

OpenText Network Detection & Response

Identify and eliminate blind spots in the network



Benefits

- Visibility
- Context
- Detection
- Response

OpenText™ Network Detection & Response (NDR) is leading the next generation of advanced network detection and response solutions for the enterprise. Fusing detection, forensic analysis and proactive threat hunting, OpenText Network Detection & Response empowers high-performance enterprise security teams with total visibility into network traffic. With signature inspection, stateful anomaly detection and machine learning-powered malware conviction, OpenText Network Detection & Response empowers security teams to effectively defend against known threats and to illuminate those otherwise unseen.

OpenText Network Detection & Response provides organizations with 360-degree protection, end-to-end visibility and context for direct answers and powerful insight to take immediate action.

The solution provides complete visibility of east-west traffic across network environments in real time and full-spectrum threat detection that extracts and stores high-fidelity metadata, including an indexed threat hunting repository.

A multi-faceted suite of best-in-breed threat detection allows organizations to thoroughly inspect network traffic from every angle. Users can find unknown, hidden threats to conduct retrospective network traffic analysis and historical data testing to determine if threats infiltrated the environment prior to known indicators being available. They can use meaningful visualizations and flexible network views to see everything in a single pane of glass or create custom views for what matters most for their network.

“MAD Security is growing extremely rapidly; we’ve increased our client base by a factor of three in just a few years, and our goal is to grow a further 400 percent in the next three years. We targeted a NDR solution that could scale to help us hit that growth target while keeping our analyst team lean.

“Thanks in large part to OpenText [Network Detection & Response], we can now detect and correlate events, investigate the data and notify the client in an average of just 6.5 minutes—less than half our SLA.”

Jeremy Conway,
CEO, MAD Security

OpenText Network Detection & Response eliminates security blind spots through real-time network visibility. Organizations can see everything on their network via high-fidelity metadata and SmartPCAP, take advantage of full-spectrum threat detection and reduce noise and optimize detection with multiple detection engines examining the network from every angle. Users can thoroughly and proactively investigate detected threats and hunt down unknown threats that did not generate an alert with forensic precision. With seamless response and extensive integrations, organizations can correlate alerts in real time, enrich existing workflows, automate responses, and prevent threats. OpenText Network Detection & Response is the only end-to-end network detection and response platform that allows both security teams and the entire enterprise to collaborate better, reduce security risk, and solve network problems faster than ever before.

Next-gen sensors

- Total network visibility of internal and web-bound traffic

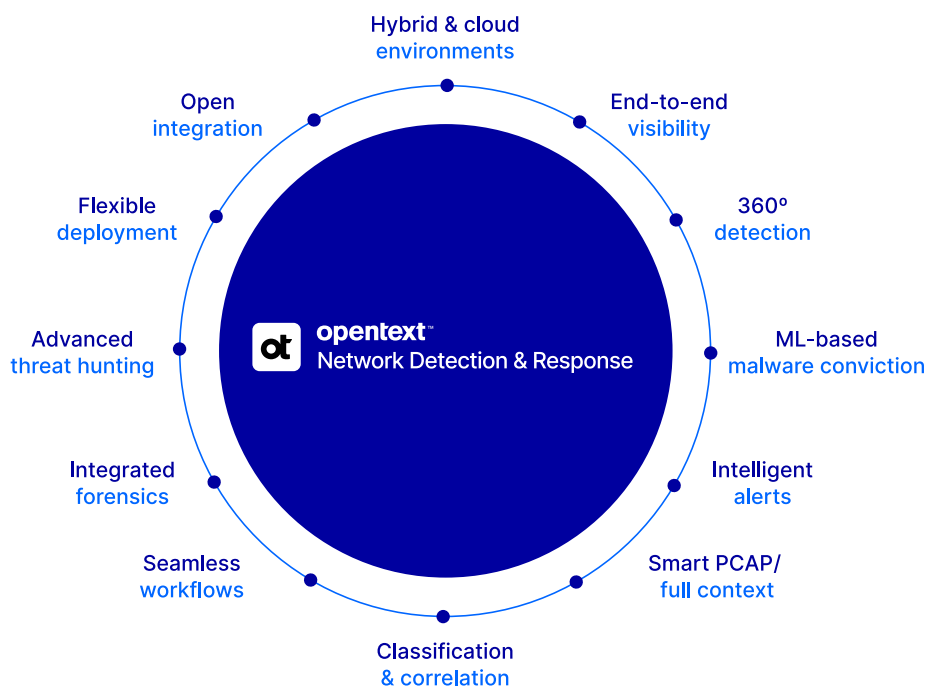
Powerful centralized management

- Customizable dashboards for response, analysis, forensic investigation, and threat hunting

Smart data nodes

- Intelligently extracts and stores rich network metadata within a smart scalable repository for efficient threat hunting and incident response

Protect from all sides



Product features chart



See



Know



Act

- **Total network visibility**
See everything happening on the network
- **Full-spectrum threat detection**
Use signature inspection, anomaly detection and ML-based malware conviction
- **High-fidelity metadata**
Gain a better understanding with rich metadata from every transaction
- **Proactive threat hunting**
Leverage indexed enriched data repository
- **Smart PCAP**
Quickly access relevant metadata
- **Forensic investigation**
Effectively investigate events with network packets
- **Better detection**
Take advantage of automated analysis, prioritized workflows
- **Faster response**
Clear queues faster than ever
- **Customizable and flexible**
Tune easily with a wide breadth of integrations

Services

[Next-gen Services ›](#)

Resources

[Security – OpenText Blogs ›](#)

[OpenText threat detection and response solutions ›](#)

