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_

01

ALL GOOD CYBERSECURITY should start with the network_

*Hackers gonna hack: Cybersecurity is all day, every day_*

*Global threat landscape_*

Cybersecurity is no longer a choice but a strategic necessity for organizations of all sizes, from startups to global corporations. In 2024, the average cost of a data breach reached a record high of $4.88 million (IBM)[1]. If cybercrime were a country, its estimated global damage of $9.5 trillion USD in 2024 (Cybersecurity Ventures) would make it the world's third-largest economy[2], outpacing the GDP of many nations. These staggering statistics underscore **a critical transformation:** cybercrime has escalated from being sporadic to a pervasive and persistent threat.

For the fourth consecutive year, **cyber incidents have been ranked as the first global risk**, according to the Allianz Risk Barometer 2025. They now represent the number one risk in 20 countries worldwide.

This evolution is driven by three major factors_

> Accelerated digitization of society and growing interconnectivity, complicating IT, OT, IoT, and cloud environments.

> The emergence of new technologies transforming society is making cybersecurity tasks more complex and increasing operational fatigue.

> Slowness in CyberSecurity, while technologies evolve quickly with early adoption by sophisticated adversaries.

A THREAT AMPLIFIED BY GEOPOLITICAL CONTEXT_

International tensions and major events have spurred a rise in targeted cyberattacks. The French National Cybersecurity Agency (ANSSI) highlights worrying trends:

> Increased industrial espionage targeting critical sectors like defense, telecommunications, and digital services.

> Resurgence of ransomware, affecting vulnerable targets such as local governments, healthcare ecosystem, and energy infrastructure.

> Destabilization and misinformation attacks, leveraging DDoS, data breaches and information manipulation to tarnish reputations.

Simultaneously, cyberattacks continue to evolve, **becoming more professionalized** through "as-a-service" models. Criminal platforms, such as those dismantled during operations like "Cronos", "Endgame" and "PowerOff", exemplify this industrialization of threats.

1. https://www.ibm.com/reports/data-breach

2. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/

GROWING SOPHISTICATION OF ATTACK TECHNIQUES_

Modern cyberattacks employ increasingly stealthy and complex techniques, making detection more challenging. While social engineering techniques like phishing remain prevalent, new vectors are emerging, fueled by technological advancements like generative AI (GenAI). This has enhanced both the initial exploitation and post-exploitation phases of attacks.

By 2025, organizations must brace for the persistence of traditional threats (DDoS, ransomware, info-stealers) while proactively addressing malicious innovations.

CHALLENGES FOR BUSINESSES_

Businesses face a dual challenge when it comes to cybersecurity. From a technical perspective, **the lack of visibility into network activities and the proliferation of connected devices, particulary IoT and BYOD, have significantly expanded the blind spots** of attack surface and opportunities for adversaries. The use of multiple security solutions increases operational costs, fatigue and complexity, yet often fails to deliver proactive protection. Moreover, while a compromise can occur within minutes, the delay in detecting cyberattacks often leads to responses that come too late, after significant damage has already been done.

On the organizational side, human factors remain a critical vulnerability. Beyond a lack of risk awareness, many organizations overestimate their defenses and underestimate the sophistication of attacks, often leading to repeated compromises in similar ways—a dangerous complacency that exposes them to ongoing threats. This is compounded by increasingly stringent regulatory requirements and disruptive changes, such as the shift to hybrid work models post-COVID-19, which have redefined how data is accessed and secured.

Beyond technical and organizational issues, **reputation has emerged as a major concern. Cybersecurity incidents carry not only monetary costs but also significant reputational damage.** A single breach can erode customer trust, harm brand image, and result in long-term financial and operational repercussions, making robust cybersecurity a critical business priority.

*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.**

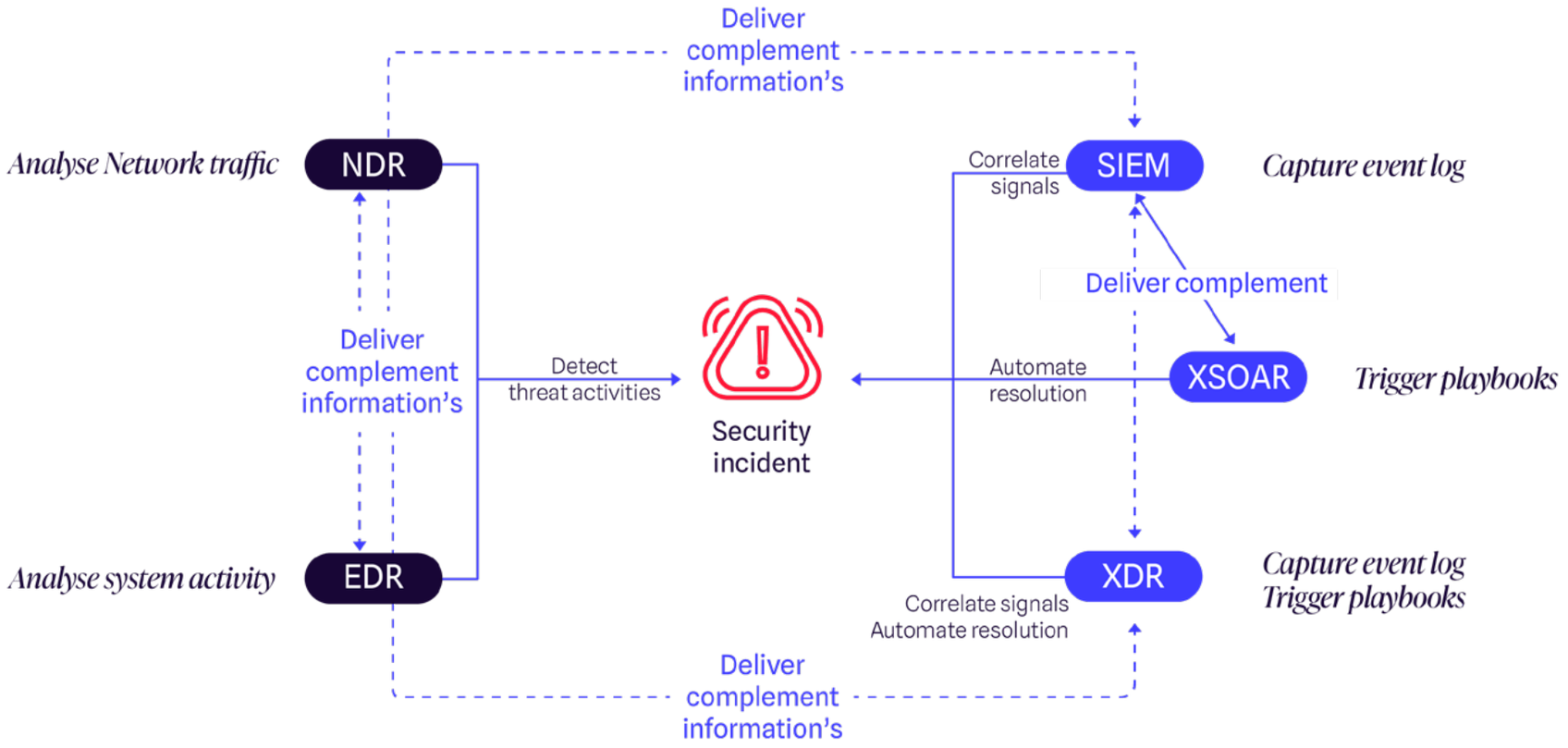
EDR focuses on analyzing system activity and endpoints, while **SIEM** captures and correlates event logs to provide contextual insights into potential threats. **SOAR** takes this a step further by automating responses with triggered playbooks, streamlining incident management. **NDR** complements these 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.

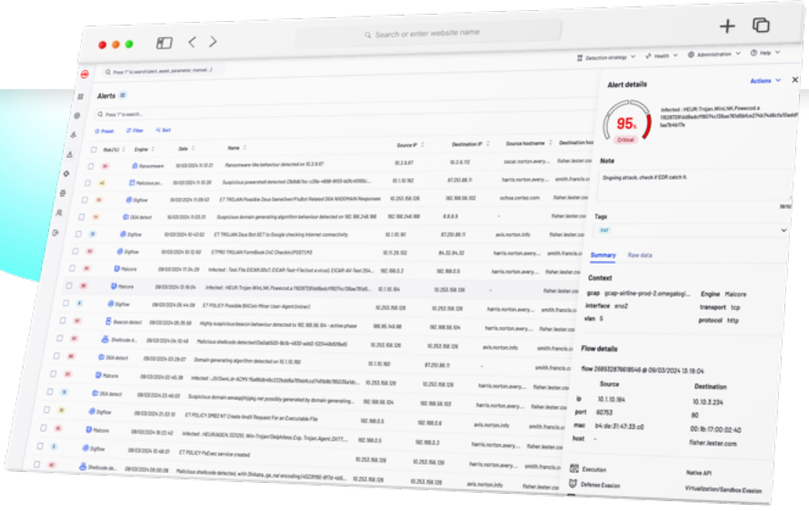
> Simplify security management: Unify detection, investigation, and response in a single platform for streamlined operations and reduced complexity.

