Network Detection and Response

XDR without NDR is just EDR

Stop security threats before they strike

Detect the undetectable and stop evasive attacks. Trellix Network Detection and Response (NDR) helps your team focus on real attacks, contain intrusions with speed and intelligence, and eliminate your cybersecurity weak points.

Adapt to new threats automatically

Detect common threats in your network and data centers—while automatically adapting so you can anticipate and respond to new and dynamic threats.

Protect across your network to the cloud

Keep your cloud, IoT, collaboration tools, endpoints, and infrastructure safe. Automate your responses to adapt to the changing security landscape.

Configure to your organization's needs

Integrate with any vendor and improve efficiency by surfacing only the alerts that matter to you.

TRELLIX NETWORK SECURITY PRODUCTS

Trellix Network Security

- Automatically spot suspicious network behavior and prevent attacks that elude traditional signature- and policy-based security.
- Detect and block advanced threats and lateral attack movements in real time.
- Accelerate resolution of detected incidents with concrete evidence and actionable intelligence.

Trellix Network Forensics

- Identify and resolve a broad range of security incidents faster.
- Determine the scope and impact of threats and re-secure your network.
- Visualize events before, during, and after an attack to keep incidents from happening again and again.

Trellix Intrusion Prevention System

- Inspect all network traffic to prevent new and unknown attacks.
- Streamline security operations with real-time event correlation across all sources.
- Monitor your network for malicious activity and block intrusions the moment you identify them.

Detect and prevent threats other products miss

CAPABILITY	BENEFIT
Signatureless threat detection	Detects multiflow, multistage, zero-day, polymorphic, ransomware, and other evasive attacks
Real-time and retroactive detection	Monitors known and unknown threats in real time and enables back-in-time threat detection
Multivector correlation	Automates validation and blocks attacks across email, endpoint, and other security vectors
Lateral movement detection	Detects formerly undetectable suspicious network traffic within the network
DoS and DDoS prevention	Prevents malicious traffic from reaching your network, while allowing legitimate traffic to get through
Inbound/outbound SSL decryption	Detects malware and other advanced threats in inbound and outbound encrypted traffic
MultiOS, multifile, and multiapp support	Supports heterogeneous endpoint environments for a wide range of applications
Hardened hypervisor	Provides evasion proofing by hiding traces of virtualization

Proactively respond to and quickly contain incidents

CAPABILITY	BENEFIT
Real-time inline blocking	Stops attacks instantly
Advanced intrusion prevention	Performs deep inspection of network traffic to detect and protect against malware callbacks and other advanced threats
Integrated security workflows	Pivots from detection to investigation and response
High availability	Provides resilient defense
Signature-based IPS detection with noise reduction	Automates and accelerates alert noise triaging to eliminate manual overhead
Riskware detection and categorization	Categorizes critical and non-critical malware to prioritize response resources
Actionable contextual intelligence	Accelerates advanced threat containment by providing in-depth information about the attack and attacker

Quantify incident impact and improve response quality

CAPABILITY	BENEFIT
Rich context	Reviews specific network packets, connections, and sessions before, during, and after an attack
Retrospective threat hunting	Integrates threat intelligence for back-in-time IOC threat analysis and provides automatic alerts to IOCs present in your network days or weeks earlier
Breach impact reduction	Accelerates forensics process with a single workbench with immediate one-click pivot to session data from alerts