ALASTAIR PATERSON

CEO and Co-Founder

Harmonic Security

Headquarters: San Francisco, CA

Employees: 70+

Annual Revenue: Private Company, Series A Funding

PROFILES IN *Confidence*

For Alastair (Al) Paterson, building security companies has never been about reaching the destination. It is about the challenge of creating something that helps organizations solve real problems during periods of major change.

As a serial entrepreneur and cybersecurity leader, Al previously founded Digital Shadows, a threat intelligence company that grew to more than 500 enterprise customers before being acquired in 2022. After the acquisition, he found himself in an unfamiliar position.

"I'd gone from managing 160 people to zero," he recalls. "I thought the acquisition and destination was where I wanted to get. But I realized that I'd enjoyed building it, and that was where the real fun was. It's the journey as much as anything else."

That realization coincided with another major event. Just months after the acquisition, ChatGPT was released and organizations around the world began racing to understand what AI would mean for their businesses. For Al, the opportunity was immediately obvious.

"I became very passionate about the AI era very quickly," he explains. "My immediate reaction, given all my security heritage, was no enterprise is just going to roll this stuff out. They're going to need to get it live for competitive reasons, but there's going to be a whole host of security, legal, and compliance challenges around this."

That observation became the foundation for Harmonic Security. Founded in 2023, Harmonic helps organizations accelerate AI adoption safely by providing visibility, governance, and security controls across the rapidly expanding AI ecosystem. As enterprises embrace AI tools, agents, copilots, and automated workflows, Harmonic enables organizations to understand how AI is being used, where data is flowing, and how to apply the appropriate safeguards without slowing innovation.

For Al, the mission has remained consistent from day one. "I kept asking myself how we can help accelerate safe, fast AI adoption in the enterprise," he recalls. "That became the founding goal with Harmonic."

BUILDING FOR A MOVING TARGET

Unlike many cybersecurity categories that emerge around a specific problem, Al believes AI represents something fundamentally different. "This is not one of those times," Al observes. "The whole world is being hit with this AI tsunami, and security teams are having to become AI experts overnight."

That reality has shaped how Harmonic operates. When the company launched, the primary concern for many organizations centered on browser-based use of tools like ChatGPT and the risk of sensitive information being exposed through employee interactions. Since then, the landscape has evolved dramatically. AI capabilities have become embedded into enterprise applications and increasingly autonomous agentic systems.

As a result, Harmonic has had to evolve alongside the market. What began as a platform focused on AI-related data protection has expanded to address broader governance challenges, including agent management, prompt injection attacks, visibility into AI usage, and oversight of increasingly complex AI workflows.

"It isn't a static thing," Al notes. "We're seeing it move from browser usage to applications, to engineering workflows, to agents, and now cloud-hosted agents and team-based AI environments."

For many organizations, keeping pace with those changes has become one of the biggest challenges of AI adoption.

WHY TRADITIONAL SECURITY APPROACHES FALL SHORT

Al believes one of the biggest misconceptions organizations have is assuming AI can be managed using the same security approaches that worked in previous technology eras.

The challenge is not simply protecting data. It is understanding how employees interact with AI systems, how agents operate autonomously, and how sensitive information moves through increasingly dynamic environments. "Those are not things that

you can cover with the old world of rules and DLP from the previous era," he explains.

That belief has become one of Harmonic's primary differentiators. While many legacy vendors have added AI messaging to their existing platforms, AI believes the underlying technology was not built for how AI is actually being used today.

People no longer interact with technology through rigid workflows. They treat AI systems as advisors and collaborators, and as autonomous agents capable of performing actions on their behalf. AI comments, "You can't govern that with the prior generation's tools."

To address those challenges, Harmonic developed proprietary language models designed specifically to identify sensitive information, detect prompt injection attacks, and monitor potentially risky AI behavior. These capabilities allow organizations to move beyond traditional compliance-driven controls and gain visibility into how AI is being used across the enterprise.

"We're in a very different era now," AI notes. "People are feeding AI data in different forms, spinning up agents, and using these tools in ways we've never seen before."

TURNING SECURITY TEAMS INTO AI ENABLERS

As Harmonic has worked with organizations across financial services, healthcare, technology, and many other industries, one trend has become increasingly clear to AI. The most successful security leaders are not the ones trying to slow AI adoption. They are the ones helping the business embrace it responsibly.

"There's a tension between the business and the security organization," he explains. "The CEO may conclude that AI adoption is existential to the company and that they've got to move quickly."

In that environment, security teams face a choice. They can position themselves as obstacles, or they can become strategic partners helping the business move forward safely. AI sees a significant opportunity for security leaders who choose the latter.

"The huge career opportunity is for security teams to be AI native and pro AI enablement, and saying yes and leaning in," he emphasizes.

Increasingly, organizations are creating AI steering committees to guide adoption efforts. In many cases, CISOs are taking leadership roles within those groups, helping shape governance, risk management, and business strategy. For AI, that shift represents a broader evolution in the security profession.

"If you become known for being an enabler in AI and being very AI savvy, understanding what the tools do and using them yourselves while putting the right controls around it, that is one hell of a career opportunity," he points out.

He believes the future belongs to security leaders who spend time understanding how employees actually work and helping teams use AI more effectively. "If you say no, then the business is just going to stop asking you," he cautions.

LEADING AT THE SPEED OF AI

The pace of change in AI has also reshaped how AI thinks about leadership and company building. Unlike traditional software companies that can plan product roadmaps years in advance, Harmonic operates in an environment where major developments can emerge within weeks.

"The idea that you're going to build a twelve-month enterprise roadmap that you stick to is ridiculous for a company like us," AI explains. Instead, the company focuses on maintaining a clear mission while remaining agile enough to adapt as the market evolves.

Every week, the team evaluates what has changed in the AI landscape, what it means for customers, and how those developments should influence product direction. "We're very clear about what is changing in real time," he notes. "What does that mean for product? What does it mean for marketing? And what does it mean for our customers?"

That approach extends to the company culture as well. One of Harmonic's core values is what AI describes as flourishing in the unknown. Team members are encouraged to embrace uncertainty in order to adapt quickly, and to view ambiguity as an opportunity rather than an obstacle.

AI shared, "It's all about people that actually embrace the uncertainty and can function very quickly." For AI, that mindset is essential in an industry where change is constant.

THE NEXT CHAPTER OF AI ADOPTION

As organizations move beyond early experimentation, AI believes the conversation around AI is becoming more sophisticated. Initially, many discussions focused almost exclusively on risk. Today, leaders are asking different questions.

How is AI being used? Which teams are driving adoption? Where is the organization generating value? And what measurable business outcomes are being achieved?

To help answer those questions, Harmonic recently introduced capabilities designed to provide visibility into AI usage patterns across organizations. The goal is not simply to understand risk, but to help leaders understand adoption, enablement, and return on investment.

"This is becoming more than a risk conversation," AI points out. "It's becoming an enablement and ROI conversation as well." That evolution reflects what he sees across the broader market.

Organizations are no longer asking whether AI will become part of their business. They are trying to determine how to adopt it effectively, securely, and at scale. For AI, helping customers navigate that challenge remains the mission.

As the AI landscape continues to evolve, Harmonic's role is not to slow adoption, it is to help organizations move faster with confidence, providing the visibility and controls needed to embrace the opportunities of the AI era while managing the risks that come with it.