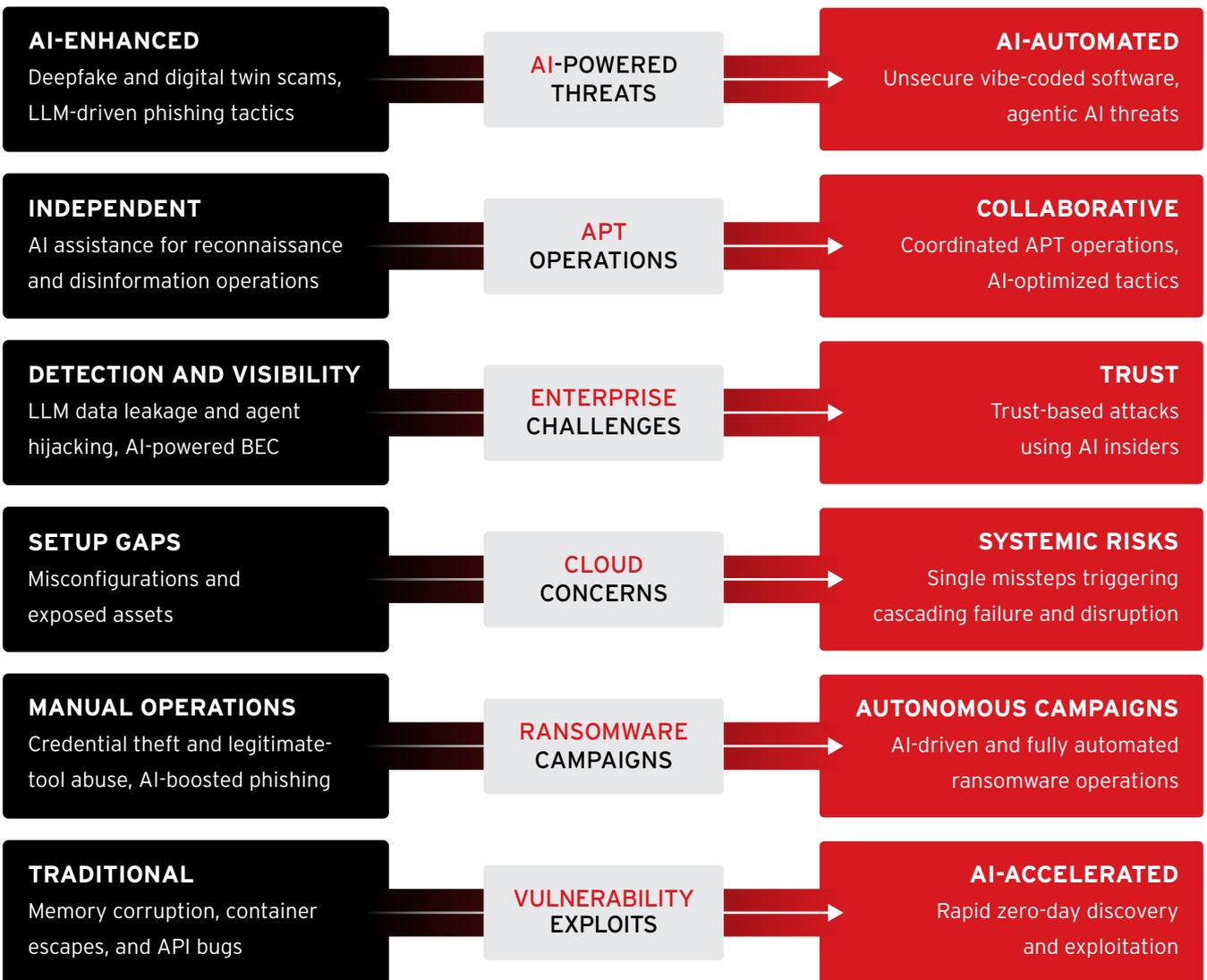TREND MICRO™

THE AI-FICATION OF CYBERTHREATS

In 2026, AI, automation, interconnected systems, and large-scale operations will fuel innovation, but they will also determine