PROFILES IN *Confidence*

JEFF SPEAR

CISO
Tufin

Headquarters: Boston, MA

Employees: 500+

Annual Revenue: Private Company

Before Jeff Spear led security teams, he led teams through some literal storms. In one of the earliest moments of his career, Jeff learned how maintaining clarity and composure in a difficult situation can shape outcomes, a lesson that would later guide how he fosters teams and manages risk.

"I grew to lead our Deployment Engineering team when Superstorm Sandy hit and caused massive disruption along the east coast," Jeff recalls. "Our CISO noticed how I communicated and stayed calm under pressure and asked me to join the security team to lead disaster recovery programs for our enterprise clients. That's when I realized security combined my technical curiosity with my desire to help others understand and manage risk. That experience changed everything for me."

Since then, Jeff has built and led security programs across multiple industries, from healthcare and hospitality to financial technology. Each role taught him something new about leadership and adaptability. "I've had the opportunity to build programs from the ground up, lead through acquisitions, and help companies define what good security looks like," he says.

BUILDING A SECURITY CULTURE

Jeff views building a security culture as shaping habits and mindsets across every part of the organization, and as an extension of Tufin's mission to help enterprises develop and maintain their network security posture.

"The company's position in the security industry adds unique pressure to do security exceptionally well. If we're in the business of helping customers achieve Zero Trust through our solutions, we have to embody that internally," Jeff says.

Before accepting the role, he focused on a few key criteria. "I wanted to ensure there was an appetite to invest in people and tools," he explains. "Budget and staffing don't have to be perfect, but there has to be willingness to grow." He also prioritized executive alignment. "I met with the entire C-suite during my interviews," he says. "I wanted to make sure the 'C' in CISO meant something, that I'd have a real seat at the table."

Those conversations confirmed what Jeff hoped, that Tufin values security as a business enabler rather than an obstacle. "The culture was supportive from day one," he says. "Security is viewed as part of how the company delivers value, not just as a cost center."

SHAPING THE MODERN SECURITY PROGRAM

Jeff divides his program into four core areas: governance and compliance, security programs, application security, and security operations. Within those areas, he oversees everything from cloud and identity security to resilience and secure code development. "It's a model that's worked for me because it aligns with both product-based organizations and traditional enterprises," he explains.

Application security remains one of his biggest priorities. "We're a product organization, so secure code is everything," he says. "My focus is to make sure we can ship secure software as efficiently as possible without slowing innovation."

AI AND THE FUTURE-READY ENTERPRISE

Like many of his peers, Jeff sees artificial intelligence as both a powerful tool and an emerging challenge. "AI is top of mind for every CISO right now," he says. "For me, it's about using AI across our security program to do more with less, while managing the risks it introduces."

When Tufin procures new technologies, AI included, security is at the center of the conversation. "We have a solid third-party risk management process that ensures security is involved in every decision," he explains. "When we licensed enterprise AI tools, I was part of the discussions with vendors, reviewing SOC 2 reports and secure development practices. It's just part of how we operate."

He also points out that the rise of AI-generated code brings new complexity. "A developer using AI can produce code one hundred times faster," he says. "That's great for productivity, but it also means we need smarter ways to review and test that code for vulnerabilities. The scale is different now."

Still, Jeff views AI as an accelerator for good. "It's about balance," he says. "AI can improve detection, automate response, and make security operations more efficient. The key is using it responsibly and transparently."

GROWTH AND LEARNING

Jeff's approach to leadership was shaped by a lesson early in his career. "One of my directors introduced me to the concept of a growth mindset, the idea that you add 'yet' to every challenge," he says. "If you don't understand something, it just means you don't understand it yet."

That perspective has stayed with him, especially in a field as dynamic as cybersecurity. "Security changes daily," he says. "The best thing I can do for my team is create a culture where learning is constant and curiosity is rewarded."

He encourages his teams to embrace challenges and remain flexible. "I tell them they don't have to know everything," he says. "What matters is their ability to adapt and find the right answers."

THE VALUE OF COMMUNITY

For Jeff, community and peer collaboration have been vital to his growth as a leader. "I wouldn't have had any of my roles if it weren't for the relationships I've built through networking," he says. He credits in-person events and conferences as valuable learning opportunities.

"The best place to network in my experience has been through in-person events, whether that's the big conferences like Black Hat, DEF CON, or RSA, or the smaller regional ones like ISC chapter meetings or SecureWorld in Boston," he says.

"I find less value in the sessions and more value in the people who are in the sessions with me," he says.

Those relationships, built on trust and shared experience, create a network of peers he can turn to when evaluating new technology or solving complex problems. "If I'm looking at a technology and I know someone who's already used it or done a proof of concept, it saves so much time. Instead of testing three different products, I might only test two because I can trust their experience," he explains.

At this stage of his career, Jeff sees his role not only as protecting systems but also as empowering people, both within Tufin and across the security community. "Security is ultimately about enabling the business to move with confidence," he says. "My job is to create an environment where teams feel supported, informed, and equipped to make good decisions."

Whether navigating literal storms early in his career or the evolving challenges of modern cybersecurity, Jeff returns to the same principles: clarity, curiosity, and connection. "If we stay adaptable, invest in our people, and continue learning from one another, we can meet any challenge ahead," he says. "That is what makes this work meaningful and what makes Tufin a place where security can truly thrive."