioritizes the management of large volumes of security incidents across multiple infrastructures and clients. Its centralized view enables security teams to monitor and respond to threats across all environments at a glance, ensuring efficient multi-client incident management. Its collaborative capabilities empower all stakeholders to respond swiftly and effectively, minimizing the impact of intrusions and ensuring comprehensive containment.

CTI_

> *Gatewatcher CTI_*

Our Cyber Threat Intelligence (CTI) contextualizes your investigations and enhances your detection capabilities. Directly actionable, this threat intelligence enables a proactive defense approach by exposing vulnerabilities— including users—before they can be exploited.

GEN AI_

> *Generative AI Assistant_*

Our generative AI assistant, revolutionizes how SOC teams approach cybersecurity by streamlining every stage of security operations from the skills reinforcement to incident management, alongside security policy enhancement.

With intelligent task allocation, enriched incident processing, and rapid, tailored remediation, its main benefits are:

> Task distribution for optimized workflows
> High-quality, concise response synthesis
> Incident identification, understanding, and qualification
> Fast, secure, and customized threat mitigation

DEEP VISIBILITY_

> *Deep Visibility_*

Gain advanced visibility into your network traffic, both real-time and historical, through deep packet inspection (DPI) to detect anomalies and understand critical interactions. Adapted to all infrastructures, this multi-layer analysis provides deep insight into network behaviors, enabling fast and informed decision-making.

