7AI

THE AGENTIC SECURITY REVOLUTION: HOW AI IS TRANSFORMING CYBERSECURITY

CONTENTS

CONTENTS

1 DEFINING "AGENTIC AI" AND "AGENTIC SECURITY"

WHAT IS AGENTIC AI?

Agentic AI refers to systems that can make decisions and taking actions without the need for continuous human oversight. These systems are designed to operate autonomously, learning from their environment and adapting their behavior based on new information. Unlike conventional AI models that require human input to process tasks, agentic AI can analyze vast amounts of data and execute decisions on its own.

The key characteristics of agentic AI include:

AUTONOMY The system can function without human input, executing tasks in real time.

ADAPTABILITY Agentic AI can adjust its behavior based on new data, adapting to threats or changes in the environment.

LEARNING These systems can learn from past actions and improve over time, leading to smarter, more efficient decisions.

HOW AGENTIC AI RELATES TO CYBERSECURITY

In the cybersecurity space, agentic AI doesn't replace existing detection systems like email security, EDR (Endpoint Detection and Response), or vulnerability scanning tools. Instead, it enhances their value by processing alerts from these systems and autonomously acting based on the insights provided.

For example, when an email security tool flags a potential phishing email, agentic AI steps in to analyze the alert, investigate its context across different systems, and decide on an appropriate response, such as isolating the account or blocking future emails from the source. By doing this, agentic AI removes the burden of manually investigating and responding to alerts, allowing human analysts to focus on higher-order tasks.

WHAT IS AGENTIC SECURITY?

Agentic security is the application of agentic AI in the cybersecurity domain, using AI to handle alert responses from existing detection systems without the need for human intervention. Instead of simply detecting threats on its own, agentic security systems take input from external sources such as EDR platforms, threat intelligence feeds, and email security systems, and then carry out investigations, come to conclusions, and implement mitigations or responses.

For instance, after receiving an alert from a vulnerability scanner that highlights an unpatched system, an agentic security platform might autonomously review the potential impact, correlate it with other security intelligence, and then either recommend or carry out remediation steps—such as applying a patch or isolating the vulnerable system. This end-to-end automation allows for a faster, more efficient response to potential threats.

By taking alerts from a variety of systems and acting on them, agentic security optimizes the use of existing security infrastructure.

2 THE THREATS AND OPPORTUNITIES AI BRINGS TO CYBERSECURITY

AI-DRIVEN ATTACKS: THE DARK SIDE OF AI'S POTENTIAL

As AI becomes more accessible, it's not only being adopted by defenders but also by attackers who can use it to automate and scale their operations. **The ability to generate and execute sophisticated attacks using AI is becoming a reality**, increasing the number of threats that cybersecurity teams must contend with. However, most security breaches begin with something as simple as an alert from a detection system—an EDR flagging an unusual process, or a vulnerability scanner identifying a critical patch that needs attention.

For example, AI-generated phishing attacks are a growing concern. AI can craft realistic phishing emails based on the social media data of a targeted user, making the messages more personalized and harder to detect. While email security tools can identify many of these threats, alert fatigue can set in, making it difficult for human teams to investigate and mitigate every threat.

Additionally, AI-enhanced malware can dynamically alter its behavior to evade detection. Threat intelligence platforms often catch these advanced threats, but generating alerts isn't enough. It's here where agentic security can take over—analyzing the alerts generated by detection systems and autonomously investigating the full scope of the threat.

AI AS A DEFENSIVE TOOL: USING ALERTS FROM EXISTING SYSTEMS

While attackers can leverage AI, defenders have access to AI systems that can process and respond to alerts generated by various cybersecurity tools. **AI has the potential to alleviate the burden of alert fatigue**, where security teams are overwhelmed by the volume of alerts coming from different systems such as EDR, email security, and vulnerability scanners. Agentic security doesn't just detect threats on its own—it uses the alerts from these systems and acts on them quickly.

For example, an EDR might flag a suspicious process running on a device. Instead of relying on a human analyst to investigate, the agentic security system automatically analyzes the context of the alert, correlates it with other data, and decides whether to quarantine the device, block the process, or trigger additional investigation steps across other tools like SIEM (Security Information and Event Management).

