Trellix

5 Top GenAI Strategies for Stronger Network Detection and Response

Eliminate alert fatigue, close talent gaps, and boost ROI with GenAI-driven NDR

Table of Contents

Introduction

The cybersecurity landscape has reached an inflection point. As security leaders, you're navigating an unprecedented convergence of opportunity and risk where generative AI (GenAI) promises to revolutionize network detection and response (NDR)—while introducing new complexities that demand strategic consideration.

Attackers are increasingly using AI for sophisticated phishing, vishing, and social engineering attacks, with AI enabling threat actors to streamline and automate each stage of the cyber kill chain. This creates competitive pressure for defenders to adopt AI-enhanced NDR capabilities to maintain detection efficacy.

In addition, the average cost of a data breach reached a record high of $4.88 million in 2024, representing a 15% increase since 2020.[1] Traditional NDR solutions struggle with sophisticated attacks that are becoming more effective and harder to detect, and are occurring at an alarming rate and scale.

Navigating the journey to GenAI adoption

The issue, then, isn't whether to embrace GenAI, but how to do so while maintaining security, compliance, and operational excellence. The organizations that master this balance will gain decisive advantages in threat detection, response efficiency, and operational resilience. Those that delay risk falling behind in an accelerating threat landscape where traditional approaches are increasingly insufficient.

Your journey toward AI-enhanced network detection and response starts here—by following the practical steps we outline in this guide to enhance cybersecurity operations with GenAI.

Today's network security reality calls for GenAI

- Networks span multicloud environments, hybrid infrastructures, and expanding device ecosystems.
- Traditional detection methods struggle with the volume, velocity, and sophistication of modern threats.
- Adversaries increasingly leverage AI to enhance their capabilities, creating a defensive arms race.
- Security operations centers require intelligent automation to augment human expertise.

[1] "Top 10 CISO Statistics and Trends in Cybersecurity for 2024," SOCRadar, Sept. 25, 2024.

Critical operational challenges to consider

A number of factors can complicate the decision to adopt GenAI, including the following:

Budget Constraints vs. Security Demands

Security leaders face mounting pressure as multiple industry forecasts show significant cybersecurity budget increases for 2025.[2] This reflects the urgent need to address expanding attack surfaces and AI-driven threats.

However, recent research estimates that GenAI will cause a more than 15% incremental spend on application and data security through 2025.[3] This creates a challenging scenario where security executives must justify additional AI investments while managing existing budget constraints.

Data Sovereignty and Model Training Risks

According to a recent study, many organizations lack adequate protections and governance to securely implement GenAI.[4] Gaps in data security present a significant risk for exposing network data during GenAI model training or inference.

69%

Risk of AI-powered data leaks

47%

Lack of AI-specific security controls

55%

Unprepared for AI regulatory compliance

40%

Lack of protection for AI-accessible data

94%

Lack an advanced AI security strategy

[2] "2025 cybersecurity budget: How to allocate funds for maximum protection?" NordLayer, Dec. 17, 2024.
[3] "Cybersecurity In 2024: Startling Insights from Over 1000+ CISOs," Software Analyst Cyber Research, Jan. 24, 2024.
[4] "New Study Reveals Major Gap Between Enterprise AI Adoption and Security Readiness," PR Newswire, Jun. 4, 2025.

Alert Fatigue and False Positive Management

Security teams are overwhelmed with tools (more than 30 on average), which can be a hindrance rather than a help.[5] GenAI promises to reduce this complexity, but early implementations often struggle with accuracy, requiring careful tuning to avoid exacerbating the false positive problem that already plagues traditional NDR solutions.

Data Sovereignty and Model Training Risks

Network detection requires analyzing sensitive network telemetry data. In a recent survey, about 69% of security leaders cited AI-powered data leaks as their top security concern in 2025, yet nearly half (47%) have no AI-specific security controls in place.[6] This creates a significant risk when implementing GenAI for NDR, as network data could inadvertently be exposed during model training or inference.

Talent Shortage Meets AI Complexity

Seventy-four percent of CISOs identified human error as their organization's biggest cyber vulnerability in 2024, up from 60% in 2023.[7] Yet hiring cybersecurity talent continues to be a challenge, driven by rapid advancements in technology struggling to keep pace with demand.[8] The introduction of GenAI for NDR adds another layer of complexity, requiring specialized skills that are even scarcer in the market.

