KEVIN PAIGE

CISO
ConductorOne

Global Headquarters: Portland, OR

Employees: 85

Annual Revenue: Private Company

PROFILES IN *Confidence*

A VISION ROOTED IN OPERATIONAL EXCELLENCE

With over two decades in information technology and cybersecurity, Kevin Paige brings a rare blend of technical depth and business fluency to the CISO role. “I’m a seasoned Information Technology & Security Leader with over 20 years of results,” he says. “I deliver solutions that optimize performance, security, and efficiency for both the private and public sectors.”

From cutting costs and increasing capability to driving enterprise risk mitigation, Kevin sees cybersecurity not as a constraint, but as a lever. “You can’t be just a gatekeeper anymore. You have to align security to broader company goals.”

IDENTITY: THE QUIET RISK NO ONE HAS SOLVED

If there’s one area keeping Kevin up at night, it’s identity. “I think the one that’s quietly growing is identity and access management,” he says. “It’s always been a risk, but it’s always been hard to deal with.”

That complexity has only deepened with the explosion of SaaS platforms, API ecosystem and now AI agents. “We currently see an issue managing human and non-human identities, and now you’re going to see AI agents acting as human users, potentially talking to other AI agents to help solve problems for the users. There’s a continuing trend of more and more identities that need to be understood and managed.”

Despite 25 years of effort, Kevin says legacy identity solutions still fall short. The real opportunity, he says, is to treat identity as both a security control and a productivity enabler. “Usually it’s, ‘Oh no, here comes security.’ But if you can automate identity and access, give people what they need when they need it, and take it away when they don’t, you can increase productivity and make security look like superheroes.”

WHAT THE BOARD STILL DOESN’T GET

Kevin is candid about the gap between board expectations and cybersecurity realities. “I think the biggest issue is ‘when’ to do security. Security is treated as a cost-center that is expected to be responsible for all security issues in a company, with an assumption something can get bolted on afterward to address security issues and risks.”

He bristles at buzzwords like “shift left.” “Security shouldn’t have to shift left. It should already be part of how people build software and products. It should be instinctual.”

The failure to embed security early, especially in emerging technologies like AI, has real consequences. “People are building agents, giving access to all their data, and then someone finds out the CEO’s vacation schedule and salary through a prompt. It’s like, ‘Oh, maybe we shouldn’t have done that.’”

OVERVALUED: VULNERABILITY MANAGEMENT. UNDERVALUED: IDENTITY.

When asked about program areas that organizations misjudge, Kevin doesn’t hesitate. “Vulnerability management is overvalued. We spend so much time tracking every single vulnerability, cradle to grave. It can be a waste of time.”

He’s not minimizing risk, just reframing it. “Only 1% of vulnerabilities actually matter. We should be solving the root problems, like patch management, instead of managing symptoms.”

On the flip side, identity remains woefully underprioritized. “There are still software vendors charging for SSO. Still apps that don’t support MFA. In 2025, that’s unacceptable.”

AI: THE SECURITY INDUSTRY'S NEXT RECKONING

Like many leaders, Kevin is pouring time and energy into the AI wave, but he's doing it with caution. "AI's barely born, especially LLMs. And we don't know where it's going yet."

He sees AI not only as a new threat surface, but as a test of foundational maturity. "We've got agents, vector databases, real-time SaaS integration, what happens when someone gets in the middle and owns everything?"

He's tracking issues from input validation to model hallucination, but the real risk is speed without guardrails. "Everybody wants to go fast. But if you're going fast with no focus or direction, where are you going? You're going nowhere fast."

SINGLE PANE OF GLASS?

Kevin isn't afraid to call out industry clichés, and one in particular draws his ire. "Single pane of glass, that's probably the one I dislike the most," he says. "Even as a metaphor, it doesn't make any sense."

He laughs about how marketing teams pitch it. "We joke: 'Oh, you mean a dashboard?' It's never one pane. And if it is, that's not even good enough for my house anymore, I need double pane."

SECURITY AS INNOVATION, NOT OVERHEAD

Perhaps Kevin's most important message is about perception. "Security can't be a cost center. That mindset is part of the problem."

He draws a parallel to physical safety. "People get in their cars and put on their seatbelts without being told to do so. They expect airbags and anti-lock brakes. So why don't we apply that same thinking to how we build technology?"

For Kevin, the future of cybersecurity is clear: less friction, more trust, and a permanent seat at the table. "Security isn't separate from innovation, it is innovation. And when we build it in from the start, we make everything stronger."