AI's Double-Edged Role in Cybersecurity: Opportunistic Threats to Industrial-Scale Impacts

Bora Suri Venkata Reddy[1], S. Srinivasan[2]
[1]*Research Scholar, Dept of Computer Science and Engineering, AMET University, Chennai*
[2]*Professor, Dept of Advanced Computing Sciences, AMET University, Chennai*

Abstract: Artificial Intelligence (AI) is now a transformative force in cybersecurity, often described as double-edged sword. It empowers defenders with advanced tools for threat detection and response while simultaneously equipping attackers with sophisticated capabilities to launch more effective and scalable assaults. This duality particularly pronounces with AI accelerating both protective innovations and malicious exploits. The phrase "Fortune Hunter to Industrial Deep Dive" is a progression: AI starts as an opportunistic "fortune hunter" for cybercriminals—enabling quick, targeted gains through tools like personalized phishing or deepfakes—and evolves into a vehicle for deep, systemic attacks on industrial sectors, such as critical infrastructure and manufacturing. Fortune Cyber 60 - 2025 defines an annual ranking of 60 venture-backed startups poised to shape the future of digital defense. Fortune magazine lists spotlight companies addressing the seismic shifts driven by AI, from escalating threats to groundbreaking protections. It underscores a pivotal moment: It redefines the very battlefield.

Keywords: CISO, Fortune Cyber 60, Lightspeed partners, SOAR, UEBA, Deepfakes, ransomware, Mirai Botnet

I. METHODOLOGY

- Data from 500+ startups analyzed by ARR, growth, and market impact.
- Validated by Lightspeed partners, CISO network, and Fortune editorial review.
- Reflects real-time market shifts and investment patterns in cybersecurity innovation.

II. NEED FOR AI-DRIVEN CYBERSECURITY

- Global spending forecast to exceed $520 billion in 2026, doubling since 2021.
- AI-driven security solutions drive rapid growth and new market segments.
- India's cybersecurity market growing at 20%+ CAGR, driven by digital transformation and regulatory mandates.

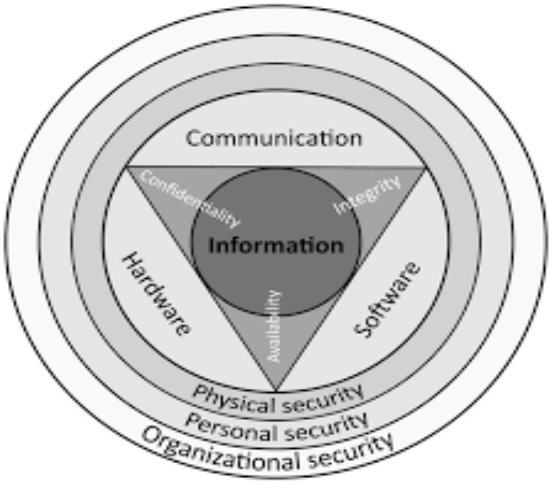


Fig1: Deep-Dive in Cyber-Security

Targeted sectors in Industry:

- The reports include public administration, transport, digital infrastructure and services, finance, and manufacturing, with essential entities representing 53.7% of the total number of recorded incidents
- State-aligned activities against EU Member States continued at a steady tempo, with state-nexus cyberespionage activities notably targeting the public administration sector, and Foreign Information Manipulation and Interference (FIMI) increasingly targeting EU audiences.
- It was mainly driven by low-impact DDoS campaigns targeting EU Member States' organization's websites, with only 2% of incidents leading to service disruption
- The strains Akira and SafePay were among the most deployed, with a few incidents resulting in service disruptions.

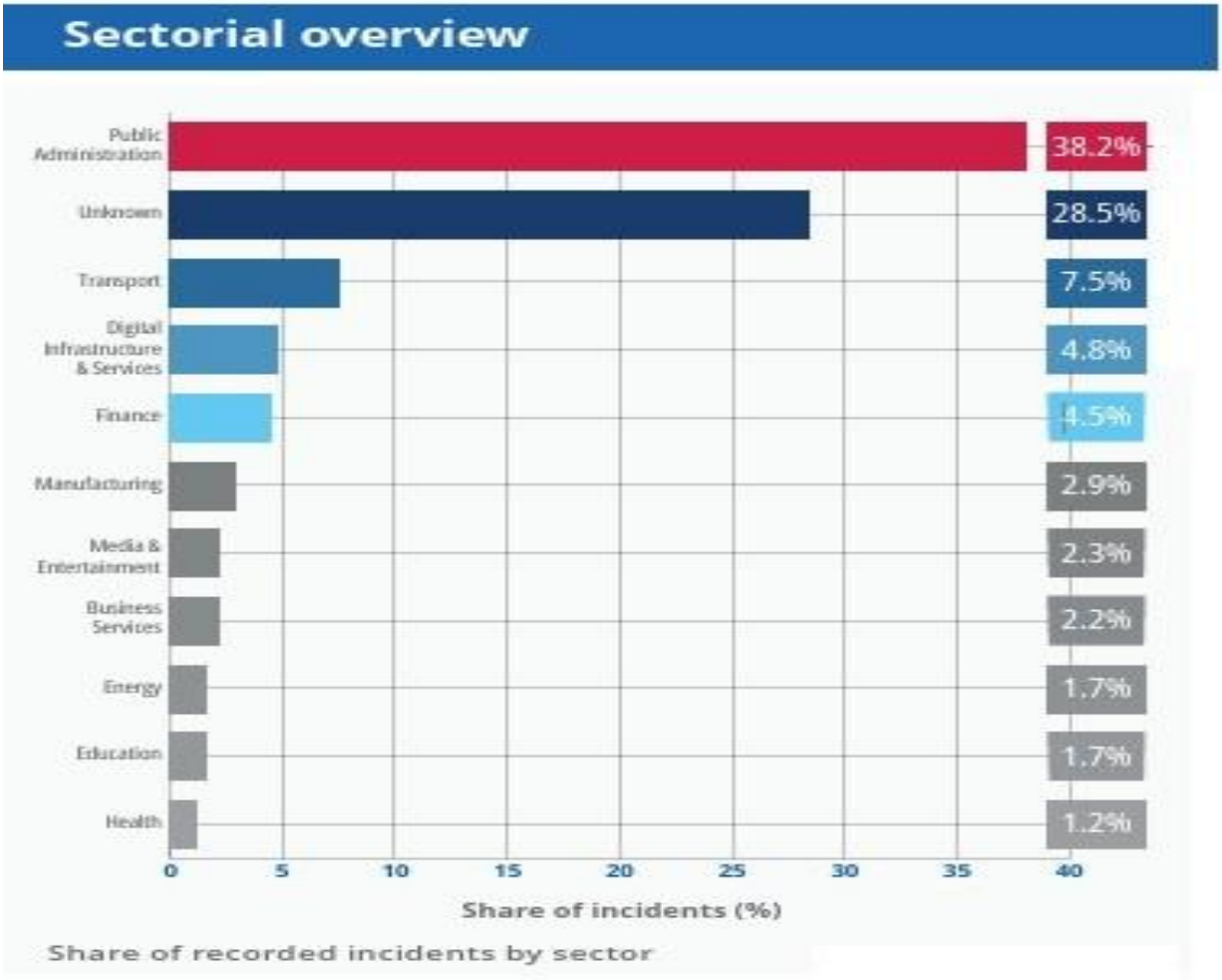


Fig2:Sectoral Overview

Defense Frameworks: Building Resilience Amid Inequity

GCO 2025 advocates a "security-first" mindset, urging strategic investments in AI governance, supply chain mapping, and collaborative ecosystems (e.g., via CERTs and ISACs). Key recommendations include modernizing legacy systems, upskilling for AI defense, and aligning with frameworks like NIST Cybersecurity Framework or EU's NIS2. However, disparities persist: Only 15% of organizations in Europe/North America lack confidence in national preparedness, versus 42% in Latin America. Smaller firms (SMBs) face acute challenges, with 35% reporting insufficient resilience—seven times higher than in 2022.

