Zscaler Q1 2026 Earnings Call – November 25, 2025

Forward-Looking Statements

Unless otherwise noted, all numbers presented will be on an adjusted, non-GAAP basis. Reconciliation of GAAP to the non-GAAP financial measures is included in our earnings release.

This document contains forward-looking statements that involve risks and uncertainties, including, but not limited to, statements regarding our future financial and operating performance, including our financial outlook for the second quarter of fiscal 2026 and full year fiscal 2026, and the expected impact of the acquisitions of Red Canary™ and SPLX. There are a significant number of factors that could cause actual results to differ materially from statements made in this press release, including but not limited to: macroeconomic influences and instability, geopolitical events, operations and financial results and the economy in general; risks related to the use of AI in our platform; our ability to identify and effectively implement the necessary changes to address execution challenges; risks associated with managing our rapid growth, including fluctuations from period to period; our limited experience with new products and subscriptions and support introductions and the risks associated with new products and subscription and support offerings, including the discovery of software bugs; our ability to attract and retain new customers; the failure to timely develop and achieve market acceptance of new products and subscriptions as well as existing products and subscription and support; rapidly evolving technological developments in the market for network security products and subscription and support offerings and our ability to remain competitive; length of sales cycles; useful lives of our assets and other estimates; and general market, political, economic and business conditions.

Additional risks and uncertainties that could affect our financial results are included under the captions “Risk Factors” and “Management’s Discussion and Analysis of Financial Condition and Results of Operations” set forth from time to time in our filings and reports with the Securities and Exchange Commission ("SEC"), including our Annual Report on Form 10-K for the fiscal year ended July 31, 2025 filed on September 11, 2025, as well as future filings and reports by us, copies of which are available on our website at ir.zscaler.com and on the SEC’s website at www.sec.gov. You should not rely on these forward-looking statements, as actual outcomes and results may differ materially from those contemplated by these forward-looking statements as a result of such risks and uncertainties. Additional information will also be set forth in other filings that we make with the SEC from time to time. All forward-looking statements in this press release are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

CEO Commentary

We had a strong start to our fiscal year. In Q1, Annual Recurring Revenue or ARR growth accelerated to 26% year-over-year and RPO growth accelerated to 35%. Combining our strong free cash flow margin of 52% and revenue growth of 26%, we operated at Rule-of-78, making us one of the rare companies consistently outperforming the coveted Rule-of-40 metric. We are one of the only five enterprise SaaS companies with over $3 billion dollars in ARR, growing at over 25%.

The continued success of our three growth pillars, AI-Security, Zero Trust Everywhere and Data Security Everywhere, is driving our strong top line performance. ARR from these three growth pillars accelerated in the quarter. I'm particularly pleased with our AI-Security pillar, which grew over 80% year-over-year and has already exceeded our FY26 target of $400 million dollars ARR, three quarters earlier than expected. With this strong demand, I expect AI-Security ARR to exceed half a billion dollars by the end of this fiscal year.

Diving deeper into our AI-Security pillar - while enterprises are leveraging AI to drive innovation and accelerate productivity, the proliferation of AI is also making them increasingly susceptible to attacks. One of the largest AI companies recently reported that a bad actor hijacked its AI coding assistant to autonomously perform a large-scale cyberattack against multiple organizations. This incident highlights two important trends. First, threat actors are using AI to dramatically increase the speed, effectiveness, and blast radius of attacks. We have been predicting an increase in this type of automation by AI agents, and we are now seeing it happen. Second, just like users, an organization's AI agents are also becoming the weakest link in their security. It is only a matter of time before millions of AI agents interact with each other across enterprises. Imagine a threat actor hijacking even one of an organization's trusted agents and thereby accessing critical corporate resources and sensitive information, resulting in a serious breach.

We have a long history of securing users with our Zero Trust Exchange which enabled our customers to safely adopt the latest technologies such as mobile, cloud and SaaS. Over 45% of Fortune 500 companies and nearly 40% of Global 2000 companies have adopted our Zero Trust Exchange and trust Zscaler to secure their businesses.

- With the rise of Consumer GenAI applications, including ChatGPT, Perplexity, and more, security issues related to access control, data loss and content moderation, made enterprises cautious about allowing employees access to these popular apps. We extended our Zero Trust Exchange to provide visibility into thousands of GenAI Apps, enabling enterprises to inspect prompts and responses, and enforce proper guardrails for safe and secure use of GenAI Apps. Several large enterprises adopted our GenAI solution in the quarter, including a G2K Technology company, a Fortune 500 communications equipment company, and a large healthcare software provider.
- **As AI adoption moved beyond Consumer GenAI apps into building and running Enterprise AI applications,** we introduced solutions in three key categories to secure them.

