Data sheet

Enterprise Security Services

Managed Detection and Response

Our **Managed Detection and Response** (MDR) service combines human and machine expertise with leading technologies and threat intelligence to detect and disrupt hard-to-find attacks.

The threat landscape continues to become more dynamic and sophisticated while the attack surface expands and becomes more complex to secure.

Lean security teams lacking the right skills results in disjointed incident management and undetected attacks, especially sophisticated attacks from advanced persistent threat actors.

Adding more security layers increases complexity and generates even more logs and alerts that go untreated.

> **"Shifting our approach to MDR reduced the** impact of security incidents."
>
> **CISO,** regional bank

Organizations turn to more tools in the hope that the next generation of technology will improve the situation. Using technology alone, however, is not the solution. Extracting value from that technology depends on your ability to operate it and on specialist configurations by dedicated teams.

A single, intelligent solution for managing threats

MDR is a scalable, cloud-native, security analytics and response platform. It combines an intelligent security analytics service with threat intelligence across the enterprise. Integrated with our strategic technology partner ecosystem, it delivers a single solution for:

- Attack detection
- Threat visibility
- Response actions

Make a good thing better

Through APIs and automation, our security platform is fully integrated with market-leading technologies. This allows us to:

- Analyze event and evidence data
- Validate and investigate threats and suspected threats
- Classify or verify the classification of security incidents
- Notify you and provide details and investigation reports contextualized information
- Implement required, supported and agreed actions to minimize impact

Pervasive threat intelligence

Our MDR service has infused threat intelligence into its underlying technologies:

- **Automated threat detection** continuously updates adversary threat insights and related infrastructure.
- **Threat infrastructure fingerprinting** utilizes TI that fingerprints adversary infrastructure to identify a threat when infrastructure is reused or repurposed by differing threat actors.
- **Continuous threat actor infrastructure identification** uses automated discovery and continuous scanning across worldwide infrastructure.
- **Threat intelligence integration** is the power to analyze and match events with threat indicators to produce security alerts and automated responses, ensuring that we improve both detection and response metrics.

MDR process flow

Our curated technology stack provides native protection capabilities while monitoring data for suspicious activity. Advanced analytics using artificial intelligence and machine learning (AI/ML) detect events that merit closer examination. Humans investigate the incident and disrupt threats by implementing response actions.

> **"NTT's platform and threat** intelligence deliver better outcomes."
>
> Security analyst

MDR provides:

- Several service tiers and deployment options
- Add-ons that expand detection capabilities and response actions: MDR for Endpoint, and Security Device Management (SecDM) for MDR
- 24x7 security-analyst-driven investigation and disruption of attacks using NTT's threat hunting capabilities, delivered from certified, accredited, specialized and secure delivery locations
- Continuous monitoring of log and event data for in-scope/contracted devices and sources
- NTT's expertise, experience, advanced analytics and external threat intelligence
- Response actions for supported technologies
- Comprehensive, MITRE ATT&CK framework-aligned incident reports to enable a rapid response
- Access to MDR dashboards and incident reporting on our Services Portal
- Digital Forensics and Incident Response for support in the event of critical incidents
- Real-time and long-term threat correlation to enable historical data analytics and analysis

Achieve your resilience goals with MDR

Advanced analytics and anomaly detection find more threats

An advanced analytics engine leverages our big data threat intelligence and an extensive machine learning framework. Our algorithms continuously harvest vast amounts of data from exclusive sources that are applied to multiple supervised and unsupervised ML stages. We train existing ML models, extract features for new ML models, create behavior and pattern signatures, and generate indicators of compromise. As a result, our robust detection algorithms quickly and accurately identify suspicious and malicious activity – which is why more security incidents are initially detected by our methods than by the native detection capabilities of any single technology.

Threat hunting with evidence data

Evidence data is like having all the clues from a crime scene, enabling the detective to develop plausible theories. MDR security analysts use the platform's threat hunting capabilities to find advanced threats, going from one piece of evidence to another until they find an attack path that leads to a security incident.

Rapid response with threat containment, digital forensics and incident response

After detecting signs of initial compromise, it is imperative to respond as fast as possible to reduce potential impact. MDR response capabilities include options to implement threat containment actions. For incident management and coordination of major incidents, the MDR service includes 24x7 access to our Digital Forensic and Incident Response team.

Expert guidance and oversight

You'll have access to a subject matter expert in cybersecurity with a strong operational focus to ensure you realize the value of the MDR service. Our Information Security Manager provides support as part of a long-term relationship, enabling them to develop a deep understanding of your environment and business.

Finding business efficiencies and complementing in-house skills

Hiring, training and retaining expert security staff can be difficult, especially if you want 24x7 security operations. The most experienced security analysts rarely work night shifts over the long term. And even if you have the budget for it, investing in in-house capabilities may not be the most efficient use of corporate resources. MDR delivers the security outcomes you're looking for without any operational challenges, so you can confidently focus on your core business

MDR security analysts use the platform's **threat hunting capabilities** to **find advanced threats,** going from one piece of evidence to another until they find an attack path that **leads to a security incident**.

Why NTT?

Extensive track record

We mitigate 2 billion security threats every year.

Full lifecycle

We turn goals into outcomes through a lifecycle of services.

Next-generation analytics capabilities

Our advanced analytics are based on decades of ML algorithm development and threat intelligence.

Global scale

We deliver services in over 200 countries across 5 regions.

If you'd like to find out more about MDR or are interested in other services, speak to your Client Manager or contact us here: services.global.ntt