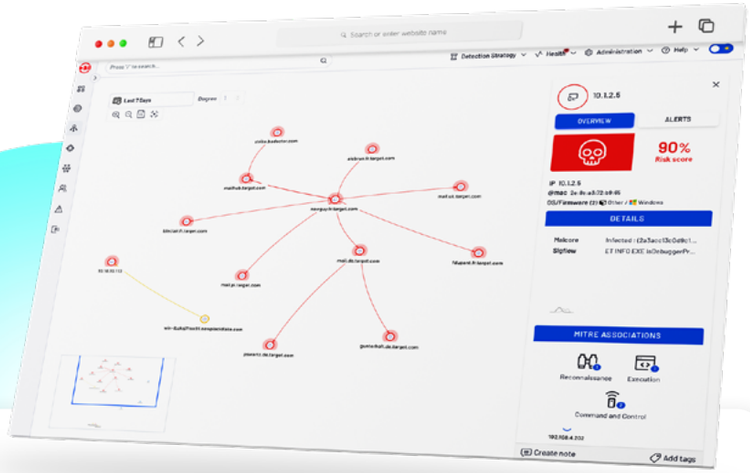
*Scope of action of Gatewatcher NDR Platform: detect, analyze, respond, anticipate_*

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*_

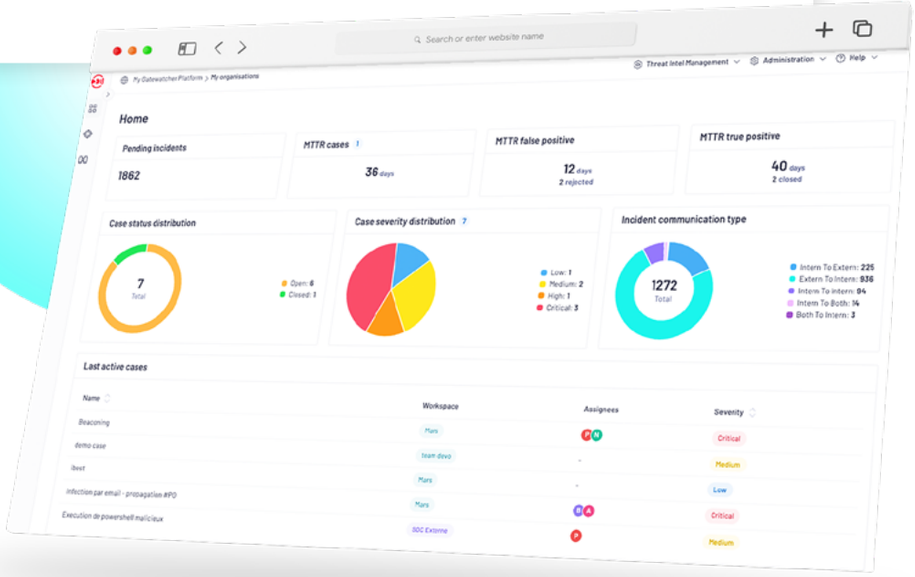
NDR systems empower security / SOC teams to investigate incidents comprehensively by:

> 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.

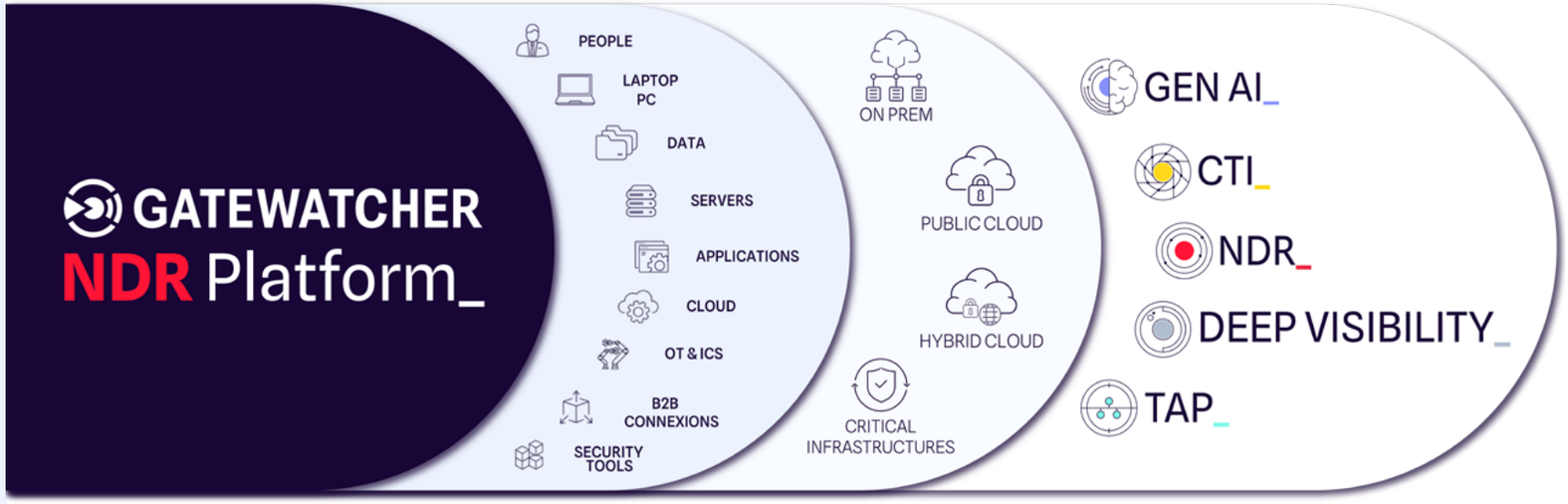
> Fast, targeted threat response: Accelerate remediation with tailored, automated response strategies that adapt to your business needs.

> 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.

The techniques at the heart of our protection model: a combination of complementary detection engines for complete coverage of the kill chain _

Gatewatcher's innovative approach to threat detection leverages a comprehensive suite of analytic engines, each tailored to detect specific types of cyber threats, through a combination of static detection (signatures, code) and intelligent detection (AI/ML).

BEHAVIOR ANALYTICS: SUPERVISED MACHINE LEARNING_

This engine excels in detecting anomalies and behavioral patterns, even on encrypted traffic, through advanced supervised ML models. Its key components include:

> *DGA Detect:* Identifies threats from Domain Generation Algorithms used in malware communications, preventing botnet communication and data exfiltration.

> *Network Behavior Analytics (NBA):* Tracks and analyzes patterns in network traffic to detect deviations indicative of potential threats such as active reconnaissance, brute force attacks, execution, discovery, lateral movement, and data exfiltration. This allows early identification of malicious activities, including data staging and unauthorized access attempts.

> *Ransomware Detect:* Focused on identifying signs of ransomware attacks by spotting unusual encryption activities or data exfiltration behaviors before full-scale encryption begins.

> *Beacon Detect:* Detects beaconing behavior often used in Command and Control (C2) communications by malicious actors, enabling early intervention.

Coming soon: a future enhancement aimed at monitoring and securing Active Directory environments from exploitation, including privilege escalation and unauthorized access.

Gatewatcher's unified approach_

By combining these engines, Gatewatcher delivers a robust, multi-faceted detection platform capable of addressing both known and unknown threats.

This unified approach ensures comprehensive network protection by leveraging:

> **Static detection:** Signature-based methods for precision against known threats.

> **Dynamic analysis:** Behavioral and heuristic approaches for detecting unknown threats.

> **Proactive threat intelligence:** Real-time and historical IoC correlation to enhance situational awareness and mitigate risks.

This multi-engine strategy ensures **Gatewatcher NDR platform** is not only effective against evolving cyber threats but also future-proofed to adapt to new attack vectors.

SIGNATURE-BASED DETECTION_

Utilizing static detection methods, **the Sigflow Engine identifies threats by comparing code and files against known malicious signatures.** By relying on regularly updated databases of Indicators of Compromise (IoCs), Sigflow ensures high accuracy in detecting previously cataloged threats.

Its integration **with the CTI module** further enhances its effectiveness by automating the generation of new rules for emerging threats.

PAYLOAD ANALYSIS_

Focusing on heuristic detection, this category of engine dissects and analyzes code to identify malicious payloads:

> *PowershellDetect:* Monitors for suspicious scripts or commands executed via PowerShell, including encoded or obfuscated payloads, uncovering exploitation attempts with high precision.

> *ShellcodeDetect:* Identifies injected shellcode often used for exploitation or privilege escalation, including polymorphic or dynamically changing shellcodes that evade traditional detection.

MALWARE ANALYSIS_

Dedicated to Advanced Virus (AV) detection, this category employs:

> *Malcore:* A multi-engine solution analyzing files and binaries using both static and heuristic methods. It processes over 6 million files per day and integrates various anti-malware engines to deliver comprehensive real-time detection.

> *Retroanalyzer:* Works in tandem with Malcore to store and periodically reanalyze files flagged as suspicious, leveraging evolving heuristics and signature updates to detect malware missed during initial scans.

> *GScan:* allows users to submit any files and get deep harmfulness insights.

