Evolver

AI Shockwaves in Cybersecurity

A Post-Productivity Era Transformation

October 2025

AI Shockwaves in Cybersecurity: A Post-Productivity Era Transformation

From Productivity Gains to Industry Disruption

Artificial intelligence has already boosted productivity in cybersecurity by automating routine tasks such as cyber threat identification and accelerating cyber-attack response and remediation workflows. However, as Gartner observes, "the real disruption will come when AI forces entire industries to rethink value, pricing and even the relevance of their core offerings, especially with the application of agentic systems."[1] In other words, beyond incremental improvements, a second wave of AI "shockwaves" is emerging – one that drives deeper, systemic changes in how the cybersecurity field operates. These shockwaves represent the secondary and tertiary impacts of AI, where core products may become obsolete, new business models emerge, and roles across the value chain are transformed[2]. Few cybersecurity leaders feel fully prepared for this shift – Gartner notes that less than 30% of technology leaders are pursuing AI initiatives aimed at true industrywide disruption[3]. Yet those who embrace this next era can redefine cybersecurity's future, rather than be disrupted by it.

Rethinking Value, Pricing, and Offerings in Cybersecurity

In a post-productivity AI era, cybersecurity organizations, including U.S. Federal Information Technology (IT) System Integrators (SIs) and commercial Managed Security Services Providers (MSSPs) must reconsider what "value" means for their cyber services and solutions. Traditionally, value has been measured in breached thwarted or compliance achieved. Agentic AI (autonomous AI agents) could fundamentally expand this value by providing "autonomous, real-time defense" – detecting threats, making decisions, and acting at machine speed without waiting for human input[4][5]. For example, AI-driven defensive models can monitor networks like a digital immune system, spotting anomalies and neutralizing attacks "before humans even know something is wrong."[6] This level of responsiveness could make near-instant breach containment and self-healing systems a standard expectation in the future, dramatically increasing the value of security by minimizing damage. Indeed, experts predict that by 2035 we may see self-healing cybersecurity ecosystems that proactively predict vulnerabilities, apply patches, and adapt defenses autonomously[7] – a radical step beyond today's reactive post-incident remediation.

Pricing models for security solutions are also poised to change under AI's influence. As AI automates more of the work, the cost of delivering certain security functions will drop, pressuring providers to pass savings on or adopt new pricing strategies. Customers already report that many cybersecurity products "fall short of expectations in terms of automation [and] pricing," and they seek more cost-efficient, AI-enabled solutions [8]. In response, many organizations are moving away from labor-intensive subscription services toward outcome-based pricing or performance-based pricing models (for example, charging by incidents prevented or by risk reduced). Furthermore, if AI-driven platforms commoditize basic security (making some core protections effectively "free or obsolete" over time[9]), cybersecurity companies will need to innovate new premium offerings and value-added services, including Security-as-a-Service offerings. We could see open-source or low-cost AI security agents tackling common threats, forcing traditional players to rethink how they differentiate their products and justify pricing in an AI-saturated market.

Perhaps the most jarring impact will be on the relevance of core cybersecurity offerings themselves. AI shockwaves tend to rewrite the rules – analogous to how past innovations made once-core technologies redundant. In cybersecurity, tools like signature-based antivirus or standalone intrusion detection systems (IDS) and related endpoint detection systems could be rapidly outpaced by AI-driven cloud platforms that predict attacks and neutralize malware autonomously within seconds[10]. If an AI agent can continuously enforce zero-trust policies across cloud environments and automatically isolate compromised devices[11], it reduces reliance on many point products and manual interventions. Startups at the "edges" of the industry

are already leveraging AI to replicate and surpass legacy solutions – these fast-acting AI "copycats" can quickly offer comparable protection at lower cost[12]. This puts pressure on incumbents to evolve or risk their core offerings becoming irrelevant. In short, value in cybersecurity may shift from selling individual tools to delivering holistic, AI-managed "security as a service" outcomes. Pricing will need to reward proactive prevention and resilience rather than reactive cleanup, and legacy offerings must either embed AI or be left behind in the new value chain.

The Future Vision: Autonomous and Adaptive Cybersecurity

What might cybersecurity look like after these AI shockwaves fully hit? Envision a future where data security systems are intelligent, autonomous, and adaptive by design. In this scenario, organizations deploy swarms of AI agents across their networks and endpoints, each continuously learning and taking action to protect digital assets. Cyberthreat detection and response become largely autonomous: agentic AI monitors logs, user behavior, and network traffic 24/7, correlating signals from endpoints, cloud workloads, and IoT devices to spot stealthy attacks (even novel zero-day exploits) in real time[13]. The moment a cyber threat indicator is recognized, the AI agents collaborate to contain it – revoking a compromised account's access, isolating affected systems, and initiating incident response playbooks within seconds[14][15]. This kind of instantaneous containment drastically reduces "dwell time" (the duration an attacker lingers in a system); in fact, autonomous AI responders could cut incident investigation times by up to 90% by filtering out false alerts and focusing on truly critical events[16][17].