TAP_

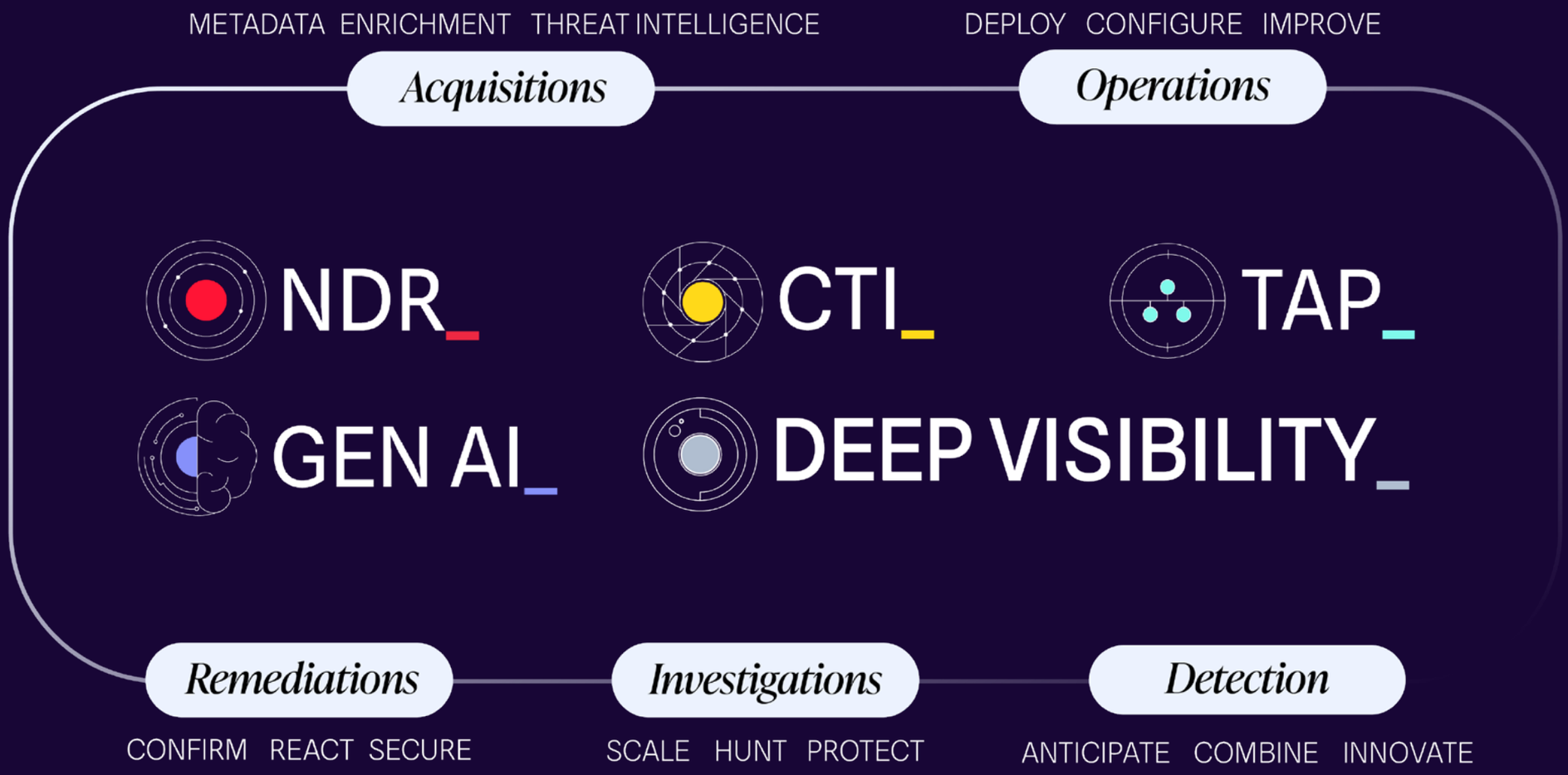
> *Gatewatcher TAPs_*

Gatewatcher offers a complete range of qualified optical and copper TAPs designed to cover all your network monitoring and detection needs. These secure TAPs integrate seamlessly into your network, ensuring the protection of the detection system with diode functionality to prevent reverse traffic. This ensures reliable data collection without compromising system integrity, delivering full-spectrum visibility to your network operations.

Conclusion_

Cyber threats are no longer occasional disruptions. They are persistent, evolving, and deeply embedded in the fabric of digital operations.

Traditional security approaches remain essential, but today's threats demand a broader perspective. Network Detection & Response (NDR) enhances cybersecurity by providing the deep network visibility and proactive detection needed to stay ahead of evolving threats.



Why?

Because speed, visibility, and adaptability define cybersecurity success_

> *Detection at first contact:*

Modern attacks move fast—NDR enables early detection, reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to contain threats before they escalate.

> *Beyond known threats:*

Signature-based security is reactive; NDR identifies unknown, stealthy, and emerging threats through behavioral analysis and AI-driven detection.

> *The full picture, always:*

IT, OT, IoT, and cloud environments are deeply interconnected - NDR ensures holistic visibility across all network layers, eliminating blind spots.

> *From overwhelmed to empowered:*

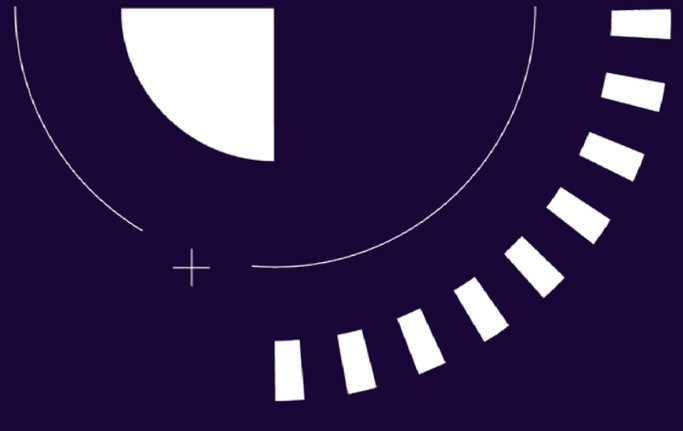
SOC teams face alert fatigue and operational overload. NDR prioritizes and contextualizes threats, allowing faster, smarter decision-making.

A shift in cybersecurity thinking_

Security is no longer about defending a perimeter; it is about understanding and controlling digital movement. Attacks no longer knock on the front door—they hide in legitimate traffic, exploit overlooked vulnerabilities, and adapt in real time.

The organizations that embrace continuous monitoring, rapid response, and intelligent automation are the ones that will thrive in an era where digital risk is an everyday reality. NDR is not just a tool—it is a mindset shift, a commitment to resilience, and an enabler of secure, sustainable business growth.

Cybersecurity is no longer about reacting.
It *is about anticipating*



*Easy as_*

NDR_

CTI_

TAP_

GEN AI_

DEEP VISIBILITY_

ABOUT_

A leader in cyber threat detection, Gatewatcher has been protecting the critical networks of businesses and public institutions around the world since 2015. Our Network Detection and Response (NDR) and Cyber Threat Intelligence (CTI) solutions analyze vulnerabilities, detect intrusions and respond quickly to all attack techniques. Gatewatcher provides a real-time, 360° view of cyber threats across the entire network, in the cloud and on-premises thanks to the combination of AI with dynamic analysis techniques.