the trajectory of emerging threats. Our predictions report highlights the trends that will shape the next year and surface new security priorities.
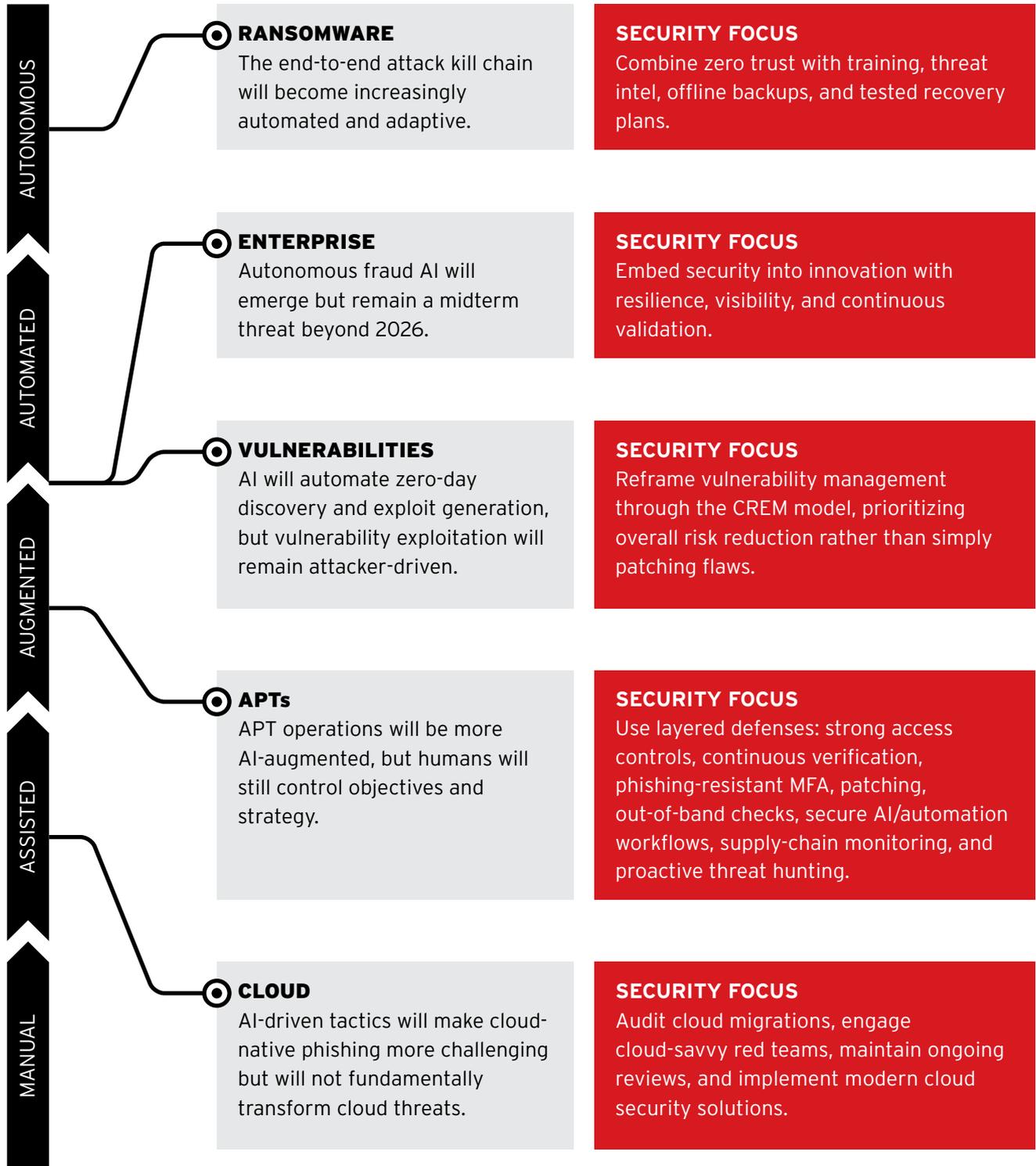
The Biggest Shifts

