MarketReport

Market Report Paper by Bloor
Author **Fran Howarth**
Publish date **March 2020**

MDR market guide

Reducing the costs and risks of cybersecurity investments

> “Complexity and resource constraints are a major burden for any organisation where security is concerned. MDR services will help to overcome those restraints and help organisations to overcome those constraints and realise real business value from the investments that they make.”

Market description

This market guide segments vendors within the still emerging managed detection and response (MDR) services market. It is a wide and varied market and this guide includes information pertaining to some of the main players in the market.

The rising complexity of security technologies and a lacked of skilled resources throughout the cybersecurity profession are leading organisations to seek help in the form of services to manage their security investments. This cuts across organisations of all sizes and in all industries. MDR services provide them with the proactive protection that they need to defeat the security threats that they face.

More details of why MDR services are needed are contained in the sister publication *"Managed detection and response services… key to winning today's security battles."*

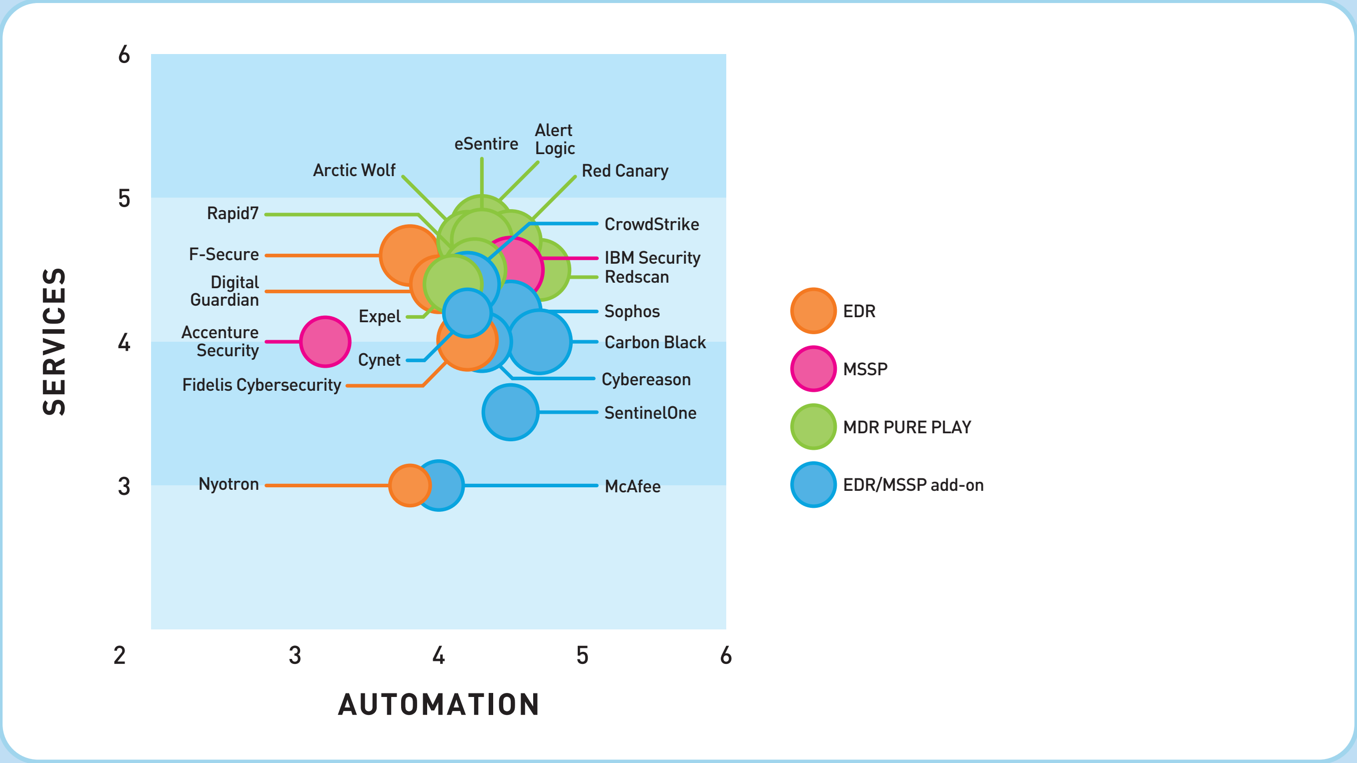
Model monitoring

The criteria and underlying scores for the vendors are outlined in the section "**Methodology and scoring**," on page 12.

