Network detection and response (NDR)

MarketUpdate

Market basics

NDR is one flavour of the market for threat detection and response technologies focused, as the name suggests on telemetry captured from network activity from all parts of the technology estate. It is complementary to and sits alongside other technologies in the detection and response space but is considered to be among the most vital owing to the number of threats that traverse networks. Without requiring agents to be installed on devices, NDR is invisible to attackers who will not be aware that they are being observed, thus making it extremely in threat detection.

Through NDR, the effectiveness and productivity of security teams will be increased dramatically, enabling staff to focus on real threats rather than chasing down false positives. With a core focus on threat management, NDR provides not only automation of key tasks, but also expert guidance for beleaguered security teams.

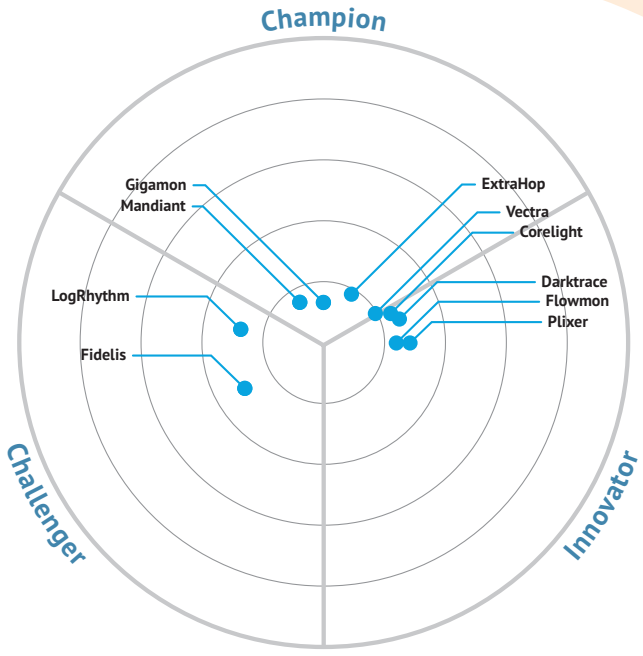
Artificial intelligence is core to NDR offerings in the form of machine learning, advanced and behavioural analytics that provide context regarding what is occurring, providing real evidence of the existence of advanced threats anywhere on the network. Correlated with threat intelligence information regarding the latest threats seen and those impacting specific regions or industry sectors, the level of information provided can underpin threat hunting activities that will enable even unknown and hidden threats to be uncovered. The resulting evidence is presented as detailed metadata that can be fed into systems such as a SIEM as fully validated alerts that provide detail as to what has actually occurred. This makes it extremely effective in guiding security teams in the most effective response.

Another key advantage is that the underlying complexity of the technology and processes involved is hidden from security teams so that they can get on with the job at hand without having to sift through reams of information to find valuable nuggets that they contain. With a serious skills shortage in the cybersecurity industry, training times will be reduced, enabling staff to become productive earlier and potentially increasing retention by providing more interesting assignments to valuable staff.

Vendor landscape

All of the vendors included in this market update offer NDR capabilities that they have developed themselves or via acquisition. Some have been operating in this space since long before the term NDR was coined and have spent years monitoring networks on behalf of organisations, often at massive scale. These include Corelight, ExtraHop, Flowmon, Gigamon, Plixer and Vectra. LogRhythm added NDR to its portfolio of products through acquisition of MistNet at the beginning of 2021 and Fidelis acquired Cloud Passage during 2021 to further build out its extended detection and response (XDR) capabilities. Darktrace is a younger vendor, describing its capabilities as self-learning AI. It underwent an IPO in 2021. Mandiant has sold off FireEye and remains a public company. This puts it in a strong position to offer technology-agnostic services.

Figure 1:
The highest scoring companies are nearest the centre. The analyst then defines a benchmark score for a domain leading company from their overall ratings and all those above that are in the champions segment. Those that remain are placed in the Innovator or Challenger segments, depending on their innovation score. The exact position in each segment is calculated based on their combined innovation and overall score. It is important to note that colour coded products have been scored relative to other products with the same colour coding.



