REPORT

Cyberthreat Predictions for 2026

Industrialized Cybercrime and the Acceleration of the Attack Life Cycle

FORTINET

Table of Contents

Introduction

The *2026 Cyberthreat Predictions Report* continues Fortinet's ongoing analysis of how technology, economics, and behavior intersect to shape global cyber risk. The picture emerging for 2026 is one of acceleration. Adversaries will increasingly operate as industrial systems, using automation, specialization, and AI to scale both attack speed and reach.

For CISOs and security leaders, this means re-architecting defenses to operate at the same speed as adversaries. Security programs designed for linear response can no longer keep pace with an ecosystem characterized by parallel automation and rapid exploitation.

The coming year will not be defined by a single new technique or malware strain, but by the refinement and industrialization of those that already exist. We expect threat actors to focus less on innovation and more on throughput—the ability to move from reconnaissance to monetization in the shortest possible time. This shift is reshaping the economics of cybercrime and forcing defenders to compress detection and containment cycles across every environment.

In practice, this means:

- A ransomware affiliate launching 10 attacks in the time it once took to coordinate one.
- An AI model parsing terabytes of stolen data in minutes to identify which targets to extort first.
- A security operations team racing to isolate an infected endpoint before automated lateral movement begins.

Together, these scenarios illustrate a single reality: Velocity now defines risk. As the line between human and machine operations blurs, both attackers and defenders are adapting to an environment where milliseconds can define outcomes.

FortiGuard Labs' 2026 predictions explore this evolution from multiple perspectives—how adversaries are industrializing, how defenders are adapting, and how collaboration across public and private sectors will shape deterrence and resilience in the years ahead.

The unifying theme across these predictions is *convergence*. Offense and defense now evolve through the same forces—AI, automation, and the cloud—each shaping the other's rate of adaptation. The contest ahead will be decided less by who has the most advanced tools than by who can integrate intelligence, technology, and decision-making into a single, continuous system.

Executive Summary

The global threat environment in 2026 will be defined by speed, automation, and scale. Cybercrime will continue to mature into a structured industry supported by specialized roles, automated toolchains, and AI-driven decision-making. Attack groups will increasingly operate more like enterprises than independent actors, measuring success not by innovation but by throughput, such as the rate at which they can turn access into profit.

For defenders, this represents a pivotal shift. Security operations can no longer rely on static configurations or periodic assessments. To address today's rapidly evolving challenges, they must operate as an adaptive system, continuously learning, adjusting, and responding to real-time conditions.

Two forces are driving this evolution. The first is the industrialization of cybercrime, as automation and AI integrate into every stage of attack development and deployment. The second is the acceleration of the attack life cycle, in which the time between compromise and consequence continues to collapse. Attackers who once needed days to monetize access can now do so in hours by automating reconnaissance, data analysis, and extortion.

These changes are already visible. A compromised cloud workload may trigger an AI-driven privilege escalation script within seconds. A stolen database can be quickly parsed by generative AI (GenAI) to identify high-value records before the victim even realizes the breach has occurred. Pre-infected botnets and access brokers now provide turnkey infrastructure for ransomware affiliates, enabling near real-time campaign launches.

For defenders, the implication is clear. Threat intelligence, exposure management, and incident response must operate as one continuous system. Readiness will increasingly be measured by the ability to act at AI-level speeds to translate threat intelligence into containment before disruption occurs.

This report examines both sides of that equation. The Adversaries section explores how attackers are industrializing their operations, while the Defenders section focuses on how organizations can operationalize threat intelligence and automation to match that velocity. Together, they point to a single conclusion: The contest between offense and defense has become a race of systems, not individuals.

Update on Our Predictions for 2025

Many of the developments forecast in FortiGuard Labs' *2025 Cyberthreat Predictions Report* have materialized faster than expected. What were emerging patterns a year ago—AI-assisted threat operations, Crime-as-a-Service (CaaS) specialization, and geopolitical fragmentation—are now defining characteristics of the global threat landscape.