The following bar chart visualizes the prevalence of major threat vectors reported in the GCO 2025 survey (percentages represent organizations identifying each as a "high-impact" risk in 2025):

This chart underscores ransomware and supply chain risks as the leading barriers to resilience (54% of large organizations), exacerbated by AI tools enabling faster attack scaling.

The education sector remained the most targeted industry worldwide, facing an average of 4,656 attacks per organization per week—a 7% year-over-year increase. Next in line were government entities, which experienced 2,716 weekly attacks (+2% YoY), closely followed by associations and non-profit organizations with 2,550 attacks per week, marking a striking 57% YoY surge. This sharp rise against associations and non-profits underscores how threat actors

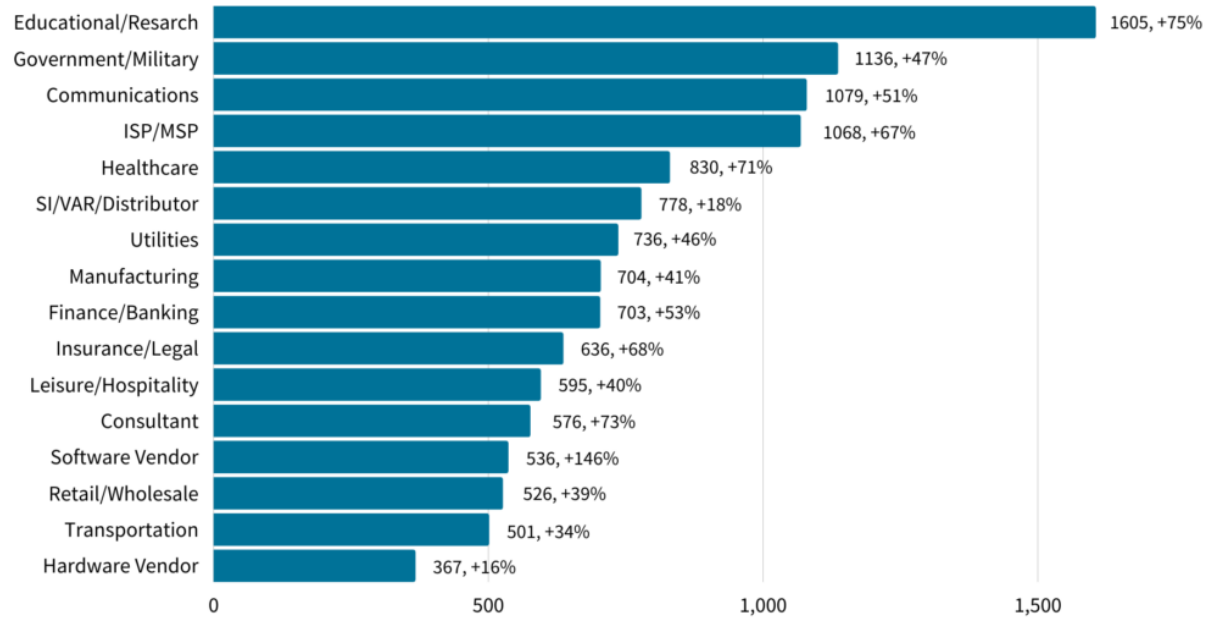


Fig3: Global Average Weekly Cyber Attacks

Most Targeted Industries

From an industry perspective, industrial manufacturing emerged as the hardest-hit sector, representing 12% of all reported victims, as attackers continue exploiting operational dependencies and legacy systems. The Business Services sector followed closely at 11%, with consumer goods & services at 10%, signaling a sustained focus on industries with high data value and low tolerance for operational downtime.

Deep Dive into Industrial Cybersecurity

The risks escalate in industrial environments (e.g., Operational Technology/OT, Industrial IoT/IIoT, and critical infrastructure), where AI-enabled attacks can cause physical disruption beyond data loss.

- Vulnerable Ecosystems: Industrial systems, often legacy and interconnected via IT/OT convergence, face expanded attack surfaces. Botnets, ransomware (e.g., WannaCry's impact on manufacturing), and zero-day exploits target IIoT devices.
- AI-Powered Industrial Threats: Attackers use AI for precise targeting, such as manipulating sensors in power grids or automating intrusions in supply chains. Deep learning models can evade traditional IDS in distributed IIoT networks.
- High-Stakes Impacts: Breaches in sectors like energy, manufacturing, or transportation led to outages, safety risks, or economic losses. AI accelerates polymorphic attacks or exploits unknown flaws.
- Defensive Applications in Industry: On the flip side, AI enables anomaly detection in OT networks, zero-trust architectures, and predictive maintenance to preempt failures from cyber causes.

Threat Trends: Escalating Complexity and Key Vectors

The GCO 2025 identifies cybercrime as the dominant threat, with ransomware, AI-enhanced phishing, and supply chain attacks surging. Globally, 72% of organizations reported heightened cyber risks in the past year, up from previous editions, while nation-state espionage influences strategies for 60% of firms. Emerging threats like deepfakes and modular ransomware kits have proliferated, with underground markets facilitating initial access sales.