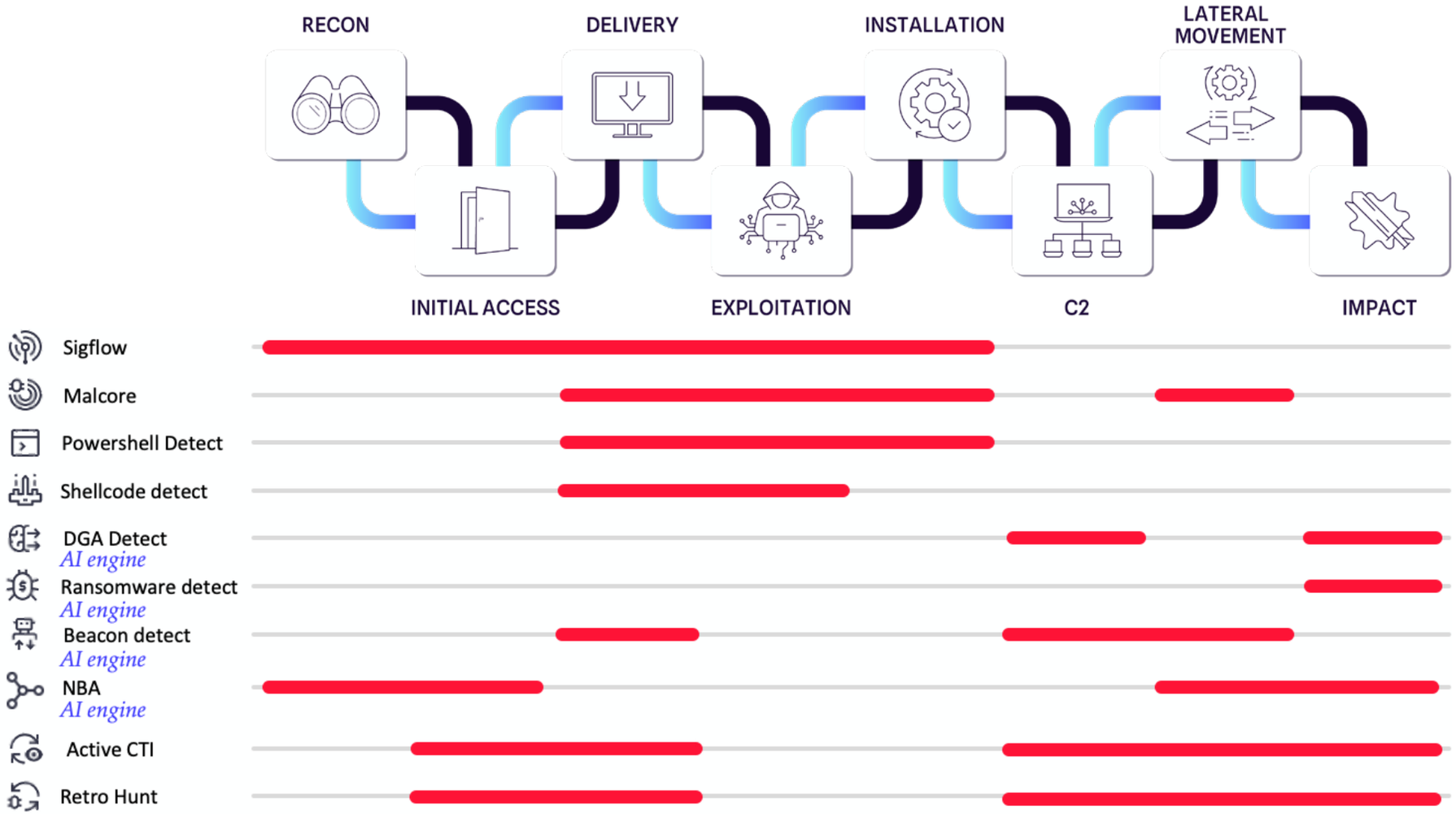
CTI ENGINES_

These category of engines integrate **real-time threat intelligence** to uncover Indicators of Compromise (IoCs):

> *Active Hunt:* Continuously scans for active threats by correlating IoCs with live network activity, ensuring rapid response to emerging risks.

> *Retro Hunt:* Re-examines historical network activity and metadata to identify patterns linked to newly discovered threats, providing retroactive visibility into past attacks.

Engine combination provide *full kill chain coverage*_



*Our vision: hindsight, insight & foresight_*

Gatewatcher NDR platform is designed to foster a state of cyber resilience, equipping organizations with the tools to detect, mitigate and respond to increasingly sophisticated and multifaceted cyber threats. These threats, often unexpected and continuously evolving, demand constant vigilance and proactive strategies. Their impact extends beyond immediate operational disruptions, posing significant risks to an organization's reputation and growth.

This resilience is **built on a foundation of in-depth defense, a layered security model that goes beyond perimeter-based safeguards.** By leveraging continuous monitoring of east-west and north-south network traffic, anomaly detection, and AI-driven behavioral analysis, the platform provides real-time visibility into every facet of network activity. **It ensures that threats are detected not only at their entry points** but throughout their potential lateral movement paths within the system.

The integration of a zero-trust perspective is central to this vision. In the context of NDR, zero trust emphasizes the principle of "never trust, always verify" at the network layer. **This involves monitoring and validating all network traffic, regardless of origin or destination,** with the assumption that any communication could be compromised. By analyzing behavioral patterns, correlating events, and applying AI models trained to detect subtle deviations from expected traffic flows, the platform enforces continuous validation of trustworthiness across the network.

Built on a security-by-design approach, **our solution effectively limits the ability of attackers** to exploit unchecked pathways and reduces the blast radius of potential breaches.

Gatewatcher's expertise in machine learning and relational analysis between users and IT assets provides a unique ability to offer a comprehensive 360° view of potential risks. By remaining independent of the underlying infrastructure, the platform delivers precise threat detection and equips operational teams with the insights and agility required for rapid response.

Finally, **we view cybersecurity as more than an obligation;** it is an enabler of business growth and innovation. By ensuring the integrity, availability, and confidentiality of critical systems, the platform allows organizations to maintain trust with stakeholders, capitalize on digital opportunities, and sustain long-term success.

GATEWATCHER

Cybersecurity for business *serenity_*

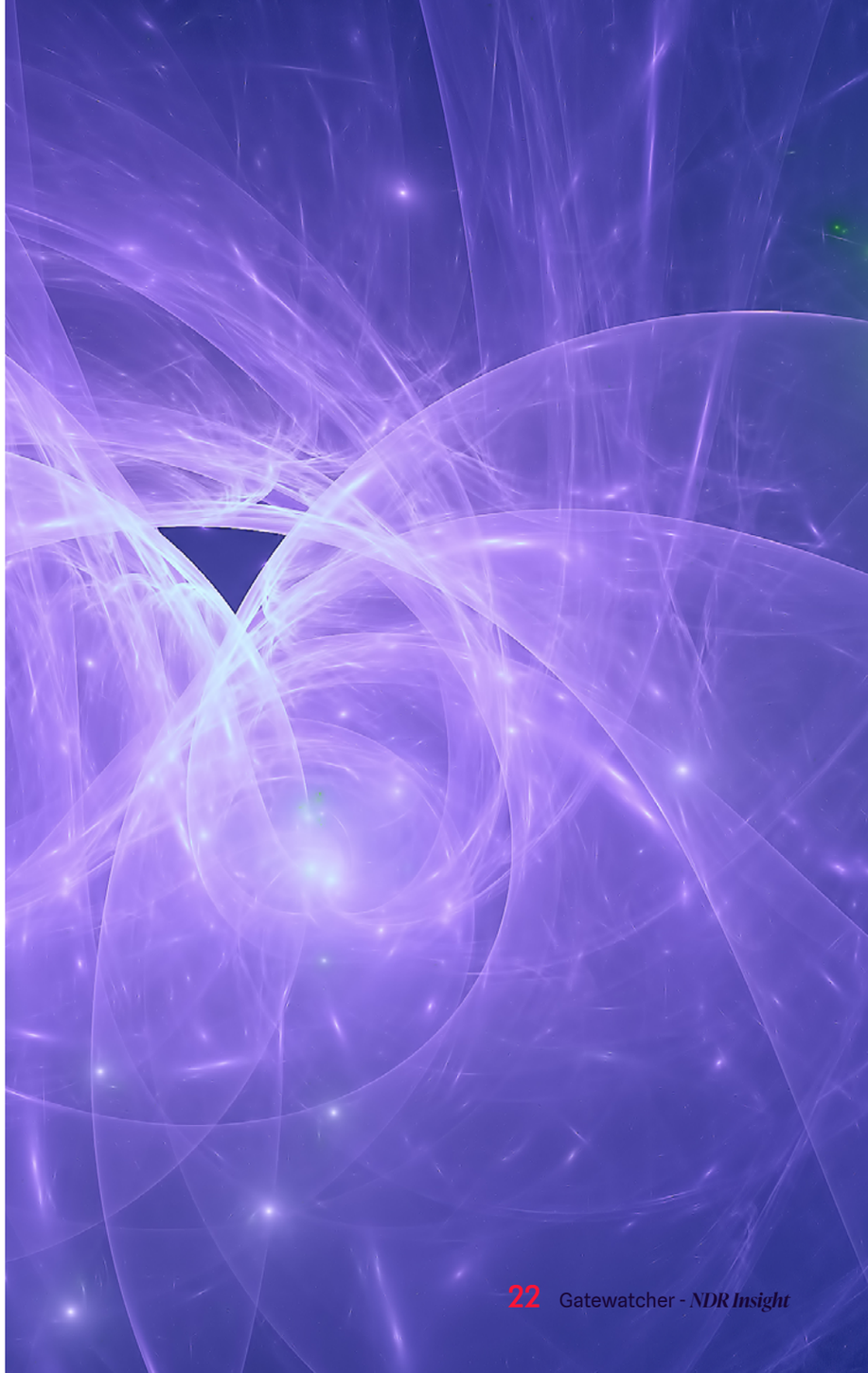
gatewatcher.com

Artificial Intelligence at the heart of our **NDR platform_**

Artificial Intelligence (AI) and Machine Learning (ML) are the cornerstones of **Gatewatcher NDR platform.**

These technologies drive the innovation and efficiency that define our approach to cybersecurity, enabling advanced threat detection, rapid response, and unparalleled adaptability in the face of an ever-evolving threat landscape.

When combined with the capabilities of our Cyber Threat Intelligence (CTI), AI and ML elevate the performance of NDR to a new level of precision and proactivity.



*What does AI bring to detection and response?*_

The incorporation of AI and ML into NDR provides tangible benefits for clients, enhancing both detection and response capabilities.

These advantages include:

> *More precise* recognition_

AI and ML analyze vast amounts of network data, uncovering patterns and anomalies that static, rule-based systems might overlook. This advanced pattern recognition ensures that threats—known, unknown, and hidden—are identified with greater accuracy.

> *Faster* reactions_

Automated detection and response processes enable near-instant reactions to potential threats. This reduces the Mean Time to Respond (MTTR) and minimizes the operational and financial impact of security incidents.

> *Enhanced adaptability* to evolving threats_

Continuously learning and adapting, AI and ML models respond to shifting attack patterns and emerging threat vectors. This adaptability ensures that clients remain protected against dynamic and sophisticated cyberattacks.

> *Reduction* in false positives_

By differentiating between normal and abnormal network behavior, AI reduces false alarms (false positives). This allows security teams to focus on genuine threats, optimizing resource allocation and improving operational efficiency.

> *Proactive* threat hunting_

AI empowers security experts to proactively search for threats within the network before they escalate. Hidden threats, such as those in encrypted traffic or zero-day exploits, can be detected and neutralized early.

> *Automated* reactions and defensive measures_

AI-driven automation enables swift defensive actions, such as IP blocking, device isolation, or patch application, immediately upon detection of a threat. This minimizes potential harm and data loss while improving response efficiency.

> *Improved* incident response_

AI-assisted systems prepare relevant incident data automatically, offering deeper insights into the scope and root cause of incidents. This aids security teams in taking effective remedial measures and accelerating system recovery.

