SOLUTION BRIEF

Trellix® Network Detection and Response

Disrupt attackers at every stage while accelerating response

Highlights

Eliminate blindspots and risk. Extended visibility and risk prioritization for complex networks (IT, OT/ICS, IoT, and cloud)

Disrupt attackers at every stage. Multilayered detection across each stage of the MITRE ATT&CK framework and Attack Path Discovery

Accelerate investigation and response. GenAI-driven alert prioritization, enrichment, investigation, and active response

Beyond traditional detection: Why network security must evolve

Modern network security teams face an unprecedented challenge that's growing exponentially. Enterprise networks have become vastly more complex, spanning on-premises data centers, multicloud environments, remote endpoints, IoT devices, and third-party integrations that create intricate webs of interconnected systems. Cyber assets are proliferating at breakneck speed across this distributed infrastructure while the vulnerability landscape expands relentlessly, with each new connection point introducing potential attack vectors.

This explosive growth in both scale and complexity has fundamentally transformed the attack surface, creating countless blind spots and overwhelming traditional security approaches that were designed for simpler, more centralized network architectures.

The encryption revolution, while essential for privacy and compliance, has created an invisible network where sophisticated threats operate undetected. Legacy security tools that rely on deep packet inspection are rendered ineffective, leaving organizations vulnerable to advanced attacks hiding in plain sight within encrypted communications.

Meanwhile, security operations centers are collapsing under the weight of alert fatigue. Analysts are drowning in low-fidelity notifications, forcing impossible triage decisions that leave critical threats unaddressed. The human element—already strained by a global cybersecurity skills shortage—becomes the weakest link in an increasingly automated attack landscape.

133%
year-over-year increase in cyber assets to protect[1]

61%
year-over-year increase in the number of vulnerabilities[2]

95%
of traffic is encrypted, creating massive security blind spots[3]

43%
of organizations hit with ransomware were hit more than once[4]

67%
of alerts are ignored due to alert fatigue[5]

Traditional network security tools weren't designed for this reality. Point solutions generate fragmented visibility, lack contextual intelligence for risk prioritization, and fail to provide the automated investigation capabilities that overwhelmed analysts desperately need. As attack sophistication increases and adversaries maintain persistence for weeks, organizations need a fundamentally different approach to network detection and response.

Trellix Network Detection and Response: Risk-based intelligence for modern network security

Trellix Network Detection and Response (NDR) transforms network security through intelligent risk prioritization—automatically focusing security teams on threats that matter most to their specific environment. By combining comprehensive visibility across hybrid infrastructures with AI-powered analysis and automated investigation capabilities, Trellix NDR cuts through the noise to deliver actionable intelligence that enables confident, rapid response.

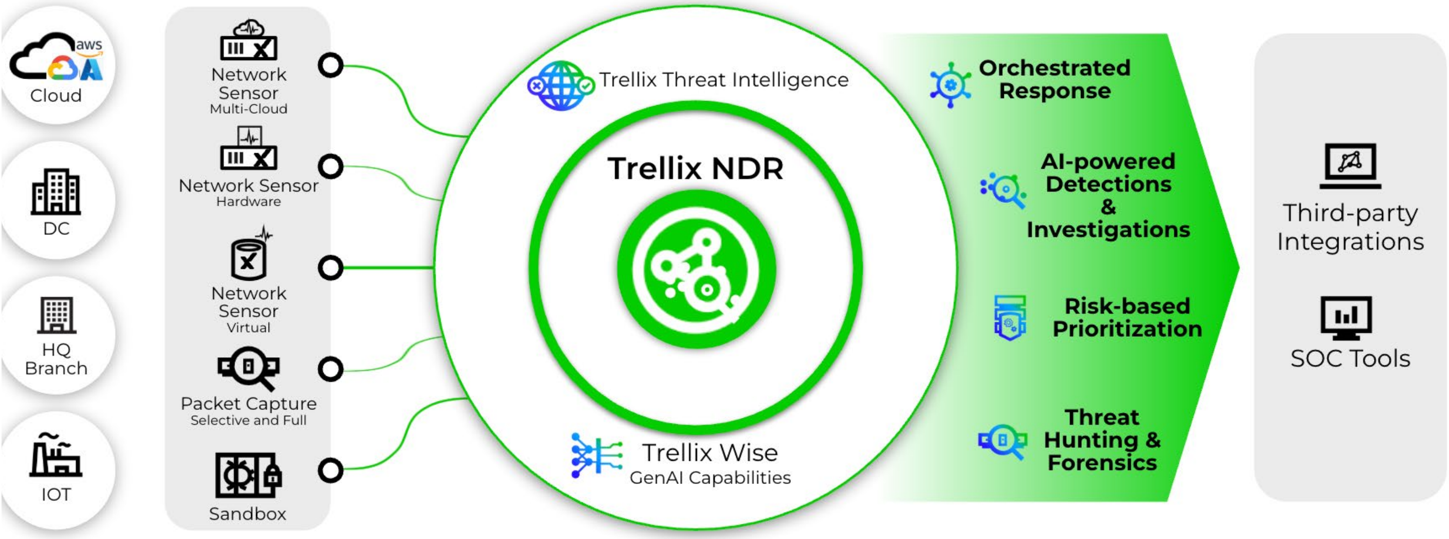
Unlike traditional network security tools that overwhelm analysts with generic alerts, Trellix NDR employs sophisticated risk-based aggregation that considers asset criticality, vulnerability exposure, and MITRE ATT&CK tactics to surface only the threats that pose genuine business risk. The solution seamlessly analyzes encrypted traffic without decryption, detects advanced threats across all attack stages, and provides streamlined investigation workflows that transform junior analysts into effective threat hunters.

