OPSWAT.

DATASHEET

COMMERCIAL

MetaDefender NDR

Always-On Network Defense for Modern Enterprises

Help organizations detect, investigate, and respond to network threats faster without disrupting business operations. Built for high-performance environments, MetaDefender NDR delivers deep network visibility, advanced threat detection, and seamless security integration across on-premises, hybrid, and regulated environments.



Key Capabilities

Complete Network Visibility: Continuously monitors north-south and east-west traffic to provide full visibility across data centers, cloud, and branch environments.

Advanced Threat Detection: Machine learning and behavioral analytics identify zero-day attacks, lateral movement, and stealthy threats that bypass traditional controls.

Encrypted Traffic Analytics (Without Decryption): Inspects SSL/TLS metadata, certificates, handshakes, and flow statistics to detect threats while preserving privacy and performance.

Integrated Threat Intelligence: Enriches alerts with MetaDefender InSights intelligence for faster triage, higher confidence detections, and reduced analyst fatigue.

Retroactive Threat Hunting (Retrohunting): Reanalyze historical network traffic to uncover previously missed threats and reduce attacker dwell time.

Rapid Incident Correlation: Automatically correlates network events to accelerate investigations and shorten time to containment.

Security Orchestration & Automation: Integrates with SIEM, SOAR, Sandbox, Multi-AV, and EDR platforms to streamline analysis and response workflows.

OT/ICS Network Visibility and Protection: Delivers passive, agentless monitoring of operational technology environments with native support for Modbus, DNP3, BACnet, S7comm, ENIP/CIP, and IEC104 protocols. Detects threats and anomalies across industrial control systems without disrupting production processes or sensitive equipment.

Use Cases

Breach Detection & Response
Detect intrusions in real time and stop attacks before they impact operations or customers.

Threat Hunting & Forensics
Reconstruct attack timelines and investigate incidents with enriched, context-aware intelligence.

Ransomware Prevention
Identify early indicators such as beaconing and lateral movement to stop ransomware before encryption and disruption.

Data Loss & Exfiltration Detection
Detect unauthorized data transfers, covert channels, and insider threats to protect sensitive business data.

Zero Trust Enablement
Support Zero Trust strategies with continuous network visibility and behavioral validation.

Compliance & Audit Readiness
Maintain continuous monitoring and reporting aligned with industry and regulatory frameworks such as NIST, ISO, SOC 2, PCI-DSS, HIPAA, GDPR, and regional privacy regulations.

Disconnected & Restricted Environments
Operate fully on-prem or in isolated networks where cloud-dependent tools are impractical or prohibited.

OT and IT Convergence Security
Unify visibility across IT and OT networks in a single platform, enabling security teams to detect lateral movement between corporate and operational environments, enforce segmentation policies, and respond to cross-domain threats without deploying separate tooling for each environment.

Proven at Scale
Trusted in highly regulated, performance-critical environments for over 15 years

On-Prem & Offline Ready
Full functionality without mandatory cloud connectivity

Built-In Threat Intelligence
Autonomous enrichment without external dependencies

High-Throughput Performance
Supports up to 40 Gbps per sensor for enterprise and data-center scale

Open Integration
Works seamlessly with existing security stacks (SIEM, SOAR, EDR, Sandbox)

Actionable Dashboards
Real-time visibility into threats, anomalies, and risk posture

Get Started

Talk to one of our experts today. Scan the QR code or visit us at opswat.com/get-started or email sales@opswat.com



OPSWAT.
Protecting the World's Critical Infrastructure

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc. Rev. 2026-07