AI in operational use

The 2025 report predicted that AI would move from experimentation to full operational deployment. That shift has already occurred. GenAI is routinely used for social engineering, credential harvesting, and automated scripting. The next phase, now emerging, involves autonomous agents capable of managing multiple attack functions without human input.

Expansion of CaaS models

Integrated underground economies have matured into platform-style marketplaces. Access brokers, data resellers, and malware developers now operate as interconnected suppliers, allowing smaller actors to launch sophisticated attacks with minimal resources.

Target diversification

Predictions of expanded targeting across operational technology (OT), cloud, and supply chains have proven accurate. Ransomware groups increasingly blend data theft, disruption, and extortion, often striking multiple tiers of vendors simultaneously. Critical infrastructure and healthcare remain disproportionately affected, particularly in areas where modernization has outpaced security.

Data as a primary asset

Data theft has transitioned from a byproduct of intrusion to a monetized commodity. AI-driven analysis now converts raw data into actionable intelligence, turning information into a currency of extortion and influence.

Together, these developments confirm a broader shift from opportunistic attacks to structured operations. Industrialized cybercrime, once a projection, has become the baseline from which new threats emerge.

The Next Phase of Attack: 2026 Offensive Capabilities Predictions

As 2026 unfolds, cybercrime continues to industrialize. Automation, AI, and specialization will continue to converge, enabling attacks to be produced at scale. FortiGuard Labs anticipates several developments across offensive capabilities.

AI-enabled cybercrime agents

The defining change of 2026 will be the emergence of purpose-built, autonomous cybercrime agents. These systems will extend far beyond the early FraudGPT, WormGPT, and similar models seen on underground forums in 2025. Designed for specific operational tasks such as credential theft, phishing, or lateral movement, these agents will execute against entire segments of the attack chain without requiring human oversight.

This shift will drive an explosion in capacity. Entry-level criminals will be able to manage complex campaigns, while experienced actors will scale operations across thousands of targets. Automation will continue to lower costs while amplifying both reach and frequency.

The AI arms race

AI is accelerating the tempo of cyber conflict. Offensive models are already identifying and exploiting weaknesses in defensive systems faster than human analysts can respond. The result is a continuous feedback loop of adaptation between attack and defense. Detection, containment, and mitigation must increasingly be automated, as a human-led response alone cannot match the speed of machines.

GenAI will accelerate data monetization and extortion: GenAI will become more central to post-compromise operations. Once attackers gain access to large datasets (through infiltration or by purchasing access on the dark web), AI tools will analyze and correlate massive volumes of data in minutes, pinpointing the most valuable assets for extortion or resale.

These capabilities will enable adversaries to identify critical data, prioritize victims, and generate tailored extortion messages at scale. By automating these steps, attackers can quickly transform stolen data into actionable intelligence, increasing efficiency and profitability.

For defenders, this trend underscores the importance of integrating SecOps capabilities, such as NDR, EDR, and CTEM, to detect unusual data movement and flag early signs of AI-assisted extortion before damage escalates.

Critical infrastructure in the crosshair: Attackers are expected to increasingly focus on high-impact sectors, such as manufacturing, healthcare, and utilities. The Ransomware-as-a-Service (RaaS) model is already expanding into OT environments, where data theft, extortion, and service disruption now converge in a single playbook, and this trend will continue.

Destructive payload development: Techniques once limited to military or nation-state use, such as firmware corruption and device bricking, will increasingly be repurposed by criminal syndicates for financial leverage. Industrial IoT environments are especially vulnerable as Sat-to-Cell infrastructure expands, providing new vectors for remote disruption.

Shifts in the cybercriminal ecosystem

The fourth generation of cybercrime: Cybercrime is entering its fourth industrial phase, blending automation, integration, and specialization. Credential dumps will continue to evolve into curated "intelligent combo lists" enriched with metadata and behavioral analytics. Dark web marketplaces already operate like legitimate e-commerce platforms, complete with customer service, reputation systems, and escrow services powered by AI, and these systems will become more refined.

