Strengthen your business resilience with AI-powered security operations

Managed Extended Detection and Response (MXDR)

Enterprises are facing a new class of cyberthreats driven by AI-enabled adversaries. Attackers now automate complex, multistage attacks at machine speed, exploit expanding digital footprints and target supply chains with increasing precision. At the same time, security teams are burdened by tool sprawl, alert fatigue, skills shortages and tightening global regulations.

NTT DATA Managed Extended Detection and Response (MXDR)
Powered by Palo Alto Networks Cortex XSIAM®

Our service enables organizations to shift from reactive security to AI-driven, outcome-focused and **autonomous security operations**. Our services deliver unified visibility, advanced analytics and intelligent automation through an agentic AI-powered platform to proactively prevent, detect, and respond to threats across the enterprise and stay ahead of adversaries. This highly modernized platform is backed by skilled and dedicated **Information Security Managers (ISMs), digital forensic experts and certified security professionals.**

Five core strategic elements of our service

01 AI platform

A powerful cloud-native AI engine that unifies security technologies with 1100+ ready-to-use integrations and applies 2900+ ML driven models along with 13000+ out-of-the-box detectors to detect advanced and emerging threats

02 Proactive threat management

Continuously strengthens security posture through actionable intelligence, threat hunting, digital risk monitoring, attack-surface validation and breach simulations

03 Automation

Streamlines security operations with automated playbooks, enabling faster, consistent and reliable incident response

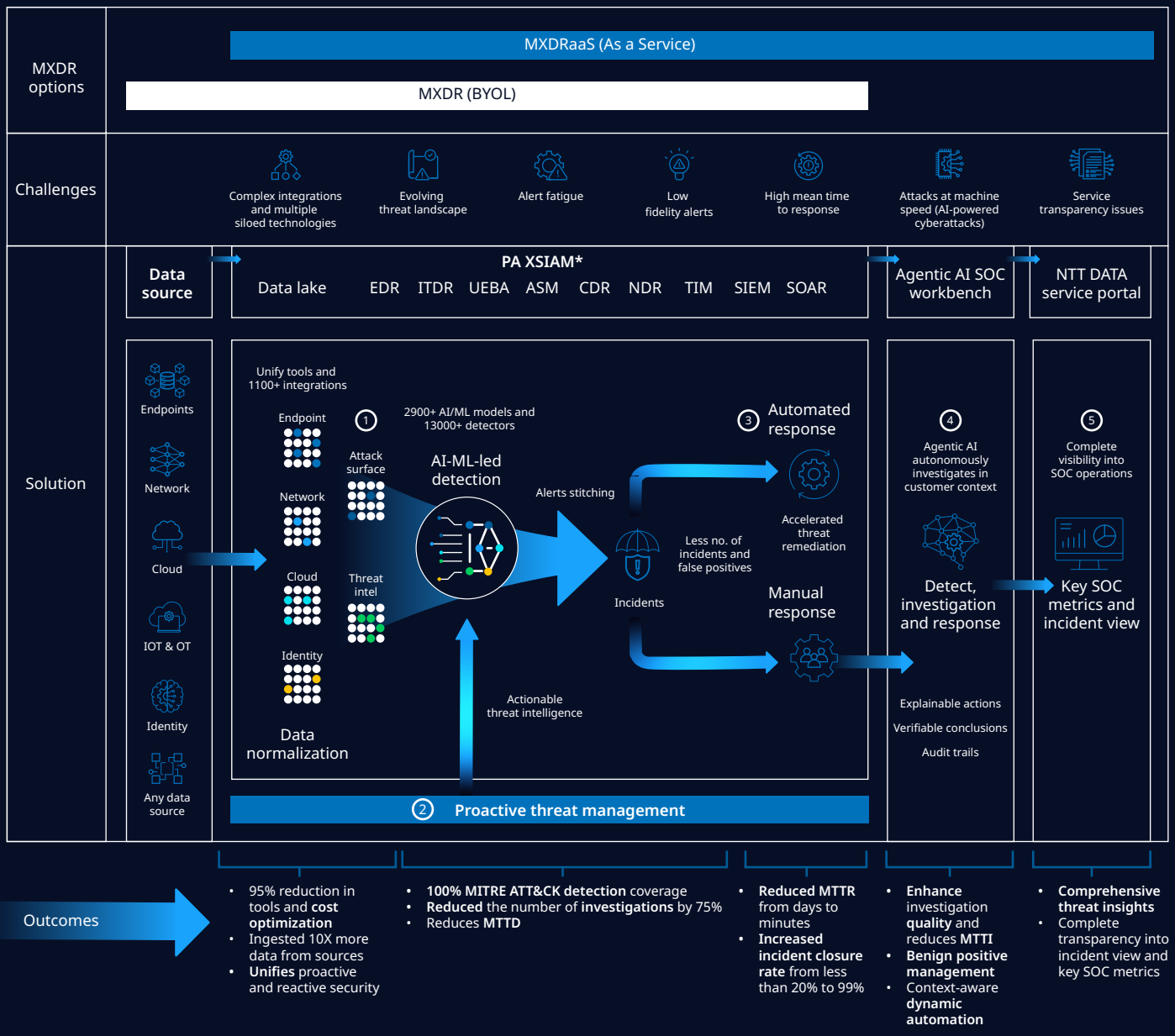
04 Autonomous SOC

Delivers intelligent, agent-driven automated triage at machine speed and dynamic automation to enhance investigation quality, manage noise and accelerate incident response

