KuppingerCole ANALYSTS

Tata Communications MDR

Warwick Ashford

December 19, 2023

This KuppingerCole Executive View report looks at the managed detection and response (MDR) market and at how solutions address key challenges, with a review of the MDR service and related supporting services from Tata Communications.

Content

Figures

Introduction

Industrialized cyber-criminal operations and increased nation state sponsored cyber espionage activities mean that most organizations are under continual cyber-attack, but the worldwide shortage of cybersecurity skills means many organizations are struggling to keep up with attackers, and security teams are often overwhelmed by the number of security alerts being generated by a multitude of security systems.

These and other related factors are driving the growth and evolution of the managed detection & response (MDR) market for solutions that manage a collection of cybersecurity technologies or an integrated platform for a client organization to provide advanced cyber threat detection and response capabilities, including security operations center as a service (SOCaaS) solutions.

MDR solutions are typically backed by teams of security experts that provide round-the-clock monitoring, analysis, response, and remediation, as well as advice on how to improve the client organization's cyber security posture. MDR solutions, therefore, go beyond traditional managed security services (MSS) from managed security service providers (MSSPs), which typically focus on compliance reporting and helping customer organizations to meet security compliance requirements.

All organizations, regardless of size, face similar cyber threats and therefore need advanced cybersecurity detection and response capabilities. Smaller organizations often lack the budget and skills to do this, while all organizations struggle to fill cybersecurity positions.

MDR solutions mean that even smaller organizations can tap into the benefits of having a large team of experts with relevant technologies continually on call to detect and respond to incidents and help guide investments, strategies and processes without the cost and challenges of finding and retaining people with the necessary skills.

Where there is little or no in-house threat detection and response capability, MDR solutions help enterprises to outsource the majority of their security operation, including security related management of networks, endpoints, applications, websites, databases, and security logs. Many MDR services enable organizations to outsource their SOC completely if they do not have the resources to act on recommendations for containing threats, and in a growing number of cases, MDR services support automated response capabilities.

Where there is some in-house security capability, MDR can be used to supplement this whenever necessary to ensure that an organization has at its disposal all the cyber security skills and capabilities required to deal with high-risk threats and critical incidents.

Even large organizations with in-house security teams find it challenging to manage security information & event management (SIEM), network detection & response (NDR), endpoint detection and response (EDR), security orchestrations, automation, and response (SOAR), and even identity & access management (IAM) systems to deliver the required security outcomes. As a result, they are turning to MDR service providers to help with this, as well as provide rapid automated containment capabilities for common threats.

Business benefits of MDR:

- Strengthen organizations' ability to monitor and detect security threats and respond to security incidents 24/7.
- Continually improve overall security strategy and posture.
- Provide a comprehensive view across the fragmented IT environment.
- Enable in-house security teams to focus on and manage strategic security initiatives.
- Increase value from existing security investments.

Operational benefits of MDR:

- Helping customer organizations deal with high volumes of security alerts.
- Reducing the time that it takes to identify and mitigate security incidents.
- Providing advanced analytics of threats and user behavior.
- Rationalizing, updating, and integrating/coordinating security tools.
- Improving visibility and governance of business IT environment across the whole enterprise.
- Providing tools and expertise to deliver or augment EDR, XDR, and SOAR capabilities.
- Monitoring and supporting compliance with cybersecurity regulations.

Evidence of the increased demand for MDR solutions can be seen in the rapid growth in the market. KuppingerCole Analysts predicts that the compound annual growth rate (CAGR) of the MDR market will be 20.1%, suggesting a market size of approximately $3.88bn by 2025.