Who should care?

This document is intended to help anyone involved in security purchasing decisions understand what is available and what type of services are best suited to their needs.

> **"This document is intended to help anyone involved in security purchasing decisions understand what is available and what type of services are best suited to their needs."**



Introduction

It may sound counter-intuitive, but at the heart of every managed detection and response (MDR) service is automation. Without a high level of automation, an MDR service cannot be successful for your organisation. But without a high level of service provision, your organisation is effectively left on its own to deal with highly complex automation. The two must go hand in hand. And that is how the MDR market has come about.

MDR service providers can manage automated technology on behalf of an organisation, providing value-added services on top that include an orchestrated response to threats and incidents that are uncovered through the automation technologies that they are using.

All MDR services should help an organisation to manage risk associated with cybersecurity threats. There should also be a knock-on effect of being able to improve the achievement of compliance objectives through advanced monitoring and reporting capabilities, but this is really more of a bonus than a prime objective in selecting such services. However, it does indicate the importance of including more than just the security or wider IT team in the decision-making process. Cybersecurity risk is a business risk and should be given the priority that it deserves. Stakeholders from throughout the organisation should have input and decisions should be driven from the top to ensure that decisions made are in line with overall business objectives.

> “Cybersecurity risk is a business risk and should be given the priority that it deserves. Stakeholders from throughout the organisation should have input and decisions should be driven from the top to ensure that decisions made are in line with overall business objectives.”

Questions to ask before making a decision

1 To what extent does your organisation wish to outsource processes?

If you have a fully staffed security operations centre, you may wish just to have help with detecting advanced threats more efficiently. If you are less confident in your response capabilities, you may wish to have advice, services and guidance. If you do not have the resources to staff a SOC yourself, you may wish to outsource everything to a third party.

2 What existing technology and processes are in place?

If you have invested in detection and response technologies but are struggling to realise true value from them, you may wish to choose a provider specialising in that particular technology set. In this case, you have the automation, but need additional skills. If you have not yet invested in detection and response capabilities, your decision might be based on a technology vendor that appears to be the best fit for your needs and that can implement and manage that technology for you. If you have made a range of investments in technology and are looking to achieve greater visibility over them, a provider that is technology-agnostic may best suit your needs. Some of these pure play vendors also partner with leading detection and response technology vendors. If you already working with or thinking of working with an MSSP, an alternative is to look for one that provides MDR services as part of the overall service.

3 Are you looking for guidance or hands-on help?

Are recommendations provided through a portal sufficient for your needs? Do you need occasional help or are you looking for a named practitioner that works closely with your team and has detailed knowledge of your environment? How much regular contact are you looking for? Are quarterly reports enough, or is more frequent interaction needed? Do you wish, and can you cater for, personnel from the service provider coming to your premises and working alongside your team?

4 What is the geographical reach of your organisation?

Although 24x7 service is a feature of most MDR services, where data is stored or resources are located might be a consideration. Some specialise in particular geographies that could be a factor in your decision. Of course, this is a prime consideration when looking for hands-on help.

5 Do you have specialised needs?

Some industry verticals have specialised needs. Organisations in highly regulated sectors might look for those that specialise in their particular regulatory compliance needs. Other industries must monitor specialised endpoints, such as medical devices in healthcare and industrial sensors in manufacturing. There are some MDR providers that focus on particular industries and their needs.