2025   **2026**

2025	AI-POWERED THREATS	2026
AI-ENHANCED Deepfake and digital twin scams, LLM-driven phishing tactics	AI-POWERED THREATS	**AI-AUTOMATED** Unsecure vibe-coded software, agentic AI threats
INDEPENDENT AI assistance for reconnaissance and disinformation operations	APT OPERATIONS	**COLLABORATIVE** Coordinated APT operations, AI-optimized tactics
DETECTION AND VISIBILITY LLM data leakage and agent hijacking, AI-powered BEC	ENTERPRISE CHALLENGES	**TRUST** Trust-based attacks using AI insiders
SETUP GAPS Misconfigurations and exposed assets	CLOUD CONCERNS	**SYSTEMIC RISKS** Single missteps triggering cascading failure and disruption
MANUAL OPERATIONS Credential theft and legitimate-tool abuse, AI-boosted phishing	RANSOMWARE CAMPAIGNS	**AUTONOMOUS CAMPAIGNS** AI-driven and fully automated ransomware operations
TRADITIONAL Memory corruption, container escapes, and API bugs	VULNERABILITY EXPLOITS	**AI-ACCELERATED** Rapid zero-day discovery and exploitation

The AI-Driven Evolution of Modern Threats

AUTONOMOUS

RANSOMWARE
The end-to-end attack kill chain will become increasingly automated and adaptive.

SECURITY FOCUS
Combine zero trust with training, threat intel, offline backups, and tested recovery plans.

AUTOMATED

ENTERPRISE
Autonomous fraud AI will emerge but remain a midterm threat beyond 2026.

SECURITY FOCUS
Embed security into innovation with resilience, visibility, and continuous validation.

VULNERABILITIES
AI will automate zero-day discovery and exploit generation, but vulnerability exploitation will remain attacker-driven.

SECURITY FOCUS
Reframe vulnerability management through the CREM model, prioritizing overall risk reduction rather than simply patching flaws.

AUGMENTED

APTs
APT operations will be more AI-augmented, but humans will still control objectives and strategy.

SECURITY FOCUS
Use layered defenses: strong access controls, continuous verification, phishing-resistant MFA, patching, out-of-band checks, secure AI/automation workflows, supply-chain monitoring, and proactive threat hunting.

ASSISTED

CLOUD
AI-driven tactics will make cloud-native phishing more challenging but will not fundamentally transform cloud threats.

SECURITY FOCUS
Audit cloud migrations, engage cloud-savvy red teams, maintain ongoing reviews, and implement modern cloud security solutions.

MANUAL

High-Impact Threats in 2026

PREDICTION	RISK	LIKELIHOOD	SCOPE
Deepfake and other synthetic media exploitation	Critical	High	Wide
Collaborative APT operations	Critical	High	Wide
AI-driven identity and session hijacking	Critical	High	Wide
Insider infiltration through AI-generated identities	Critical	High	Wide
Automated ransomware operations	Critical	High	Wide
AI-accelerated zero-day exploitation	Critical	High	Wide
Cloud misconfigurations and GPU exploits	Major	High	Narrow
Supply chain–delivered ransomware	Major	High	Narrow
AI supply chain attacks (MCP and model compromise)	Significant	Medium	Narrow
Autonomous AI agents as attack vectors	Moderate	Low	Narrow

The Bottom Line: Why These Predictions Matter

As AI becomes embedded in both enterprise operations and cybercriminal tactics, how can organizations fully harness its potential while avoiding its risks?

THREAT	C-LEVEL SOLUTIONS	BUSINESS BENEFIT
AI attacks	AI-powered email security	Protect brand and trust
APTs	Zero trust and threat intelligence	Safeguard assets and IP
Enterprise risks	Vulnerability management and SOAR	Minimize downtime
Cloud attacks	Cloud security and data loss prevention	Secure cloud transformation
Ransomware	Advanced detection and response, backup, and recovery	Ensure business continuity
Vulnerabilities	Patch automation and app security	Reduce risk exposure

Learn how to stay ahead and strike the right balance between innovation and security.
Download the full Trend Micro Security Predictions for 2026 report.