PROFILES IN *Confidence*

JACOB COMBS

CISO & Chief Product Security Officer

Tandem Diabetes Care

Headquarters: San Diego, CA

Employees: 2,500+

Annual Revenue: $1.015 Billion (GAAP)

For almost three years, Jacob Combs has led the security program at Tandem Diabetes Care, where his approach to cybersecurity is grounded in pragmatism and adaptability. In an industry defined by constant change, he doesn't see uncertainty as a new challenge, but as the baseline.

Rather than trying to predict every possible threat, Jacob has built his program around the core principle of resilience.

He explains, "When I joined, I focused on this idea of resilience. It's all about our ability to detect, respond, and recover to an attack that occurs. It is still very important today."

For him, that capability is a great safety net, ensuring the organization can withstand what it cannot predict. It also allows the business to move forward with confidence, knowing that even in the face of increasingly complex attacks, they have a strong, resilient security program.

AUTOMATION WITH CONTEXT

For Jacob, the most immediate impact of AI is not just automation, it is automation with context.

"Automation has always been here, but now we have context," he says. "It is not only automating and moving quickly, but gathering and analyzing the context to give my team the ability to make a decision very quickly."

This added layer of context is critical in reducing noise and improving prioritization. It represents a shift from reactive security to more informed decision making.

"Now we can understand priority right away," he explains, describing how enriched insights help teams cut through things like false positives, and focus on what truly matters.

LEADING AI ADOPTION

Within Tandem, Jacob has positioned himself as a key leader in the company's AI journey.

"They're looking to security to help build the guardrails so they can ensure AI is done safely," he says.

In a highly regulated healthcare environment, that responsibility carries significant weight. It requires balancing innovation with compliance, while ensuring speed does not come at the expense of safety or trust.

To support this, Jacob helped establish an internal AI governance council. He says, "We've built our own internal AI governance council where we talk about these things and start planning and designing the next steps forward."

ONGOING GOVERNANCE

For Jacob, AI governance is not a one-time framework, it is an ongoing operational discipline that requires continuous oversight.

"You can't just set it and forget it. You must manage it into the long term to make sure it's still functioning and not drifting or making mistakes," he explains.

That shift introduces a new layer of complexity. Unlike traditional systems, AI requires continuous measurement over time, with clear accountability for outcomes and performance.

As Jacob sees it, organizations are not just managing technology, they are managing behavior. "It's almost like managing another employee, but a lot faster," he says, pointing to the need for clear rules around access and oversight as these systems begin to operate more autonomously.

CONTROLLED PATH FOR AI

Jacob is taking a deliberate, controlled path when it comes to AI.

“We’ve solidified around Copilot because it keeps our data inside, and we’re essentially blocking the rest until we get official agreements and licensing in place,” he explains.

This measured approach allows his team to build confidence in how AI is deployed, while minimizing unnecessary exposure. It also creates a foundation for scaling more advanced use cases over time.

As the organization evolves, new challenges are emerging, particularly around autonomous systems.

“If we start using these agents and they start making decisions on their own, where does that human in the loop preside? What are the rules and performance management structures we have around that?”

DRIVING EFFICIENCY ACROSS THE ORGANIZATION

Jacob is also using AI to reshape how his team spends their time.

Rather than applying AI to security tooling, he has focused on eliminating low-value work. By offloading administrative tasks, his team can concentrate on higher-impact activities.

“I want my team to be able to focus on security work, and AI is helping because they can spend less time on things like project updates and documentation,” he says.

This shift not only improves efficiency but also elevates the role of the security team, allowing them to spend more time on their core work.

BALANCING INNOVATION WITH RISK

As AI enthusiasm grows across the business, Jacob often finds himself balancing momentum with caution. His role is to enable progress without exposing the organization to unnecessary risk.

“I’m trying to balance the need for the business to move forward without having to potentially lose our shirt because we take some outsized risk.”

As Tandem expands its AI capabilities, Jacob is prioritizing one critical area: data. With data moving faster than ever, maintaining control becomes essential.

Jacob comments, “A big one for me is around data security, because that is so crucial to having functional AI systems. As this data starts flying around at superhuman speeds, how are we going to make sure that we’re not losing anything or sending anything out inappropriately?”

LOOKING AHEAD

As the pace of change continues to accelerate, Jacob sees the next year as a balancing act between innovation and discipline. AI will continue to evolve, and with it, the expectations placed on security leaders.

For Jacob, success will not come from trying to predict every outcome, but from building systems that can adapt in real time. His focus remains on enabling the business to move forward confidently, while he supports growth.