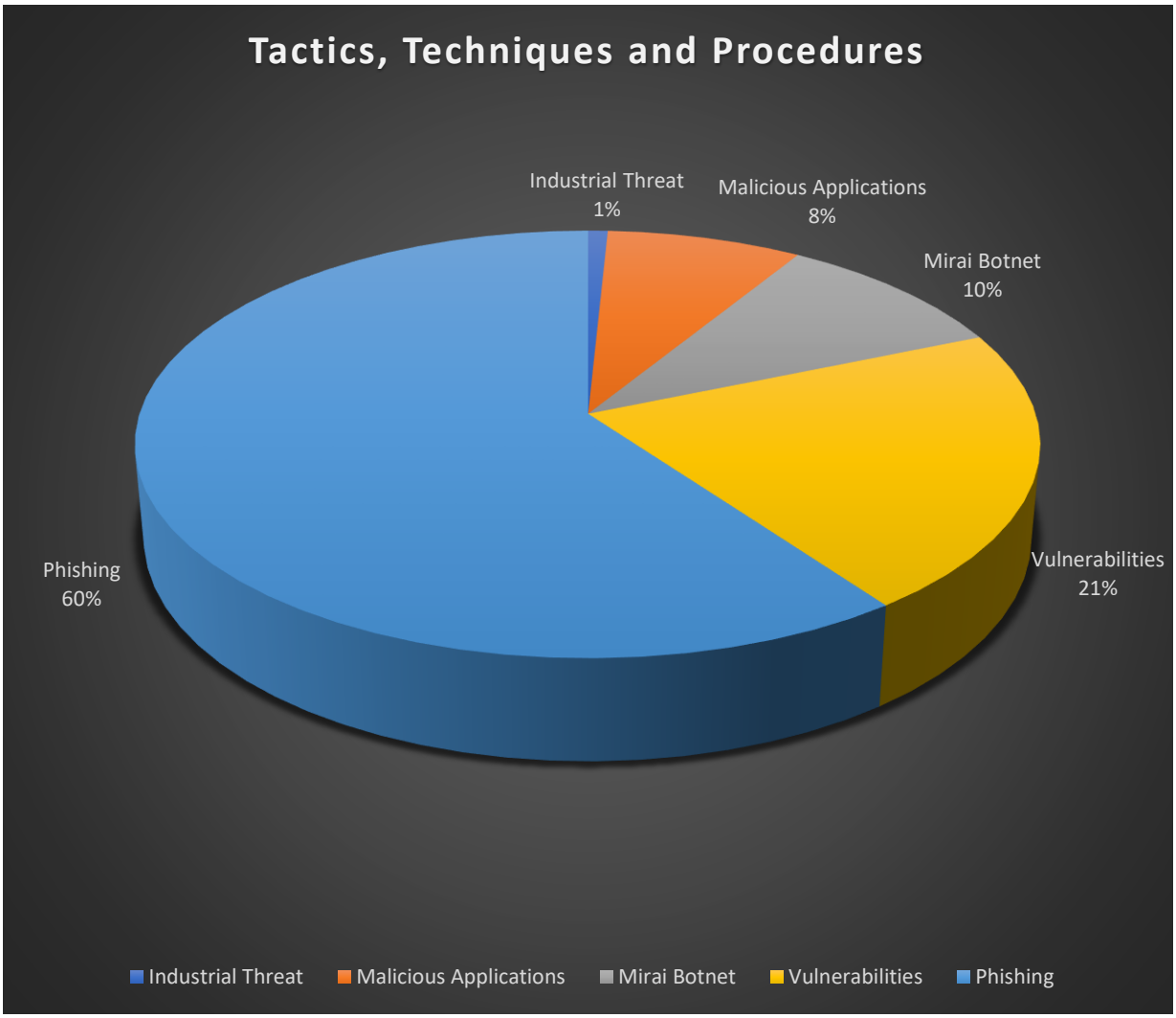


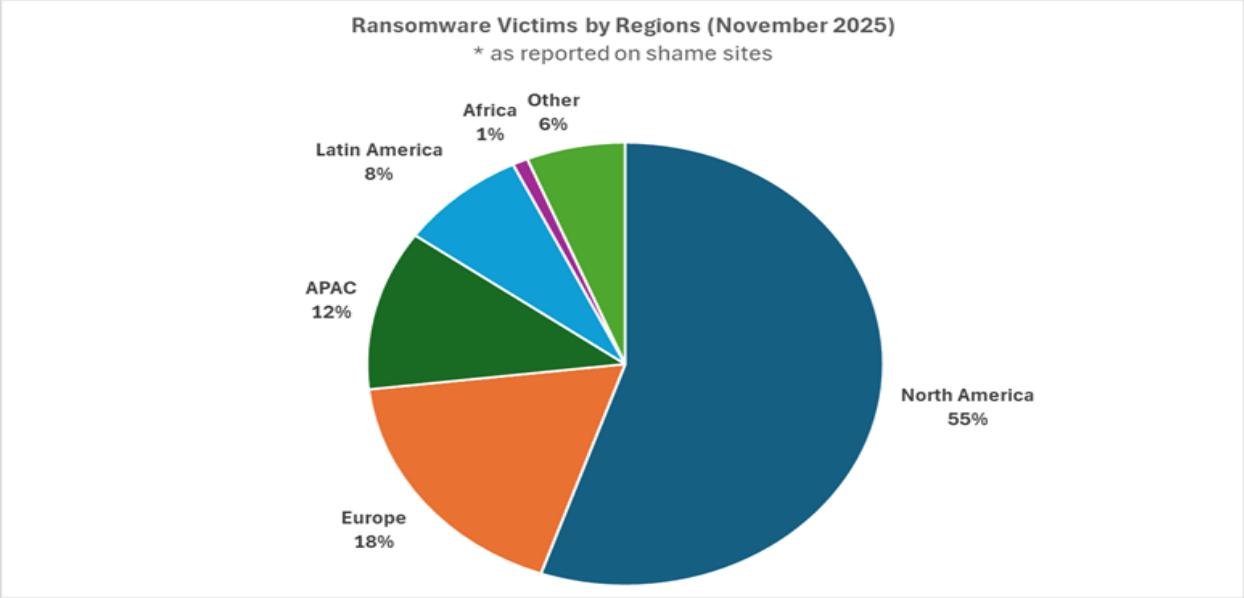
Fig 4: Threat Trends through Ransomware

Ransomware Dominance: Ransomware incidents rose 25% year-over-year in 2025, per Cyble's Global Cybersecurity Report, often targeting critical sectors like energy and finance.

- AI-Enabled Threats: Phishing attacks increased 1,200% since generative AI's rise in late 2022 (McKinsey data cited in CompTIA's State of Cybersecurity 2025).
- Geopolitical Spillover: 33% of CEOs cite cyber espionage as a top concern, with state-sponsored attacks blurring into criminal operations.

Ransomware Trends: 22% YoY Increase in Global Attacks

- Ransomware activity intensified notably in November 2025, with 727 reported attacks, marking a 22% increase compared to the same period last year and underscoring the persistence of double-extortion operations worldwide. North America remained the epicenter of ransomware activity, accounting for 55% of all disclosed incidents, followed by Europe with 18%, reflecting continued pressure on Western critical infrastructure and service-driven industries