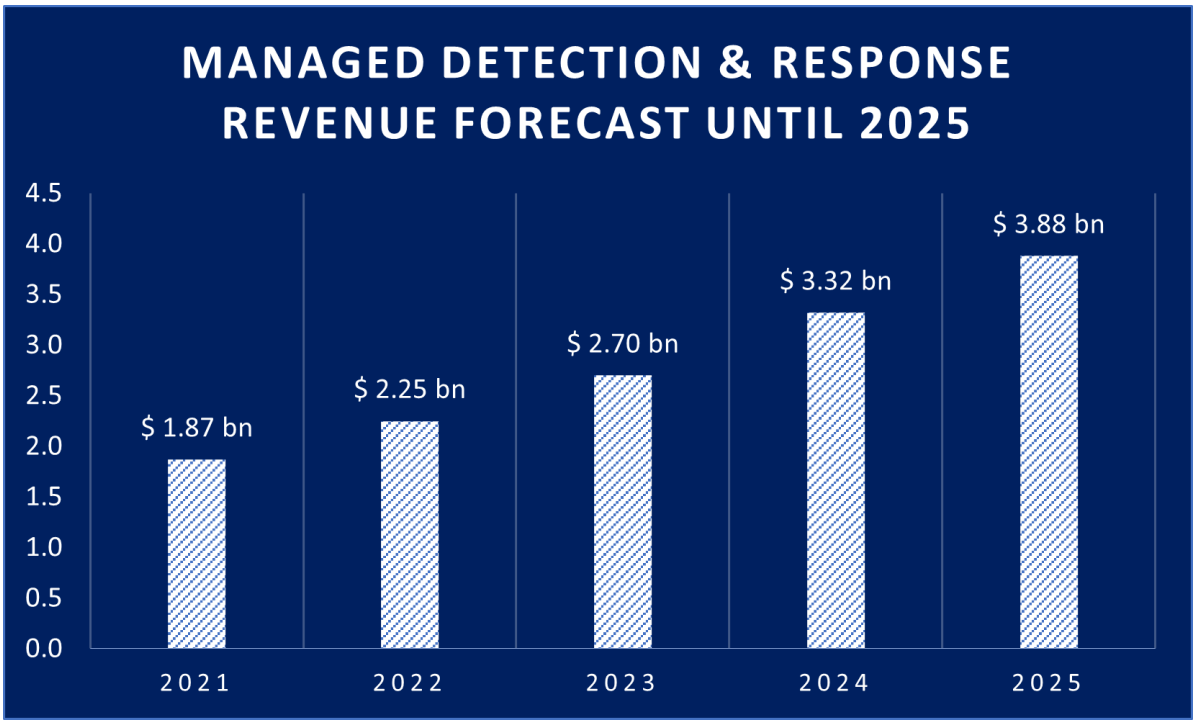

Figure 1 KuppingerCole projected MDR market growth

Product Description

Tata Communications is a global public company providing a range of communication services, network services, cloud services, and cybersecurity services, including MDR. It was founded in 2002 and is headquartered in Mumbai, India.

Tata Communications MDR is among the product leaders in the KuppingerCole Managed Detection and Response (MDR) Leadership Compass 2023 and is part of the company's cyber threat detection and response portfolio, combining several security platforms (SIEM, native SOAR, EDR, NDR, and user and entity behavior analytics (UEBA)).

Tata Communications is able to support all forms of digitalization, with network, cloud infrastructure, security, communications, and IoT solutions. Cyber threat detection and response is a key pillar of the security portfolio, which is made up of MDR/managed SOC, managed SIEM, captive SOC, and EDR solutions. The core MDR service, therefore, is supported by a range of additional services that include key MDR add-ons, enterprise security capabilities, and digital transformation building blocks.

There are five key MDR add-ons:

- Advanced threat hunting.
  - Retro-hunting of indicators of compromise (IoCs).
  - Iterative hunting of attacker tactics, techniques, and procedures (TTPs).
  - Situational/customized hunting.
- Brand monitoring.
  - Monitoring of internet for brand abuse and fake websites.
  - Monitoring of Domain Name for new registrations.
  - Social media monitoring for brand abuse, phishing, and malware.
  - Monitoring App stores and internet for rogue/malicious mobile apps.
  - Monitoring of social media for fake profiles of key executive staff.
  - Monitoring of dark web for data loss recovery.
  - Site take down for phishing/fake sites.
  - Alerting if source code is copied and re-hosted.
  - Monitoring of spam email traffic.
  - Monitoring of known malicious and blacklisted URLs and IP addresses.
  - Customer website scanning for malware and blacklisting.
  - Third-party vendor assessment.
- Red teaming as a service.
  - Simulating real-world attacks.
  - Testing of effectiveness of security measures.
  - MDR improvement based on red teaming exercises.
  - Comprehensive reporting on security posture and gap assessment.
- Malware analysis.
  - Automated and on-demand file scanning.

- Forensic retainer services.
    - Full forensic capabilities.

There are four main areas of enterprise security capabilities provided by Tata Communications, broken down into greater detail in Figure 2.

- Cyberthreat detection & response.
- Advanced network security.
- Security assessment and consulting services.
- Cloud security.

Tata Communications also provides a range of building blocks for digital transformation that collectively deliver a “digital fabric” for end-to-end visibility and management that can be consumed through APIs and include:

- Connected infrastructure for cloud, network, and Edge.
- Connected solutions for IoT and private networks.
- Connected experiences for remote workforce, customers, and the media & entertainment vertical.