Agentic security platforms can seamlessly process alerts from email security systems, identifying phishing attacks, isolating affected accounts, and preventing further malicious activity without human involvement. This helps cybersecurity teams get out of a reactive cycle and into a proactive, automated security posture.

CASE STUDY: HOW AGENTIC SECURITY STREAMLINES THREAT RESPONSE

Consider a scenario where a vulnerability scanner flags an unpatched critical system, and at the same time, an EDR tool flags unusual behavior on an endpoint. These are typically handled by separate teams, each generating alerts that need to be triaged. With agentic security, AI can correlate these two seemingly unrelated events, identify that the unpatched system and the affected endpoint are connected, and then automatically apply patches or isolate the compromised devices without needing human intervention.

By receiving alerts from multiple systems, investigating correlations, and acting, agentic security bridges the gaps that manual processes leave behind.

BALANCING THE SCALES: THE OPPORTUNITY AND THREAT AI POSES

AI is both a threat and an opportunity in the cybersecurity space. Attackers use AI to automate large-scale, sophisticated attacks, but defenders now have agentic security at their disposal to handle the deluge of alerts from existing detection systems. This shift enables defenders to act more quickly and effectively, ensuring that critical threats are dealt with before they can cause widespread damage.

In the next chapter, we will explore why the manual approaches to cybersecurity we've relied on won't be sufficient in an era of exponential change and how agentic security presents a viable solution for the future.

3 THE CHALLENGE OF ITERATIVE PROGRESS IN AN ERA OF EXPONENTIAL CHANGE

EXPONENTIAL TECHNOLOGICAL GROWTH AND ITS IMPACT ON CYBERSECURITY

The pace of technological change has accelerated rapidly over the last few decades, bringing us into an era where exponential growth is the new norm. Moore's Law predicted that computing power would double every two years, but today, innovations like AI, cloud computing, and quantum computing are pushing growth far beyond traditional expectations. **This accelerated development has created a paradox for cybersecurity** professionals: while technology is advancing at an unprecedented rate, the systems and processes we've relied on for cybersecurity have only seen iterative improvements.

Historically, cybersecurity has been reactive, relying on human teams to deploy patches, respond to alerts, and manually address threats as they arise. Over time, incremental changes—such as improved firewalls or more sophisticated malware detection systems—have helped maintain some level of defense. But in a world where AI-driven attacks are happening at machine speed, iterative improvements can no longer keep up.

The manual, time-consuming nature of traditional cybersecurity methods is a significant bottleneck. Security operations teams are often overwhelmed by the sheer volume of alerts and the complexity of identifying and mitigating new threats. In fact, it's estimated that over 70% of security professionals experience alert fatigue, which reduces their ability to respond effectively.

WHY MANUAL EFFORTS WON'T CUT IT ANYMORE

Manual, human-centered processes in cybersecurity have always struggled to keep pace with the increasingly sophisticated tactics of attackers. Now, **the gap between these processes and modern threats has widened** even further due to exponential technological growth. Traditional approaches to cybersecurity—based on signatures, manual investigations, and human-led responses—are simply too slow, too limited in scope, and too error-prone to handle the current landscape.

1. VOLUME OF ALERTS: Security systems today generate an overwhelming number of alerts, far too many for any human team to manage. Threat intelligence platforms, EDR systems, and vulnerability scanners are vital, but they often overwhelm security teams with notifications of potential threats that require investigation.

2. SPEED OF ATTACKS: With the rise of AI-enhanced attacks, cyber threats now operate at machine speed. An AI-driven malware strain can infect hundreds of systems before human teams even have a chance to begin their investigation. Human response times are simply no match for the automated systems attackers are employing.

3. COMPLEXITY OF THREATS: Cyber threats are no longer isolated to single attacks or malware instances. Today's adversaries use multi-vector attacks, combining phishing, malware, data theft, and network infiltration. Investigating these complex, interwoven threats requires a level of speed and scale that humans simply cannot achieve.