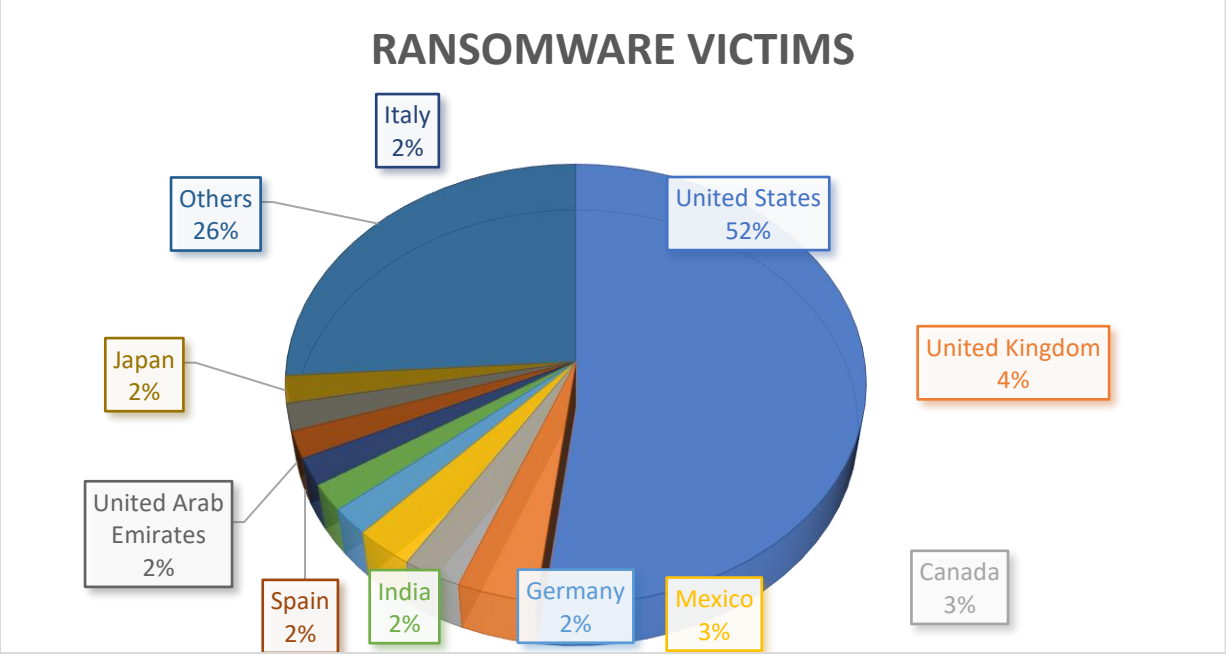


Fig 5: Ransome Victims

are increasingly exploiting sectors with limited security resources but highly valuable data and public-facing digital services.

At the national level, the United States dominated the victim landscape with 52% of global cases, while the United Kingdom and Canada followed distantly at 4% and 3%, respectively.

Recent guidance emphasizes secure-by-design AI, governance, and human oversight to mitigate risks in critical infrastructure.

Balancing the Sword: Strategies for the Future

To harness AI's benefits while countering its risks:

- Adopt ethical AI practices, explainable models, and robust governance.
- Implement zero-trust principles and hybrid human-AI defenses.
- Invest in training, regulations (e.g., EU AI Act), and collaborative threat intelligence.
- Prepare for emerging trends like agentic AI, which could automate multi-step attacks but also enhance autonomous defenses.

As of December 2025, AI is reshaping cybersecurity into an arms race. Organizations that proactively

embrace AI for defense—while vigilantly addressing its misuse—will be best positioned to thrive in this evolving landscape. The transition from opportunistic "fortune hunting" attacks to profound industrial disruptions underscores the urgency: AI is not just a tool, but a pivotal battleground.

AI - Guardian:

AI enhances cybersecurity to process massive datasets at speeds impossible for humans, enabling proactive and automated defenses.

- Threat Detection and Prediction: Machine learning algorithms analyze patterns in network traffic, user behavior, and anomalies to identify threats in real-time. For instance, AI-powered systems can detect zero-day exploits or unusual activity that traditional rule-based tools miss.
- Automated Response: Tools like Security Orchestration, Automation, and Response (SOAR) platforms use AI to isolate compromised systems, block malicious IPs, or remediate incidents swiftly, reducing damage from breaches.
- Vulnerability Management: AI prioritizes patches and forecasts potential weaknesses, helping organizations focus on high-risk issues amid overwhelming vulnerability volumes.
- Behavioral Analytics: User and Entity Behavior Analytics (UEBA) establish baselines and flags deviations, countering insider threats or advanced persistent threats (APTs).

AI bolsters endpoint protection, cloud security, and predictive analytics, with many organizations investing heavily to address talent shortages and rising attack volumes.

AI - Fortune Hunter:

Cybercriminals leverage the same AI technologies to lower barriers and amplify attacks, turning opportunistic exploits into high-yield operations.

- Sophisticated Phishing and Social Engineering: Generative AI crafts hyper-personalized emails, deepfakes, or voice clones, making scams more convincing and scalable. Attackers can impersonate executives or create realistic lures at minimal cost.
- Malware Evolution: AI generates polymorphic malware that evades signature-based detection or automates code for reverse shells and exploits.
- Adversarial Attacks: Bad actors use AI to poison models (e.g., adversarial examples that fool detectors) or automate reconnaissance.
- Scale and Speed: Low-entry tools like open-source large language models enable even novice attackers to launch "customized attacks at scale," from ransomware to identity theft.

The "fortune hunter" phase exploits AI's accessibility, with cybercriminals using it for quick financial gains, as seen in rising deep-fake-driven fraud and AI-enhanced social engineering.

AI Attacker's Arsenal: Amplifying Threats at Scale

AI's dark side empowers cybercriminals to operate with unprecedented speed, sophistication, and stealth, turning traditional defenses obsolete. What once took weeks of manual effort—crafting phishing emails, generating malware, or impersonating executives—now happens in seconds, scaled across millions of targets.

- Sophisticated Phishing and Deepfakes: Generative AI tools like offensive large language models (LLMs) such as Worm-GPT enable hyper-personalized attacks. CISOs report AI-generated phishing and deepfakes as top concerns, with 41% anticipating deepfake audio/video exploits in the coming year. In the Global Cybersecurity Outlook 2025, 47% of organizations flagged adversarial GenAI advances as their primary worry, citing scalable, evasive tactics.
- Autonomous Agents and Malware Evolution: Attackers leverage AI for autonomous agents (expected by 58% of CISOs) that chain prompts adversarial, inject vulnerabilities via data poisoning, or exfiltrate models. Code-generation tools, used by 65% of projected threats, automate malware creation, embedding it into legitimate software supply chains.
- Shadow AI and Internal Risks: "Ghost" AI tools—unsanctioned deployments by employees—expose data privacy gaps. 49% of CISOs view shadow AI as a major governance challenge, with incidents like prompt injection or model theft surging. This internal proliferation expands the attack surface, as 91% of surveyed organizations detected attempted AI attacks.

These threats aren't hypothetical; they're operational. The result? An "Internet X"—a new digital frontier

where AI escalates the arms race, demanding defenses that match its velocity.

AI Defender's Edge: Automating Resilience

Yet, the same technology fueling attacks equips defenders with proactive, intelligent tools. Across the Cyber 60, nearly every company integrates AI to automate rote tasks, triage alerts, and predict breaches—addressing a crippling skills gap where only 16% of CISOs feel confident in their teams' AI expertise. 88% plan to hire or reskill within six months, but AI bridges the void now, slashing response times by up to 10x and eliminating alert fatigue.

Key defensive paradigms include:

- Agentic AI for Autonomous Response: Platforms deploy self-learning agents that investigate incidents without human prompts, adapting in real-time.
- Non-Human Identity (NHI) Security: With AI agents proliferating, securing machine identities—keys, tokens, APIs—becomes paramount, preventing lateral movement.
- Governance and Red Teaming: Tools monitor AI usage, enforce guardrails, and simulate attacks to harden models against jailbreaks.

Investment reflects this optimism: 88% of CISOs expect budget hikes, with 86% dedicating over 5% to AI security. The market splits between consolidated platforms (47%) and AI-native point solutions (53%), signaling a maturing ecosystem.