- **First, AI asset discovery and posture management.**
  AI applications and agents are being developed and deployed today without full visibility for IT teams to safeguard them. To provide organizations with visibility and control, last year we introduced an AI asset discovery solution called AI-SPM. AI-SPM can detect unauthorized AI applications, prevent over-permissions for AI agents, and strengthen governance for model deployments. In Q1, several customers including a leading software solution provider, a global 2000 manufacturer, and a leading insurance company, purchased AI-SPM from Zscaler. With our recent acquisition of SPLX, we are extending our AI-SPM capabilities by unifying discovery of LLMs, workflows, and MCP servers. These capabilities enable customers to meet evolving regulatory requirements for AI to be transparent and explainable, among others.
- **The second key area of innovation is AI Red Teaming.**
  As part of AI lifecycle, customers need to regularly test their applications for vulnerabilities. With SPLX, we now deliver AI red teaming to enable automated and continuous testing of AI apps at scale. Our AI Red teaming solution integrates with customers' CI/CD pipelines, making it easy to test for hallucination, bias, behavior drift, and more. Several customers, including a Fortune 150 transportation company and a Fortune 100 service provider, have already deployed AI Red Teaming.
- **The third key area of innovation is AI Guardrails.**
  Customers need AI guardrails for inline policy enforcement for acceptable use of AI, for cyber security and for data loss prevention. In-line policy enforcement is one of our key differentiators, which we seamlessly deliver through our Zero Trust Exchange at scale as we process half a trillion transactions daily. Our AI Guard solution leverages this core competency for runtime protection. Zscaler AI Guard sits between the applications and LLMs, inspecting prompts and responses in-line, to enforce customer defined policies.
  To share an example, this quarter a leading consulting firm purchased our AI Guard to secure their use of public AI applications and their private in-house applications such as AI chatbots and AI agents.

With our platform capabilities, we are securing over 90 billion AI/ML transactions per month. As AI and AI agents define the next era of transformation, we are further extending our platform to secure AI agents, agentic workflows and AI applications.

In addition to securing the use of AI, we are leveraging AI to deliver Agentic Operations, including Agentic SecOps and Agentic IT-Ops.

In our Agentic SecOps, we are making great progress towards delivering an AI-Powered SoC that simplifies customers' operations and automatically hunts for threats. In August, we acquired Red Canary to combine their Agentic technology with our Data Fabric technology to deliver actionable SoC insights for our customers. This quarter:

- a Fortune 500 Financial Services company,

- a Global 2000 healthcare equipment company, and
- a Global 2000 energy company, and more, purchased our Agentic SecOps solution.

In our Agentic IT-Ops, we are introducing several Zscaler Digital Experience or ZDX innovations to enable faster resolution to application and network performance issues. Our innovations like the ZDX Copilot continue to resonate with customers and have driven over 80% year-over-year growth in bookings of ZDX-Advanced-Plus in the last 12 months.

I'm very pleased to see continued momentum for our AI-Security solutions. As I mentioned, we are expecting AI-Security ARR to surpass half a billion dollars by the end of fiscal 26.

Turning to our second growth pillar, we continue to see strong momentum in Zero Trust Everywhere, which includes Zero Trust Users, Zero Trust Branch, and Zero Trust Cloud. Three quarters ago, we introduced Zero Trust Everywhere and set a goal to secure 390 enterprises with Zero Trust Everywhere by the end of fiscal 26. I am delighted to share that we now have over 450 Zero Trust Everywhere enterprises – achieving our goal three quarters ahead of our target date. Our Zero Trust Everywhere customers benefit from reduced cost and complexity by eliminating legacy network and security products. This expanded relationship through Zero Trust Everywhere also creates follow-on demand for data security and AI security.

One of the key components of Zero Trust Everywhere is Zero Trust Cloud, which allows customers to eliminate VPNs, north-south and east-west virtual firewalls, Express Route and Direct Connect networks, resulting in far better cybersecurity. To share a customer example:

- In an 8-figure TCV win, an existing million-dollar plus Fortune 500 healthcare customer adopted our Zero Trust Cloud solution along with ZDX Advanced Plus, Data Security modules, and more. Zero Trust Cloud secures workload communication across their VPC or virtual private cloud and SAP RISE cloud-based ERP. Without Zero Trust Cloud, the customer would have had to deploy significant number of north-south and east-west firewalls, resulting in increased cost and many months of delay. This customer told me that in the last 15 years they have not been so excited about a solution that not only brought better security but also was easy to deploy and operate.
  Just like the migration of Microsoft Exchange to Office 365 was a big tailwind to our business a few years ago, I believe the migration of SAP on-prem to SAP RISE will have a similar impact on our business.

We continue to see strong interest from customers for Zero Trust Branch, which is another key component of Zero Trust Everywhere. Zero Trust Branch eliminates the need for legacy point solutions at branches, factories, and campuses. To give you an example:

- In a 7-figure upsell win, a Global 2000 manufacturing customer more than tripled their ARR and became a Zero Trust Everywhere customer by purchasing our Zero Trust Branch, ZPA, ZDX Advanced Plus, Risk 360, and more.