As well, in a recent survey, 55% of organizations indicated they are planning to implement GenAI solutions, while only 6% feel highly confident in their AI security preparedness.[9] This number is expected to rise going forward, given that cybersecurity analysis requires advanced skills that many organizations struggle to afford or find security professionals with the necessary expertise to hire.

So how can you overcome these challenges and start reaping the benefits of GenAI? Read on for key steps to take.

[5] "Top 10 CISO Statistics and Trends in Cybersecurity for 2024," SOCRadar, Sept. 25, 2024.
[6] "New Study Reveals Major Gap Between Enterprise AI Adoption and Security Readiness," PR Newswire, Jun. 4, 2025.
[7] Ibid
[8] "A CISO's View On 2025," Cybersecurity Asia, Dec. 20, 2024.
[9] "New Study Reveals Major Gap Between Enterprise AI Adoption and Security Readiness," PR Newswire, Jun. 4, 2025.

5 strategies for successful GenAI NDR adoption

GenAI implementation offers a transformative solution to the persistent cybersecurity talent shortage by democratizing advanced security capabilities across skill levels. Modern AI platforms enable users of any experience level to perform sophisticated threat hunting and create automated responses using natural language queries, eliminating dependency on highly specialized analysts for routine operations.

This approach allows junior staff to investigate, respond, and learn on the job through AI-guided analysis that provides detailed explanations and recommended remediation actions. By augmenting human expertise rather than replacing it, AI systems enable existing teams to handle exponentially larger workloads while developing skills through continuous interaction with expert-level guidance for more resilient security operations.

But to successfully realize these goals, organizations must first address five critical barriers through integrated approaches:

Data Privacy and Sovereignty

To ensure data privacy, organizations must adopt secure AI processing that maintains complete data sovereignty, shielding sensitive network traffic while enabling sophisticated analysis. This involves deploying AI models and processing network metadata and telemetry data within controlled environments, while maintaining access to global threat intelligence.

Model Accuracy via Multivector AI

Model accuracy requires implementing multivector AI systems combining 30+ specialized machine learning models across endpoint, email, network, and sandbox data sources, integrated with real-time intelligence from billions of daily threat queries. These systems incorporate expert-guided learning that enables continuous improvement through security analyst feedback while providing explainable decision-making processes that build analyst trust.

Building the case for GenAI NDR

Before implementing GenAI NDR, assess your organization's readiness across these critical areas:

- Current alert volume exceeding team capacity (>1000 alerts/day typically justifies AI investment)
- Existing security tool integration capabilities
- Data governance policies supporting AI training
- Stakeholder alignment on AI strategy
- Baseline metrics for measuring improvement

Organizations with mature network security deployments, established incident response processes, and clear compliance requirements typically see faster GenAI adoption success. Consider starting with pilot programs in controlled environments to demonstrate value before enterprisewide deployment.

Use Case Prioritization and Business Alignment

Effective GenAI deployment requires strategic focus on high-impact use cases that demonstrate clear business value. Security leaders should begin by eliminating alert fatigue, where AI automatically triages and prioritizes threats, followed by automated investigation and summarization that reduce manual investigation time.

Advanced use cases include AI-powered threat hunting that identifies sophisticated attacks missed by traditional tools and predictive analytics that anticipate emerging threats or potential attack paths. Each implementation phase should target specific operational pain points while building foundational capabilities.

For sustained organizational transformation, success depends on measuring concrete outcomes such as reduced mean time to detection, increased investigation capacity, and improved analyst productivity, rather than focusing solely on technical performance metrics.

Top Network Security Use Cases for GenAI

Eliminate alert fatigue

Automate alert investigation and summarization

Deploy AI-powered threat hunting

Anticipate emerging threats with predictive analytics

Enhance existing analyst skill sets

Governance, Compliance, and Value Realization

Effective GenAI implementation requires building governance and accountability into system architecture, ensuring AI enhances rather than complicates compliance postures.

This involves comprehensive documentation systems automatically tracking all AI decisions, investigation steps, and time savings for audit purposes, while providing transparent decision trees for regulatory review. Organizations must establish clear AI governance frameworks that define decision-making authority, risk tolerance, and performance standards while ensuring explainable AI processes that security teams can trust and auditors can validate.