What does AI enable in our NDR Platform?_

AI and ML provide the foundation for the analytical and automated capabilities that make Gatewatcher NDR distinct.

Key contributions include:

*> Plug-and-Detect efficiency_*

Gatewatcher NDR employs supervised ML models that are threat-focused, enabling a “plug-and-detect” approach. This accelerates deployment and immediately identifies “shadow activities” that pose significant risks, even in complex and heterogeneous environments.

*> Deep traffic analysis_*

The integration of detection engines with ML models allows for in-depth analysis of network traffic, even encrypted. This ensures that advanced threats are identified at the earliest possible stage, reducing their potential impact.

*> Detection of known and unknown threats_*

By combining synthetic analyses and advanced queries, our detection engines (static, heuristic, and ML) instantly identify threats, including zero-days, and detect what traditional systems miss, offering complete visibility over your assets and usage.

*> Continuous adaptation to network changes_*

Machine learning continuously adapts from interactions and changes within your infrastructure, automatically adapting to the evolution of environments for optimized and permanent protection.

*> Reduce SOC fatigue and work overload_*

By leveraging ML, our solution optimizes SOC efficiency. It minimizes false positives, anticipates risks and alerts, and automates responses under human supervision, helping rapid recovery and continuous protection of your operations.

*Generative AI: Attackers shouldn't have the GenAI advantage_*

> Not a tool, not a human – just an assistant.
> The aim is to accelerate and focus on what matters.

GAIA, Gatewatcher Artificial Intelligence Assistant, provides a full set of unique capabilities. It breaks security expert's duty boundaries across technical and operational daily activities. Built on cyber security best practices, GAIA integrates seamlessly not only with Gatewatcher's NDR and CTI solutions, but all types of cyber security solutions, even more (network, system, and so on), through a unique interaction entry point (prompt).

While other solutions offer a chatbot or assistant vendor locked-in, with a limited knowledge of the context of the vendor, GAIA breaks the limit and unleashes the assistant capability to any kind of context or solution from a unique prompt.

It has never been so simple to interact quickly with all of your technical solutions.

Based on existing infrastructure, security policies and authorization in place, infrastructure, security policies and authorization. With trust, each user can leverage public, semi-private and private information for every GAIA interaction. In minutes, associated telemetry helps users to highlight the purpose of each information and proactively identify missing information or misleading procedures in documentation or knowledge base. Now users (and security team leaders) can identify and plan accurate cyber resilience improvement.

If needed, your team can reinforce GAIA's capabilities by integrating new tools, exposing APIs, enabling GAIA to interact with them. Executable from Gatewatcher cloud or directly from end-user terminal. Based on their authorization level, users can select the set of actions GAIA can execute without any impact on security account or network policies. Finally, GAIA integrate customizable actions to accelerate recurrent tasks of any security expert who can be focused on valuable activities.

Focus business: GAIA propels our NDR into a new dimension_

> Simplification of investigations:

Easily understand complex alerts

> Accelerate remediation:

Reduce your MTTR through your existing solutions (EDR / FW / XDR / Azure AD / O365)

> Secure utilization:

Based on controlled, qualified, and robust sources, GAIA is a trusted assistant, reducing hallucinations and potential deviations

With **GAIA**, Gatewatcher leverages **Generative AI to strengthen SOC operations** by increasing team's skills and knowledge, anomaly detection, threat identification, incident analysis, impact qualification, decision-making processes and mitigation.. Built on a foundation of domain-specific expertise, GAIA integrates seamlessly with Gatewatcher's NDR and CTI solutions, providing precise, contextual insights that support faster and more informed responses to cyber threats.

Importantly, GAIA operates with human oversight. While it can **interact with all cybersecurity tools**, all remediation actions require manual validation. This ensures that decisions remain precise and aligned with operational needs. GAIA key benefits include faster implementation of security policies, improved accuracy in detecting threats, and reduced time to respond (MTTR), providing SOC teams with a more efficient and reliable workflow.

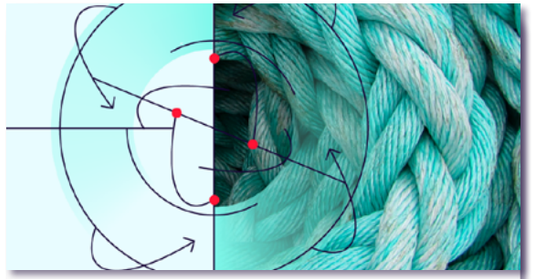
By **combining advanced generative AI with strict security protocols**, GAIA supports cybersecurity teams in navigating the growing complexity of modern threats while maintaining trust and operational control.

Enhancing NDR with comprehensive CTI for Continuous Threat Exposure Management (CTEM)

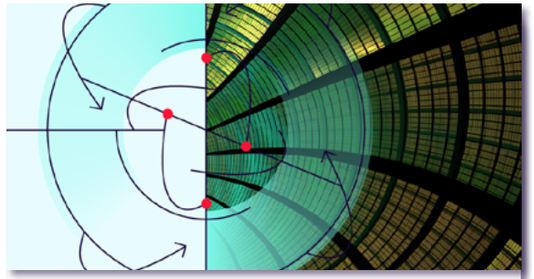
Gatewatcher's Intelligence: Identity, Brand & Exposure

Because knowing your level of exposure is essential for proactively identifying weak points, mastering your entire attack surface, both internal and external, ensures optimal protection against all types of threats. Gatewatcher extends its value proposition in Cyber Threat Intelligence (CTI) through a set of modules tailored to address the critical needs of Continuous Threat Exposure Management (CTEM). These modules provide comprehensive external attack surface management (EASM), enabling organizations to gain better visibility, take proactive measures, and respond effectively to external risks.

Each module focuses on a specific dimension of external threat management: Identity Intelligence, Brand Intelligence, and Exposure Intelligence.



[USE CASE]
Combine NDR and CTI to better understand the threat



[USE CASE]
Enhance or replace my existing NDR system

Business gain

Stay ahead of threats: The business value of EASM (External Attack Surface Management) and NDR

> Lower risk exposure, fewer security gaps

Proactively identify weak points and understand both internal and external attack surfaces to anticipate all types of threats.

> Precisely understand attacker behaviors

Leverage TTPs, precise evidence, and contextual intelligence to improve defenses against evolving threats.

> Accelerate and strengthen your response

Initiate immediate remediation, reduce dwell time, and quickly consolidate a comprehensive response with your other existing solutions.

IDENTITY INTELLIGENCE: PROTECTING EMPLOYEE-LINKED DATA BREACHES_

The Identity Intelligence module addresses risks associated with compromised employee credentials, including high-profile individuals (VIPs). This module allows organizations to swiftly respond by securing employee accounts and privileges, reducing the potential impact of a breach.

Key *Features:*

> *Automated data collection and analysis:* The module scans vast CTI sources to identify leaked data linked to monitored domains.

> *Contextualized risk identification:* It correlates compromised data with employee accounts, highlighting risks for active or former employees.

> *Actionable alerts:* Alerts are delivered via a SaaS console, enabling immediate preventive actions such as forced password resets or account deactivations.

The module enriches its detections with contextual intelligence, derived from both CTI and Gatewatcher NDR Platform, if deployed. For instance, leaked domain names are cross-referenced with company-specific domains configured in the SaaS console. These insights accelerate investigations and streamline remediation efforts. Identity Intelligence also supports automated notifications for employees or immediate remediation, simplifying security awareness and response workflows.

BRAND INTELLIGENCE: DEFENDING ORGANIZATIONAL REPUTATION AND INTEGRITY_

The Brand Intelligence module focuses on protecting corporate domains, subsidiaries, and internal projects from fraudulent activities. This proactive approach helps safeguard interconnected systems and strengthens partnerships by addressing risks posed by adversarial infrastructure.

Key *Features:*

> *Fraudulent infrastructure detection:* The module scans CTI sources to identify links between corporate assets and malicious setups.

> *Prioritized threat alerts:* Risks tied to company brands, projects, or the organization as a whole are prioritized for efficient handling.

> *Streamlined collaboration:* Alerts provided via the SaaS console allow security teams to implement detection policies and collaborate with partners promptly.

> *Threat highlighting*: By expanding on the capabilities of Identity Intelligence, Brand Intelligence highlights broader threats targeting the organization, providing advanced visibility into ongoing and potential attacks on corporate entities.

EXPOSURE INTELLIGENCE: MANAGING RISKS FROM EXTERNAL ASSETS_

The Exposure Intelligence module offers organizations a comprehensive view of their externally exposed assets and associated risks, including misconfigurations and vulnerabilities. This visibility enables prioritization of patch management and identifies improper IT practices like shadow IT.

Key *Features:*

> ***Asset discovery and risk assessment:*** The module monitors exposed technological components, identifies vulnerabilities (e.g., CVEs), and evaluates misconfigurations.

> ***Real-time contextualization:*** Incidents are enriched with relevant data for quick understanding, analysis, and remediation.

> ***Actionable insights:*** Alerts are delivered via a SaaS console, enabling immediate preventive actions such as forced password resets or account deactivations.

This module passively and continuously monitors the evolution of internet-facing components, identifying design flaws or configuration errors that increase cyber risk. By offering inventory capabilities for high-risk assets, Exposure Intelligence empowers cybersecurity teams to maintain robust defenses and anticipate threats effectively.

*Combine NDR and CTI to better understand the threat_*

> Know your enemies, know your network—stop threats before they strike
>
> Thanks to the synergy between NDR and CTI, we move from simple threat detection to contextual understanding, enabling a proactive and strategic defense.

Combining NDR with CTI revolutionizes your cybersecurity posture by providing deeper insights into adversaries and their attack methods. **This synergy enhances threat detection, contextualizes investigations, and optimizes remediation actions.** With External Attack Surface Management (EASM), you gain a complete view of your IT/OT ecosystem, uncovering shadow IT, misconfigurations, and vulnerabilities across internal and external resources.

