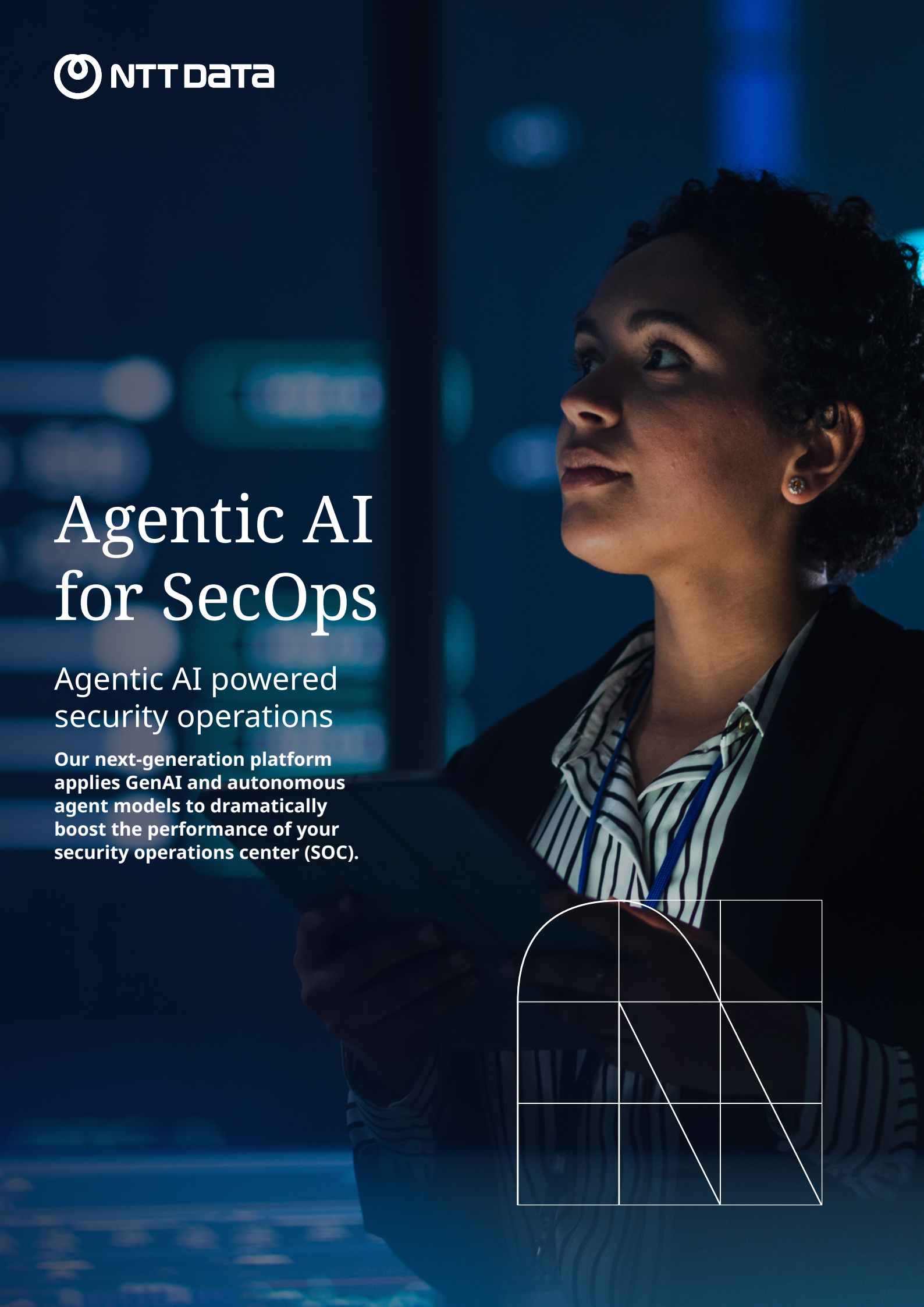

Agentic AI for SecOps

Agentic AI powered security operations

Our next-generation platform applies GenAI and autonomous agent models to dramatically boost the performance of your security operations center (SOC).