As well as making acquisitions themselves, five of the vendors have been acquired from late 2017 onwards, either by investment firms or other technology vendors. Corelight and Vectra have received substantial investments during 2021.

These factors show the vibrancy of the NDR market and it is certainly possible that more investments will be forthcoming, potentially among other vendors not listed in this market update. Integrations are essential in this market sector and more partnerships are likely to be forged, including in the XDR space.

Metrics

Bloor's bullseye methodology is based on some standard top-level criteria, which are:

- Stability and risk
- Support and location
- Value
- Innovation
- Awareness
- Adoption

This sees vendors positioned according to how they stand in terms of financial viability, customer base, funding, revenues and growth, technology depth and breadth, geographic coverage and the quality of partner networks.

Beyond this, the analyst can choose criteria that reflect the technology sector that is being evaluated. Among the criteria selected were:

- Depth of expertise
- Machine learning and analytics
- Threat detection and risk prioritisation
- Threat hunting
- Incident response
- MITRE ATT&CK engine
- Integrations
- Identity integration
- Coverage for cloud and on premises
- Extension to external networks
- Extent of telemetry
- Amount and length of data capture
- Scalability

Conclusion

NDR should be considered a fundamental capability for driving greater efficiency into security operations, helping to automate the complex processes involved in threat detection and response, along with guidance and expertise that will help security teams navigate the advanced and sophisticated threats against their networks. Integrations with SIEM systems and capabilities such as endpoint detection and response (EDR), incident response and identity controls will allow the whole picture of an incident to be seen, including detailed contextual information that will guide the most efficient response.

Network detection and response (NDR)

Vendor scores

VENDOR	STABILITY AND RISK
Corelight	★★★★
Darktrace	★★★★
ExtraHop	★★★★
Gigamon	★★★★
LogRhythm	★★★★
Vectra	★★★★
Mandiant	★★★★
Flowmon	★★★½
Plixer	★★★½
Fidelis	★★★¼

VENDOR	SUPPORT AND LOCATION
Gigamon	★★★★½
Mandiant	★★★★½
Darktrace	★★★★
ExtraHop	★★★★
Flowmon	★★★★
LogRhythm	★★★★
Vectra	★★★★
Corelight	★★★
Fidelis	★★★
Plixer	★★★

VENDOR	VALUE
Flowmon	★★★★½
Plixer	★★★★½
Gigamon	★★★★¼
Corelight	★★★★
ExtraHop	★★★★
Mandiant	★★★★
Vectra	★★★½
Fidelis	★★★½
LogRhythm	★★★½
Darktrace	★★★

VENDOR	AWARENESS
Mandiant	★★★★½
Darktrace	★★★★¼
ExtraHop	★★★★¼
Gigamon	★★★★¼
Corelight	★★★★
Fidelis	★★★★
Vectra	★★★★
Flowmon	★★★½
LogRhythm	★★★½
Plixer	★★★

VENDOR	ADOPTION
Gigamon	★★★★½
Darktrace	★★★★¼
Corelight	★★★★
ExtraHop	★★★★
Mandiant	★★★★
Plixer	★★★★
Vectra	★★★★
Fidelis	★★★½
Flowmon	★★★½
LogRhythm	★★★

VENDOR	FIT FOR PURPOSE
ExtraHop	★★★★¼
Gigamon	★★★★¼
Mandiant	★★★★¼
Vectra	★★★★
Corelight	★★★★
Flowmon	★★★★
Fidelis	★★★½
Plixer	★★★½
LogRhythm	★★★¼
Darktrace	★★½

About the author

FRAN HOWARTH
Practice Leader, Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including ***Silicon***, ***Computer Weekly***, ***Computer Reseller News***, ***IT-Analysis*** and ***Computing Magazine***. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of ***InfoToday***.

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of Mutable business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

tel: **+44 (0)1494 291 992**
web: **www.Bloorresearch.com**
email: **info@Bloorresearch.com**