Gatewatcher NDR Platform also ensures full-spectrum coverage of North-South traffic and East-West traffic, detecting threats at every stage of the kill chain. **By integrating CTI, your NDR platform prioritizes threats based on their business impact, detects attacks earlier, and improves response quality.** With full visibility and context, you can identify vulnerabilities, adapt defenses to attacker behaviors, and respond faster to incidents (MTTR), ensuring robust, proactive protection.

02

MAXIMIZING NDR:
Effective implementation and strategic utilization_

*Seamless deployment and integration to my existing solutions: Comprehensive coverage across environments and perimeters_*

Gatewatcher NDR Platform ensures comprehensive coverage across diverse IT and OT environments, including hybrid and private cloud infrastructures, legacy OT systems, and multi-tenant setups. It provides extensive visibility over East-West and North-South network traffic, detecting lateral movements often missed by traditional solutions. The platform addresses critical infrastructures, such as OT devices, Industrial Control Systems (ICS), BYOD setups, and enterprise applications, ensuring robust protection across all environments and perimeters.

For example, EDRs typically cannot effectively monitor shadow IT, deploy across servers, or provide coverage for OT environments. This results in fragmented protection, leaving many systems vulnerable. By contrast, NDR platforms ensure comprehensive, multi-environment coverage, offering visibility into external users, VIP activities, sensitive data flows, and specialized equipment. This capability closes critical security gaps and allows organizations to achieve unified threat detection and response across diverse and complex infrastructures.

Focus *Business_*

Maximizing security and operational resilience

> Reduce security gaps, strengthen control: Gain full visibility into assets and interconnections to eliminate blind spots and prevent security breaches.

> Minimize business disruptions: Secure critical IT/OT environments without operational downtime, ensuring continuous production and service delivery.

> Lower risk, faster threat response: Real-time threat detection and automated response orchestration reduce attack impact and recovery time.

> Optimize SOC efficiency, reduce costs Intelligent alert prioritization enables faster decision-making, improving incident response while reducing resource strain.

> Seamless, future-proof security integration Plug-and-detect technology ensures rapid, non-disruptive deployment, adapting to evolving infrastructures.

> Hybrid protection: Bridge industrial and digital security to uncover and mitigate hidden threats across complex IT/OT systems.

> Biomedical devices present a unique challenge because they are often outdated and rely on closed or proprietary systems, making it impossible to install security solutions like EDR. In this context, NDR plays a critical role by monitoring the network traffic around these devices and identifying any suspicious activity.
>
> Franck Baibourdian, CISO of Vaucluse Regional Hospital Group

IT_

In IT environments, ensuring comprehensive visibility and security across the network is a fundamental challenge, given the proliferation of devices, users, and applications. NDR platforms address this complexity by continuously monitoring network activity, detecting anomalies, and identifying vulnerabilities.

Key capabilities for *IT environments* include:

- *Real-time asset inventory:* Automated discovery and mapping of IT devices, applications, and services, providing a clear picture of the network's infrastructure.
- *Traffic analysis:* Monitoring all internal and external communications to identify unauthorized access, shadow IT, or misconfigurations that could expose sensitive systems.
- *Threat detection and behavioral insights:* Using AI-driven analysis to detect advanced threats, including lateral movement, data exfiltration, or malware propagation, across IT systems.
- *Business continuity assurance:* Rapid detection and response mechanisms ensure minimal disruption to IT operations during incidents.

By providing visibility into all IT components, including those at the network's edge, NDR enables organizations to enforce security policies effectively, strengthen existing defenses, and mitigate risks in real time.

OT_

Operational Technology (OT) environments present unique security challenges due to their reliance on specialized protocols, legacy systems, and high uptime requirements. NDR platforms extend coverage to OT systems, ensuring seamless monitoring and protection without disrupting critical operations.

Key capabilities for *OT environments* include:

> *Industrial asset identification:* Mapping and monitoring OT devices and legacy systems, to provide a complete inventory of industrial assets.

> *Protocol-specific detection:* Support for industrial communication protocols such as OPCUA, DNP3, MODBUS, IEC104 and S7COM (or data transfer format such as DICOM) allowing for precise identification of anomalies or threats.

> *Lateral movement detection:* Identifying unauthorized connections or data transfers between IT and OT systems to prevent the spread of threats.

> *Policy enforcement:* Ensuring that all traffic complies with predefined security policies while identifying and mitigating non-compliant communications.

> *Tailored response:* Identifying unauthorized connections or data transfers between IT and OT systems to prevent the spread of threats.

NDR platforms empower organizations to secure their OT environments against both external attacks and insider threats. With this coverage, even highly specialized and sensitive OT assets become resilient to modern cyber threats.

IOT_

IoT *coverage*

> *360° visibility:* Identification and tracking of IoT devices, their behaviors, and network communications to detect compromised or misconfigured devices.

> *Behavioral analysis:* Detection of anomalies using AI and Machine Learning to identify threats.

> *IoT protocol support:* Monitoring of the MQTT (Message Queue Telemetry Transport) protocol to detect anomalies.

> *Multi-environment protection:* Blocking lateral movements between IoT, OT, and IT to limit the impact of an IoT compromise in critical environments.

> *Vulnerability management:* Enriching analysis with CTI insights to identify vulnerabilities and link compromised IoT devices to known threats (botnets, malware, etc.).

> *Minimal impact:* Passive and non-intrusive data collection to ensure performance without disruption.

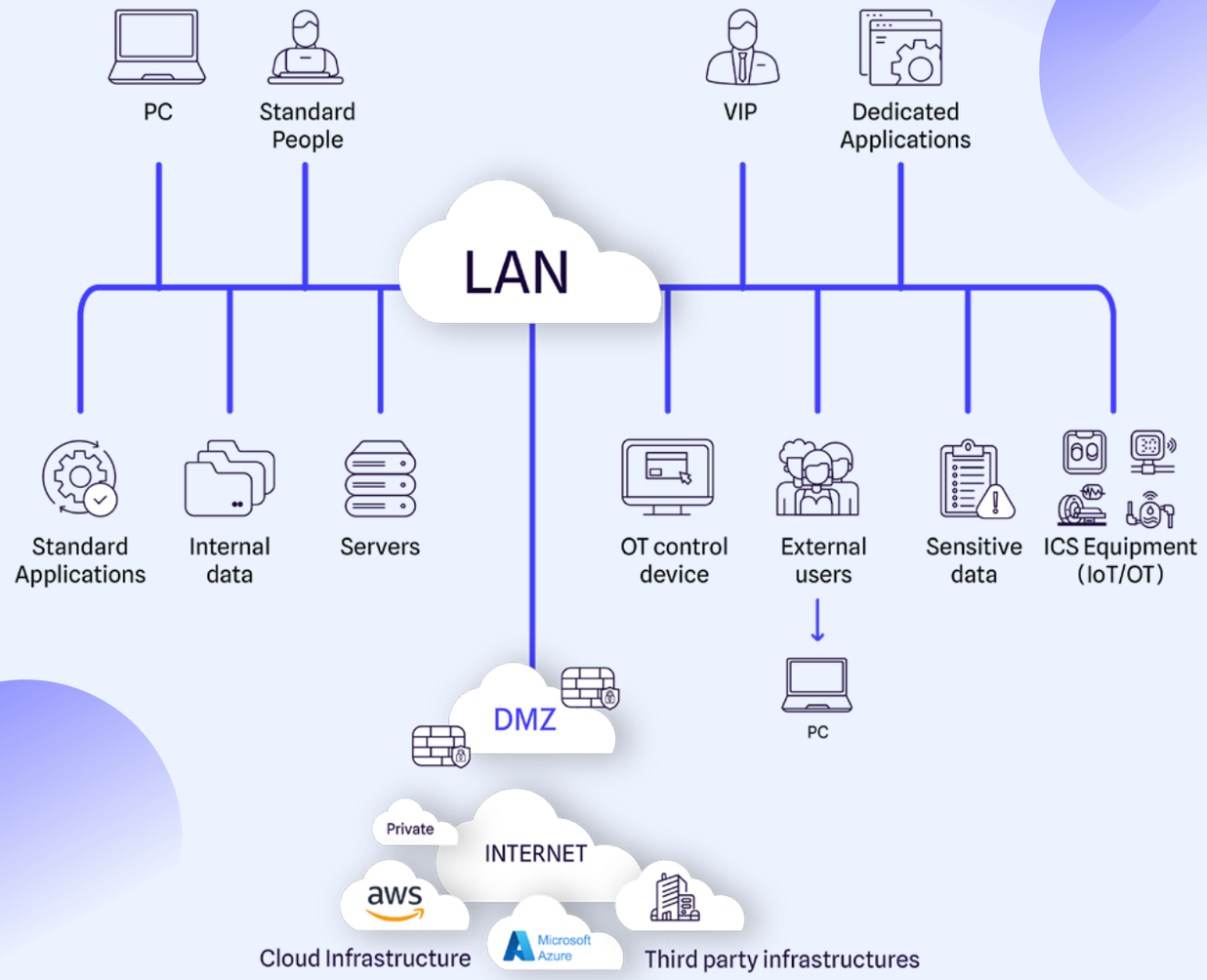
> Leverage a single solution to protect both your on-premises infrastructure and your public cloud.