Beyond response, AI will drive a proactive immune system for cyber defense. Future platforms will continually scan for vulnerabilities or misconfigurations in IT environments and fix them before attackers can exploit them. For instance, an AI agent might detect an unpatched software flaw or an open cloud storage bucket and automatically remediate it or flag it for immediate fix, effectively anticipating attacks before they occur. Gartner analysts predict that by 2030, there will be a major shift toward preemptive cybersecurity – with half of all security spending dedicated to prevention-focused, AI-driven solutions (up from less than 5% in 2024)[18]. In practice, this means simulation and digital twin technologies may be used to model attacks in advance, allowing AI systems to reinforce defenses proactively. Security teams will run continuous AI-driven "purple teaming" exercises, where an AI red team tries to breach the organization's digital twin and an AI blue team fortifies it, all in an automated loop [19]. The insights from these simulations enable real networks to be hardened preemptively – a stark contrast to today's predominately reactive posture.

Importantly, humans will still play a vital role, but their focus will evolve. Mundane, repetitive Tier-1 analysis (like sifting through benign alerts or log data) will largely be offloaded to AI. This addresses the chronic talent shortage – a global shortfall of 3.4 million cybersecurity professionals – by using AI as a "force multiplier" that handles volume work[20]. Meanwhile, human experts can concentrate on higher-level strategy, creative threat hunting, and oversight of AI systems. In fact, leading organizations are already reorganizing security teams to co-evolve with AI – machines handling scale and speed, humans providing supervision, ethical judgment, and strategic guidance[21]. The roles within cybersecurity will shift to new specialties like AI model auditors, security orchestration engineers, and AI ethics officers might emerge, while some traditional analyst roles become less prevalent. Overall, the culture of cybersecurity could become more collaborative and interdisciplinary, blending data science with classic infosec expertise.

However, this autonomous future also introduces new challenges that will shape cybersecurity strategy. Cyber-attack groups including both Nation-State cyber-attack groups and organized criminal cyber-attack groups, are actively leveraging AI as well – and at a frightening pace. CISOs now rank AI-powered cyberattacks as their top concern, cited by 80% of CISOs in a 2025 survey[22]. Threat actors are using generative AI to craft highly convincing phishing lures, deepfake social engineering, and even to discover vulnerabilities faster than ever. There is a very real prospect of "fully autonomous, AI-driven cyberattacks" hitting organizations by 2027[23], where malware and bots independently adapt and spread without human command. Cyber-attack

groups leveraging these independent AI threats combined with a lack of security mitigation built into new AI software tools means the future might see AI-vs-AI skirmishes: defensive AI agents battling offensive AI code in a digital battleground at lightning speed. The attack surface will also include AI systems themselves – malicious actors might attempt to poison the datasets or manipulate the algorithms of enterprise AIs. New frameworks are already emerging to address this, such as the OWASP Agentic AI Security guidelines that outline threats unique to autonomous agents and how to mitigate them[24][25]. Enterprises will need to extend their cybersecurity programs to cover AI governance, validation of AI decisions, and the authentication of AI agents operating in their environment[26][27]. Building digital trust in an era full of automated agents – knowing which bots to permit and which to block – will become a foundational aspect of security strategy[28][29].

In summary, the future state of cybersecurity post-AI shockwave is one of autonomous cyber resilience, which is focused on the continuity of operations. Cyber defenses will be embedded, always-on, and intelligent – drastically reducing the window of opportunity for attackers. Security will be less visible as a separate siloed function and more an intrinsic property of all digital systems (much like safety features in modern cars). Yet, maintaining control and trust in these autonomous systems will be paramount. Enterprise strategists must start imagining this future now, so they can steer their organizations toward it by deliberate design rather than by scrambling to catch up.

Steps to Catalyze the Post-Productivity AI Shockwave in Cybersecurity

Achieving this transformative cybersecurity vision requires proactive leadership and strategic investment. Below are key steps for enterprise strategists to develop the post-productivity era AI "shockwave" in their cybersecurity programs:

1. **Embed AI into Core Data Security Workflows:** Integrate AI deeply into every layer of cybersecurity operations, rather than as a superficial add-on. Identify high-volume, high-speed tasks (e.g. monitoring, threat detection, user access reviews) and deploy AI co-pilots or agents to handle them end-to-end. By infusing AI at the core of workflows, organizations accelerate innovation and set the pace of change[30]. For instance, use machine learning to dynamically triage alerts, or employ agentic AI to continuously test and improve your defenses. This deep cybersecurity integration ensures that as threats evolve, your security reaction is instantaneous and adaptive.