The human supply chain: By compromising trust within the organization, attackers gain persistence that technology alone cannot easily detect. As a result, insider recruitment will intensify, and ransomware operators will increasingly target employees through coercion, blackmail, or financial incentive.

Converged crime: Fraud, trafficking, and money laundering networks now overlap, creating resilient, hybrid enterprises that diversify risk and profit streams while complicating enforcement efforts. To capitalize on this, traditional organized crime and cybercrime will continue to merge.

Botnets as the hidden infrastructure of industrialized cybercrime: Botnets will remain the backbone of cybercrime. Pre-infected endpoints and IoT devices traded as ready-made access kits accelerate the rapid deployment of ransomware or data exfiltration. As this underground economy expands, it will enable attackers to integrate services—such as credential theft, botnet rental, and data extortion—into scalable business models.

Integrated SecOps capabilities, including NDR, EDR, and CTEM, will be crucial in providing continuous visibility into lateral movement, command-and-control activity, and exposure posture, enabling defenders to disrupt attacks before they escalate.

The expanding cybercrime economy: According to the World Economic Forum, the average annual cost of cybercrime is expected to increase to more than $23 trillion by 2027.[1] Industrialized ransomware, automated fraud networks, and converged crime models will drive this growth. Over time, however, sustained international cooperation and targeted disruption campaigns may begin to constrain this expansion.

Offensive Capabilities Overview

Adversaries in 2026 will operate as integrated industries, scaling attacks through automation, shared infrastructure, and AI-augmented decision-making. The key shift is not in how they will attack but in how efficiently they execute. Success will now be determined by operational throughput: the speed at which intelligence can be monetized.

The most capable threat groups will function as semi-autonomous enterprises, supported by AI agents, access brokers, and botnet operators who provide services on demand. Their advantage lies in their ability to continue to industrialize every stage of the attack chain, from reconnaissance and intrusion to extortion and laundering.

In this environment, the distinction between advanced persistent threat and organized cybercrime will continue to blur. The same automation pipelines, machine learning models, and infrastructure can serve espionage or financial objectives interchangeably. Attackers will continue to refine their efficiency by reusing proven playbooks and layering AI-driven adaptations on top.

For defenders, understanding these industrial dynamics is essential. The adversary's edge will increasingly be measured in velocity and scale, not ingenuity. Countering that advantage will require visibility into how these ecosystems operate and disruption of the automation supply chains that sustain them.

Defending at Machine Speed: 2026 Defensive Capabilities Predictions

Adversaries now operate as industries. Standardized playbooks, automation pipelines, and AI augmentation will continue to define their advantage. As a result, the defining variable for cyber defenders in 2026 will not be sophistication, but throughput.

Because attackers will continue to exploit the same AI and cloud platforms that defenders rely on, capabilities diffuse quickly. Productivity, not innovation, will determine impact. The key risk metric for defenders will be velocity. Adversaries will continue to accelerate their ability to quickly move from reconnaissance to ransom. Defensive strategies must be calibrated to interrupt that cycle before it completes.

Adopting a threat-informed defense strategy

As adversaries automate, defenders must do the same. Resilience will depend on a threat-informed defense model that connects intelligence, exposure management, and incident response within a unified operational framework.

Operationalizing SecOps to machine speeds: Defending at the velocity of today's threats requires more than automation. It requires context. Threat-informed defense must leverage real-world intelligence to anticipate attacker behavior and guide decisions across every stage of operations.

FortiGuard Labs intelligence enables defenders to map active threats using frameworks such as MITRE ATT&CK and CTEM. Through continuous validation and simulation, defenders will need to measure how their controls perform against observed tactics and techniques.

At the same time, incident response must evolve from a standalone function to a coordinated capability. Unified visibility across endpoints, networks, and clouds, combined with external attack surface intelligence, will enable faster containment and more comprehensive situational awareness.