Features to look for

To protect themselves against a wide range of security threats, organisations are looking for greater visibility into activity over their networks to find anomalous events, determine root cause and to determine the best response. Capabilities must cover threat detection, analysis, response and remediation on a 24x7 basis, covering monitoring of and performing security analytics on endpoints, user behaviour, applications, the network and cloud services.

The key categories of technology to look for include endpoint detection and response, network traffic analysis, threat intelligence and hunting, behavioural and security analytics, and orchestration and response.

Consider the extended network. Organisational networks are no longer defined by the walls that have been built around them. A parallel can be seen in identity and access management systems. During the 1990s, most such technologies focused on provisioning and managing access to an organisation's own users for technology deployed on-premise. Today, that is no long sufficient. Mobile devices are pervasive and allow network users to work from anywhere, freed from the confines of needing to be in the office to access the technology and information resources that they need. Extending resource access out to contractors, business partners and customers has become a must. There are also a much wider range of endpoints being attached to networks, from medical devices to those that make up the internet of things. These are increasing being seen as attack vectors by hackers and must be protected. Security and visibility over all endpoints is essential.

Some MDR providers have their roots in endpoint detection and response since endpoint data is key. Endpoints are a key attack vector and many attacks will be found there. But wider coverage will be provided by those who have extended those capabilities to network resources. Features to look for include asset discovery, data packet capture, log and event correlation, network and endpoint behaviour monitoring, vulnerability scanning and monitoring, isolation or blocking of infected endpoints or systems, and root cause analysis to provide details of what exactly has happened so that an appropriate response can be made. Many providers will provide integration with data sources such as a SIEM system, either that owned by the customer or one that they provide and manage.

Why outsource endpoint protection?

There has been much innovation in the endpoint space, which promises greater convenience for users, but which also introduces new threats. Today's endpoint devices can provide a steppingstone into the core network, where the most sensitive data and targets are to be found.

According to the Ponemon Institute, 68% of respondents reported in 2019 that they had experienced one or more endpoint attacks that successfully compromised data assets and/or IT infrastructure during the year, up from 54% in 2017. The cost per endpoint breach is also skyrocketing, averaging $9 million in 2019, up more than $2 million over 2018.

Whilst the need for endpoint protection is clear, 55% state that they lack in-house expertise to manage it, 50% that they lack in-house resources and 41% report that it is too complex to manage in-house. As a result, 69% either outsource endpoint protection or plan to do so.

User and device behaviour and activity monitoring is essential for detecting threats aimed at the network, adding context to activity and behaviour seen in order to make better sense of it. The same is true for activity taking place in cloud-based services, which can be a treasure trove for corporate information owing to the ease with which such services can be accessed as and when needed. Increasingly, other devices such as industrial sensors and smart controls are being connected to networks,

> **Capabilities must cover threat detection, analysis, response and remediation on a 24x7 basis, covering monitoring of and performing security analytics on endpoints, user behaviour, applications, the network and cloud services.**

increasing the threat vector yet further. Organisations should look for a service that can ingest data and activity feeds from all devices that connect to the network to ensure that there are no gaps in their security coverage. All data sources should be continuously monitored to provide protection on a 24x7 basis.

Coverage for advanced threats is essential. Long gone are the days when technology could only protect against known threats for which countermeasures had been developed—known as signature-based defences. Today's technologies incorporate advanced analytics, threat intelligence, forensics and contextual information regarding how an event occurred. Many also deploy machine learning, which enables predictions to be made with limited human supervision regarding which events seen are likely to be malicious.

Organisations that wish to more proactively search for previously unknown threats or malicious activity can make use of threat hunting services offered by many MDR providers. Threat hunting combines the use of machine learning and behavioural analysis techniques that delve into information to find indicators of compromise and suspicious activity such as lateral movement across a network with the use of threat intelligence to understand the tactics, techniques and procedures used by attackers and to look for indicators of compromise. It provides organisations with a better chance of catching an attack early in order to limit the resulting damage.