These challenges are exacerbated by the fact that **cyber defense traditionally relies on human-led, manual interventions** at every step of the process—from alert triage to investigation, mitigation, and response. As technology continues to evolve exponentially, this approach becomes less and less feasible.

WHY ITERATIVE IMPROVEMENTS WON'T BE ENOUGH

Cybersecurity innovations to date have often been iterative, meaning each new solution builds incrementally on previous versions. Firewalls become smarter, antivirus software adds more signatures, and vulnerability scanners improve at identifying weaknesses. But the speed at which threats evolve far outpaces the gradual improvements of these tools.

In this context, iterative progress is no longer sufficient:

PATCH-AND-RESPOND MODELS: Organizations are stuck in a loop of applying patches after vulnerabilities are exposed. This reactive approach cannot keep pace with the discovery of zero-day vulnerabilities, and organizations are often still exposed during the critical window between vulnerability disclosure and patch deployment.

MANUAL TRIAGE: Even as tools improve, security operations centers (SOCs) still rely on analysts to manually review alerts, which results in slow and inconsistent responses. As the number of devices, applications, and potential attack surfaces increases exponentially, SOCs become overwhelmed by the volume of alerts.

INCIDENT RESPONSE TIMES: The more sophisticated the attack, the longer it takes to analyze and respond to it. Traditional response models simply cannot keep up when attackers are using AI to automate their offensive strategies.

To address these issues, a new approach is required—**one that scales as quickly as threats and can respond to them in real-time**.

HOW AGENTIC SECURITY SOLVES THE CHALLENGE

Agentic security presents a paradigm shift by moving away from manual, iterative processes to a more automated, intelligent approach. By leveraging AI to act based on alerts from various cybersecurity systems—such as EDR, email security, threat intelligence, and vulnerability scanners—agentic security transforms how organizations detect and respond to threats.

Here's how agentic security addresses the challenges of exponential change:

1. AUTOMATING RESPONSE: Instead of relying on human teams to triage, investigate, and mitigate threats, agentic security systems process alerts from detection tools and act on them autonomously. This drastically reduces the time between detection and response, allowing organizations to neutralize threats before they cause significant damage.

2. SCALING AT MACHINE SPEED: While humans can only handle so many alerts at once, agentic security can scale indefinitely, managing thousands or even millions of alerts simultaneously across different systems. By offloading repetitive tasks to AI, security teams can focus on strategic analysis and decision-making.

3. CONTEXTUAL INVESTIGATION: Agentic AI systems don't just respond to individual alerts in isolation; they analyze them in the context of broader activity. For example, an EDR alert might indicate a suspicious process on a single endpoint, but agentic security systems will also pull in data from other sources, like threat intelligence feeds, to provide a comprehensive understanding of the threat and take action accordingly.

4. SPEED AND PRECISION: With AI handling investigations and responses, the organization gains a significant speed advantage. A process that might take a human analyst hours—such as investigating an alert, correlating it with other alerts, and executing a remediation plan—can be done by agentic AI in seconds.

By automating responses to alerts from multiple systems, agentic security ensures that organizations can finally keep pace with the rapid evolution of cyber threats.

The era of exponential technological change has exposed the weaknesses of traditional, manual cybersecurity approaches. Iterative improvements are no longer sufficient to meet the speed, scale, and complexity of modern cyber threats. Organizations need to embrace agentic security, which leverages AI to automate responses and handle the volume of alerts that today's security tools generate.

In the next chapter, we will dive into specific use cases where agentic security demonstrates its effectiveness—such as email security, EDR, and vulnerability management—showing how these systems work together to create a seamless, automated security solution.

4 HOW AGENTIC SECURITY WORKS— USE CASES

Agentic security is more than just an idea; it represents a transformative shift in how security operations handle alerts, investigate incidents, and execute responses. By leveraging existing systems like EDR, email security, vulnerability scanners, and threat intelligence feeds, agentic security doesn't replace these tools but amplifies their effectiveness. This chapter will explore specific use cases where agentic security excels, from handling email threats to streamlining endpoint detection and response, demonstrating its real-world impact.

