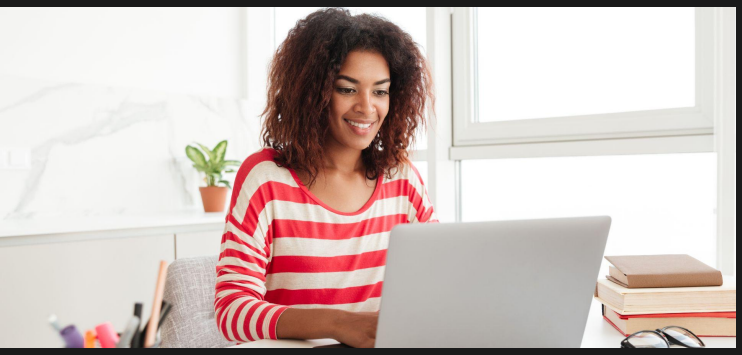
Trellix



Trellix Network Detection and Response

As an existing Network partner, Trellix is pleased to collaborate with the customer on advancing their security maturity journey towards Trellix Network Detection and Response (NDR).

The current and future state below explains customer's situation and reason to action

Current State

Complex Network Attack Surface: Adoption of zero trust initiatives, SASE models, alongside cloud migration introduces significant security blind spots and poorly managed assets.. This complicates seamless network protection.

Sophisticated Threats Continue to Go Undetected: Disconnected network security tools and visibility gaps hinder early detection of unknown, late stage attacks.

Overwhelmed Security Teams: Alert fatigue leads to SOC teams ignoring alerts and missing critical threats. Alerts lacking context hinders their actionability.

Attack Mitigation Takes Too Long: Analysts lack timely response to alerts that matter due to siloed tool noise and manual workflows.

Future State

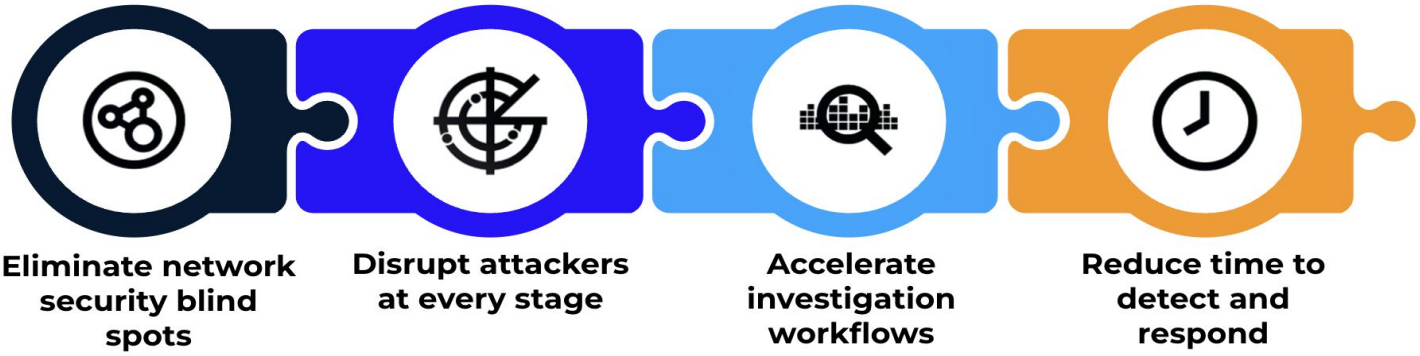
Extend Visibility Across Complex Networks: Blind spots are eliminated across the distributed, dynamic network environment with increased visibility of assets that access the network.

Multi-Layered Detection: Address sophisticated and unknown threats by disrupting attackers at every stage, using a variety of high-fidelity detection techniques.

AI-Powered Investigation: Transform alert investigation with Trellix Wise generative AI that asks and answers key questions by correlating data from multiple sources, dramatically accelerating time to insight.

Accelerated Response: Aggregating, correlating, and leveraging actionable network telemetry uplevels SOC-focused workflows, providing needed MTTI and MTTR reduction.

Trellix brings unparalleled, industry leading NDR experience with a proven record of excellence to support customer's security maturity journey to NDR.



Trellix Network

Investigator - NDR Capabilities

Visibility Dashboards

Track changes in network activity, explore ports, protocols and assets for advanced threat hunting

MITRE ATT&CK Integration

Trellix NDR with Wise automatically detects and maps network activities to MITRE techniques, gathering supporting evidence and providing enhanced visibility into complete attack chains.

Detection Dashboards

Intuitive visualization of attacker patterns including scope and techniques. Integration with Threat Intel and MITRE ATT&CK Mapping

AI-Powered Investigation

Transform alert investigation with Trellix Wise generative AI that asks and answers key questions by correlating data from multiple sources, dramatically accelerating time to insight.

Asset Discovery

Extend visibility and automatically map discovered assets to device type, including new devices. Additional correlation with sensor alerts and telemetry

Investigate Workflow

Automated alert enrichment and SOC-focused workflows accelerate investigation combining alerts into Incidents that are actionable.

Why the customer should move to the Trellix NDR offering now?

Network environments are becoming more complex as the number of cyber assets increased by 133% YoY.

69% of organizations experienced a cyber attack involving unknown or poorly managed assets.

Lacking complete network visibility hinders early attack detection as 80% of successful breaches are from zero-day exploits.

Gaps in visibility translate to an average attacker dwell time of 16 days before being discovered.

Without NDR as a first line of defense compliment to EDR, sophisticated attacks will continue to go undetected.