Threat hunting uses mix of human expertise and automation, with the human expertise being necessary to generate alerts regarding attacks that go undetected by automated tools. It requires the organisations sift through endpoint and network data. Data from endpoints are particularly useful for providing evidence of malicious activity that would be missed by security controls such as SIEM systems, which generally lack coverage of such data. Endpoints are preferred conduits for attackers, but many organisations struggle to get the most out of endpoints controls that access endpoint user activity and forensics. Threat hunting is a capability originally offered by many MDR providers focused on endpoint detection and response, but is now being offered by a wider selection.

According to the SANS Institute, 61% of organisations report a measurable improvement in their overall security posture of at least 11% through threat hunting, with 12% reporting an improvement of more than 50%. The areas of greatest improvement were more robust threat detection capabilities, a reduced attack exposure and fewer false positives from alerts.

Some organisations, especially those that rely on endpoints such as internet of things devices and medical systems that are generally not covered by existing detection technologies, may wish to consider the provision of deception techniques that can identify attacks originating on such devices, protecting against exploits such as data exfiltration and ransomware.

Some providers offer penetration testing and red and blue teaming to improve the effectiveness of detection and response. Such services help organisations to test how well their security programme performs in terms of protecting critical assets, including the data, systems and people that are of real importance to an organisation. They can show where the security programme is performing well, as well as highlighting gaps that have been overlooked.

The SANS Institute has identified red teaming as being one of its 20 critical security controls, enabling organisations to improve organisational readiness to combat the threats that they face, improve training for defenders and gauge current performance levels. They provide objective insights regarding the existence of vulnerabilities, and the efficacy of defences and mitigating controls, including those planned for future implementation.

> **“Organisations should look for a service that can ingest data and activity feeds from all devices that connect to the network to ensure that there are no gaps in their security coverage. All data sources should be continuously monitored to provide protection on a 24x7 basis.”**

Different flavours of MDR

Endpoint detection and response

There are many MDR providers that have their roots as vendors of EDR technology. These MDR providers leverage EDR technologies that collect and analyse behavioural data from endpoints and users to identify patterns of activity that could be anomalous or malicious. They provide services on a 24x7 basis to organisations that include threat detection, investigation, analysis and response to supplement in-house teams or to provide a completely outsourced service to those lacking internal resources.

Some MDR providers in this space have developed their own EDR technology, which forms the basis of their services. Others deploy best-of-breed EDR technology from other vendors, with some offering their customers a choice of which they want to have deployed. Some offer response services themselves, using their own staff, whilst others make use of partners who are closely integrated with their offering. Potential customers should take decisions not only on the basis of the underlying technology, but also of the strength of the services offered, such as number and expertise of the resources they have dedicated to the service.

EDR solutions can integrate into a number of tools, including malware analysis, network forensics, SIEM systems and threat intelligence, as well as security automation, orchestration and response tools. Increasingly, coverage is being extended to cloud usage, covering virtualised environments that include those from the major providers such as AWS and Azure, as well as more traditional endpoints in order to cater to hybrid environments, which are increasingly becoming the norm.

> “Potential customers should take decisions not only on the basis of the underlying technology, but also of the strength of the services offered, such as number and expertise of the resources they have dedicated to the service.”

Pure play MDR service providers

Other MDR providers, sometimes known as pure play MDR players, offer services that are in large part technology-agnostic to integrate with the current capabilities of an organisation, although some do work with preferred technology vendor partners in certain areas. Such providers need to have a breadth of technology expertise, but their offerings can be considered to be more service-driven. A key consideration

Examples of MDR vendors in the EDR space

- Carbon Black
- CrowdStrike
- Cybereason
- Cynet
- Digital Guardian
- Fidelis Cybersecurity
- F-Secure
- Nyotron
- Sentinel One
- Sophos

Examples of pure play MDR providers

- Alert Logic
- Arctic Wolf
- eSentire
- Expel
- Rapid7
- Red Canary
- Redscan

is the amount of telemetry that they can ingest to correlate and analyse events across a wide range of systems, covering the network, endpoints, on-premise systems and, increasingly, cloud services. This enables far greater targeted analytics. Many offer ancillary services such as intrusion detection and prevention, and vulnerability assessment and management, penetration testing and red teaming.