Moving to Data Security Everywhere. We offer a comprehensive data security portfolio with eight modules providing data discovery, data classification, posture management, data loss prevention, and more. Customers are eliminating data security point products in their environment by consolidating data security functionality on our unified platform. To share an example:

- In a 7-figure new logo ACV win, a large healthcare provider purchased 5 out of our 8 data security modules for their 23,000 users. This enterprise chose Zscaler over a leading CASB vendor, due to our integrated platform which delivers data security across all channels, for all types of data.

I'm excited to share that our Data Security Everywhere ARR accelerated to approximately $450 million dollars.

The growth across our three pillars is powered by our strong go-to-market engine. One of the key initiatives we recently introduced was our Z-Flex program, which enables customers to commit to a spend and provides flexibility to swap or activate additional modules without undergoing new procurement cycles. Z-Flex is driving meaningful upsells and reduced sales cycle, and it is consistently exceeding my expectations. Z-Flex generated over $175 million dollars in TCV, growing over 70% quarter-over-quarter. To share a couple of customer examples:

- An existing large aerospace customer made a multi-year, 8-figure TCV commitment under the Z-Flex program, increasing their annual spend with us by over 40%. As part of the flex commitment, the customer added nine new modules including Asset Exposure Management, Identity Threat Detection, Unified Vulnerability Management, Email DLP, and expanded commitments for data security.
- In a 7-figure upsell win, a Fortune 500 business services provider more than doubled their annual spend with us as they expanded adoption of 9 modules under the Z-flex program.

In conclusion, our business is benefiting from the strong tailwinds from the combination of Zero Trust and AI security. The best AI Security is built on the foundation of Zero Trust. Our clear leadership in Zero Trust security combined with our comprehensive AI Security offerings, positions us well to capture the large and growing AI security market. And with our strong go-to-market engine, we are well positioned to exceed $10 billion dollars in ARR.

CFO Commentary

We exceeded our growth targets in Q1 and operated at Rule-of-78 for the quarter. We ended Q1 with over $3.2 billion in ARR, reflecting approximately 26% year-over-year growth. ARR from each of our three growth pillars accelerated in the quarter, including on an organic basis. Q1 revenue was $788 million, growing 26% year-over-year, 10% sequentially, and exceeding the high end of our guidance. Geographically, the Americas accounted for 58% of revenue, EMEA for 27% of revenue, and APJ for 15% of revenue. Our Remaining Performance Obligation, or RPO, grew approximately 35% year-over-year to $5.9 billion, with approximately 47% classified as current RPO.

We closed Q1 with 698 customers generating over $1 million in ARR and 3,754 customers exceeding $100,000 in ARR, demonstrating the strategic role we play in customers' digital transformation journeys.

Turning to the rest of our Q1 financial performance, our gross margin was 79.9% as compared to 80.6% last fiscal year Q1. I would like to remind investors that we are introducing new products that are experiencing strong growth and are optimized for faster go-to-market rather than margins. This will continue to influence our gross margins on a quarterly basis. We plan to optimize new products for margins over time as they scale.

Operating expenses increased 11% sequentially and 23% year-over-year, reaching $458 million. Operating margin was 21.8%, towards the higher end of our long-term range and growing by approximately 40 basis points year-over-year. Our free cash flow margin for Q1 was 52%, including data center CapEx at 2% of revenue. We ended the quarter with $3.3 billion in cash, cash equivalents, and short-term investments.

Next, let me provide our guidance for Q2 and full year fiscal 2026. As a reminder, these numbers are all non-GAAP.

For the second quarter:

- We expect revenue in the range of $797 million to $799 million, reflecting year-over-year growth of approximately 23%.
- Gross margins to be approximately 80%.
- Operating profit in the range of $172 million to $174 million.
- Net other income of approximately $19 million
- Earnings per share in the range of $0.89 to $0.90, assuming a 21% tax rate and 170 million fully diluted shares.

For the full year fiscal 26:

- ARR in the range of $3.698 billion to $3.718 billion, reflecting year-over-year growth of 22.7% to 23.3%. We anticipate approximately 47.8% of Net New ARR to be recognized in the first half.
- Revenue in the range of $3.282 billion to $3.301 billion, reflecting year-over-year growth of 22.8% to 23.5%.

- Operating profit in the range of $732 million to $740 million.
- Earnings per share in the range of $3.78 to $3.82, assuming a 21% tax rate and approximately 170.5 million fully diluted shares
- Free cash flow margin to be approximately 26.0%-26.5%

With a large market opportunity and customers increasingly adopting the broader platform, we will invest aggressively to position us for long-term growth and profitability.