These systems should maintain detailed logs of all automated actions, remediation steps, and analyst interactions to support compliance reporting and demonstrate the rationale behind AI-driven security decisions.

Transparent ROI Measurement

Equally important is establishing clear ROI measurement frameworks that provide transparent cost reduction tracking through resource optimization and efficiency multipliers. Dashboards should demonstrate real-time cost savings, immediate reductions in manual investigation time, decreased breach risk through improved detection, and quantifiable productivity gains reportable to leadership.

GenAI NDR requirements

Once you have developed your GenAI NDR strategy and business case, what capabilities should you look for in a solution? Here some key requirements:

AI-Powered Alert Triage and Prioritization

Integrating AI-driven alert triage can greatly minimize the number of alerts requiring human attention, enabling security teams to concentrate on real threats instead of being overwhelmed by false positives.

AI-Enhanced Threat Hunting and Investigation

AI-driven threat hunting automates the detection of security risks by analyzing logs, endpoint behavior, and network anomalies, continuously learning from security data and correlating multiple signals.

Automated Incident Response and Remediation

Automatically complete routine, standardized tasks to expedite the incident response process and increase SecOps teams' efficiency and effectiveness, reducing mean time to detect (MTTD) and mean time to respond (MTTR). Modern GenAI-based security automation provides advanced threat identification, management, and remediation capabilities with vastly higher ongoing ROI.

Predictive Security Analytics

AI's ability to analyze historical attack data, threat intelligence feeds, and vulnerability data enables AI to identify patterns and predict future attacks. This allows security teams to implement preventative measures and strengthen defenses before an attack. GenAI enhances a security platform's ability to predict and prevent threats by building behavioral models from historical data, shifting cybersecurity from reactive to proactive.

Operational Excellence Through AI-driven Automation

Practical GenAI application centers on comprehensive alert lifecycle automation addressing critical operational challenges. Organizations should implement AI systems capable of automatically investigating 100% of alerts in under three minutes, eliminating missed threats due to overwhelming volumes.

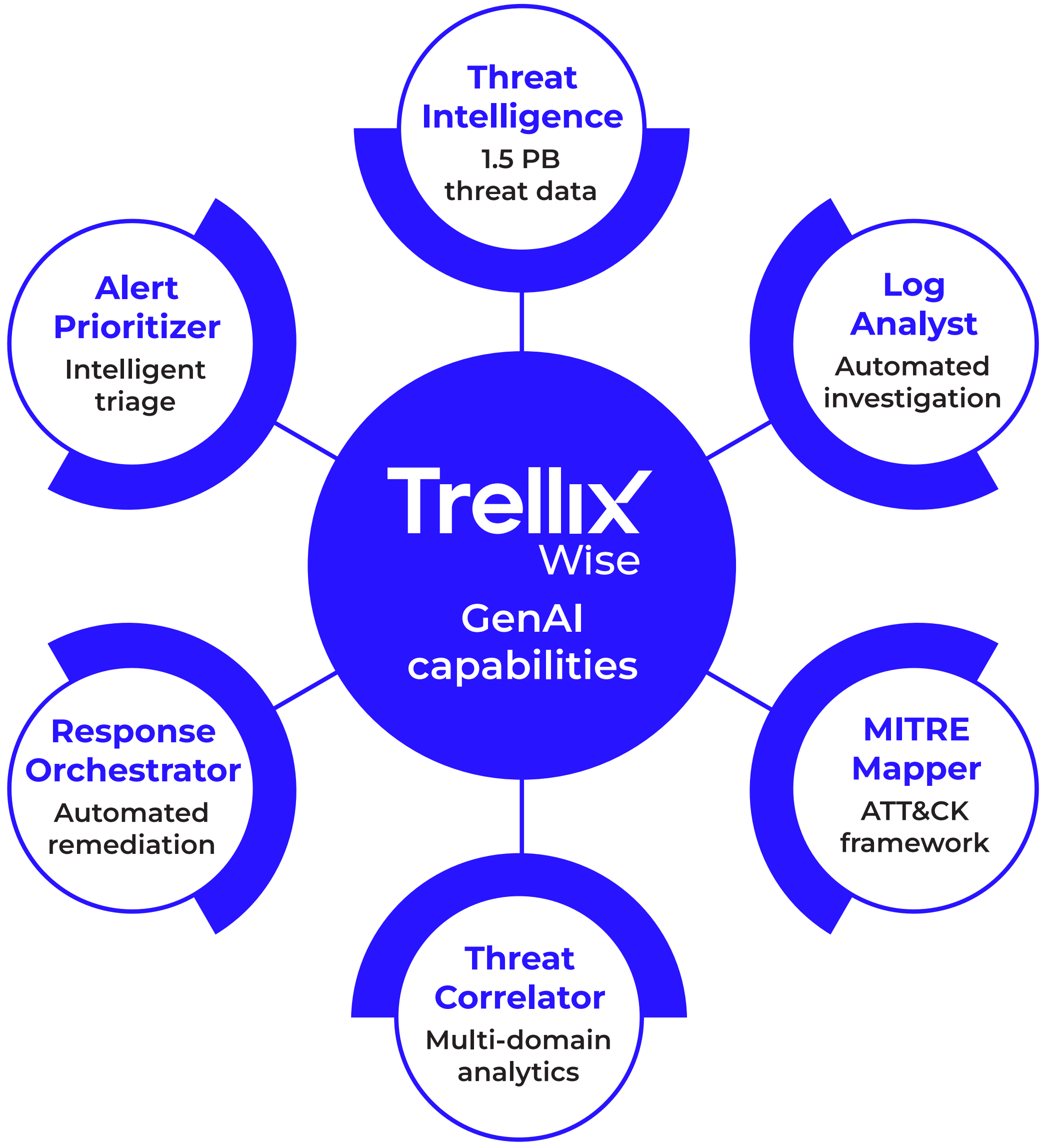
This involves intelligent prioritization mechanisms that surface only critical alerts requiring human attention. Automation extends to evidence gathering, performing deep investigations across multiple data sources that would otherwise require three to five analysts working for hours. These implementations should consistently deliver measurable outcomes.

