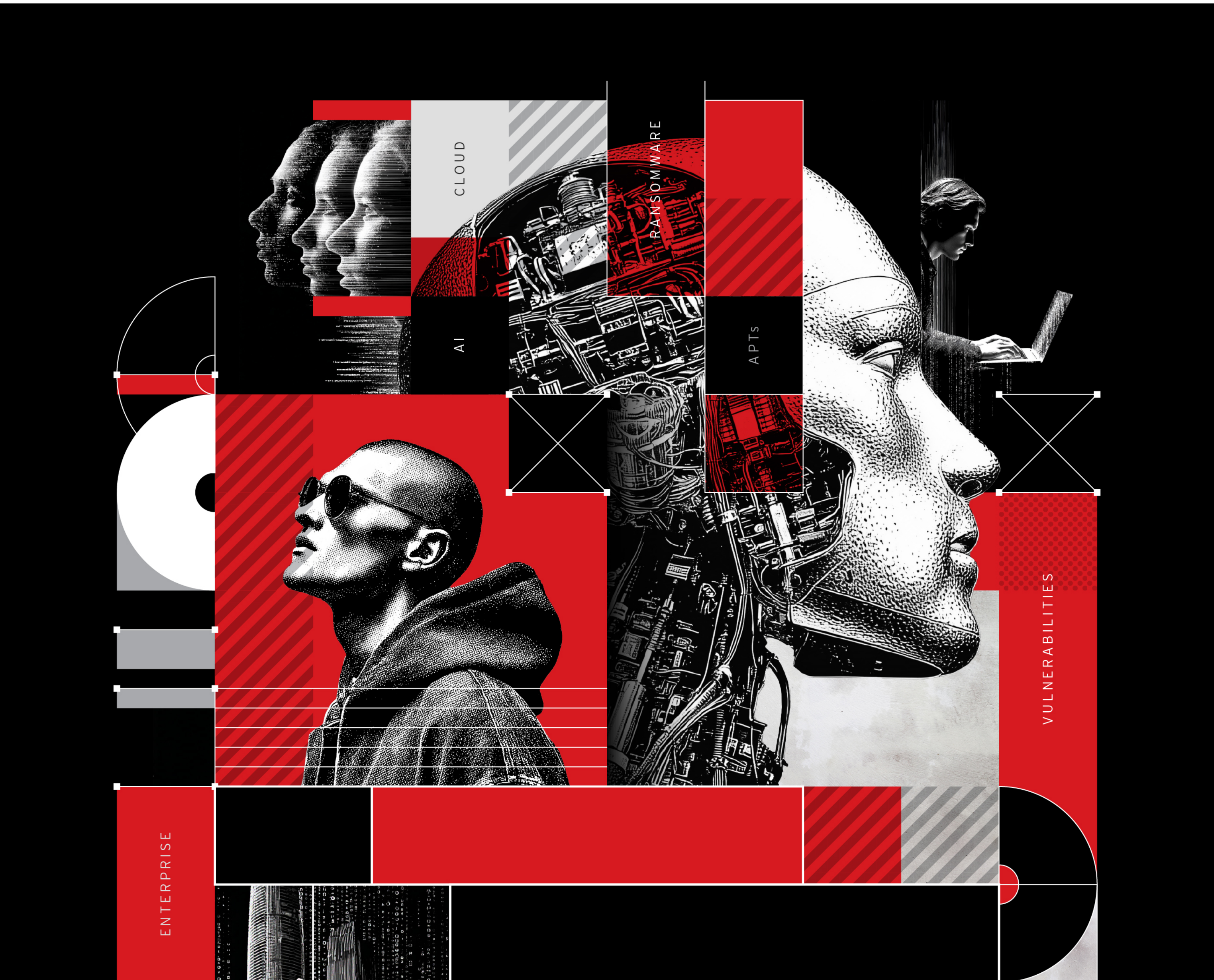
Key Takeaways for
Business Leaders

Trend Micro Security Predictions for 2026

What the AI-fication of Cyberthreats Means for Business Leaders

AI is now embedded in daily operations, and attackers are using it just as effectively. In 2026, threats will move faster, require less human involvement, and take advantage of the complexity in cloud environments, identity systems, and third-party tools. The priority for leaders is clear: Reduce exposure, strengthen controls, and build resilience that can withstand disruption.



Key Takeaways for Business Leaders

AI Will Become a New Point of Compromise

AI agents are speeding up workflows, but they can also make decisions inside core systems without human oversight. If they are manipulated, attackers can move data, change access, or approve actions silently. AI-generated code will also continue creating weaknesses before teams notice them.

FOCUS AREAS

Govern AI agents

- Treat agents as employees with permissions.
- Monitor their activity.
- Require checks before they carry out sensitive actions.

Cloud Vulnerabilities Will Cause the Most Serious Incidents

Multi-cloud and hybrid setups will remain difficult to govern. Misconfigurations, exposed APIs, and weak permissions will continue to open the door to attackers. Once inside, they can move easily across cloud services, containers, identity systems, and the tools connected to them.

FOCUS AREAS

Improve cloud visibility

- Track assets, roles, and settings in real time.
- Remove excessive permissions and check SaaS connectors.
- Treat every external integration as a potential entry point.

Ransomware Will Become Largely Automated

Ransomware groups will further use automation to find weaknesses, infiltrate systems, and tailor extortion. Attacks will become more personal and more targeted, supported by stolen data and manipulated content.

FOCUS AREAS

Strengthen recovery

- Maintain offline, tamper-proof backups.
- Test restoration frequently and incorporate it into business continuity testing.
- Close fast-movement pathways across cloud and identity systems.

Vulnerabilities Will Outpace Traditional Patching

AI will accelerate the discovery of flaws in software, cloud services, and AI-enabled tools. AI-generated code will also introduce new weaknesses. Unpatched IoT and OT systems will remain an easy entry point.

FOCUS AREAS

Prioritize by exposure

- Fix issues that present the greatest business risk.
- Focus on gaps in identity, cloud access, and external-facing services.
- Test regularly under realistic attack conditions.

Cyberattacks in 2026 will be defined by speed and automation. Organizations that improve visibility, tighten cloud and identity controls, and build strong recovery capabilities will be the ones that stay resilient.

Download the full report, "The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026."