Figure 2 Enterprise security capabilities in detail (source: Tata Communications)

The core MDR service can be deployed as cloud only, on premises only, or in a hybrid model, in which case, on-premises elements include a virtual appliance and agents installed on the network for NDR and endpoints for EDR. There is a simple licensing model based on events per second (EPS), which can include EPS metrics derived from the number of log sources feeding into the service.

Tata Communications uses a five-step approach to 1) Identify key data assets across heterogeneous IT environments. 2) Ingest log data from assets into a single data lake. 3) Enrich logs using threat intelligence, correlation rules, and data models. 4) Investigate logs to

decrease threats by analyzing similar historical patterns and dependencies. 5) Involve human expertise for threat response and enabling security automation.

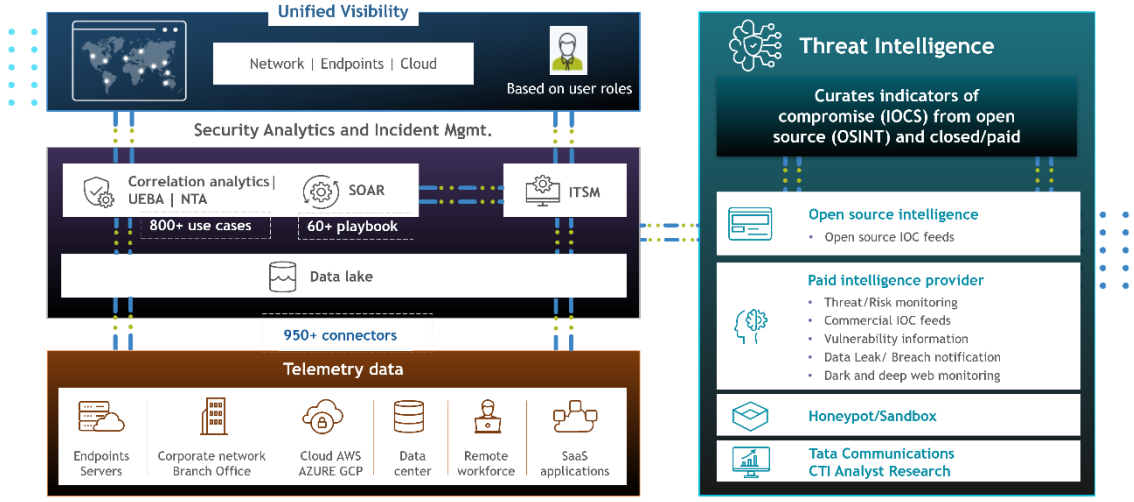

Figure 3 Key components of Tata Communications MDR (source: Tata Communications)

The service covers Windows and Linux but not Mac OS, Android, or iOS, while coverage includes all major browsers, except Safari. The service provides continuous monitoring and analysis of all major business IT environments and systems, including Edge computing environments, and provides detection and response services across several environments, including remote workers but not all on-premises applications, and excluding medical and industrial IoT, OT environments, and mobile devices.

Tata Communications MDR includes prebuilt integrations with four third-party EPDR products (CrowdStrike Falcon Endpoint Protection, Microsoft Defender for Endpoint, SentinelOne Singularity Platform, and TrendMicro), 22 NDR products, seven SIEM solutions, and 15 behavior analytics products, but custom integrations can be built for other third-party products if the necessary APIs are available.

There is good support for cloud computing, with the service providing continuous monitoring and analysis of cloud applications and cloud data stores, with detection and response capabilities across all cloud services and applications, and the ability to identify data loss across cloud infrastructure. Cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments are available as part of the company's cloud security and security assessment & consulting services portfolio.

Tata Communications MDR is able to detect threats across the entire customer hybrid IT estate, do network-based detections including full packet capture and inspection, and detect a wide range of malicious activity, including ransomware attacks but not evasive malware. The service includes attacker behavior analytics.

Detection time is reduced through the combined use of security analytics on the data lake, user behavior analytics, multi-cloud security capabilities, network behavior analytics, business application monitoring, compliance management, threat hunting, anti-phishing capabilities in the deep and dark web, and cyber threat intelligence capabilities.

The service is able to disrupt threats automatically, while attack blocking capabilities include the disruption of malicious network communications and account suspensions. However, the service does not include post-remediation support to validate that a threat has been neutralized or verify that it has not resurfaced, nor does it support activity monitoring for forensic analysis.

Tata Communications MDR is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, and quarantining files but not carrying out sinkholing actions or preventing registry changes. The service includes its own SOAR functionality with multiple playbooks to improve MTTR and has integrations for 21 third-party SOAR solutions, with custom integrations available.