USE CASE 1: AUTOMATING EMAIL SECURITY RESPONSES

Email continues to be one of the primary attack vectors for cybercriminals, with phishing being the most common form of attack. Organizations often deploy advanced email security systems to detect phishing emails and other malicious attachments, but these tools still generate a significant number of alerts that require manual investigation and response.

With agentic security, the process looks different:

1. ALERT CORRELATION: When an email security system flags a suspicious email, agentic security takes over by correlating that alert with other relevant data, such as the recipient's behavioral patterns, related endpoints, and any known threat intelligence.

2. AUTONOMOUS INVESTIGATION: The agentic security platform investigates the email, checking for signs of phishing, malware, or malicious intent by cross-referencing threat intelligence feeds.

3. AUTOMATED RESPONSE: Based on the investigation, the system can autonomously isolate the account, block the email source, and prevent further emails from the malicious sender—all without human involvement. It can even notify the user of the action taken and provide a summary of the response.

By handling the entire process—from alert to remediation—agentic security drastically reduces the time to respond and eliminates the risk of human error in phishing mitigation.

USE CASE 2: STREAMLINING ENDPOINT DETECTION AND RESPONSE (EDR)

Endpoint Detection and Response (EDR) tools are vital for identifying suspicious activity on individual devices within a network. However, the sheer volume of alerts generated by EDR systems often overwhelms security teams, making it difficult to respond quickly and effectively.

Agentic security offers a solution by taking input from EDR systems and handling much of the investigation and response automatically:

ALERT MANAGEMENT: When the EDR tool flags an anomaly, such as a suspicious process running on a device, agentic security takes the alert and begins its own investigation.

CROSS-TOOL INTEGRATION: Instead of investigating the alert in isolation, agentic security pulls data from other sources, such as vulnerability scanners or SIEMs, to build a fuller picture of the threat. This gives it the context to make a more informed decision.

REMEDIATION: Based on the findings, the agentic security system can automatically isolate the compromised device, terminate the suspicious process, and even trigger patches if a known vulnerability is involved. It can do all of this without waiting for human intervention, allowing for rapid response to even complex endpoint threats.

This use case highlights how agentic security optimizes EDR tools by speeding up the time between detection and response while ensuring no critical alerts are missed.

USE CASE 3: AUTOMATING THREAT INTELLIGENCE PROGRAMS

Threat intelligence feeds are essential for staying ahead of emerging threats, but they often flood security teams with more information than they can process. It's common for organizations to struggle with integrating threat intelligence into actionable responses, leaving many threats unaddressed.

Here's how agentic security changes that:

REAL-TIME INTEGRATION: Agentic security systems continuously ingest and process threat intelligence feeds, correlating them with alerts from other tools such as email security or EDR.

AUTOMATED INVESTIGATION: When a threat is detected, agentic security investigates the alert in the context of existing threat intelligence, identifying known tactics, techniques, and procedures (TTPs) associated with the threat actor.

PRESCRIBING ACTION: The system autonomously prescribes or executes the appropriate response. For example, if the threat intelligence feed indicates that a particular malware strain is circulating, the agentic security platform can identify all endpoints at risk, quarantine them, and begin the patching process—all without human oversight.

This use case shows how agentic security can take what was once a reactive process (reviewing threat intelligence after an attack) and turn it into a **proactive, automated defense strategy.**

USE CASE 4: VULNERABILITY MANAGEMENT AT SCALE

Vulnerability scanning is critical for identifying weaknesses within an organization's infrastructure. But even when vulnerabilities are identified, the manual process of prioritizing, patching, and responding to them creates delays that leave organizations exposed.

Agentic security helps by automating the response to vulnerability alerts:

ALERT PROCESSING: When a vulnerability scanner identifies an unpatched system or weak configuration, the agentic security platform processes the alert and cross-references it with known exploits, vulnerability severity, and the current threat landscape.

AUTOMATED PRIORITIZATION: The platform then automatically prioritizes the vulnerability based on the potential impact and whether active exploits are being used against it in the wild.

