Prepare your business for frontier AI risks

Frontier AI Readiness Assessment

Identify your most critical frontier AI cyber risks, validate exploitable attack paths and prioritize remediation based on business impact with our structured assessment.

Frontier AI is changing cyber risk at unprecedented speed and scale

Vulnerabilities are discovered and exploited faster than ever, while AI-powered adversaries can automate increasingly complex attack workflows with minimal human involvement.

- **From weeks and days to hours and minutes**
  The window between vulnerability discovery and exploitation continues to shrink.
- **80% to 90% autonomous execution**
  Cyberattacks now require significantly less human effort.
- **Capability doubles every few months**
  Frontier AI models can autonomously complete increasingly complex cyber tasks

Why traditional security falls short

If your security processes were designed for a human-paced threat landscape, the gap between identifying risk and reducing it will continue to widen.

- Vulnerability backlogs are prioritized by severity instead of exploitability
- There is limited visibility of the attack paths that matter most
- Ownership across cloud, identity, infrastructure and security teams is fragmented
- Detection and response capabilities are not validated against AI-enabled attacks
- Governance frameworks are unable to address evolving threats
- Remediation cycles cannot match today's attack timelines

What you need to know

- Which attack paths pose the greatest business risk
- How they could be exploited
- How quickly they can be closed
- How you can transform your cybersecurity for AI-era resilience

A clear view of frontier AI readiness and a path to action

Our Frontier AI Readiness Assessment is a structured 90-day advisory engagement that helps you identify your most critical exposures to frontier AI-enabled cyberthreats, validate the attack paths most likely to succeed, prioritize remediation based on business impact and develop a cybersecurity transformation roadmap to build AI-era resilience.

The engagement progresses through three stages, taking you from assessing your current readiness to validating critical exposures and developing a practical roadmap to strengthen cyber resilience.

NTT DATA's 90-day Frontier AI Readiness Assessment

Engagement principle: validate the critical few, scale across the rest, and convert findings into decisions the business can fund and teams can execute.

Days 1-15

Assess readiness baseline

- Business context and crown jewels
- Exposed assets and dependencies
- Current tooling and operating model
- AI-amplified threat scenarios

Output: baseline view of where the enterprise is most exposed.

Days 16-60

Validation and prioritization

- Attack path validation
- Exploitability-led prioritization
- NTT DATA-orchestrated partner depth for critical assets
- NTT DATA-led scalable estate review

Output: validated critical paths and prioritized exposure backlog.

Days 61-90

Transformation roadmap

- Readiness scorecard
- Remediation backlog and owners
- Detection and governance gaps
- 3-12-month transformation plan

Output: Sequenced roadmap for resilience improvement.

Advisory-led and outcomes-focused

We take an advisory-led approach to the engagement, working closely with your teams as we progress through the various stages of the assessment. These include:

- Executive and stakeholder workshops for business alignment
- Security and architecture reviews
- Attack path analysis and validation
- Readiness scoring and evidence review
- Transformation roadmap development sessions
- Executive reporting and recommendations

Practical outputs for prioritizing action

The assessment serves as a strategic decision-support tool for security and business leaders, delivering practical outputs to help you prioritize action and make informed decisions.

Assessment output	Business value
Frontier AI readiness scorecard	Evidence-based readiness score with confidence ratings
Critical asset mapping	Visibility of business-critical assets and dependencies
Attack path validation	Attack paths prioritized by reachability, exploitability and business impact
Prioritized remediation backlog	Clear actions, ownership, timelines, expected risk reduction and validation criteria
Detection and governance review	Identification of operational and governance gaps
Transformation roadmap	Actionable 3-to -12-month cybersecurity transformation plan
Risk mitigation strategy	Risk mitigation aligned with your business priorities
Stakeholder reporting	Materials to support executive, board and audit discussions

Why NTT DATA

NTT DATA combines expertise across cybersecurity, cloud, risk and AI with a pragmatic, model-independent approach to help your strengthen cyber resilience while supporting business growth and innovation.

- **7,500+** cybersecurity professionals worldwide
- Global delivery across **70+** delivery centers in **50+** countries
- **20+** next-generation Cyber Defense Centers providing global SOC operations
- End-to-end cybersecurity services, from assessment through implementation
- Launch partner in Project Glasswing, advancing industry collaboration on frontier AI security

Take a proactive approach to Frontier AI risks

Our structured assessment helps you make informed security decisions and accelerate remediation.

Schedule a Frontier AI Readiness Assessment with NTT DATA to establish a prioritized roadmap for AI-era cyber resilience.

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.

NTT DATA

