PROFILES IN *Confidence*

DEB BRIGGS

VP & CSO
NETSCOUT

Headquarters: Westford, MA

Employees: 2,000 (as of 3/31/25)

Revenue: $822.7 Million (as of FY25 ending 3/31/25)

Deb Briggs approaches cybersecurity with a practical mindset shaped by experience and scale. As Chief Security Officer at NETSCOUT, she leads security in an environment where visibility and performance are core to both the business and its customers. Her role requires balancing innovation with control, especially as artificial intelligence rapidly changes how organizations operate.

Rather than viewing AI as a single initiative, Deb breaks it down into focused, actionable areas. Her approach is grounded in real use cases and an understanding that security teams must evolve just as quickly as the technology itself.

AI AS A THREE-PART STRATEGY

For Deb, AI is not one problem to solve, but several. "For us, it is a three-dimensional problem," she explains.

The first area is automation of structured processes, where AI can immediately create efficiency. Deb focuses on applying AI to repeatable, high-volume tasks such as customer questionnaires/audits, RFP responses, and other standardized workflows. These are areas where consistency matters and where automation can significantly reduce manual effort while improving speed and accuracy.

The second area is security operations, where AI can support detection and response. While the potential is significant, Deb remains realistic about current limitations. Deb says, "Rather than replacing analysts, the goal is to augment and upskill them."

The third area is governance and visibility, which she sees as the most critical and challenging. As AI adoption grows across the business, maintaining control becomes increasingly difficult. "Because we are very AI-forward and we want people to get the most they can out of tools, we have to make sure we have strong governance in place," she explains.

THE REALITY OF AI ADOPTION

One of the biggest challenges Deb highlights is the gap between how quickly businesses want to move and how prepared they are to manage the risk.

"Right now, businesses just want free reign with AI. At the same time, many users do not fully understand the implications of data protection," explains Deb.

This creates an environment where AI can unintentionally expose information that was previously harder to access. For Deb, this is not a theoretical concern. It is happening now, and it is forcing organizations to confront long-standing issues around data management and control. Agentic AI is moving faster than most can imagine. The conversation is no longer about what it can do, but how we control identity, access, and logging. Not as enhancements, but as foundational requirements. This is a case where the tools and controls have not kept up with the rapid growth of the technology.

GAINING VISIBILITY INTO THE UNKNOWN

To address these challenges, Deb focused first on understanding the scope of AI usage across the organization. "We have an AI inventory tool," she says.

What she discovered was immediate and eye-opening. "Just three days in, it found 300 AI apps, and I almost fell off my chair," she recalls. Within a short period of time, that number continued to grow.

This level of visibility changed the conversation. Her experience is similar to many other security leaders in her position, it is becoming clear that AI is already widespread

and largely untracked. For Deb, this reinforced the need for continuous monitoring and stronger governance.

BUILDING GOVERNANCE THAT SCALES WITH THE BUSINESS

As AI adoption accelerates, Deb has focused on building governance structures that can scale alongside the business. "There is an AI governance committee," she says, describing a cross-functional approach that brings together key stakeholders to guide responsible AI use. Deb notes, "What's interesting about this committee is the speed at which it needs to operate to keep up with AI acceleration inside and outside our business."

For Deb, effective governance goes beyond policy. It requires alignment, clear ownership, and the right level of support to ensure it works in practice. "This does not come without resources," she explains, emphasizing that governance must be backed by investment and shared accountability across the organization.

Her approach reflects a broader leadership mindset. Governance is not about slowing innovation, but about enabling it in a way that is sustainable. By building the right structure and support around AI, Deb is helping NETSCOUT move forward with confidence while maintaining control.

AVOIDING THE MISTAKES OF THE PAST

Deb draws a clear parallel between the rise of AI and earlier challenges in identity and access management, where rapid growth outpaced visibility and control. She sees the same pattern emerging again as organizations quickly adopt AI without fully understanding what is being built, who owns it, or how it is being used.

Her concern is not the technology itself, but the lack of structure around it. Without clear ownership and foundational controls, AI agents can quickly multiply and introduce risk in ways that are difficult to detect or manage.

For Deb, the priority is ensuring that organizations do not repeat past mistakes. By establishing stronger visibility and accountability early, she is focused on helping the business scale AI in a way that is both controlled and sustainable.

AI AS A FORCE MULTIPLIER

Deb sees AI as a practical way to scale security operations, particularly in areas that are structured and data-intensive. Functions like vulnerability management and analysis are well suited for AI, where large volumes of information need to be processed quickly and consistently.

Rather than replacing people, her focus is on enabling them. AI allows her team to move faster, reduce manual effort, and spend more time on higher-value work that requires judgment and experience.

She also highlights AI's ability to analyze and correlate massive amounts of data at a speed that would not be possible manually. When applied thoughtfully, these capabilities strengthen the team's effectiveness and allow security to operate at a level that keeps pace with the business.

LEADING AT THE PACE OF CHANGE

She describes the current moment of AI with a familiar analogy. "I feel like I am in that *I Love Lucy* episode where the chocolates are coming down the conveyor belt. Right now, it is manageable, just like AI, but as the episode continues they cannot keep up, and the chocolates start flying everywhere. Lucy ends up covered in chocolate, stuffing it in her apron. The question that none of us know is how fast that AI conveyor belt can be turned up."

That uncertainty captures the challenge facing security leaders today. The pace of innovation continues to accelerate and expectations from the business are increasing.

At NETSCOUT, Deb is focused on building a program that can keep up. One that combines visibility and governance, and ensuring her team is prepared not just for where AI is today, but for how quickly it will evolve.