PATCH MANAGEMENT: Agentic security can autonomously trigger the patching process, ensuring that critical vulnerabilities are addressed immediately. For vulnerabilities requiring more complex remediation, it can generate detailed action plans for the security team to follow.

This use case highlights the power of agentic security in reducing the time between vulnerability discovery and resolution, while also ensuring the most critical vulnerabilities are dealt with first.

These use cases demonstrate how agentic security can be applied across different areas of cybersecurity to enhance existing systems and automate responses to threats. Whether it's handling email security, EDR, threat intelligence, or vulnerability management, agentic security empowers organizations to respond faster and more efficiently, allowing human teams to focus on higher-level tasks.

5 WHY 7AI IS UNIQUELY POSITIONED TO BUILD THE FIRST AGENTIC SECURITY PLATFORM

THE EXPERTISE AND BACKGROUND OF THE 7AI TEAM

Building the first fully agentic security platform requires more than just ambition—it demands deep expertise in both AI and cybersecurity. 7AI is uniquely positioned for success because of the combined experience of its leadership and technical teams, who have spent years at the forefront of AI development and security innovation.

Key team members include individuals who have:

PIONEERED AI RESEARCH at leading technology companies, contributing to foundational breakthroughs in autonomous systems.

LED CYBERSECURITY OPERATIONS at some of the world's most targeted organizations, gaining firsthand experience in defending against sophisticated, state-sponsored attacks.

BUILT SUCCESSFUL AI PLATFORMS in adjacent industries, giving 7AI the benefit of a robust, well-tested technological foundation.

With decades of experience, this team understands the unique challenges that modern security teams face and is well-equipped to design an agentic security platform that can work seamlessly alongside existing security infrastructure. Their expertise ensures that 7AI can create a system that not only automates responses to alerts but does so in a way that integrates with and enhances the tools organizations are already using.

LIOR DIV CO-FOUNDER AND CEO

Lior Div is a seasoned cybersecurity expert with extensive experience in both the private sector and military intelligence. As the co-founder and CEO of Cybereason, he has helped transform the company into a global leader in endpoint detection and response (EDR). His background in Israeli military intelligence, where he specialized in cyber operations, gives him a deep understanding of threat landscapes and how to combat them. Lior's proven track record of building successful cybersecurity companies and his visionary leadership make him uniquely suited to guide 7AI in pioneering the agentic security revolution.

YONATAN STRIEM AMIT CO-FOUNDER AND CTO

As co-founder and Chief Technology Officer of Cybereason, Yonatan Striem Amit is a brilliant technologist with deep expertise in AI and machine learning applied to cybersecurity. He has overseen the development of advanced AI-driven security platforms capable of detecting and mitigating threats in real time. With his background in system design and big data analytics, Yonatan's technical acumen is crucial for developing 7AI's agentic security platform, which relies on the automation of complex security operations across vast data sets.

ALLEN LIEBERMAN CHIEF PRODUCT OFFICER

Allen Lieberman is a highly experienced product leader with a track record of developing and scaling innovative cybersecurity products. As Chief Product Officer at 7AI, he drives product strategy and innovation, ensuring that 7AI's agentic security platform meets the needs of modern organizations. Previously, Allen was CPO at Tessian, where he led AI-driven email security solutions and oversaw the company's acquisition by Proofpoint. His earlier roles at VMware Carbon Black, where he led product management for endpoint security, give him deep expertise in cloud security and product execution.

NATHAN BURKE CHIEF MARKETING OFFICER

Nathan Burke is an accomplished marketing leader with deep experience in the cybersecurity industry. He has previously held senior leadership roles at Axonius, Hexadite (acquired by Microsoft), and CloudLock (acquired by Cisco), where he successfully launched innovative security solutions and built strong brands. Nathan's expertise in bringing cutting-edge technologies to market makes him uniquely suited to lead 7AI's marketing efforts, focusing on scaling the company's brand and establishing it as the leader in agentic security.