2. **Adopt an AI-First Data Security Model:** Rethink your data security architecture and services from an "AI-first" perspective. This means designing new solutions and even business offerings that leverage AI's capabilities as a foundation. Consider how products or managed services could be "AI-driven – especially agentic AI-driven – with AI embedded into everyday user experiences."[30] For example, an identity management service might incorporate an AI that learns normal user behavior and autonomously flags anomalies, or a managed detection service might guarantee a level of threat containment achieved by AI within seconds of intrusion. An AI-first model also implies restructuring processes to allow AI to make many decisions autonomously. To do this responsibly, establish clear guardrails for AI actions (e.g. define which responses can be fully automated vs. which require human sign-off) and embed compliance and ethics checks into AI workflows. By treating AI as the new engine of your data security strategy (rather than a pilot project on the side), you position your organization to capture the full disruptive potential of these technologies.

3. **Innovate Bold, Experimental AI & Cybersecurity Initiatives:** To leap from incremental improvements to true breakthrough innovation, dedicate resources to experimentation at the fringes of your current cybersecurity practice. Launch spinoff projects or innovation pods to explore radical applications of AI[31] – for example, autonomous penetration testing agents that continuously probe your systems for weaknesses, or AI assistants that interact with employees to coach them on security

best practices in real time. Encourage a culture of strategic foresight by envisioning "what-if" scenarios (e.g. *What if our SOC was 90% automated? What if AI could predict tomorrow's phishing tactics?*). Some experiments will fail, and over 40% of early agentic AI projects may be canceled by 2027 due to rising costs and complexity[32]. However, the lessons from these bold trials are invaluable. By incubating such ventures outside the pressures of day-to-day operations, you can discover new business models and capabilities ahead of competitors. Keep these experimental efforts insulated enough to take risks but ensure knowledge flows back into the core security team. The goal is to create an internal engine of AI-driven disruption before an external player does it for you.

4. **Forge Strategic AI & Cybersecurity Partnerships and Ecosystems:** No single organization can navigate the AI revolution and cybersecurity challenges alone. Build partnerships with AI-focused startups, vendors, research labs, and universities to gain early access to breakthroughs and specialized expertise[33]. For example, collaborate with startups working on advanced threat AI or join forces with cloud providers embedding security AI into their platforms. Such partnerships not only provide innovation insights but also influence emerging standards.

   Additionally, participating in open-source AI and cybersecurity communities[34] – contributing data, code, or research – to help shape the direction of AI in security. Many cutting-edge tools (from machine learning models for malware detection to frameworks for explainable AI decisions) are being developed in open collaborations. By engaging, your organization stays at the forefront and can rapidly scale investments and lessons learned across a broader ecosystem[35]. This step also means aligning with industry consortia or initiatives (such as the OWASP Agentic AI initiative or the NIST AI Risk Management Framework) to collectively address challenges like AI safety, ethics, and interoperability. A rich network of partnerships will amplify your capabilities and ensure you are influencing, not just observing, the next wave of disruption.

5. **Develop AI & Cybersecurity Governance and Human-in-the-Loop Frameworks:** As you deploy powerful AI agents in cybersecurity, it's critical to manage the risks that come with them. Develop robust AI governance frameworks that define how AI models are trained, tested, monitored, and controlled. This includes instituting oversight mechanisms such as regular bias and error audits of AI decisions, implementing "kill switches" or fallback plans for AI actions, and ensuring compliance with emerging AI regulations. A key aspect is maintaining transparency and trust – security teams should be able to explain an AI's reasoning for major decisions (e.g., why it quarantined a CEO's device or blocked a financial transaction) to avoid a "black box" crisis. As one tech CEO notes, success with agentic AI requires "accuracy and transparency… demonstrating the reasoning process and planned steps" so that humans maintain confidence[36]. Incorporate human-in-the-loop checkpoints for high-impact actions: even as AI runs autonomously, design your operations such that humans can step in during exceptions or emergencies. Training your staff is equally important – upskill analysts and engineers in data science and AI literacy so they can effectively manage and co-pilot these systems. By combining strong governance with skilled human oversight, you mitigate the ethical and safety risks, paving the way for sustainable AI-driven growth in cybersecurity.