05 Single pane of glass

Provides full visibility of SOC performance, threats, SLAs and cost drivers through a client service portal

Managed Extended Detection and Response



Outcomes

- 95% reduction in tools and **cost optimization**
- Ingested 10X more data from sources
- **Unifies** proactive and reactive security

- **100% MITRE ATT&CK detection** coverage
- **Reduced** the number of **investigations** by 75%
- Reduces **MTTD**

- **Reduced MTTR** from days to minutes
- **Increased incident closure rate** from less than 20% to 99%

- **Enhance** investigation **quality** and reduces **MTTI**
- **Benign positive management**
- Context-aware **dynamic automation**

- **Comprehensive threat insights**
- Complete transparency into incident view and key SOC metrics

*XSIAM instances can be located in any GCP region that supports the PA XSIAM platform

Strengthening your security operations

NTT DATA MXDR is available through bring-your-own-license (BYOL) or as-a-service models. We support organizations of all sizes and across industries.

Security monitoring and detection of threats:

24x7 security monitoring with advanced analytics leveraging PA XSIAM reducing the Mean Time to Detect (MTTD) threats

Platform management:

Platform management including system health monitoring, capacity management and troubleshooting

PA XSIAM modules support:

ASM, ITDR, TIM, EDR, SIEM, SOAR, UEBA

Agentic AI workbench:

Leveraging agentic AI workbench for automated triaging and context aware dynamic incident response automation at machine speed

Endpoint protection:

Fully managed EDR including policy management, alert detection and remote isolation capabilities can be rapidly deployed

Threat hunting:

Security analyst-driven investigation and disruption of attacks using NTT DATA's threat-hunting capabilities

Response:

Threat response using agentic AI and Security Orchestration Automation and Response (SOAR) reducing Mean Time to Respond (MTTR)

Threat feeds:

Ingestion of commercial along with NTT DATA's proprietary threat intelligence

Expertise and experience:

NTT DATA's expertise, experience, advanced analytics and external threat intelligence

Service portal:

Single pane of glass, MITRE ATT&CK aligned incident view and key SOC metrics

Digital Forensics and Incident Response (DFIR):

For the provision of incident response support in the event of critical incidents

MXDR service packages

Silver

- 24x7 incident detection
- Platform management
- EDR policy management and remote isolation
- Agentic AI SOC workbench
- Threat hunting
- Threat feeds
- Use case development and tuning
- Out-of-the-box playbook deployment
- Service portal access
- Monthly service reviews
- Security incident reporting
- DFIR
- ASM

Gold

- All Silver capabilities
- Quarterly service reviews
- With customer context
  - Custom playbooks: 5 per year
  - Targeted threat hunting: 10 per year
  - Customized use cases: 10 per year

Platinum

- All Gold and Silver capabilities
- With customer context
  - Custom playbooks: 10 per year
  - Targeted threat hunting: 24 per year
  - Customized use cases: 20 per year

The top 4 capabilities of smarter, faster, lean and future ready SOC

Resilience: End-to-end integrated and automated services that secure digital transactions, protect information and data, and safeguard against downtime to ensure workforce productivity.

Improved speed and efficiency through Agentic AI workbench, orchestration, automation, and AI-driven threat intelligence and digital forensics.

Less complexity as it provides a unified view of security across your organization.

AI-driven intelligence from the MXDR platform and through our 24x7 security operations centers, improves the detection of hard-to-find and advanced threats.

Why NTT DATA

We bring global expertise, industry-leading frameworks and a scalable platform to help you move from reactive compliance to proactive resilience.

Proven global security scale

Global delivery across five continents, 2 billion security threats mitigated every year

Embed AI in cyber defense

Embedded agentic AI that improves operational efficiency, investigation quality, and accelerates detection and response

Flexible and predictable service delivery

Flexible service tiers with predictable pricing

Glocal delivery model

Local-language and sovereign SOC support backed by a global delivery model

Unmatched NTT DATA threat intelligence

Global threat telemetry ingestion powered by the world's 4th largest IP backbone for early threat visibility and alerts

Visit nttdata.com to learn more.

NTT DATA is a $30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.