STRATEGIC PARTNERSHIPS WITH INDUSTRY LEADERS

7AI's strategic partnerships with leading technology companies set it apart from other emerging players in the cybersecurity space. These partnerships enable 7AI to leverage cutting-edge advancements in AI and computing power, which are critical to building a platform that can process millions of security alerts in real time.

NVIDIA: As a global leader in GPU technology, NVIDIA provides 7AI with access to the powerful, high-performance computing capabilities required for AI-driven cybersecurity. GPUs are essential for handling the massive data processing tasks involved in analyzing alerts, correlating threat intelligence, and automating responses. With NVIDIA's advanced GPUs and AI frameworks, 7AI is able to scale its platform quickly, ensuring that organizations of any size can benefit from agentic security.

OPENAI: 7AI's collaboration with OpenAI brings state-of-the-art natural language processing (NLP) capabilities to the platform. This allows 7AI to process and understand complex threat intelligence, correlate data across different sources, and even generate reports or communications that explain the nature of detected threats. By integrating OpenAI's models, 7AI can enhance its ability to handle the language-heavy components of cybersecurity, such as phishing detection and alert triage.

These partnerships aren't just technological—they also include joint research efforts that ensure 7AI stays ahead of the curve when it comes to emerging threats and innovative solutions. By working closely with industry leaders like NVIDIA and OpenAI, 7AI has the resources and expertise to develop a next-generation security platform.

FUNDING AND SUPPORT FROM GREYLOCK PARTNERS

A crucial advantage for 7AI is the strong backing of Greylock Partners, one of Silicon Valley's most prominent venture capital firms. Greylock's investment in 7AI not only provides the financial resources to accelerate development but also brings decades of experience in scaling disruptive technologies.

Greylock has a track record of investing in successful, high-growth technology companies, and their involvement signals confidence in 7AI's potential to become the leader in agentic security. This backing gives 7AI the ability to move quickly and decisively as it brings the first agentic security platform to market.

6 THE 7AI AGENTIC SECURITY PLATFORM: BUILT TO HANDLE MODERN SECURITY CHALLENGES

At its core, the 7AI platform is designed to address the most pressing challenges faced by modern security teams:

ALERT OVERLOAD: Security teams are overwhelmed by the volume of alerts generated by EDR tools, email security systems, and threat intelligence feeds. The 7AI platform alleviates this burden by automating alert triage, investigation, and response, freeing up human analysts for higher-level decision-making.

SPEED OF RESPONSE: Cyberattacks are happening faster than ever before. The 7AI platform operates at machine speed, enabling organizations to neutralize threats before they cause significant damage. By automating responses, 7AI ensures that no critical alert slips through the cracks.

SCALABILITY: Whether an organization is a small business or a multinational enterprise, the 7AI platform can scale to meet their needs. By leveraging NVIDIA's GPU technology and OpenAI's models, the platform can process millions of alerts simultaneously, ensuring that even the largest organizations can maintain robust security without overwhelming their human teams.

7AI isn't a replacement for existing security tools—it's a force multiplier. The platform integrates seamlessly with popular EDR, email security, threat intelligence, and vulnerability scanning systems, allowing organizations to leverage their current security investments while enhancing their capabilities through agentic AI.

7 THE FUTURE OF SECURITY: JOIN THE AGENTIC SECURITY REVOLUTION

7AI is at the forefront of the agentic security revolution, and the timing couldn't be more perfect. Cyber threats are evolving at an alarming rate, and traditional security approaches simply aren't keeping up. The 7AI platform represents a paradigm shift in how organizations can defend themselves against modern attacks—by harnessing the power of agentic AI to automate and accelerate their security operations.

For those who want to be part of something revolutionary, 7AI offers two distinct opportunities:

PROSPECTIVE EMPLOYEES: Join a team that is building the future of cybersecurity. 7AI is recruiting talented engineers, AI researchers, and security professionals who want to work on the next big thing in AI-driven defense. Be part of a fast-paced, innovative environment where you can shape the future of security.