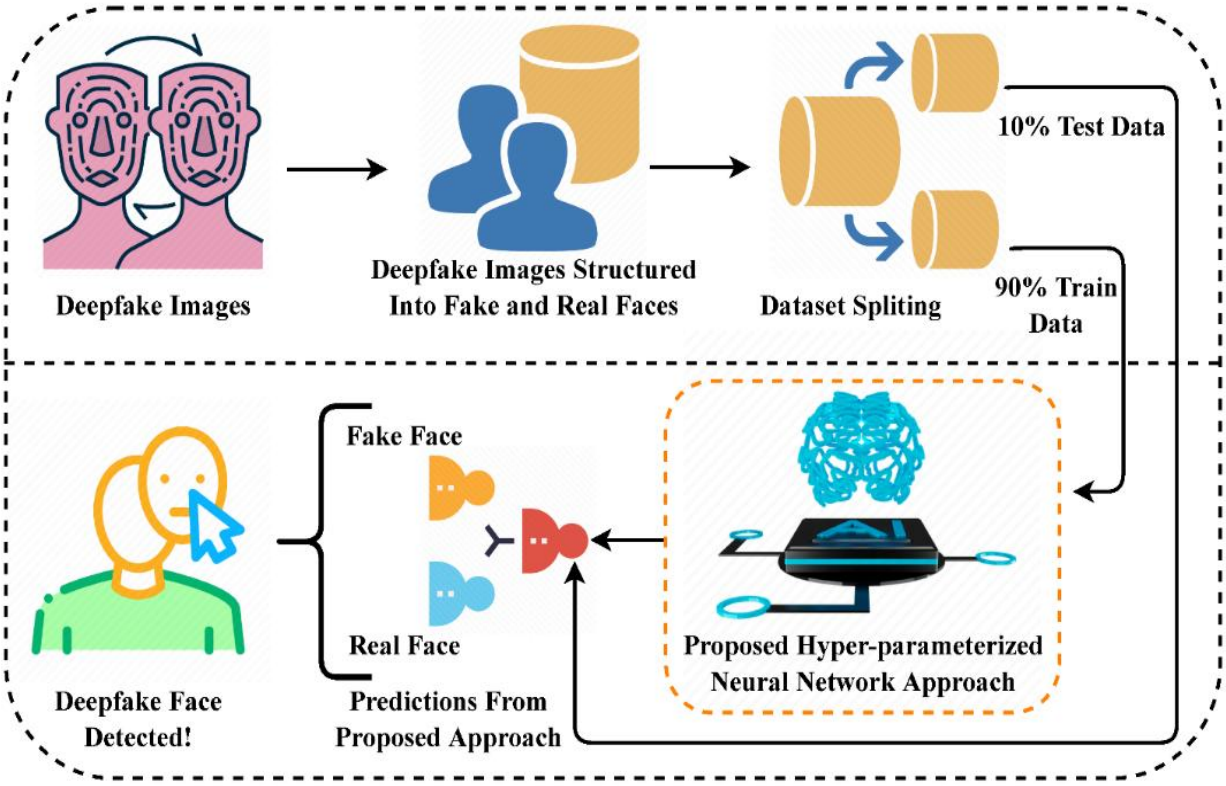


Fig 6: Architecture of Deepfakes Face Detection

Deepfakes—hyper-realistic AI-generated audio, video, or images that impersonate real people—have evolved from novelty to a potent weapon in cybercriminals' arsenals. By exploiting trust in visual and auditory cues, attackers use deepfakes to supercharge social engineering, enabling sophisticated phishing, fraud, and impersonation scams. As of late 2025, deepfakes are driving a surge in cyber incidents, with financial losses soaring and detection becoming harder.

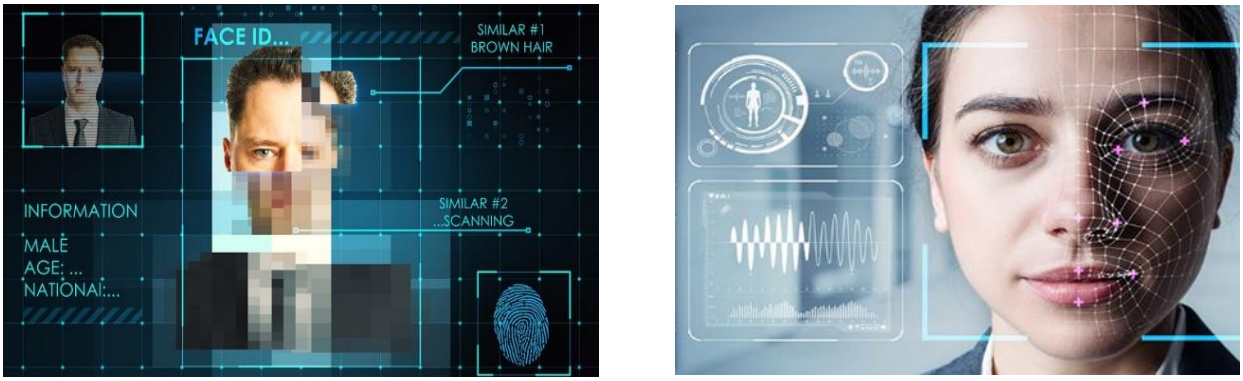


Fig 7: Face-Id

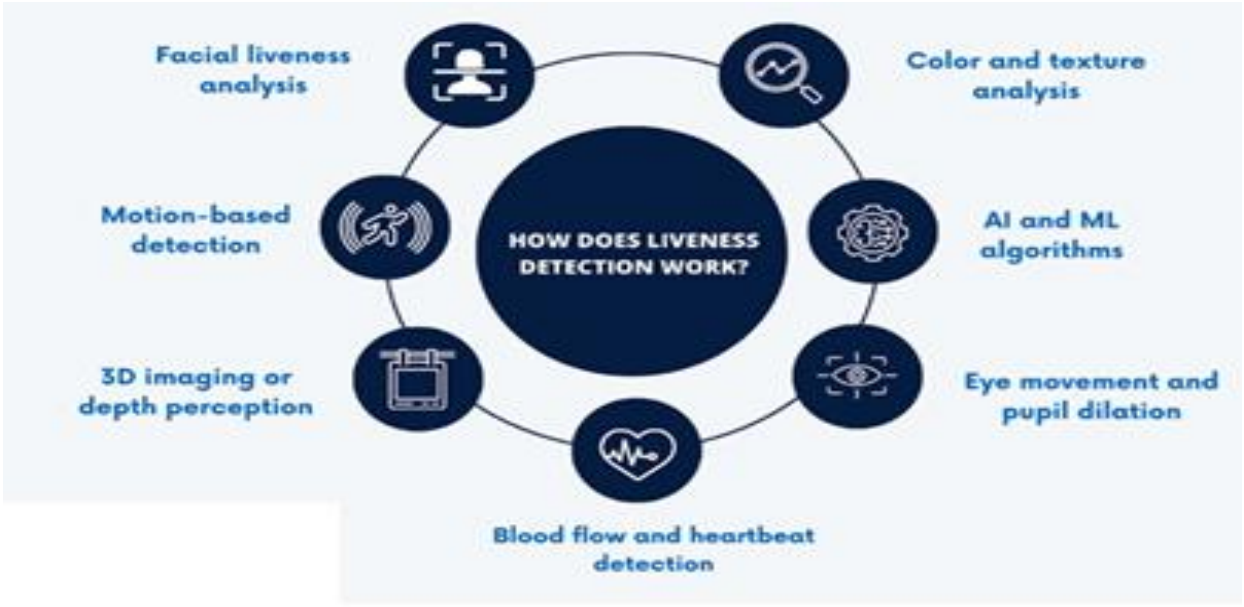


Fig 7: Liveness Detection

Feature	Active Liveness Detection	Passive Liveness Detection
User Interaction	Requires prompts (e.g., turn your head, blink, smile)	No interaction needed — works silently in the background
User Experience	Interruptive, sometimes confusing or frustrating	Seamless and invisible to the user
Speed	Slower, as it requires waiting for user action	Faster, occurs automatically during image capture
Spoof Resistance	Effective, but spoofable with deepfake videos or coordinated attacks	Highly resilient due to AI-driven analysis of natural traits
Deployment Scenarios	Better suited for controlled environments	Ideal for high-volume, user-centric applications