Your path forward—Trellix NDR with Trellix Wise™

The challenges facing your security operations—alert fatigue, talent gaps, sophisticated threats, and mounting compliance pressures—require more than incremental improvements. They demand a fundamental transformation powered by proven GenAI technology.

Trellix NDR with Trellix Wise GenAI capabilities delivers exactly this transformation through innovative multi-agent AI architecture that addresses every barrier outlined in this guide.

Built on over a decade of AI modeling and 25 years of analytics expertise, Trellix Wise transforms your security operations from reactive to proactive. The platform automatically investigates every single alert using 1.5 petabytes of threat intelligence and real-time operational data from 660 million endpoints processing 60 billion queries daily.



Trellix NDR delivers proven results

<3 minutes
for automatic alert investigation and summarization

50% reduction
in analyst workload

300% improvement
in mean time to respond (MTTR)

8 hours
of SOC work recovered per 100 alerts

What makes Trellix NDR with Trellix Wise different

- **On-device AI Architecture:** Local large language models process sensitive data without cloud dependency, ensuring data privacy while delivering real-time threat analysis through specialized AI agents that work continuously to detect, correlate, and respond to sophisticated attacks.
- **Multi-agent Intelligence Network:** Interconnected specialized AI agents including Log Analysts, MITRE framework mappers, and Threat Correlators work together to provide comprehensive threat detection, reducing false positives through intelligent data correlation across multiple security domains.
- **Alert Fatigue Elimination:** Intelligent AI agents automatically investigate 100% of alerts in under three minutes, prioritizing only critical threats that require human attention while providing comprehensive evidence gathering and analysis that would otherwise require multiple analysts working for hours.
- **Automated Threat Intelligence:** AI agents automatically correlate findings with MITRE ATT&CK frameworks and generate actionable remediation recommendations, transforming complex security data into clear, prioritized insights that enable rapid response and strategic defense planning.

The future of network detection and response isn't coming—it's here. Organizations worldwide are already experiencing the transformational impact of GenAI-powered security operations that work as intelligently as threats demand.

Ready to transform your security operations?

Discover how Trellix NDR with Trellix Wise can eliminate alert fatigue, close talent gaps, and deliver measurable ROI starting today.

Request a demo

To learn more, visit trellix.com.