Stay ahead of the threat curve

Why AI is now a strategic imperative

With bad actors leveraging AI to automate and scale their attacks, traditional security operations are overwhelmed by alert fatigue, false positives and long response times. And if that's not enough, security teams face growing pressure to do more with less.

The problem isn't just the scale of attacks happening using AI: it's also the speed, context and coordination. Manual triage takes too long, and investigations often lack full visibility. Talent shortages also make it harder to build deep expertise at every level of the SOC.

The answer?

Fight fire with fire — or rather, AI with AI. Specifically, agentic AI. A new generation of intelligent, autonomous agents purpose-built to augment and accelerate your security perations.

Introducing Agentic AI for SecOps

NTT DATA's Agentic AI for SecOps is a next-generation platform that applies GenAI and autonomous agent models to dramatically boost the performance of your security operations center (SOC).

These AI agents work across your entire SecOps stack, covering alert triage, threat hunting, endpoint protection, vulnerability management and much more. In short, it helps you automate, accelerate and improve how security gets done.

From L1 automation to advanced threat hunting, agentic AI learns from your environment and continuously evolves to enhance detection accuracy, speed up response times and take some of the pressure off human analysts.

An autonomous assistant for your entire security operations stack

Agentic AI works as an intelligent automation layer across all tiers of SecOps. It integrates with security information and event management (SIEM), security orchestration, automation and response (SOAR), case management tools and telemetry data to deliver real-time context, decision support and, where appropriate, automated action.

It can help you with:

- **L1 alert triage optimization:** The rapid ingestion and correlation of alerts, historical comparisons and smart filtering help to reduce false positives and streamline escalation.
- **Autonomous investigations:** Agentic AI can automatically query your threat intelligence, endpoint and network tools to build comprehensive investigation reports for your L2 teams to review.
- **Threat-hunting acceleration:** It can ingest tactics, techniques and procedures (TTPs) from threat-intelligence feeds and run automated detection queries for proactive threat discovery.
- **AI-augmented analyst support:** Enhance the SOC analyst experience with generative AI prompts, summaries and reporting accelerators — a considerable benefit when you consider the pressures the modern-day analyst deals with.

Delivering better outcomes

Based on the work we've done with some of our clients, we've found that embedding agentic AI into your SOC environment could produce the following benefits:

25% to 40% reduction in false positives	28% to 56% increase in true positive identification	Faster mean time to detect (MTTD) and respond (MTTR)	Improved analyst productivity and experience	Shift-left security skill enablement for L1 teams

When you break it down, the true benefits of agentic AI are that you can do more, do it faster and, most importantly, do it better.

Use cases: Real results in action

Email security automation

Using agentic AI, you can correlate phishing alerts with user behavior and threat intelligence, investigate autonomously, and isolate accounts or block malicious sources. And you can do all this without human intervention.

Endpoint detection and response (EDR)

Agentic AI automatically investigates anomalies flagged by EDR tools, integrates with your other security data sources and enables you to apply remediations like device isolation and patching.

Automated threat intelligence management

You're able to continuously ingest threat-intelligence feeds, correlate them with alerts and prescribe proactive actions such as endpoint quarantining or vulnerability patching.

Get started

1. **Explore use cases:** Identify where AI can have the greatest immediate impact in your organization.
2. **Build the business case:** Pilot Agentic AI for SecOps in a controlled environment and validate recovery speed, threat visibility and compliance outcomes.
3. **Phased implementation:** Use our benchmarks to quantify potential productivity and risk-reduction benefits.
4. **Scale with confidence:** Following your initial success, look to expand across domains using our agentic AI platform and managed services to scale your AI-powered SecOps.

Why NTT DATA

With a proven track record in large-scale cybersecurity deployments and deep partnerships with leading platforms like Microsoft Security Copilot, NTT DATA can help you go beyond implementation to embed AI into your security fabric, with resilience and trust at the core.

Flexible agentic AI framework

Our framework works with your existing tools and workflows via API integration.

Accelerated outcomes

Our pretrained AI agents deliver out-of-the-box automation and speed up time to value.

Innovation with guardrails

Built-in governance ensures safe, auditable AI adoption.

> "Let's elevate the capabilities of every analyst on your team, together."

Visit nttdata.com to learn more.

NTT DATA is a trusted global innovator of business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.


NTT DATA