Mirai Botnet: The Mirai botnet is one of the most infamous pieces of malware in cybersecurity history. Named after the Japanese word for "future", it is a self-propagating worm that infects Internet of Things (IoT) devices running Linux, turning them into remotely controlled "bots" or "zombies." These compromised devices form a botnet—a network used primarily for launching massive, distributed denial-of-service (DDoS) attacks by flooding targets with traffic.
cameras, DVRs, routers, and other embedded systems, which often ship with default credentials that users rarely change.

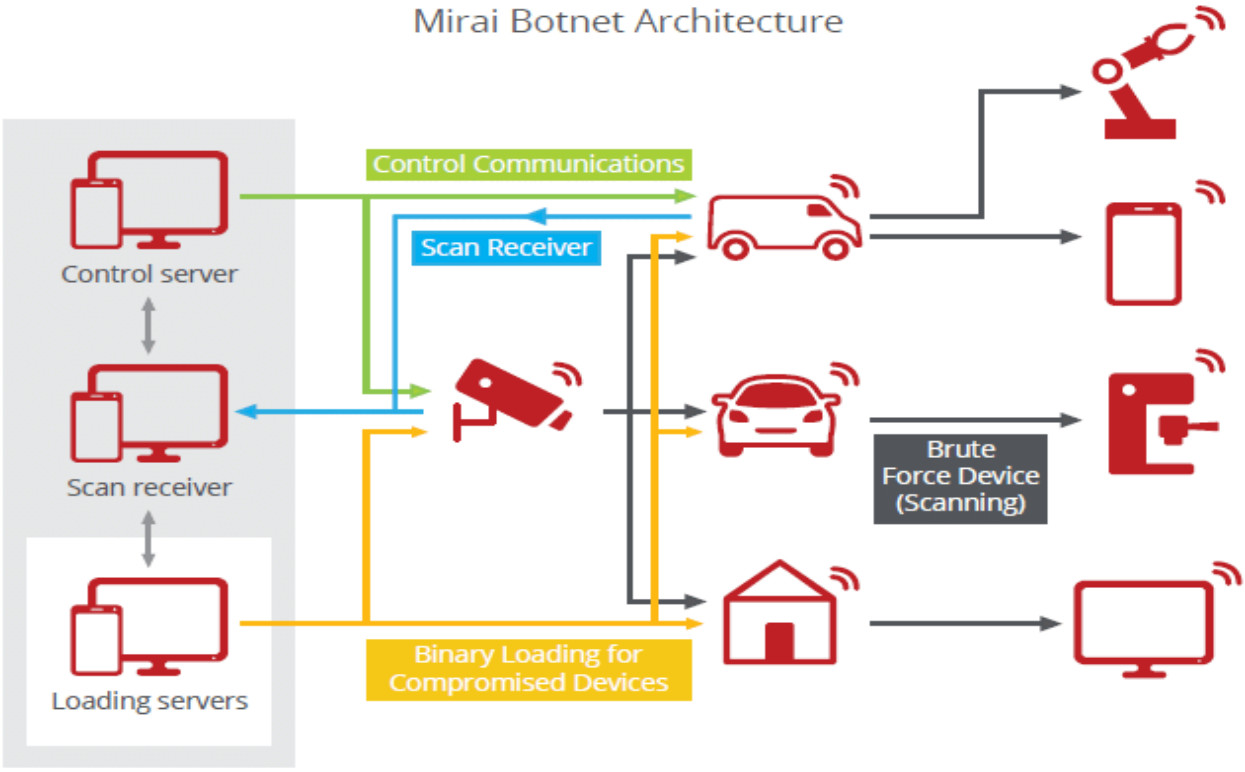


Fig 8: Mirai Botnet Architecture

Mirai Remains a Threat

- Scale: Can en
- Fig 8list hundreds of thousands of devices quickly.
- Evasion: Memory-resident, kills competitors, uses packed binaries.
- Impact: DDoS volumes in Tbps range; some variants add data theft or mining.
- As of 2025, active exploitation continues, with surges in >1 Tbps attacks.

Spotlight on Fortune Cyber 60 Innovators: Turning AI Against Itself

The Cyber 60—sorted by stage (early, early growth, growth) and ranked by annual recurring revenue (ARR)—features trailblazers wielding AI to counter AI threats. Here's a curated selection of AI-centric companies, their funding, and innovations:

Company	Stage	Funding Raised	Key AI Innovation	Addresses Threat
7AI	Early	$36M	Dynamic Reasoning tech for autonomous agents that contextualize threats, slashing false positives and enabling machine-speed decisions.	AI-generated malware and autonomous attacks.
Cogent	Early	$11M	World's first AI Taskforce automating the full vulnerability management lifecycle, from scan to patch.	Code-generation exploits and supply chain risks.
Drop-zone AI	Early Growth	$57.25M	Pre-trained agents for playbook-free alert triage and investigation, reducing MTTR dramatically.	Shadow AI and insider threats.

Company	Stage	Funding Raised	Key AI Innovation	Addresses Threat
Prophet Security	Early Growth	$41M	Agentic SOC platform automating triage, investigation, and response—10x faster than manual processes.	Deepfakes and prompt injection.
Doppel	Growth	$54M	AI-native Social Engineering Defense using threat graphs to detect impersonations across channels.	AI-powered phishing and fraud.
Virtue AI	Growth	$30M	Lifecycle security for AI agents/models, including real-time red-teaming and compliance.	Model exfiltration and data poisoning.
Witness AI	Early Growth	$27.5M	Monitors shadow AI, enforces policies on chatbots/models for unified risk visibility.	Unsanctioned AI usage and governance gaps.
Abnormal AI	Growth	$546M	ML-driven email security stopping inbound attacks and detecting compromised accounts.	Generative phishing campaigns.
Cyera	Growth	$1.3B	AI-native data security for visibility and protection across AI-dependent environments.	Synthetic identity fraud.

Table1: Fortune 60 Innovation

These firms exemplify the Cyber 60's ethos: 94% of CISOs have assessed or plan to assess AI threat surfaces, prioritizing tools like secure inference platforms (54%) and LLM red teaming (49%). Acquisitions like Cato Networks' purchase of Aim Security for AI deployment safety further signal consolidation.

Detailed Explanation of APCER (Attack Presentation Classification Error Rate)

Definition: APCER is the proportion of attack presentations (using the same PAI species) that are incorrectly classified as bona fide presentations. In simpler terms, it measures how often the PAD system fails to detect a spoof and mistakenly accepts it as a real, live user. A PAI species refers to a category of attack instruments produced by a common method (e.g., all printed photos on matte paper or all silicone masks).