Identity Will Become the Core of Security Operations in 2026: In 2026, identity will shift from a supporting control to the operational backbone of security. As organizations adopt more automation, AI-driven workflows, and autonomous decision-making systems, security teams will need to manage not only human identities but a rapidly expanding range of non-human identities across their environments.

These include automation agents, ephemeral identities created during CI/CD or cloud deployments, AI-powered processes executing SecOps tasks, and machine-to-machine workflows that require authentication, authorization, and auditing—just like human users.

Two critical realities will shape this evolution:

1. **Every automated action will require its own identity.** Agents, scripts, and AI processes will need unique credentials, policies, and behavioral baselines to ensure accountability and prevent cross-contamination between systems.
2. **Identity will become a primary attack surface.** The compromise of a single automated identity could enable large-scale lateral movement, privilege escalation, or data exposure in seconds.

To counter these risks, security operations must integrate identity across every detection and response layer by:

- Applying strict least-privilege and time-bound access controls for both human and non-human identities.
- Monitoring identity behavior across EDR, NDR, SIEM, SOAR, and CNAPP platforms to detect deviations—not only anomalies from endpoints or networks.
- Enforcing strong governance, auditing, and privacy controls as automated identities interact with sensitive or regulated data.

Identity—human and machine—will become the central control point for trust, accountability, and automation in 2026. Organizations that operationalize identity within their security operations will be better prepared for the next wave of industrialized, AI-driven threats.

Next-generation threat Intelligence models: Predictive intelligence will become foundational to effective defense. Frameworks such as MITRE CTID and Attack Flow extend beyond mapping known tactics to modeling adversary intent. By combining global telemetry with AI-driven analytics, defenders can anticipate attacker movement and allocate resources accordingly.

Accelerated operational cycles: Speed is the other critical element of threat-informed defense. CTEM will need to play a more central role in supporting continuous discovery, validation, and remediation to link exposure data directly to operational workflows. Integrated SecOps capabilities must enable detection and containment to occur in minutes, transforming readiness from a reactive to an anticipatory process.

Industry disruption and collaboration

Incentivizing the disruption of cybercrime: Innovation in defense should not be limited to technology. Incentive-based models are expected to emerge further to better align private-sector efforts with public enforcement. Cybercrime bounty programs that reward infrastructure takedowns and intelligence sharing will need to continue to narrow the gap between private and public missions.

Holding threat actors accountable: Attribution and disruption efforts will gain further traction. Operations such as Serengeti 2.0 (an INTERPOL-led anti-crime campaign in Africa supported by partners including Fortinet) will continue to demonstrate how coordinated international action can dismantle criminal infrastructure and enable high-impact arrests.

Such operations have already marked a turning point. Law enforcement and private-sector collaboration are becoming more synchronized, combining intelligence, technical expertise, and legal authority to disrupt cybercrime ecosystems from within. We expect this trend to continue.

Enhancing resilience

Strengthening deterrence and prevention: To effectively combat cybercrime, prevention must begin long before the first compromise. To that end, FortiGuard Labs anticipates the expansion of education and deterrence programs targeting youth and at-risk populations, especially those drawn into online crime ecosystems. The goal is not punitive but preventive, redirecting potential offenders before they enter the cybercrime economy.

Preventive deterrence will also gain traction as part of a broader strategy to erode the recruitment pipelines that sustain organized cybercrime. Many entry-level offenders are motivated by opportunity rather than ideology. Providing legitimate pathways, such as education, training, and early intervention, can transform potential offenders into future defenders.

Fortinet actively participates in such efforts through partnerships with law enforcement, academic institutions, and nonprofit organizations. Such partnerships are expected to continue expanding across the industry. By broadening access to training, contributing intelligence to disruption campaigns, and strengthening local capacity, such private-public collaborations will help reduce both the supply of new cybercriminals and the conditions that enable recruitment.

To be effective, the evolution of deterrence must mirror that of defense itself: proactive, intelligence-driven, and focused on long-term resilience.

