Qualys Q3 FY2025 Earnings Prepared Remarks

Foster City, Calif., – November 4, 2025 – Qualys, Inc. (NASDAQ: QLYS), a leading provider of disruptive cloud-based IT, security, and compliance solutions, today announced financial results for the third quarter ended September 30, 2025.

Blair King, Investor Relations

Good afternoon, and welcome to Qualys' third quarter 2025 earnings call.

Joining me today to discuss our results are Sumedh Thakar, our president and CEO, and Joo Mi Kim, our CFO. Before we get started, I would like to remind you that our remarks today will include forward-looking statements that generally relate to future events or our future financial or operating performance. Actual results may differ materially from these statements. Factors that could cause results to differ materially are set forth in today's press release and our filings with the SEC, including our latest Form 10-Q and 10-K. Any forward-looking statements that we make on this call are based on assumptions as of today, and we undertake no obligation to update these statements as a result of new information or future events.

During this call, we will present both GAAP and non-GAAP financial measures. A reconciliation of GAAP to non-GAAP measures is included in today's earnings press release. As a reminder, the press release, prepared remarks, and investor presentation are available on the Investor Relations section of our website. With that, I'd like to turn the call over to Sumedh.

Sumedh Thakar, president and CEO

Thanks, Blair, and welcome to our third quarter earnings call.

With threat actors continuing to reduce time-to-exploit at a fast pace, I believe the future of cybersecurity is moving from Attack Surface Management to Risk Surface Management using agentic AI-powered proactive risk management with business quantification and automated remediation. Against this backdrop, we continued to execute well in Q3, demonstrated by another quarter of solid revenue growth and profitability.

Platform Innovation:

Over the past couple of years, I've had the privilege of meeting with hundreds of CIOs, CISOs, and security leaders worldwide. From those conversations, one theme has stood out - the need to operationalize cyber risk management in business terms to align budget spend with business risk. CISOs are looking for a practical approach to consolidate tools where possible and empower their teams to use best-of-breed where it makes sense. They want to seamlessly unify their security toolset into a centralized risk fabric that provides an alternative to single-vendor platformization by operationalizing the management of multiple risk vectors to effectively measure, communicate, and ultimately remediate the organization's security posture. The ROC (Risk Operations Center), powered by Qualys' ETM, delivers on this ask. At our recently concluded "ROCon" Risk Operations conference in Houston, where we elevated the business risk conversation to feature a specialized CFO and board track, our customers validated this approach. With the broadening of the agenda for ROCon, the attendance was up 20% over last year's event. While traditional Security Operations Centers (SOC) focus on detecting breaches after they happen, Qualys is pioneering the first agentic AI Risk Operations Center (ROC), a new category in cybersecurity designed to centralize an organization's response to threats, before they impact the business. Powered by our Enterprise TruRisk Management (ETM) solution, the ROC processes several petabytes of high-fidelity data every day, normalizes and correlates intelligence from both Qualys and non-Qualys sources, and equips AI and humans to collaborate in real-time, detecting and responding to threats at machine speed. This isn't about more alerts - it's about actions that close blind spots because attacks can exploit them. Unlike traditional Continuous Threat Exposure Management (CTEM) tools that simply highlight exposures but lack adequate native remediation capabilities, our differentiated ETM solution combines Cyber Risk Quantification (CRQ), CTEM, and native remediation operations to fix the risks that matter most, quickly, and at scale. By aligning security and IT decisions directly with business priorities, we are providing organizations with measurable, proactive risk reduction that boards and customers value. Early adoption is already validating the model, with Proof-of-Concepts (POC) continuing to convert to commercial deployments, underscoring both the scale of this opportunity and its parallels to the early days of Vulnerability Management, Detection, and Response (VMDR®).

And we're not stopping there. Our R&D engine is continuing to deliver innovations, rapidly expanding our platform, and positioning Qualys for larger upsell opportunities. In doing so, Qualys is now extending several proven, module-native capabilities into ETM, empowering organizations to harness them seamlessly across their entire attack surface. By democratizing trillions of security exposures from both Qualys and third-party tools, including vulnerabilities, mis-configurations, and identities, aggregated by our ETM solution, we are unleashing a sophisticated, predictive platform that leverages a combination of the Qualys TruRisk framework, our TruLens capabilities, and a mission-ready, agentic AI workforce operating autonomously from discovery to remediation with full ITSM integration. This unique combination of capabilities identifies trending threats in real time, benchmarks risk against peers, assesses organizational impact, and quantifies risk in clear, actionable terms that matter most to the business. As a result, security and IT teams can continuously prioritize, ticket, and remediate threats based on organizational risk associated with emerging exposures targeting specific industries, asset types, and identities. We believe these most recent additions to our ETM solution further advance our differentiation in the market, enhance security operations, and significantly accelerate measurable outcomes for customers.