The service includes the support of a dedicated threat hunting team, regular automated and manual threat hunting including retrospective threat hunting and regular reporting on the findings. The service applies threat intelligence from the company's threat intelligence team, NetFlow Data, customer deployments, honeypot environments, technology partners, industry bodies, commercial threat intelligence feeds, and a large number of open-source intelligence feeds. Additionally, Tata Communications generates threat intelligence from the internet traffic visibility it has as a Tier one ISP as well as from deep and dark web monitoring. The service also includes connectors to five cyber threat intelligence sources.

The service is able to capture East-West traffic for insider threat detection, it can detect and respond to insider threats, phishing attacks, and abuse of privileged access. It also includes user behavior analytics.

Tata Communications offers a service for assistance with initial setup of the service and the services of an expert team for assisting with incident analysis and remediation. Incident handling is provided as part of standard service support, but support services and documentation is available only in English. On-site support is available only in the APAC region.

Customers can use the service to outsource their SOC entirely or SOC analysts from Tata Communications can work as an extension of the internal SOC or security team. The service includes regular risk assessment reporting but does not include assistance in developing security and governance policies. There is a dedicated analyst or team allocated to each customer, and continual strategic and security improvement planning is included as part of the standard subscription.

The Tata Communications MDR service is well supported by the company's wider cybersecurity and threat management capabilities, with supporting services in the company's key portfolio areas of advanced network security, security assessment and consulting, cyber threat detection and response, and cloud security. The core MDR service is further strengthened by a real-time network analytics platform that can leverage the company's global network data as the carrier of 30% of global internet routes. Tata Communications also connects 60% of cloud providers to their businesses, and 80% of mobile users to their service providers.

Strengths and Challenges

The Tata Communications MDR service is a mature solution with a good balance of key capabilities, with high scores in cloud support, threat detection, and automation functionality, and scoring well in terms of enterprise IT environment coverage, response capabilities, insider threat detection, threat intelligence, and administration support. The solution has good internal security and a wide range of functionality. Tata Communications also provides a wide range of premium services, including key MDR add-ons, enterprise security services, and building blocks for its digital fabric concept to provide end-to-end visibility and management, Zero Trust security, and analytics and reporting enabled by device intelligence, locational intelligence, and situational awareness (DILISA) that can be consumed by customers' applications via APIs. These additional services help to make the core MDR service more robust and more impactful in managing customers' cybersecurity.

Although scoring well in terms of deployment, interoperability, usability, and innovation, these are all areas in which there is room for improvement.

Tata Communications plans to address these areas with chat bots within the portal, a mobile application, more automation within threat hunting, AI support on SOAR to suggest playbooks, and collaboration functionality to identify analysts within organizations with experience in similar incidents all on the MDR service roadmap.

The Tata Communications MDR service is suitable for organizations of all sizes, particularly those looking for a wide range of supporting security and infrastructure services, as well as those with specific regulatory compliance requirements who are looking for a wide ranging MDR capability that is easy to use, has a high degree of interoperability for ROI purposes, has a good range of insider threat detection, and has strong support for cloud computing.

Strengths

- Simple licensing model.
- Flexible deployment options.
- Interoperable with a wide range of third-party security products with more than 950 integration connectors available.
- Strong MDR coverage of cloud computing environments.
- Good range of detection and response capabilities.
- Maps threats to MITRE ATT&CK® framework.
- Wide range of automated response capabilities.
- Built in SOAR functionality as well as a wide range of SOAR integrations.
- Strong threat intelligence, data analytics, and threat hunting capability.
- A wide range of support services can be added to the core MDR service.

Challenges

- Coverage of a wider range of operating systems would support more customers.
- Expanding MDR coverage to include all on-premises applications, IoT, OT, and mobile devices would strengthen the offering.
- Adding activity recording would help customers conduct forensic analysis of incidents.

- Adding assistance in developing security and governance policies would complement the risk assessment reporting and increase the value of the service to customers.

Related Research

Leadership Compass: Endpoint Protection, Detection & Response
Leadership Compass: Network Detection & Response (NDR)
Market Compass: Security Operations Center as a Service (SOCaaS)
Market Compass: Cybersecurity for Industrial Control Systems
Buyer's Compass: Security Operations Center as a Service (SOCaaS)
Leadership Brief: Do I Need Endpoint Detection & Response (EDR)?
Leadership Brief: The Differences Between Endpoint Protection (EPP) and Endpoint Detection & Response (EDR)

About KuppingerCole

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

For further information, please contact clients@kuppingercole.com.