The wider MDR services offered by providers in this space will be especially useful for those with complex IT environments, although this does not necessarily mean that they are purely for large enterprises. Whilst individual technologies are themselves complex, the sheer volume of technologies and vendors that many organisations have invested in will lead some organisations to consider investing in this flavor of services. They will be particularly useful for those that have inherited technologies as a result of mergers and acquisitions. Many have tiered offerings that enable organisations to choose what level of service is best for them and to move up or down the tiers as needs change.

MSSPs

Another class of MDR providers offer technology and services as add-ons to the wide, but shallow offerings of managed security services providers (MSSPs). Many organisations utilise MSSP services for their IT service management needs and others would be interested in taking such services if they offered more advanced MDR capabilities on top of other services, which many are now doing.

The table (right) shows MDR providers offering add-on services to MSSPs and MSSPs who themselves offer MDR services.

The importance of telemetry

The word telemetry comes from the Greek for remote and measure. In IT terms, it refers to data that is collected from multiple points to give a complete view of network activity. By gaining a complete view, organisations will be better able to effectively manage threats and make more informed decisions regarding what actions to take.

However, the sheer volume of data that must be collected from multiple sources makes it a challenge to make sense of the data. This is compounded by an ever growing array of data sources as data must be collected from endpoints, networks, security controls and cloud services. The data that must be collected includes NetFlow, packet capture, endpoint forensics, and log and event data to provide information about where data is flowing, from what devices and to what IP addresses. A key challenge is to narrow all that data into a tractable stream in order to find signals through the noise that can be used for targeted analytics.

It is beyond the means of most organisations to collect, normalise and analyse such huge data sources, which is where it makes sense to outsource to MDR providers, some of which are handling hundreds of terabytes of telemetry information per month. They will provide the eyes and ears that organisations need in order to understand how threats and vulnerabilities uncovered through analysis of such information impacts them, and what is the best response to take.

MSSPs

- Accenture Security
- IBM Security

MDR providers offering add-on services to MSSPs

- Carbon Black
- CrowdStrike
- Cybereason
- Cynet
- McAfee
- SentinelOne
- Sophos

Further considerations

A further factor to consider is whether the MDR provider offers services from its own facilities or can provide *"boots on the ground"* should a serious incident occur, where staff from the provider will work alongside an organisation's security responders to provide a swifter, more efficient resolution of the problem. Any organisation that would like a more hands-on service should consider whether it is included in the service or is provided as a retainer, and where the resources are located. Even where a hands-off service is preferred, the location of the provider's security operations centre may be an important consideration. Some providers are actively expanding their geographic reach.

Pricing is another consideration. Some MDR vendors offer tiered pricing, with services provided in the lower tiers offering less support than those at higher levels, where the MDR provider will likely offer much higher levels of guidance that is more tailored to the organisation's specific environment. In general, pricing that is on the basis of coverage in terms of per user, device, server or sensor is easier and more predictable than pricing based on volume of traffic monitored.

Where staffing is concerned, pertinent questions will include the total number of employees, especially those involved in service provision, and their levels of expertise. A more personalised service will be provided by MDR providers that give their customers named analysts and engineers who can be reached directly and will be familiar with the customer's environment, rather than the customer being routed via a central phone number or online service. Many vendors will offer regular communications, such as a monthly or quarterly meeting with customers in order to discuss progress. Owing to the sophisticated and expanding nature of the services offered and the speed with which new threats are being encountered, a key consideration can be whether the service provider actively encourages its practitioners to engage in security research in addition to providing services to clients. Some include development staff who work to ensure that the services they offer keep up with fast changing technology environments. The varied nature of the work offered and ability to advance their skills are real draws for practitioners looking to work in such environments and is key to why such providers are able to attract and retain talent.