Formula:

$$\text{APCER} = \frac{\sum_{i=1}^{N_{\text{PAIS}}} \text{Res}_i}{N_{\text{PAIS}}}$$

N_{PAIS}: The total number of attack presentations for a specific PAI species.

- Res_i: Equals 1 if the i-th attack is misclassified as bona fide (false acceptance), and 0 if correctly identified as an attack.

This results in a percentage or proportion (e.g., 0.05 or 5%), where lower values indicate better security against spoofs.

$$\text{BPCER} = \frac{\sum_{i=1}^{N_{\text{BF}}} \text{Res}_i}{N_{\text{BF}}}$$

N_{BF}: The total number of bona fide presentations.

- Res_i: Equals 1 if the i-th genuine presentation is misclassified as an attack (false rejection), and 0 if correctly accepted as bona fide.

Like APCER, it is expressed as a proportion or percentage, with lower values preferred for better user experience.

Navigate the Balance: Strategies for 2025 and Beyond

AI's double-edged nature demands a holistic approach: Invest in AI governance (e.g., policy automation for third-party risks, cited by 50% of CISOs), augment workforces with agentic tools, and foster explainable AI for accountability. As 82% of leaders deem vendor AI strategies critical, partnerships with Cyber 60 innovators offer quick ROI amid rising incidents.

In 2025, cybersecurity isn't about outpacing AI—it's about outsmarting it. The Fortune Cyber 60 proves that by harnessing AI's "secret sauce," organizations can tilt the scales toward defense, securing a resilient digital future. As threats evolve, so must we: proactive, adaptive, and unyieldingly vigilant.

Cybersecurity investing is one of the pillars of global enterprise practice, and a focus area of deep immersion and commitment. Report from CISO survey conducted Wakefield Research surveyed that 200 CISOs at companies with $500 million or more in revenue on the intersection of AI and cybersecurity. The results reveal a market at an inflection point. Most organizations have already experienced AI-related security incidents, yet confidence in defensive capabilities remains strikingly low. Despite this gap, investment signals are unequivocal. The threat is no longer theoretical but operational.

A credible source like the World Economic Forum's Global Cybersecurity Outlook 2025 confirm the 66% expectation of AI's impact while only 37% with assessment processes and Capgemini's research (noting 97% of organizations faced GenAI-related incidents in 2024). The World Economic Forum's *Global Cybersecurity Outlook 2025* (GCO 2025), released in collaboration with Accenture on January 13, 2025, provides a comprehensive analysis of the evolving cybersecurity landscape. It emphasizes unprecedented complexity driven by geopolitical tensions, rapid AI adoption, sophisticated cybercrime, supply chain vulnerabilities, regulatory pressures, and a widening skills gap. The report is based on surveys of over 300 global organizations, including C-suite leaders, and highlights how these factors amplify threats to economies, societies, and critical infrastructure. While the full report (available as a PDF) contains visual diagrams and infographics—such as radar charts on risk perceptions, bar graphs on AI impacts, and flowcharts for resilience frameworks and visualized key quantitative trends below using data from the report and related analyses (e.g., ENISA Threat Landscape 2025 and Deloitte's Cyber Threat Trends 2025). These charts focus on prominent threat trends and defense framework adoption.

Adoption trends show progress in foundational defenses but lags in advanced areas:

- Zero Trust & AI Assessment: 63% of organizations have implemented zero trust models, but only 37% assess AI tools for security pre-deployment.
- Skills & Collaboration: 67% report underinvestment in AI cybersecurity skills, while 72% prioritize public-private partnerships.

The pie chart below breaks down framework adoption rates from the GCO 2025 and EY analysis, showing the distribution of maturity levels across global organizations:

This distribution highlights a shift toward mature frameworks (up 12% from 2024), but the 15% "insufficient" segment—largely SMBs—signals growing inequity, as larger enterprises invest more in proactive tools like AI-driven XDR.

Strategic Recommendations for 2025

To navigate these trends, GCO 2025 outlines actionable steps:

1. Prioritize AI Security: Implement pre-deployment assessments and ethical AI guidelines to counter the "AI paradox" (high impact expected, low preparedness).
2. Enhance Supply Chain Visibility: Map dependencies and adopt shared risk models to mitigate the top resilience barrier.
3. Foster Collaboration: Join global initiatives like the WEF's Cyber Polygon exercises for threat intelligence sharing.
4. Invest in Human Capital: Address the skills gap (projected 3.5 million unfilled roles globally) through training in cloud security and DevSecOps.
5. Adopt Quantitative Risk Metrics: Use tools like Cyber Risk Index to align budgets with threats, targeting a 15% global spending increase forecasted by Gartner.

For deeper dives, download the full GCO 2025 report from the World Economic Forum website, which includes detailed infographics on regional disparities and scenario-based resilience models. These trends align with complementary reports like ENISA's Threat Landscape 2025 (analyzing 4,875 EU incidents) and CrowdStrike's Global Threat Report, reinforcing the need for adaptive, ecosystem-wide defenses.

Key strengths:

- Threat breakdown: The discussion of AI-enhanced phishing/deepfakes, polymorphic/ fileless malware, adaptive botnets, and smarter credential attacks aligns with current trends. Reports from Microsoft, CrowdStrike, and Check Point in 2025 emphasize how AI lowers barriers for attackers, enabling faster reconnaissance, personalized social engineering, and evasion of traditional detections.
- Defense strategies: Framing solutions around programmable (custom policies for rapid adaptation), adaptable (behavioral analysis and real-time learning), and autonomous (automated mitigation with zero-trust) security is spot-on. These mirror recommendations from leaders like Darktrace (self-learning AI), CrowdStrike (agentic AI for response), and Palo Alto Networks (AI-driven platforms). Combining these with zero-trust architecture and behavioral fingerprints effectively counters AI's speed and sophistication.

- Compliance angle: Linking threats to regulations like GDPR/CCPA/PCI DSS is practical, as breaches often trigger fines and reputational harm beyond direct losses.

Practices to be Adored:

- Fight AI with AI: Deploy defensive tools like user/entity behavior analytics (UEBA), anomaly detection, and generative AI for threat simulations/hunting. Solutions from Fortinet, Sentinel One, or Microsoft Security Copilot can predict and neutralize attacks at machine speed.
- Employee training and verification: With deepfakes rising, enforce multi-factor authentication (MFA), out-of-band verification for sensitive requests, and awareness programs on AI-generated content.
- Secure your own AI: Assess tools before deployment (addressing that 37% gap), monitor for data poisoning, and use robust governance frameworks.
- Layered defenses: Combine endpoint detection/response (EDR/XDR), threat intelligence sharing, and regular patching—fundamentals remain critical even against advanced threats.

AI-augmented security is essential for resilience. Businesses ignore the risk falling behind in future era where attacks are not just frequent but intelligently adaptive. (e.g., charts of threat trends or defense frameworks).

The widespread adoption of AI has revolutionized how cyber threats are created and executed. Traditional security methods, such as signature-based antivirus solutions, rule-based intrusion detection systems and perimeter firewalls, are no longer sufficient. Businesses must adopt a proactive cybersecurity approach to identify and neutralize risks before they cause damage.

Despite this scenario, as the World Economic Forum's latest Global Cybersecurity Outlook reports, "While 66% of organizations expect AI to have the most significant impact on cybersecurity in the year to come, only 37% report having processes in place to assess the security of AI tools before deployment."