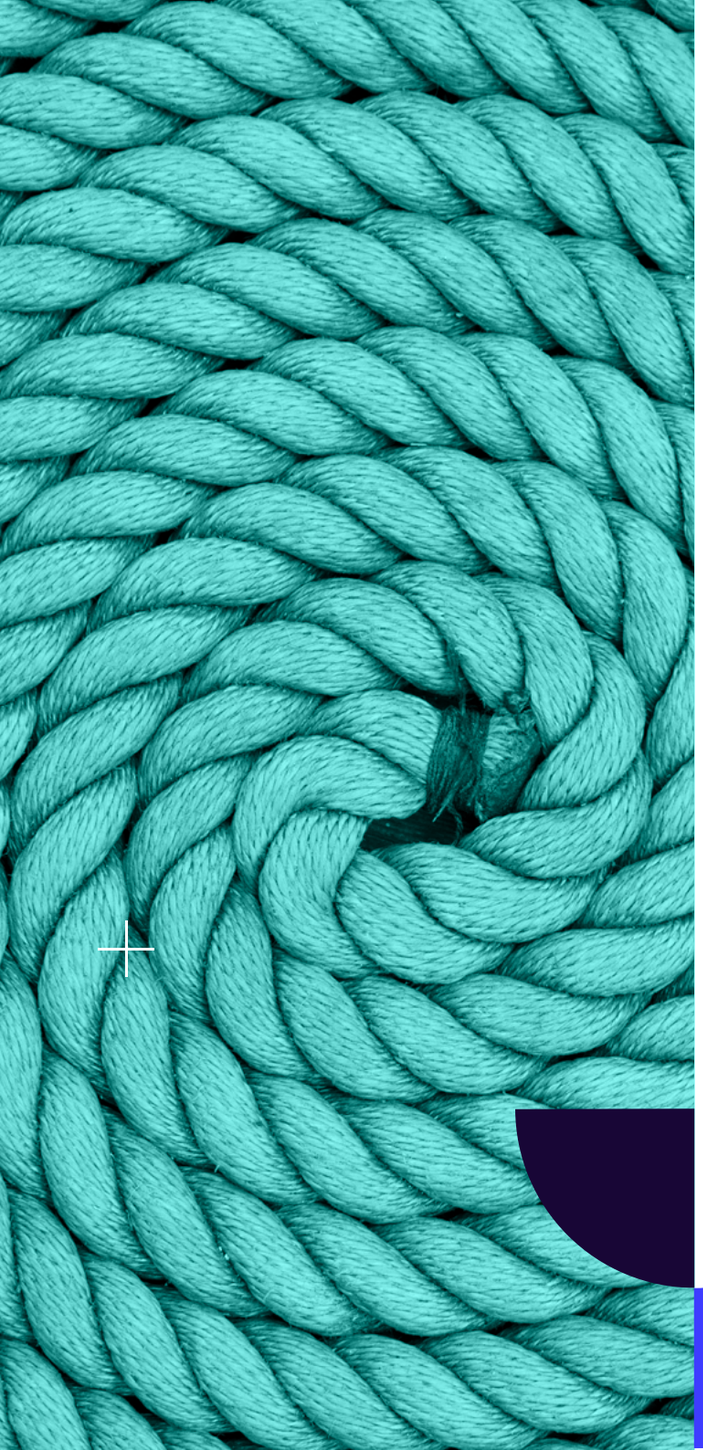
CLOUD_

NDR platform provide deep visibility, advanced threat detection, and efficient response for public cloud environments. They map and monitor all assets, including workloads, containers, and VMs, while addressing challenges like shadow IT and expanding attack surfaces. By analyzing North-South and East-West traffic, NDR detects zero-day vulnerabilities, encrypted anomalies, and lateral movements, ensuring robust protection without disrupting operations.

Key capabilities for *Cloud environments* include:

- *Real-time inventory:* Mapping and monitoring cloud assets such as VMs, containers, and workloads.
- *Traffic analysis:* Continuous visibility into North-South and East-West network flows to identify anomalies.
- *Threat detection:* Identifying zero-day vulnerabilities, encrypted traffic anomalies, and resource impersonation.
- *Prioritized alerts:* Aggregating and scoring alerts based on real-time business impact.
- *Automated response:* Orchestrating one-click remediation and integrating with third-party tools to streamline response efforts.





*Our NDR platform: Tailored value for every role_*

> *Less is more*

Our NDR platform is designed to deliver measurable benefits tailored to the unique concerns and priorities of business leaders, cybersecurity executives, and technical security teams. By addressing each stakeholder's perspective, it ensures alignment between business continuity, strategic security objectives, and operational efficiency.

FOR BUSINESS-LEVEL LEADERS (CEOS, CFOS, ETC.)_

> *Secure growth, controlled risks, optimized costs*

At the business level, the focus is on ensuring business continuity, rationalizing cybersecurity costs, managing risk, and achieving global governance. Our NDR platform empowers leaders to safeguard their products and services, ensuring uninterrupted availability even during cyber crises. By providing a clear understanding of organizational exposure and offering actionable insights into global risks, the platform enables effective decision-making and continuous compliancy. It transforms cybersecurity from a reactive cost center into a proactive investment, fostering trust and resilience in critical operations.

FOR CISOS AND CIOS _

Strategic oversight, tactical excellence, continuous improvement.

Security leaders prioritize balancing strategic foresight with operational effectiveness. Our NDR platform supports them by enhancing security governance and rationalizing strategy. It allows CISOs and CIOs to control their attack surface, anticipate threats, and enforce security best practices across the organization. By delivering advanced visibility and automated responses, it equips them to manage cyber crises efficiently while continuously improving the organization's security posture.

FOR SOC ANALYSTS AND ENGINEERS_

Proactive defense, precision response, empowered operations

SOC engineers are the front line of defense, requiring tools that empower both proactive threat hunting and reactive incident response. Our NDR platform equips them to:

> Proactively spot abnormal behaviors, leveraging advanced behavioral analytics to detect threats at their earliest stages.

> Exploit threat intelligence, integrating actionable insights to stay ahead of evolving attack vectors.

> Conduct detailed threat hunting and forensic investigations, identifying vulnerabilities and understanding attack patterns.

On the reactive side, the platform enhances their ability to:

> Qualify signals effectively, reducing false positives and prioritizing real threats.

> Investigate security incidents thoroughly, providing detailed context and network-wide visibility.

> Remediate intrusions quickly, deploying automated countermeasures to isolate and neutralize threats.

By bridging proactive and reactive capabilities, our NDR platform strengthens SOC engineers' ability to maintain an active defense, ensuring efficient, precise, and effective security operations.

*COCKPIT: « rull them all » with your centralized command for cybersecurity_*

Gatewatcher's Cockpit module revolutionizes incident management with its unified, SaaS-based approach, combining NDR and CTI functionalities into a single intuitive interface. Designed for both IT and OT environments, Cockpit enables centralized case management across infrastructures, whether for end-users or MSSPs. It accelerates investigations with automated incident correlation and prioritization, empowering SOC teams to focus on the most critical threats.

Key *benefits* include:

> *Tailor-made access controls* to ensure secure collaboration across all stakeholders.

> *Real-time monitoring* and actionable insights for rapid remediation.

> *Centralized management* to simplify operations, even for multi-tenant environments.

> *Plug-and-detect capability,* ensuring rapid deployment across sensitive and hybrid systems.

Cockpit provides a complete solution by aggregating and correlating NDR alerts to enhance SOC efficiency, and improve visibility. Its intelligent design correlates similar incidents, speeding up analysis and improving detection accuracy. Teams can benefit from faster investigations, automated workflows, and clear KPIs, such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), ensuring measurable improvements in incident handling.

With its flexible, unified architecture, Cockpit brings together all Gatewatcher functionalities in a single web console, offering comprehensive coverage across all perimeters. From optimizing case prioritization to securing operational continuity, Cockpit equips organizations to rule them all when it comes to cybersecurity operations.

Focus *Business_*

> **Prioritize** your investigation and remediation

> **Simplify** the management of your environments

> **Adapt** the uses and shared responsibilities of the various stakeholders involved

Focus *Business_*

> **Strenghen** your defense arsenal

> **Optimize** your SOC's activities

> **Tailor** your response to your specific environment

*REFLEX –as the new R of NDR_*

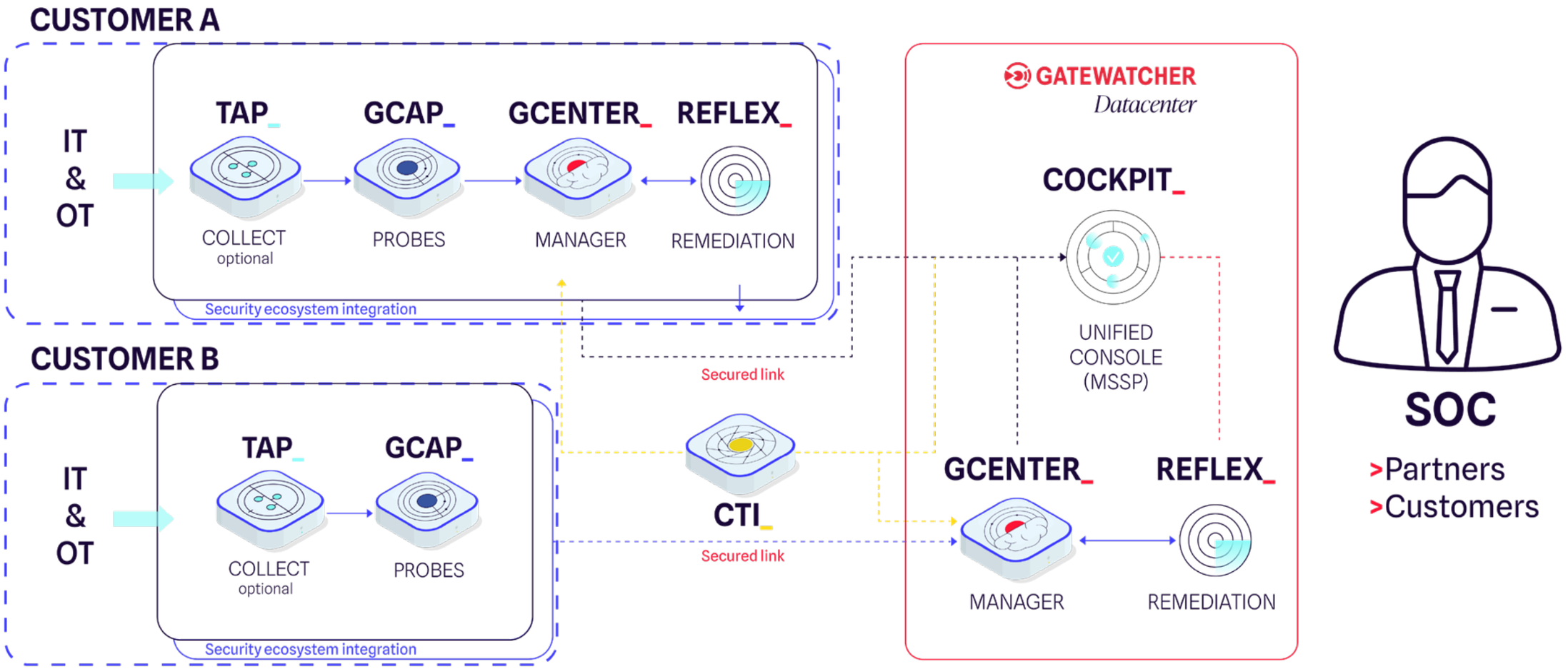
Gatewatcher's Reflex module enhances response efficiency by combining automated workflows with customizable remediation playbooks tailored to specific environments and threat scenarios. Building on the multi-vector threat detection and prioritized alerts from the NDR platform (Cockpit), Reflex enables organizations to execute precise, coordinated response actions across their infrastructure, including firewalls, endpoints, Active Directory, and cloud services.