Within the overall market, there are some MDR providers that are specialised in certain areas. These include those that cater to industrial environments, or specific industries such as healthcare or government. Others offer services such as red teaming, which go beyond penetration testing to act as an adversary would in order to test an organisation's defences. An example of an MDR provider focused on the industrial sector is Airbus.

> "A more personalised service will be provided by MDR providers that give their customers named analysts and engineers who can be reached directly and will be familiar with the customer's environment"

The vendors

As noted above, there are many flavours of MDR services. Bloor Research invited 38 vendors to brief us on their offerings. Of these, 16 responded, the majority of which provided full briefings. Accenture Security and IBM Security provided information and the scoring is based on more general briefings. In the case of Accenture, this is based on information regarding Symantec services, which it has recently acquired, in addition. Some vendors responded, but were unable to provide information within the requested timescale. They will be included in future versions of this research.

Some of the vendors included in the EDR space have capabilities that go considerably beyond pure EDR, which has been taken into account. Some of these vendors partner with other MDR providers, with their technology underpinning services offered by other vendors. A case in point is Carbon Black, which is used by four of the pure play MDR providers.

> “The MDR services market is wide and varied and this guide includes information pertaining to some of the main players in the market.”

Methodology and scoring

The MDR providers included were scored according to three main criteria – automation, services and scores from Bloor's Bullseye methodology, aggregated to form one score, which determines the size of the bubble. Within the Bullseye criteria, the following attributes were considered:

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

The individual scores are as follows:

VENDOR	AUTOMATION SCORE	SERVICES SCORE	BULLSEYE SCORE	FLAVOUR
Accenture Security	★★★⯪	★★★★	★★★⯪	MSSP
Alert Logic	★★★★⯪	★★★★⯪	★★★★⯪	MDR pure play
Arctic Wolf	★★★★⯪	★★★★⯪	★★★★⯪	MDR pure play
Carbon Black	★★★★⯪	★★★★	★★★★⯪	EDR/MSSP add-on
CrowdStrike	★★★★⯪	★★★★⯪	★★★★⯪	EDR/MSSP add-on
Cybereason	★★★★⯪	★★★★	★★★★⯪	EDR/MSSP add-on
Cynet	★★★★⯪	★★★★⯪	★★★⯪	EDR/MSSP add-on
Digital Guardian	★★★★	★★★★★	★★★★	EDR
eSentire	★★★★⯪	★★★★⯪	★★★★⯪	MDR pure play
Expel	★★★★⯪	★★★★⯪	★★★★	MDR pure play
Fidelis Cybersecurity	★★★★⯪	★★★★	★★★★⯪	EDR
F-Secure	★★★★	★★★★⯪	★★★★⯪	EDR
IBM Security	★★★★⯪	★★★★⯪	★★★★⯪	MSSP
McAfee	★★★★	★★★	★★★⯪	EDR/MSSP add-on
Nyotron	★★★★	★★★	★★★	EDR
Rapid7	★★★★⯪	★★★★⯪	★★★★⯪	MDR pure play
Red Canary	★★★★⯪	★★★★⯪	★★★★⯪	MDR pure play
Redscan	★★★★⯪	★★★★⯪	★★★★⯪	MDR pure play
Sentinel One	★★★★⯪	★★★⯪	★★★★	EDR/MSSP add-on
Sophos	★★★★⯪	★★★★⯪	★★★★⯪	EDR/MSSP add-on

Summary

No organisation has unlimited budgets for security investments and it is vital that they can achieve real value to the organisation as a whole from the investments that they make. MDR services will help organisations not only to achieve that value, but to prove it through reduced exposure to cybersecurity risks and a much better ability to recover from incidents that do occur. The MDR services market is relatively new and will continue to evolve. Choosing a provider that is right for a particular organisation is vital for reducing the costs and risks of security investments.

> **“The MDR services market is relatively new and will continue to evolve. Choosing a provider that is right for a particular organisation is vital for reducing the costs and risks of security investments.”**

FURTHER INFORMATION
Further information about this subject is available from
https://www.bloorresearch.com/technology/managed-detection-and-response/

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

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.

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**