6. **Prepare for AI-Enabled Cyber Threats and Invest in Data Resilience:** Finally, strategists must not only innovate with AI but also plan for adversaries who will do the same. The shockwave cuts both ways – if your industry is rethinking its offerings with AI, attackers are rethinking theirs too. Ensure your security strategy accounts for AI-enhanced threats: invest in AI-powered threat intelligence to spot emerging attack patterns (e.g. deepfake phishing campaigns or autonomous malware) and share these insights with the community. Scenario-plan for worst-case events like an AI agent gone rogue or a sophisticated attacker leveraging an army of bots. By war-gaming these scenarios, you can identify gaps in your defenses and resilience. Develop contingency plans (such as fallback manual

procedures if an AI system fails, or diversity in AI models to avoid single points of failure) to maintain operations under duress. Focus on building a cyber resilient architecture that can recover quickly – for instance, maintain offline backups, redundant AI systems, and robust disaster recovery drills for AI-driven components. The organizations that thrive in the post-AI era will be those that not only harness AI's power but also weather its potential misuses. Being candid about risks and staying agile in defense will ensure that your AI innovations do not inadvertently become new attack vectors. To truly be considered successful by organizations in both government and commercial sectors worldwide AI-powered cybersecurity or Security-as-a-Service must be focused on three key aspects: speed of security services, cost-effectiveness, and ensuring continuity of operations.

Conclusion: Embracing the Next Era of Cybersecurity

The emergence of agentic AI and the coming "post-productivity" shockwave present an inflection point for cybersecurity. Just as past technological revolutions forced shifts from old paradigms to new, AI's maturation will transform cybersecurity from today's labor-intensive, reactive modus operandi to a future state that is *intelligent, autonomous, and preventive*. Enterprise cybersecurity strategists should view this not with trepidation, but with optimism and urgency. By proactively applying AI to reinvent their value propositions, cost structures, and core offerings, cybersecurity leaders can deliver unprecedented levels of protection and resiliency for their organizations. The shockwaves built from the edges – the bold experiments and early adopters of today will set the standards for tomorrow[37].

Now is the time to champion forward-looking cybersecurity initiatives, to pilot new AI capabilities, and to reshape strategies around an AI-first mindset. Those who ride the wave of AI-driven innovation will help "rewrite industry rules and create new business ecosystems"[38] in cybersecurity, rather than being left behind. In the final analysis, embracing these AI shockwaves is not just about staying competitive – it's about fundamentally elevating our cyber defenses and seizing the opportunity to build a safer digital future for everyone. By planning with strategic foresight and taking bold action today, enterprises can turn the looming AI disruption into a lasting strategic advantage in cybersecurity.

About the Authors

Gregory A. Garrett is the Chief Operating Officer of Converged Security Solutions (CSS), leading expert teams within business units Evolver and eVigilant. These groups provide advanced IT, AI, cybersecurity, electronic security, and eDiscovery services to federal agencies and Fortune 500 companies. With over 25 years of executive experience and a background as a CIO, CTO, CISO, and COO, he has managed more than $40 billion in global tech contracts and served in key roles across both large and mid-sized firms. A retired U.S. Air Force Colonel and accomplished author, Garrett has also contributed extensively to industry thought leadership through 24 books, more than 150 articles, expert testimony, and over 250 speaking engagements.

Dr. Brian McElyea is an accomplished cybersecurity executive recognized for leading large-scale digital transformation initiatives and building high-performing Cyber Centers of Excellence that drive mission-aligned security outcomes. With over two decades of leadership across healthcare, defense, and federal sectors, he has guided global organizations through the complexities of risk management, compliance, and modernization with measurable results.

Sources

1. The Future of AI: What Comes After AI for Productivity [1] [2] [3] [9] [12][30] [31] [33] [34] [35] [36] [37] [38]
   https://www.gartner.com/en/articles/ai-shockwaves
2. Indian Strategic Studies: To defend against malicious AI, the United States needs to build a robust digital immune system [4] [5] [6]
   https://www.strategicstudyindia.com/2025/08/to-defend-against-malicious-ai-united.html
3. What Is Agentic AI? Definition | Proofpoint US [7] [10] [11] [12] [13] [14] [15] [16] [17] [20] [21]
   https://www.proofpoint.com/us/threat-reference/agentic-ai
4. The impact of AI on cybersecurity | McKinsey [8]
   https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer
5. Early Disruptive Trends in Cybersecurity: Preemptive Cybersecurity Solutions - Skyhawk Security [18] [19]
   https://skyhawk.security/early-disruptive-trends-in-cybersecurity-preemptive-cybersecurity-solutions/
6. 5 trends reshaping IT security strategies today | CSO Online [22] [23] [26] [27]
   https://www.csoonline.com/article/4054295/5-trends-reshaping-it-security-strategies-today.html
7. Agentic AI Security: OWASP Threats and How to Defend Against Them [24] [25] [28] [29]
   https://www.humansecurity.com/learn/blog/agentic-ai-security-owasp-threats/
8. Why over 40% of agentic AI projects will fail – and which will survive [32]
   https://trullion.com/blog/why-over-40-of-agentic-ai-projects-will-fail/
9. Experts Reveal How Agentic AI Is Shaping Cybersecurity in 2025[36]
   https://www.securityjourney.com/post/experts-reveal-how-agentic-ai-is-shaping-cybersecurity-in-2025