Evolving cybersecurity expertise: Education and training are not only central to prevention but also crucial in closing the cybersecurity skills gap that continues to challenge both the public and private sectors. The conversation around the "cybersecurity skills gap" often oversimplifies what is, in reality, a structural evolution. The challenge facing organizations today is not simply a lack of professionals but a shift in specialization. For years, cybersecurity was managed by capable IT generalists. Modern environments will increasingly require a combination of specialized skills that blend cybersecurity expertise, cloud incident response, identity and detection engineering, and AI-assisted operations.

This evolution reflects progress, as more organizations come to understand that operating in today's digital economy requires specialized skills. To that end, universities and training programs will produce more qualified cybersecurity graduates than ever, while private-sector teams must invest in continual learning and certification. The friction arises because the threat landscape—and the assurance bar for effective defense—has been changing faster than many organizations can adapt. New attack surfaces, such as cloud identity, Infrastructure-as-Code, and SaaS governance, demand skills that simply didn't exist in traditional IT security. In this sense, today's "skills gap" is less about scarcity and more about alignment and the need to match specialized expertise to the reality of machine-speed, data-driven operations will become increasingly crucial.

AI will continue to play a decisive role in this transition. As security operations become more integrated and data-centric, AI will increasingly act as the connective tissue between disciplines, connecting events, surfacing anomalies, enriching context, and identifying what humans might otherwise miss. The next generation of cybersecurity professionals will need to operate in partnership with AI-enhanced systems that augment rather than replace human expertise.

Defensive Capabilities Overview

Defenders will now face adversaries organized for scale and speed. The challenge will no longer be simply detecting or blocking individual attacks; —it will be to keep pace with an ecosystem that operates as an industry. **To respond effectively, security programs must apply the same level of operational discipline, automation, and coordination that adversaries use to scale their offense.**

Success in 2026 will depend on how well defenders can translate intelligence into action. Security operations must function as living systems: continuously collecting, validating, and acting on data to reduce exposure and compress response cycles. This evolution will transform cybersecurity from a reactive discipline into a dynamic process of prediction and adaptation.

Threat-informed defense will be central to this shift: By correlating global threat intelligence with internal telemetry, organizations can move from reacting to anticipating. Continuous exposure management through frameworks such as CTEM enables teams to validate their security posture in near real time, while integrated detection and response systems—EDR, NDR, CTEM, and SOAR—allow for rapid containment when threats emerge.

Equally important is the human dimension: AI and automation will not replace defenders but will redefine their roles. Analysts will need to operate as system architects and decision-makers, guiding machine-speed operations through context, intuition, and oversight. The most resilient organizations will be those that learn to balance human judgment with automated precision, ensuring that insight drives every automated action.

Resilience in this new environment will be measured by adaptability: Success will not depend on the size of teams or toolsets but on how effectively organizations synchronize intelligence, technology, and process into a single operational fabric. The goal is not only to withstand industrialized attacks but to evolve security operations into an industrialized defense—one capable of learning, adapting, and responding at the same velocity as the threats it confronts.

The Road Ahead

The story of 2026 will be one of transformation as much as escalation. Cybercrime is entering its industrial age, defined by automation, AI agents, and unprecedented scale. Defenders have access to the same technologies and the same opportunity to industrialize their operations. The organizations that thrive will be those that integrate these capabilities seamlessly into their security strategies and daily operations.

The defining principles of this new era will be velocity and scale—how quickly adversaries can act and how broadly defenders can respond. The next phase of cybersecurity will hinge on how effectively humans and machines operate together as adaptive systems.

FortiGuard Labs concludes that the defining challenge of 2026 and beyond is not whether automation can replace human defense but whether defenders can unite human judgment and near-instant response within a single, resilient framework that can evolve as quickly as the threat itself.

[1] Gullapalli, Vivek. "Why the Asia Pacific Region Is a Target for Cyber-Crime — and What Can Be Done About It?" World Economic Forum, 12 June 2023, www.weforum.org/stories/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/

November 13, 2025 1:39 PM / MKTG-2478-0-0-EN