



STREAMING DEFENSE

a new dimension in cybersecurity

Enhancing the Network Detection and Response (NDR) Market with Streaming Defense

MARKET PERSPECTIVE

Contents

Introduction	01
Challenges in the NDR Market	01
Streaming Defense: Enhancing the NDR Market	02
Benefits to Organizations	02
About Streaming Defense	03
Key Features & Benefits	03
Summary	03

Introduction

Defending an organization's networks from cyberattacks is a complex and ever-changing challenge. As cyber threats grow increasingly sophisticated, traditional security measures often fall short in providing the necessary protection.

Network Detection and Response (NDR) solutions have become essential for countering these advanced threats. Streaming Defense is at the forefront of this field, significantly enhancing the NDR market with its unmatched real-time threat detection and response capabilities.

This paper illustrates how Streaming Defense strengthens the NDR landscape, offering organizations robust protection against modern cyber threats and ensuring the integrity and security of their digital assets. With a focus on real-time threat termination, advanced analytics, and seamless integration, Streaming Defense provides a comprehensive solution that addresses the key challenges faced by security teams today.

Challenges in the NDR Market

The NDR (Network Detection and Response) market faces a multitude of challenges, each presenting significant barriers to effective cybersecurity:

Evolving Threat Landscape: The landscape of cyber threats is in a constant state of flux, marked by the relentless ingenuity of attackers who continuously develop sophisticated tactics to evade traditional defenses. To effectively counter these threats, NDR solutions must exhibit a high degree of adaptability, consistently refining their algorithms and methodologies to detect and neutralize emerging threats promptly.

Latency in Detection and Response: One of the primary vulnerabilities of many existing NDR solutions lies in the latency inherent in their detection and response mechanisms. Delays in identifying and responding to threats not only increase the risk of successful attacks but also amplify the potential damage inflicted upon organizations. Real-time detection and instantaneous response capabilities are imperative in the modern cybersecurity landscape, where swift action is crucial in mitigating the impact of cyber incidents.

Data Overload: The exponential growth of network traffic results in a deluge of data that overwhelms security teams, making it challenging to sift through and prioritize potential threats. Effective NDR solutions must possess robust data processing capabilities, leveraging advanced analytics and machine learning algorithms to distill the noise and pinpoint anomalous activities. By efficiently processing data, these solutions empower security teams to focus their efforts on addressing the most critical alerts, thereby enhancing their defense posture.

Integration Complexity: Integrating NDR solutions with existing security infrastructures presents a formidable challenge, characterized by complexity and interoperability issues. Achieving seamless integration requires careful planning, substantial investment of time and resources, and a comprehensive understanding of the compatibility requirements between different security tools. A harmonious integration framework is essential to ensure that NDR solutions complement and enhance the overall security architecture of the organization, rather than introducing additional complexities or vulnerabilities.

In navigating these challenges, organizations must prioritize innovation, collaboration, and a steadfast commitment to strengthening their cyber defenses. By leveraging the full capabilities of NDR solutions, organizations can effectively safeguard their digital assets and maintain operational resilience in the face of evolving cyber threats.

Streaming Defense: Enhancing the NDR Market

Real-Time Threat Detection: Streaming Defense leverages advanced AI and ML algorithms to analyze network traffic at wire speed, providing instantaneous threat detection. Unlike traditional NDR solutions that operate with latency, Streaming Defense ensures that threats are identified and neutralized in real time, significantly reducing the risk of damage.

True Real-Time Termination: Streaming Defense is the only solution that offers true real-time termination of rogue connections as soon as they are detected. This capability allows organizations to instantly isolate and neutralize threats, preventing them from escalating into breaches and causing harm.

Behavioral Analytics: By continuously monitoring network traffic and analyzing behavioral patterns, Streaming Defense can detect anomalies indicative of malicious activity. This proactive approach enables security teams to identify threats such as unauthorized access attempts, abnormal data transfers, and unusual user behavior, even before they escalate into serious incidents.

