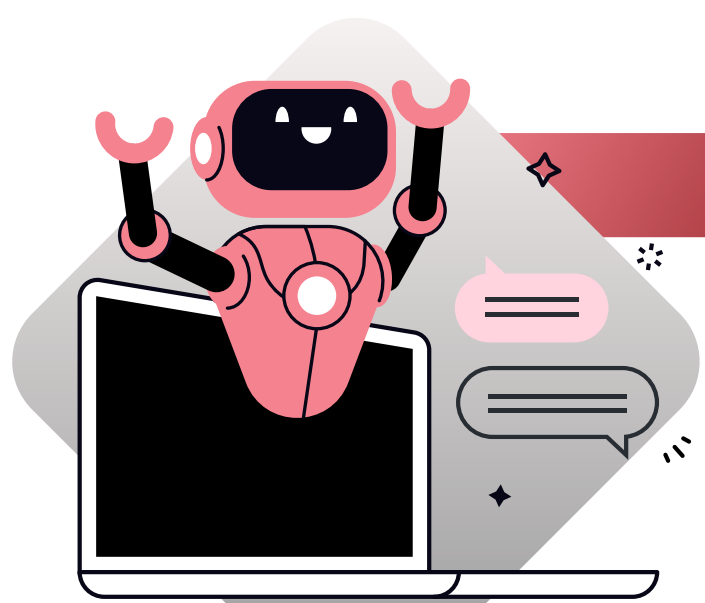


Cybersecurity forces reshaping enterprise risk in 2026

AI, regulation, and emerging threats are redefining how enterprises secure complex environments today.



Trend 1

Agentic AI expansion

Employee driven AI use is creating unmanaged attack surfaces across enterprise systems.

Insight:
IT teams must govern sanctioned and unsanctioned AI agents to reduce exposure



Trend 2

Regulatory volatility rising

Global mandates now hold boards and executives liable for cyber compliance failures.

Insight:
Strengthen cross-functional governance to prevent penalties and resilience-impacting compliance gaps.



Trend 3

Accelerating threat landscape

AI, geopolitical tensions, and rapid threat evolution are redefining enterprise risk profiles.

Insight:
Enterprises need a consolidated security platform providing an adaptative, resilient architecture that keeps pace with attacker innovation.



Trend 4

Governance under pressure

Security leaders face persistent operational strain amid structural shifts in business models.

Insight:
Modernise governance frameworks to support scalable, future-ready security programs.



Trend 5

AI-driven development risks

No code, low code, and “vibe coding” accelerate insecure AI generated code proliferation.

Insight:
Implement guardrails and secure-coding oversight for AI-augmented development workflows.

Partner with Nexon to assess, modernise and safeguard your organisation’s cyber resilience.

Get protected. Stay protected.
Don’t get caught out.

