Advanced Network Detection & Response - MetaDefender NDR - OPSWAT

Network Hunting Redefined

Give your team the unparalleled ability to inspect and analyze network sessions across your organization.

Detect and Respond

Analyze Traffic

Automate Hunting

- ## Analyze Traffic

  Analyze past and present, inbound and outbound network traffic using patented Deep File Inspection, and our RetroHunting capability.

-

Automate Hunting

Automate complex threat hunting processes with predefined analytical workflows and incident triage.

-

Detect and Respond

Leverage advanced algorithms to uncover patterns and generate valuable insights to combat cyberthreats.

-

Analyze Traffic

Analyze past and present, inbound and outbound network traffic using patented Deep File Inspection, and our RetroHunting capability.

- ### Automate Hunting

  Automate complex threat hunting processes with predefined analytical workflows and incident triage.

- ### Detect and Respond

  Leverage advanced algorithms to uncover patterns and generate valuable insights to combat cyberthreats.

- ### Analyze Traffic

  Analyze past and present, inbound and outbound network traffic using patented Deep File Inspection, and our RetroHunting capability.

Can your SOC team respond fast enough?

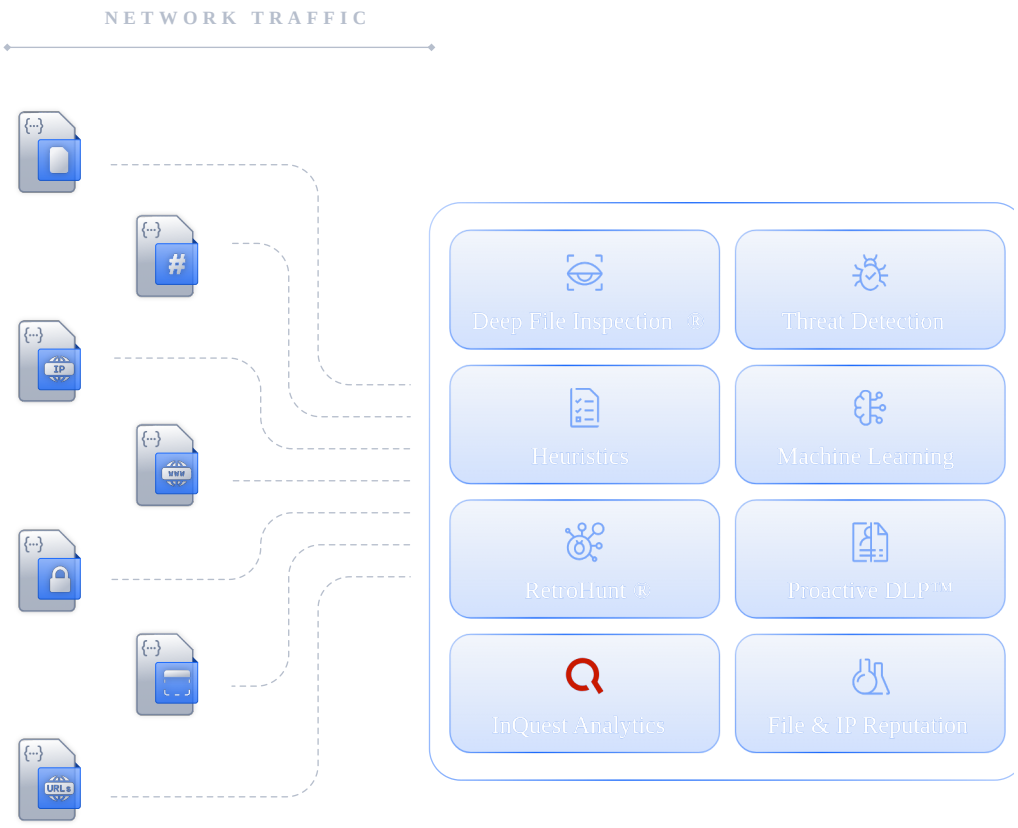
- ### Ever-Increasing Volume and Complexity of Threats

  Cybersecurity is a perpetual arms race, and keeping your network secured is an arduous, never-ending task. From exhaustion to “alert fatigue,” your team needs help staying on top of their game.

- ### Lack of Visibility

  Without the right tools and visibility, your team is forced to make decisions based on incomplete information. That can lead to missed events of interest and unnoticed patterns of activity.