Scalability and Flexibility: Streaming Defense is designed to scale with the growing needs of modern enterprises. Whether deployed in small businesses or large enterprises, it offers flexible deployment options that integrate seamlessly with existing security infrastructure. This ensures comprehensive network visibility and protection across all environments.

Automated Threat Mitigation: With automated response capabilities, Streaming Defense can instantly neutralize threats upon detection. This includes isolating affected systems, blocking malicious traffic, and alerting security teams for further investigation. By minimizing the window of opportunity for attackers, Streaming Defense helps prevent potential breaches and data exfiltration.

Comprehensive Threat Intelligence: Streaming Defense incorporates up-to-date threat intelligence from various sources, enhancing its ability to detect and respond to emerging threats. This continuous integration of threat intelligence ensures that organizations are protected against the latest attack vectors and techniques used by cybercriminals.

Simplified Integration: Streaming Defense offers straightforward integration with existing security tools and platforms, reducing the complexity and time required for deployment. This ease of integration allows organizations to quickly enhance their NDR capabilities without disrupting their current operations.

Benefits to Organizations

- 🔥 **Reduced Risk of Breaches:** By providing real-time detection and automated response, Streaming Defense significantly lowers the risk of successful cyber-attacks and data breaches.
- 🔥 **Enhanced Operational Efficiency:** Security teams benefit from reduced data overload and prioritized threat alerts, enabling them to focus on critical incidents and respond more effectively.
- 🔥 **Improved Compliance:** Streaming Defense helps organizations meet regulatory requirements by ensuring robust network security and comprehensive threat monitoring.
- 🔥 **Cost-Effective Security:** With scalable deployment options and automated threat mitigation, organizations can achieve high levels of security without incurring excessive costs.

More about Streaming Defense

Streaming Defense revolutionizes threat response by combining wire speed, in-memory, and AI processing to instantly provide security operators with threat intelligence.

This empowers them to respond faster and more effectively than ever before. Unlike alternatives that write data to disk, our solution offers analysts the unique capability to immediately terminate threats.

This new dimension in cybersecurity ensures superior security outcomes, enhances analyst experience, reduces bottlenecks, and significantly minimizes dwell time and risk.

Key Features and Benefits



Real-Time Threat Detection: Streaming Defense provides real-time monitoring and analysis of network traffic, enabling the immediate identification of attacks and threats.



Full Visibility of Threats: Streaming Defense provides comprehensive visibility into network activities, enabling organizations to detect and respond to threats swiftly and accurately.



Proactive Threat Mitigation: Streaming Defense enables organizations to take proactive measures at wire-speed to mitigate risks, such as blocking suspicious transactions, terminating unauthorized sessions, and alerting security teams to potential threats.



Continuous Adaptation: Leveraging machine learning and AI-driven analytics, Streaming Defense continuously learns from security events and adapts its detection techniques to detect emerging fraud trends and evolving attack techniques.



Exfiltration Detection: Streaming Defense includes advanced capabilities for detecting data exfiltration attempts, enabling organizations to identify and prevent unauthorized data transfers, mitigating the risk of data breaches and intellectual property theft.



Integration Capabilities: Streaming Defense seamlessly integrates with existing fraud prevention systems and security tools, enabling organizations to orchestrate coordinated response efforts and enhance overall fraud defense capabilities.



Scalability and Flexibility: Designed to scale with the growing needs of organizations, Streaming Defense offers flexibility in deployment options and licensing models, ensuring seamless integration into existing security infrastructures and workflows.

In Summary

Streaming Defense redefines the NDR market by addressing its key challenges with cutting-edge technology and real-time capabilities. By enhancing threat detection and response, providing comprehensive threat intelligence, and ensuring seamless integration, Streaming Defense empowers organizations to defend against sophisticated cyber threats effectively.

Embracing Streaming Defense as part of their cybersecurity strategy allows businesses to maintain robust network security and confidently navigate the complexities of the modern threat landscape.

See the Attack – **Contain** the Attack – **Kill** the Attack