PROSPECTIVE CUSTOMERS: Help build something truly revolutionary. By partnering with 7AI, early customers can work closely with our team to customize and enhance the platform, ensuring it meets the specific needs of their organization. Join us in setting the new standard for cybersecurity and become part of the first wave of companies to embrace agentic security.

With the backing of industry giants like Greylock Partners, strategic partnerships with NVIDIA and OpenAI, and a leadership team with unparalleled expertise in AI and cybersecurity, 7AI is uniquely positioned to build the first agentic security platform. The future of cybersecurity is here, and 7AI is leading the charge.

In the final chapter, we'll explore how **both employees and customers can become part of this exciting journey**, contributing to and benefiting from the agentic security revolution.

8 HOW TO JOIN THE AGENTIC SECURITY REVOLUTION

The agentic security revolution is more than just a technological shift—it's **an entirely new way of thinking about how organizations defend themselves** against cyber threats. As 7AI builds the first fully agentic security platform, the company is inviting both prospective employees and customers to join this transformative movement.

FOR PROSPECTIVE EMPLOYEES: BUILDING THE FUTURE OF SECURITY

If you are passionate about cybersecurity and want to work at the cutting edge of technology, 7AI offers the chance to be part of something groundbreaking. At 7AI, you won't just be developing another tool—you'll be part of a team that is redefining how organizations protect themselves in the age of AI.

Here's why you should consider joining 7AI:

INNOVATIVE TECHNOLOGY: Work on the most advanced AI-driven platform in the cybersecurity space.

COLLABORATIVE ENVIRONMENT: Be part of a highly talented team with deep expertise in AI and security.

IMPACTFUL WORK: Help build tools that have the potential to revolutionize how companies defend themselves against cyberattacks.

GROWTH OPPORTUNITIES: Be part of a rapidly scaling company, backed by industry leaders and venture capital from Greylock Partners.

At 7AI, you will have the opportunity to shape the future of cybersecurity and be part of a revolution that is changing the way organizations protect their most valuable assets.

FOR PROSPECTIVE CUSTOMERS: SHAPE THE FUTURE OF SECURITY

As an early customer of 7AI, you have the unique opportunity to partner with us in **building the next frontier of cybersecurity**. By working closely with 7AI, you can ensure that your security challenges are addressed with the most advanced AI-driven automation platform available.

Why partner with 7AI?

ENHANCED SECURITY POSTURE: Agentic security ensures that your organization can handle alerts from various systems quickly and autonomously, reducing the burden on your security teams.

FASTER RESPONSE TIMES: With AI-driven automation, your organization can respond to threats in real-time, minimizing the risk of breaches.

CUSTOMIZABLE SOLUTIONS: As an early adopter, you can work directly with 7AI to shape the platform to meet your specific needs, ensuring it delivers maximum value for your organization.

THOUGHT LEADERSHIP: By aligning with 7AI, you position your organization as a leader in the adoption of next-generation security solutions, paving the way for a more secure digital future.

This is your chance to be part of something truly revolutionary. By joining the agentic security revolution, you'll help drive the future of AI-driven cybersecurity.

9 CONCLUSION: THE AGENTIC SECURITY REVOLUTION IS HERE

The world of cybersecurity is at a tipping point. As the speed and complexity of attacks increase, traditional approaches are falling short. The agentic security revolution offers a path forward—one where AI-driven systems automate and accelerate the security process, ensuring that organizations can finally gain the upper hand against attackers.

7AI is leading this revolution, and whether you're a prospective employee looking to shape the future or a customer seeking cutting-edge solutions, we invite you to join us on this journey. Together, we can build a more secure future where AI helps us outpace the threats of tomorrow.

10 ABOUT 7AI

7AI is the first agentic security platform that harnesses the speed, swarming capabilities, and power of AI to finally give defenders the advantage over evolving threats. The 7AI agentic security platform makes decisions and acts autonomously to achieve specific cybersecurity goals without human intervention. Founded by world-renowned cybersecurity experts Lior Div and Yonatan Striem Amit and backed by Greylock, CRV, and Spark Capital 7AI is leading the agentic security revolution.

LEARN MORE AT 7AI.COM