Key strategies for strengthening defenses against AI-driven cyber threats:

The Main AI-Driven Threats Today

AI has taken social engineering to a new level, using deep learning to create highly realistic phishing content, including deepfake impersonations, making them a significant cyber threat. AI has also upgraded well-known attacks such as advanced malware and autonomous botnets.

Modern malware introduces a new level of complexity: It's self-learning and adaptive. It can change its real-time behaviors to avoid security solutions, resulting in polymorphic malware (changing its signature with each execution), fileless attacks (operating within system memory, evading signature-based detection) and AI-assisted brute-force and credential-stuffing attacks (cracking passwords and authentication mechanisms more efficiently).

In the same way, botnets have become significantly more dangerous, conducting intelligent DDoS attacks, identifying and exploiting zero-day vulnerabilities and evading detection using AI-enhanced traffic masking, continuously adapting their attack patterns to maximize disruption.

Besides security implications, all of this increases compliance risks. Non-compliance with GDPR, CCPA and PCI DSS can result in regulatory fines, legal consequences, loss of customer trust, reputational damage and operational disruptions.

How To Mitigate Security And Compliance Risk

As mentioned, the consequences of cyber threats extend beyond financial losses. In this context, outdated traditional approaches affect innovation, agility and visibility, leaving organizations vulnerable to cyber threats.

A modern cybersecurity strategy requires a multilayered, AI-powered defense system that can dynamically evolve to neutralize emerging threats. This approach must be adaptable, programmable and autonomous. It includes automation, behavioral analysis and real-time mitigation to proactively defend against sophisticated attacks while maintaining compliance with global industry standards.

Programmable Security

Programmable security uses customizable policies to quickly and accurately respond to new threats, reducing human error and ensuring consistent enforcement.

Leading companies are implementing programmable security solutions that evolve with emerging threats. For example, in e-commerce, machine learning systems automatically update reputation lists to block attacks and fraud while maintaining seamless customer experiences. Financial institutions employ customized fraud prevention policies that adjust based on risk factors, significantly reducing false positives.
These programmable approaches allow security policies to adapt automatically, creating highly efficient and responsive defense systems tailored to evolving threats. Integrating security policies with SIEMs and API gateways also provides for real-time threat detection and response, improving threat detection and response times.

Adaptable Security

Adaptable security provides businesses with a dynamic, real-time defense mechanism that improves over time and responds with precision to complex, fast-moving attacks, continuously learning and adjusting to emerging risks in real time. By analyzing vast amounts of data and user behavior, AI-driven systems can identify suspicious activities, from fraudulent transactions to insider threats, and respond immediately to mitigate them.
This self-learning capability enables businesses to stay ahead of emerging threats rather than merely reacting to known attack patterns, making it possible to anticipate threats based on evolving patterns and neutralize risks before they can impact business operations. Behavioral analysis further enhances this approach, as it detects anomalies that indicate potential security incidents, offering deeper insights into the true nature of a threat.
Adaptive security frameworks are revolutionizing enterprise defense by learning from and responding to changing threat landscapes. AI technologies create unique behavioral fingerprints distinguishing legitimate users and sophisticated bots. Organizations are also deploying predictive systems that map digital attack surfaces and anticipate vulnerabilities before attackers exploit them.

Autonomous Security

Implementing autonomous security enables acting in real time, automatically mitigating threats without human intervention. It reduces response times and minimizes risks, ensuring businesses can swiftly address potential breaches before they escalate. By continuously analyzing network traffic, user behavior and system anomalies, AI-powered security solutions can identify and neutralize threats faster and more efficiently than manual methods.
In conjunction with an autonomous response, zero-trust architecture maintains security across dynamic, multi-cloud environments by verifying every user and device before granting access, eliminating trust assumptions, and adding protection.

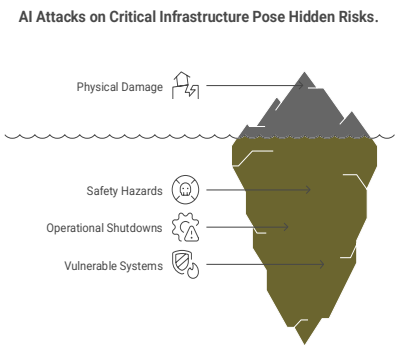


Fig 9: Hidden Risks through AI Deep Dive Attacks

III. CONCLUSION

According to Capgemini Research Institute, GenAI-related security breaches affected 97% of organizations in 2024. These new AI-driven cyber threats demand a transition from traditional, static security models to integrated AI-powered solutions that are intelligent, proactive and autonomous. These advanced defenses can continuously adapt to new threats, enforce programmable policies and automate real-time mitigation.
By implementing adaptable, programmable and autonomous security strategies, organizations can strengthen their ability to detect, prevent and neutralize sophisticated attacks while ensuring compliance with industry regulations. Investing in AI-driven cybersecurity is fundamental to safeguarding business continuity, protecting sensitive data and maintaining trust in an increasingly digital world.
38.2% Public Administration Public Administration was identified as the most targeted sector in the EU (38.5%), dominated by low-impact DDoS (94.8%),

with ransomware particularly affecting municipalities reflecting Transport Sector.

REFERENCES

[1] Removing barriers to American leadership in artificial intelligence, the white house, January 23, 2025

[2] The Artificial Intelligence Act, Official Journal version of 13 June 2024. how policymaking in the European Union works.

[3] CISO Mind-Map 2025: What do InfoSec Professionals Really Do? by Rafeeq Rehman

[4] OWASP GenAI Security Project – OWASP Top for GenAI and LLM.

[5] CISCO REPORTS FOURTH QUARTER AND FISCAL YEAR 2025 EARNINGS August 13, 2025 SAN JOSE, Calif., Aug. 13, 2025 /PRNewswire/ --

[6] Build CISO Strategic Impact and Visibility: State of the CISO, 2025 is Live! January 14, 2025

[7] Reading the ENISA Threat Landscape 2025 report Pierluigi Paganini October 06, 2025

[8] AI Used to Delete Government Databases in Breach of Cybersecurity Protocols Andrew Doyle December 5, 2025

[9] Here Comes Mirai: IoT Devices RSVP to Active Exploitation Kyle Lefton May 06, 2025

[10] The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet Feature Mar 9, 2018 by Josh Fruhlinger.

[11] A case study on Mirai Botnet Attack of 2016 D21DCS151 Apr 10, 2023

[12] OpenAI-Backed Adaptive Security Named to Fortune's Cyber 60 List Adaptive wordmark (PRNewsfoto/Adaptive Security) News provided by Adaptive Security Oct 31, 2025, 09:00 ET

[13] Fortune Cyber 60 and CRN Stellar Startups Show Enterprises Are Ready for Agentic Security Nate Burke November 13, 2025 •7AI Named to Fortune 2026 Cyber 60 and CRN 2025 Stellar Start-ups

[14] Growing over 200% y/y, SAFE Is Recognized in Fortune Magazine’s Cyber 60 List of the 60 Fastest-Growing Cybersecurity Startups Globally The honor caps a year of innovation Oct 30, 2024

[15] Safe Security Recognized in Fortune Cyber 60 for Innovation in Cybersecurity -PRNewswire, October 31, 2024