Built for the modern SOC, Trellix NDR's analyst experience eliminates context-switching between tools while its AI-powered Trellix Wise™ capability automatically enriches alerts, maps attack techniques, and recommends specific remediation steps. The result is dramatically reduced mean time to detect and respond, improved analyst productivity, and the visibility needed to stay ahead of sophisticated adversaries.

[1]. "The 2023 State of Cyber Assets Report," JupiterOne 2023.
[2] "Software Vulnerabilities Surged 61 Percent in 2024, According to New Report," Security Today, June 2, 2025.
[3] "How to Preserve Critical Traffic Visibility for Enterprise ande Network Security While Safeguarding Privacy," Enea, TLS 1.3 ECH, March 19, 2025.
[4] "Third-Party Breach Report," Black Kite, 2022.
[5] "Why SOCs Must Embrace AI," PureStorage, October 25, 2023.

Trellix NDR

Advanced Threat Detection, Investigation, Hunting, and Response



Three core capabilities that transform network security

Eliminate blind spots and risk

Comprehensive Visibility Across All Environments. Trellix NDR delivers unified visibility across on-premises, cloud, and hybrid network infrastructures through a single platform. Purpose-built virtual sensors provide native monitoring for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) environments, while advanced encrypted traffic analysis identifies threats in the 95% of communications that traditional tools cannot inspect.

Risk-based Prioritization That Actually Works. The Risk Aggregation Framework combines asset criticality, vulnerability data, and MITRE ATT&CK tactics to automatically prioritize and surface the threats that pose genuine business risk.

Attack Path Discovery. This feature proactively visualizes potential attack vectors by combining vulnerability data with network topology analysis. Security teams can identify how attackers might escalate privileges and move laterally through infrastructure, enabling preventive remediation of critical vulnerabilities before exploitation occurs.

Disrupt attackers at every stage

Multilayered Detection Across the Kill Chain. Trellix NDR employs behavioral analytics, machine learning, and threat intelligence to detect sophisticated attacks across all 14 MITRE ATT&CK tactics. Specialized detection capabilities identify DNS tunneling, ICMP exfiltration, newly registered domain communications, and SSL anomalies that signature-based systems routinely miss.

Advanced Threat Detection in Encrypted Traffic. JA3/JA3S fingerprinting, certificate reputation analysis, and encrypted traffic behavioral analysis reveal threats hiding in encrypted communications without requiring decryption—maintaining privacy compliance while closing critical security gaps.

Dynamic File Analysis. Real-time analysis of suspicious files and objects provides immediate threat verdicts, enabling instant blocking of unknown threats and malicious content before it can execute or spread throughout the network environment.

Active NDR. This capability enables immediate threat containment through automated response actions, including traffic blocking, system isolation, and coordinated response with integrated security tools to stop attacks in real-time.

Accelerate investigation and response

AI-powered Investigation Assistant. Trellix Wise automatically analyzes alerts, identifies affected entities, maps attack techniques to MITRE ATT&CK, and provides specific remediation recommendations. Junior analysts gain expert-level investigation capabilities while experienced analysts can focus on high-value threat-hunting activities.

Advanced Forensics. Complete packet capture and metadata retention provide the detailed evidence needed for thorough incident investigation. Timeline reconstruction and attack visualization capabilities enable security teams to understand full attack scope and prevent recurrence.

Streamlined Analyst Experience. The Trellix NDR Console provides risk-prioritized dashboards, one-click investigation workflows, and comprehensive alert context in a single interface. Automated response capabilities and native integrations with endpoint security, vulnerability management, and SIEM platforms enable coordinated defense across the security ecosystem.

Trellix NDR components

Trellix NDR Console

The Trellix NDR Console transforms network security operations through risk-based intelligence and streamlined analyst workflows. This centralized command center provides unified visibility across all sensor deployments, intelligent alert prioritization through the Risk Aggregation Framework, and AI-powered investigation capabilities through Trellix Wise.

Advanced forensics, Trellix Attack Path Discovery, and comprehensive integration management ensure security teams have the tools needed to detect, investigate, and respond to sophisticated threats with confidence and speed.

Trellix NDR Sensor (NX Evolution)

The foundation of network visibility you depend on should align with your specific deployment needs. The Trellix NDR Sensor provides comprehensive network monitoring and threat detection capabilities across physical, virtual, and cloud environments.

Whether you're migrating from existing Trellix Network Security (NX) deployments or implementing new network detection capabilities, the Trellix NDR Sensor delivers seamless visibility with enhanced detection capabilities, active response functionality, and intelligent event generation that scales from small networks to enterprise environments supporting up to 40 Gbps throughput.

Trellix IPS "NDR Ready"

For organizations requiring both network detection and comprehensive workload protection, Trellix IPS "NDR Ready" combines full intrusion prevention capabilities with advanced NDR functionality. This unified solution delivers the performance needed for high-throughput environments, scaling up to 240 Gbps while providing active threat containment, enhanced MITRE ATT&CK detection mapping, and the flexibility to serve both security monitoring and inline protection requirements across hybrid infrastructure deployments.

Add-on capabilities

Extend NDR functionality with specialized capabilities, including the following:

- Trellix Full Packet Capture for comprehensive forensic analysis
- Trellix IVX dynamic file analysis for real-time threat verdicts
- Trellix Attack Path Discovery for proactive vulnerability prioritization
- Third-party integrations with solutions like Skyhigh SWG, firewalls, proxies, and OT security platforms like Nozomi Guardian for complete network security coverage

Request a demo

Learn more about Trellix Network Detection and Response at trellix.com.

Copyright © 2025 Musarubra US LLC