TELARUS

Cybersecurity & AI:
A Growth Playbook for MSPs

How MSPs can Strengthen Security, Deepen Customer Engagement, and Unlock New Revenue Streams

Published July 2025

Introduction

A cybersecurity arms race is developing, with companies ramping up their defenses to keep pace with AI-driven threat actors. According to Capgemini, 61% of companies now view AI as essential for threat response while an equal share believe gen AI will enhance proactive defense strategies over the long-term.[1]

But as businesses move quickly to integrate AI into their security stacks, many are doing so without critical safeguards or supporting internal resources—putting them at risk for costly attacks. A recent F5 report found that while 71% of companies are now using AI, just 2% are highly ready for it, and often lack key elements like AI firewalls and continuous data labeling.[2]

As an MSP, you have a clear opportunity to step in and act as strategic cybersecurity partners. With your security expertise, you are well-positioned to help your customers navigate the complex threat landscape and align their AI deployments with resilient, secure cybersecurity frameworks.

You can also use cybersecurity to deliver clear business value, by building secure and resilient networks that can support emerging technologies and help drive ROI. Having a strong security foundation will ensure business continuity, support regulatory compliance, and enable companies to innovate and expand with confidence.

Read on to discover the key trends and opportunities around AI in cybersecurity, including practical use cases, governance considerations, and common blind spots. We'll also highlight steps that you can take to help customers develop cyber-resilient environments, while using AI security services as a path to deeper client engagement and new revenue streams.

Key AI Opportunities in Cybersecurity Today

The threat landscape is more dangerous and unpredictable than ever, with adversaries now using cutting-edge tools and large language models to execute sophisticated attacks. In fact, Gartner predicts that by 2027, 17% of all cyberattacks will involve generative AI. [3]

As cyber threats evolve in scale, speed, and sophistication, businesses are shifting from reactive security models to AI-first cyber defense strategies. According to Deloitte, companies are increasingly leveraging AI to analyze historical threat data, automate security processes, accelerate incident response, and enable continuous infrastructure monitoring. AI is also being used to process real-time data, understand complex threat relationships, and identify emerging attack vectors.[4]

It's not just the large enterprises who are embracing AI. SMBs are getting on board as well. In a Verizon study, 25% of SMBs said they are now using AI to boost their cybersecurity efforts. Meanwhile, a quarter of SMBs don't believe their business is investing enough in cybersecurity—highlighting a clear opportunity for growth.[5]

Key AI opportunities in cybersecurity currently include:

- **Deepfake & synthetic media identification:** Detecting suspicious content in phishing, fraud, and disinformation attacks before they reach end-users.
- **Penetration testing:** Simulating attacks to identify vulnerabilities and prioritize remediation.
- **Risk-adaptive multi factor authentication (MFA):** Adjusting authentication requirements based on user behavior and threat signals.
- **Post-quantum encryption:** Preparing for future cryptographic threats by developing AI-assisted quantum-resistant algorithms.
- **AI security copilots:** Streamlining investigation workflows and accelerating SOC response times.
- **Behavioral biometrics:** Continuously analyzing user behavior patterns to detect anomalies and prevent account compromise.

Five Key Cybersecurity Trends to Watch

1. **Proactive Security**

   MSPs are shifting away from reactive defense in favor of proactive cybersecurity strategies that anticipate and neutralize threats before they cause harm.

   This approach involves using tools like autonomous threat containment, AI-generated threat detection, behavioral biometrics, AI security copilots, and risk-adaptive MFA to stay ahead of evolving risks and minimize response times.

2. **Autonomous SOCs**

   Traditional security operations centers (SOCs) are evolving, with companies increasingly relying on AI-driven threat detection and response systems that operate 24/7. These new AI-driven SOCs can rapidly identify and neutralize threats with minimal human intervention.

   Looking forward, expect AI to analyze logs, triage incidents, and even quarantine devices in real-time—saving security teams time and allowing them to do more with less.

3. **Identity Fabric and Decentralized Access**

   In today's perimeter-less world, identity becomes the new control plane. Identity fabric solutions unify user, device, and workload identities across clouds, endpoints, and edge networks. This cohesive layer enables secure access no matter where resources live.

   Building on that foundation, Zero Trust is evolving into Adaptive Trust, where behavioral AI analyzes real-time signals such as login patterns and location to assess risk and adjust access dynamically. This shift illustrates how AI enhances cybersecurity by enabling context-aware decisions, not static rules.

4. **Quantum-Resilient Encryption**

   Quantum computing threatens to break today's encryption standards. The race is on to deploy post-quantum cryptography, with cloud-native platforms and AI pipelines already starting to adopt hybrid crypto models.

   Staying ahead of quantum threats is critical to long-term data integrity and trust.

5. **AI-Powered Insider Threat Detection**

   AI can now detect subtle insider threats such as abnormal login times, unusual data access, or changes in tone during communications. These tools are reshaping risk management across finance, healthcare, and critical infrastructure—and allowing companies to thwart attacks before they lead to costly breaches.