Identify and Eradicate Suspicious Network Activity with a Smarter Solution



Stay Ahead of the Cyberthreat Arms Race

Gain Powerful, Actionable Information

Scale as Your Network Grows

Reactive Intrusion Detection Is No Longer Enough

- **Scale as Your Network Grows**

The workload of your SOC team doesn't necessarily have to be relative to the growth of your organization or the increase of your network traffic. MetaDefender NDR automates complex threat hunting procedures and serves as a force multiplier to ensure your team doesn't become inundated with alerts or mundane analytical tasks.

- ### Reactive Intrusion Detection Is No Longer Enough

  Traditional signature-based intrusion detection tends to be reactive and relies too heavily on known, predefined patterns often evaded by sophisticated threat actors. Relying solely on these detection methods compounds your team's exhaustion and decreases their chance of detecting threats targeting your organization.

- ### Stay Ahead of the Cyberthreat Arms Race

  With continuous updates, machine learning models, and a hunt capability, your team will not only see what's happening across your enterprise, but they'll also have the latest intelligence to identify emerging threats and actively hunt them down.

- ### Gain Powerful, Actionable Information

  With advanced analytical techniques, incident response workflow, and the ability to retrospectively analyze historical artifacts via our RetroHunt capability MetaDefender NDR will empower your team with the capability to take action quickly and dynamically to mitigate threats and risks that your enterprise faces daily.

- ### Scale as Your Network Grows

  The workload of your SOC team doesn't necessarily have to be relative to the growth of your organization or the increase of your network traffic. MetaDefender NDR automates complex threat hunting procedures and serves as a force multiplier to ensure your team doesn't become inundated with alerts or mundane analytical tasks.

- ### Reactive Intrusion Detection Is No Longer Enough

  Traditional signature-based intrusion detection tends to be reactive and relies too heavily on known, predefined patterns often evaded by sophisticated threat actors. Relying solely on these detection methods compounds your team's exhaustion and decreases their chance of detecting threats targeting your organization.

- ### Stay Ahead of the Cyberthreat Arms Race

  With continuous updates, machine learning models, and a hunt capability, your team will not only see what's happening across your enterprise, but they'll also have the latest intelligence to identify emerging threats and actively hunt them down.

MetaDefender

InSights OSINT

Curated and actionable open source intelligence

Product Overview

Learn how MetaDefender NDR and InSights deliver real-time network visibility, anomaly detection, and threat correlation across IT and OT environments to detect attacks earlier and reduce dwell time.

Redefine Your Network Hunting Capabilities

Encrypted Session Analysis

Encrypted session analysis is performed against SSL/TLS connections as well as encrypted session attributes/characteristics to identify malicious activity as well as command and control activity even without inline decryption in place.

High-Performance Inspection

Swiftly detect and respond to unusual and suspicious behavior. MetaDefender NDR enables the proactive identification of potential threats at network throughput speeds of up to 40Gb per second.

Empower Threat Hunters

Streamline investigative workflows for your SOC team with our integrated incident response, intrusion analysis, remediation, event triage, and breach containment capabilities.

Breach Detection & Containment

Breach detection analysis is performed on every network connection attempt, established connection, and domain resolution attempt leveraging a compilation of applied Threat Intelligence from MetaDefender InSights as well as advanced heuristics and analytics crafted by our threat analysts.

Data Loss Prevention (DLP)

Safeguard your vital data with our Data Loss Prevention capabilities. With advanced context and content inspection of carved files, you'll be able to detect and prevent data exfiltration, ensuring the protection of PII, PHI, sensitive, proprietary, and even user-defined information within your environment.

Go Deeper and Expose More

Go beyond Layer 7 of the OSI model with Deep File Inspection® (DFI) to process content embedded within the original files extracted from the network traffic. These inspection operations typically result with an increase in the detection space of 4x for higher fidelity detections and less evasions an attacker can leverage.

Unlock the Full Potential of Our Products

Dive into OPSWAT Docs today for in-depth guides,troubleshooting tips, and valuable references.

Recommended Resources

Datasheet

MetaDefender NDR Commercial Datasheet

Empower Your SOC Team to Identify and Eradicate Suspicious Network Activity

Fill out the form and we'll be in touch within 1 business day

Trusted by 2,000+ businesses worldwide.