The use of automated and personalized playbooks allows for both rapid responses and fine-tuned actions adapted to an organization's unique context. Playbooks can handle tasks such as asset isolation, session blocking, account deactivation, and port closures. Customization options enable security teams to define workflows that align with their policies and SLAs, while predefined templates provide an efficient starting point for immediate implementation.

Reflex's strength lies in its extensive integration capabilities, supporting a wide range of APIs including platforms such as Office 365, Fortinet, Palo Alto, Crowdstrike, HarfangLab, and many others. This broad compatibility ensures seamless orchestration within existing ecosystems, whether in connected or isolated environments. Analysts can focus on high-priority threats while Reflex manages repetitive tasks, improving efficiency and reducing response times.

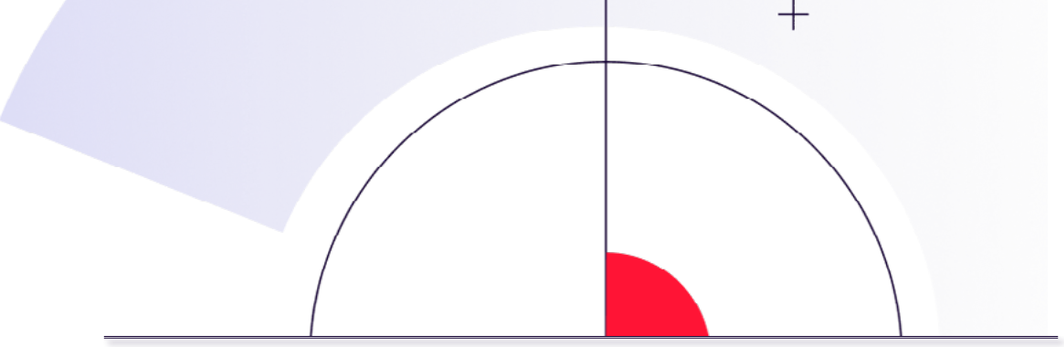
Whether deployed in SaaS or on-premises setups, Reflex delivers a flexible and scalable solution for managing complex cyber threats. By automating routine processes and enabling tailored responses, it ensures organizations can maintain operational continuity while strengthening their defense posture in dynamic threat landscapes.

Gatewatcher NDR: ecosystem interactions_



03

SECURE BY DESIGN, compliant & resilient by nature: The NDR business advantage_



*The business value of NDR: Saving time and minimizing impact_*

REDUCING THE IMPACT THROUGH FASTER RESPONSE_

In today's cyber landscape, **advanced attack techniques can bypass traditional security systems and adapt to existing defenses.** Identifying early intrusion attempts amidst an overwhelming volume of data and complex attack vectors is a significant challenge for cybersecurity teams. Relying solely on perimeter defenses or endpoint detection (EDR) can often result in delayed responses, as intrusions may already compromise critical assets by the time they are detected.

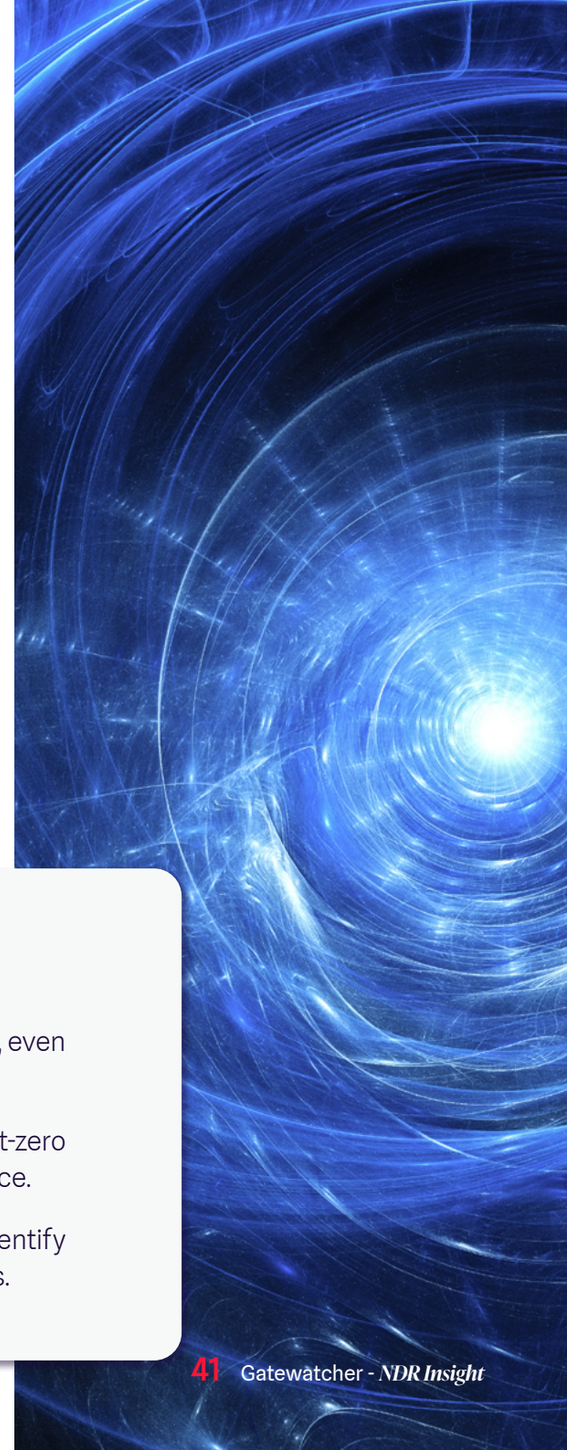
Gatewatcher NDR Platform addresses these challenges by offering real-time detection and retrospective analysis, enabling organizations to act early in the attack chain. **With its multi-engine detection approach, it identifies known and unknown threats,** including zero-day exploits, through dynamic traffic analysis even when encrypted.

Key *Features* include:

> *Real-time analysis of network traffic* to detect malicious activity early, even during reconnaissance phases.

> *Automation of retroactive analyses*, allowing identification of patient-zero and other hidden malicious activities based on updated threat intelligence.

> *Multi-layered detection system*, combining advanced techniques to identify obfuscated attacks and subtle behaviors that evade traditional defenses.



REDUCING TIME TO DETECT (MTTD)_

Dwell time is critical for mitigating business risks. **Gatewatcher NDR enables detection at the earliest stages of an attack by analyzing weak signals in network traffic**, such as suspicious protocol requests or lateral movement attempts. Early alerts allow SOC teams to investigate and act before significant damage occurs, ensuring the protection of critical business assets and minimizing downtime.

REDUCING TIME TO RESPONSE (MTTR)_

Gatewatcher NDR Platform supports faster eradication of threats by providing SOCs with detailed insights into malicious behavior. By leveraging native integrations and custom playbooks, the platform accelerates containment and remediation efforts. The reduction in MTTR directly translates into minimized disruption to operations, as faster response times prevent attackers from escalating their activities.

CRISIS MANAGEMENT AND INCIDENT RESPONSE_

In the event of a crisis, the platform enables deep forensics, bypassing the delays associated with agent-based solutions.

This approach offers:

> Comprehensive visibility into operational network traffic, ensuring attackers' vectors and patient-zero can be quickly identified

> Consolidated analysis of assets, users, and applications through synthetic and advanced query-based investigations.

> Faster initial diagnostics, crucial for containing incidents while maintaining operational continuity.

PROTECTING BUSINESS CONTINUITY_

By detecting malicious activity from the initial access stage, we help limit production disruptions. **The platform's ability to identify early-stage intrusions, such as obfuscated malware or lateral movement, enables SOC teams to act decisively.** This proactive approach ensures threats are isolated and eradicated before they escalate, safeguarding both IT and OT environments.

*The business benefits of enhanced visibility_*

UNCOVERING AND CONSOLIDATING RISKS ACROSS YOUR IT/OT ECOSYSTEM__

Visibility, on user, endpoint and application level is at the core of effective cybersecurity. The unified NDR Gatewatcher platform provides organizations with a centralized view of their assets, users, and network activity. **By leveraging network traffic observability and analysis**—the backbone of all IT activity—**the platform uncovers hidden risks, consolidates key information, and provides actionable insights** to secure business infrastructures.

> *Comprehensive asset and application discovery and mapping:*

Unlock unmatched visibility into your network with our deep observability solutions. The platform automatically identifies and consolidates all active assets, including endpoints, IoT devices, shadow IT components, and infrastructure such as servers and firewalls. This ensures a real-time inventory of assets, allowing organizations to understand their exposure and prioritize protection efforts for the most critical systems.

> *Traffic recording:* Capture every packet with precision—zero loss, total visibility. Our high-fidelity solutions scale seamlessly from edge to core networks, ensuring uncompromised performance and in-depth analysis anywhere.

> *User consolidation and analysis:*

By analyzing protocols and application layer its reinforce security team with real-time network insights, proactive diagnostics, and accelerated issue resolution. Maximize efficiency, optimize performance, and slash your Mean Time to Resolution. Risk-based scoring highlights users with abnormal behavior or heightened exposure, enabling SOC teams to focus on the most pressing threats.