   Behavioral analytics replace manual, time-consuming audits for faster, smarter threat detection.

How You Can Help with Governance

As organizations integrate AI into their environments, they must also implement comprehensive governing frameworks to avoid introducing new risks. However, a survey from Gartner reveals that just 12% of IT and data and analytics leaders have a dedicated AI governance framework in place—leaving them vulnerable to risks like ethical concerns, data privacy violations, and compliance failures.[6]

You have an opportunity to help navigate governance frameworks by:

- **Defining AI principles:** Establishing core values such as trust, transparency, fairness, safety, and explainability.
- **Developing enforceable policies and procedures:** Creating guidelines around how AI systems are built, developed, deployed, and maintained, including data handling, bias mitigation, and security protocols.
- **Establishing accountability:** Clarifying roles and responsibilities to ensure that individuals or groups are held accountable for the actions and decisions of AI systems.
- **Providing monitoring and auditing:** Implementing regular reviews to verify AI performance, policy adherence, and risk mitigation.
- **Delivering training and education:** Equipping employees with the insights to use AI safely and responsibly.

Proven Cybersecurity Conversation Starters

For MSPs, the challenge lies in getting customers to think proactively about their networks and identify weaknesses or vulnerabilities before they lead to costly incidents. This is also an effective way to drive additional sales and increase customer "stickiness."

Consider the following questions to initiate impactful cybersecurity discussions with your customers:

- **Are you confident about the integrity of your AI models and data?** Threat actors are beginning to manipulate input data and AI models to deceive systems into making flawed decisions. These attacks, which can be difficult to detect, can create harmful outputs and compromise system security.
- **Do you have full visibility across your supply chain?** Compromised AI systems can introduce downstream threats that impact all parties within a supply chain. By conducting routine security audits for third-party AI systems, companies can improve visibility and reduce risks from adversarial attacks and reduce the potential for model poisoning.
- **Are all your APIs securely configured and audited?** Application programming interfaces (APIs) are necessary for sharing data and connecting systems. However, they can provide easy entry for bad actors. Strong encryption, access controls, and authentication are critical.
- **Have you recently tested your incident response plan?** All organizations will eventually experience cyberattacks and data breaches. Having a clear, tested response strategy in place is key for containing damage and reducing recovery times.

Telarus: Your Ally for Cybersecurity Growth

There's never been a better time for MSPs to lean into technology advisory. Global spending on technology consulting is expected to grow by 7% to over $421 billion this year, with 79% of technology buyers expecting to use more consulting services.[7] Companies across all industries are actively seeking trusted advisors who can help them navigate evolving threats and achieve their business goals.

Here at Telarus, we have everything that you need to thrive in your cybersecurity practice, including:

- **World-class engineering and advanced solutions teams** to help identify and seize new opportunities.
- **Telarus Hub,** an all-in-one business platform that makes it fast and easy to connect with AI suppliers, track commissions, and grow your business.
- **Deep education, resources, and supplier guidance** around innovative AI technologies.

Telarus helps hundreds of MSPs to easily expand their capabilities and become trusted technology advisors for customers, without adding additional headcount—paving the way for faster IT solution evaluation and selection that solves critical business needs.

To learn more, schedule some time with a Telarus MSP Specialist today.

www.telarus.com/msp-campaign

Sources

1. “AI and Gen AI are set to transform cybersecurity for most organizations.” Capgemini, Nov. 2024.
   https://www.capgemini.com/news/press-releases/ai-and-gen-ai-are-set-to-transform-cybersecurity-for-most-organizations/?utm_source=chatgpt.com

2. “A quarter of applications now include AI, but enterprises still aren't ready to reap the benefits.” TechRadar. July 2025.
   https://www.techradar.com/pro/a-quarter-of-applications-now-include-ai-but-enterprises-still-arent-ready-to-reap-the-benefits?utm_source=chatgpt.com

3. “Gartner Forecasts Global Information Security Spending to Grow 15% in 2025.” Gartner, Aug. 2024.
   https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

4. “Global Future of Cyber Survey, 4th Edition.” Deloitte, 2024.
   https://www.deloitte.com/ce/en/services/consulting-risk/research/global-future-of-cyber.html

5. “2025 State of Small Business Survey: Surge in AI, cybersecurity and social media demand.” Verizon, May 2025.
   https://www.verizon.com/about/news/2025-state-small-business-survey

6. “AI Governance Frameworks For Responsible AI.” Gartner, March 2023. “AI Governance Frameworks For Responsible AI.” Gartner, March 2023.
   https://www.gartner.com/peer-community/oneminuteinsights/omi-ai-governance-frameworks-responsible-ai-33q

7. “Tech consulting spend to hit $421bn in 2025 as digital transformation projects drive demand.” Management Today. January 2025.
   https://www.managementtoday.co.uk/tech-consulting-spend-hit-421bn-2025-digital-transformation-projects-drive-demand/indepth/article/1902113