> *Proactive Network optimization:* Detect anomalies faster, pinpoint root causes instantly, and optimize bandwidth for peak efficiency. Reduce latency, enhance performance, and empower your IT team with actionable insights.

STREAMLINING RISK MANAGEMENT WITH MAPPING AND SCORING_

Gatewatcher's platform provides powerful tools to track and manage cyber risks:

> *Dynamic mapping:*

Visualize at-risk assets, users, and their interconnections, allowing SOC teams to track the propagation of threats and isolate compromised systems.

> *Risk scoring:*

Evaluate the exposure of assets and users based on their environment and activity, enabling data-driven prioritization of security actions.

> *Focused threat insights:*

Identify shadow IT, unmanaged systems, and unusual traffic flows that could indicate vulnerabilities or active threats.

PROACTIVE AND UNIFIED PROTECTION_

By consolidating assets, users, and network activity into a single, unified view, the Gatewatcher platform enables organizations to:

> *Gain complete visibility* into active and vulnerable assets across their ecosystem.

> *Prioritize incident response* based on risk, ensuring targeted protection of critical systems.

> *Detect and act on threats* early, before they can disrupt operations

*A secured solution_*

Gatewatcher places a strong emphasis on the overall security of its products. Through its comprehensive and systematic approach, **Gatewatcher ensures the secure operation of your detection solution,** a cornerstone of your defense strategy .

> The individual security of each component ensures comprehensive protection

GATEWATCHER NDR, SECURED BY DESIGN_

Any component of an application solution can contain security vulnerabilities (CVEs) of varying severity, which could potentially be exploited by an attacker.

With this in mind, **Gatewatcher systematically incorporates a security-by-design approach into its development cycles**. As a result, the risk of exploiting new vulnerabilities that could affect any component of our NDR is eliminated.

> *Hardened security at all levels* – hardware, system, session, application, and network connections – ensuring availability, integrity, authenticity, and confidentiality of data.

> *Protection against physical and remote threats* – preventing unauthorized access and ensuring resilience against external and internal attacks.

> *Granular access control* – role-based access control (RBAC) aligned with ANSSI standards, reducing risks associated with unauthorized privileges.

> *Advanced kernel hardening* – reinforced Linux security, protection against denial-of-service (DoS) attacks, memory execution restrictions, and address space layout randomization (ASLR) to counter exploits.

> *Zero-day attack mitigation* – integration of advanced security mechanisms (PaX) to block emerging threats before they can be exploited.

TRACKWATCH: CERTIFIED SECURITY FOR ADVANCED THREAT DETECTION_

Gatewatcher was the first company to receive ANSSI qualification for its detection capabilities in 2017, renewed in 2023, demonstrating the high level of intrinsic security in its technology .

Our detection system enhances identification and qualification capabilities while adhering to the most stringent security requirements:

> *Threat detection, even on encrypted traffic* – using a combination of static, heuristic, behavioral, and machine learning-based detection to identify concealed threats.

> *Intelligent threat prioritization* – aggregating alerts and assessing their criticality to enhance SOC efficiency.

> *Air-gapped deployment for sensitive environments*– fully offline operation, ensuring complete control over data and compliance with restricted network security policies.

> *Zero impact on production* – passive monitoring via certified TAP integration, avoiding disruption to business operations.

> *Advanced file analysis* – Enhance your malware detection capabilities with analysis powered by multiple antivirus engines. The platform can examine up to 6 million files per day and retrospectively analyze files flagged as suspicious after their initial processing.

TURNING COMPLIANCE CHALLENGES INTO SECURITY ADVANTAGES

As technology evolves, so does regulation. **Organizations now face increasing complexity in maintaining compliance.** Each regulation imposes specific requirements, often demanding costly adjustments to existing security frameworks. Many organizations struggle with limited or outdated technologies, significant compliance costs, and the need for a comprehensive security strategy that aligns with regulatory expectations while ensuring operational resilience.

> *Identifying and assessing risks*

A complete view of network assets is essential for understanding an organization's technical and organizational risks. Without clear visibility, security policies remain ineffective, leaving gaps in protection.

> *Protecting sensitive data and information*

Regulations require organizations to ensure the confidentiality, integrity, and availability of critical information systems. Without robust control over interconnections and data flows, sensitive information remains at risk.

> *Managing and responding to incidents*

Compliance mandates not only incident detection but also rapid response to limit business impact. Organizations must ensure that alerts are prioritized, remediation is orchestrated, and incident reporting is structured and efficient.

How *NDR strengthens* compliance and security_

With NDR, regulatory compliance is not just an obligation—it is **an opportunity to strengthen cybersecurity posture** and gain greater control over risk management.

> *Identify* all network assets in real time, providing complete mapping of IT, OT, IoT, VM, and Cloud environments, as well as attack surface analysis.

> *Protect* data and infrastructure by controlling inbound and outbound communications, securing interconnections, and maintaining oversight of all IS resources.

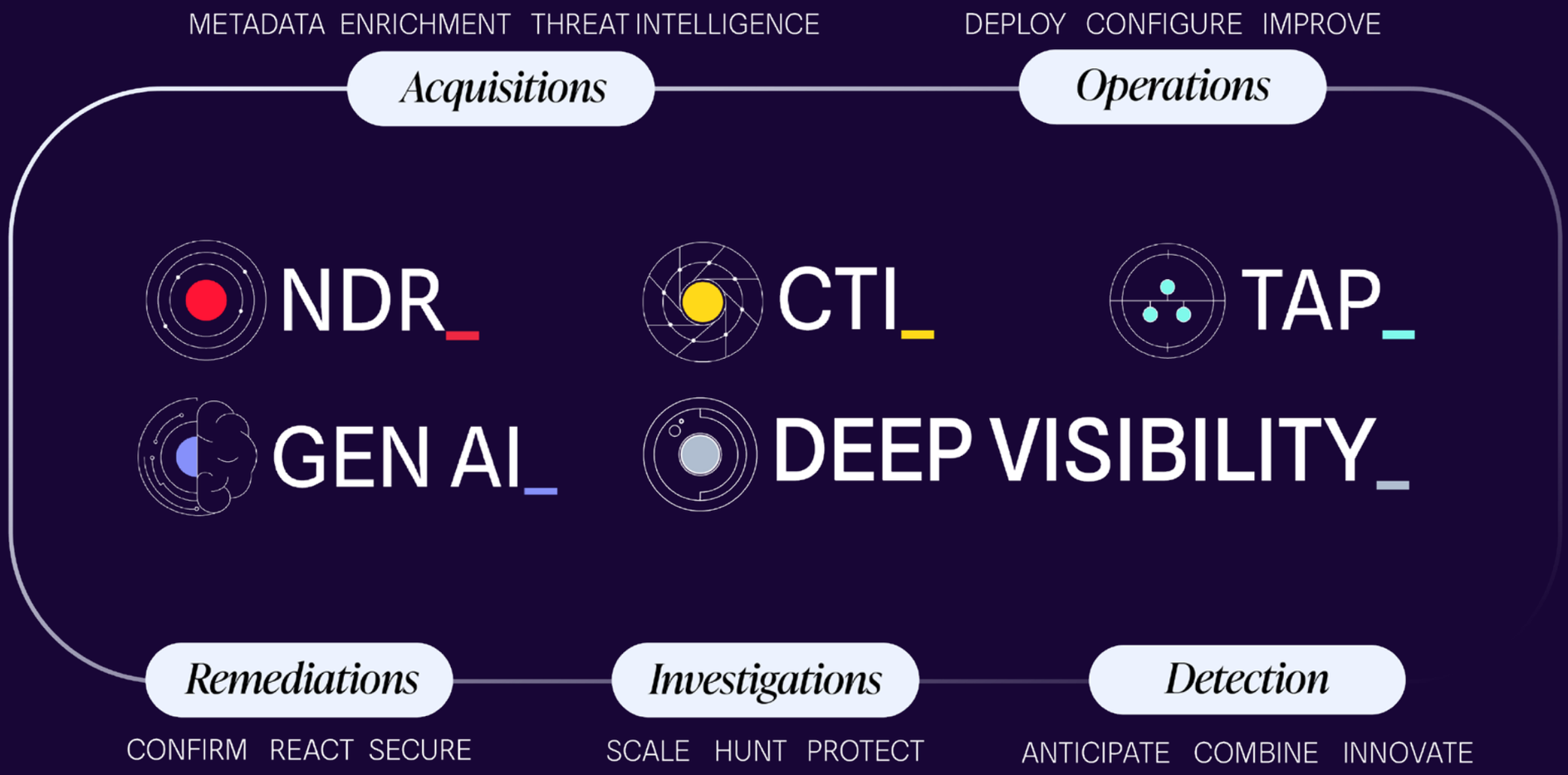
> *Detect* threats at every stage, leveraging multiple detection engines, proactive attack identification, and enhanced forensic capabilities to provide deep insight into security incidents.

> *Respond* effectively with intelligent alert aggregation, prioritized threat processing, automated remediation, seamless integration with existing security tools and rapid, detailed report generation.

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:*

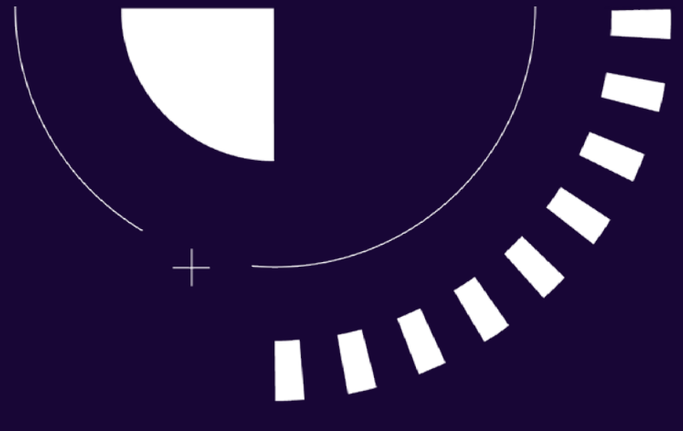
SOC teams face alert fatigue and operational overload. NDR prioritizes and contextualizes threats, allowing faster, smarter decision-making.

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.