Next up for our ETM solution, I'm particularly excited about yet another pioneering capability from Qualys, TruConfirm. TruConfirm flexes the power of our platform to confirm exploitability before customers become compromised. Using automated validation at scale, we remove the guesswork for customers by running safe exploits over the network to confirm whether attackers will succeed in their breach attempts, while closing the gap between theoretical and actual exposures. This approach further allows customers to be laser-focused on prioritizing only exploitable blind spots for the next logical step, which is automated remediation with TurRisk Eliminate.

Our industry leading capabilities are increasingly being recognized by our customers, partners, and third-party analysts. Specifically, at Black Hat, Qualys won two Pwnie awards for our outstanding contributions to threat research underpinned by our strong leadership in threat intelligence and triage. Equally important, GigaOm recognized Qualys as the leader in Patch Management, a market Qualys pioneered, with over 140 million patches deployed in the last year alone. While some competitors are only beginning to validate this strategy, Qualys has advanced well beyond patching. TruRisk Eliminate closes the unpatchable gap, enabling security and IT teams to automate an array of compensating controls when patches are deemed too risky to deploy, or simply not available. And, with adversaries increasingly exploiting vulnerabilities at AI speed, our umbrella of AI-based automated remediation solutions has evolved into a significant adoption lever, a distinct competitive advantage, and opens new market opportunities for Qualys.

Q3 Business Update:

Moving to our business update. With customers spending $500,000 or more with us growing 5% from a year ago to 211, let me share a couple of recent wins, which illustrate why organizations ready to centralize their response to cyber risk are turning to Qualys to help unify their security tools, quantify and remediate risk in their environments, and fortify their security operations.

In Q3, one of my favorite wins was with a global 700 customer that was previously only using Qualys for PCI scanning. This customer, like many organizations, was buried under fragmented telemetry, manual spreadsheets, and disconnected tools. With little automation, their teams were spending more time documenting risk than reducing it, and consequently were burdened by an onslaught of compliance audits. This customer chose Qualys to transform siloed risk signals spanning code repositories, endpoints, identity, cloud, container, and network assets into a cohesive, real-time risk management solution by consolidating Qualys and non-Qualys data. This included replacing their existing vulnerability management vendor and purchasing three additional Qualys modules, including ETM, to begin operationalizing their ROC with ingested third-party data, resulting in a mid-six-figure annual bookings upsell. By consolidating these data sources into the Qualys platform, we are delivering this customer a vendor agnostic orchestration layer with full visibility of their attack surface, centralized risk assessment, quantification, prioritization, and remediation while unleashing the operational efficiencies of security stack consolidation aligned with acceptable risk parameters for the business. With our innovative technologies, unmatched platform effect, and focus on reducing risk and friction, this win underscores Qualys' ability to eclipse legacy siloed solutions and advance our leadership in the industry. It's also an outstanding example of how we are working with our managed ROC (mROC) partners of choice to activate the ROC, and win new business. For the next phase, this customer is evaluating our TotalCloud Cloud Native Application Protection Platform (CNAPP) and TruRisk Eliminate solutions while also bringing additional third-party tools into the Qualys platform, representing a significant upsell opportunity.

Further leveraging our mROC partner ecosystem to drive new logos was a new six-figure customer win with a major airline in the Middle East. This customer chose Qualys because of our unified detection and remediation capabilities with TruRisk Eliminate.

Nearly nine months after announcing General Availability (GA) on our ETM solution and over 28 Proof of Concepts (POCs) converted to commercial deployments, we have gained valuable insights into ETM pricing and packaging. As a point of reference, we expect that for every one dollar of VMDR, ETM can drive an uplift of up to 100% now that ETM will include Cybersecurity Asset Management, as well as other ETM feature enhancements, such as those mentioned earlier, and third-party data ingestion. Given this, starting with our Q1 FY2026 earnings call, we will shift from reporting Cybersecurity Asset Management LTM bookings to ETM customer penetration, as we believe ETM will be evolving into a key pillar of growth for Qualys over the next several years.

Turning to our Federal business, we achieved a high six-figure upsell with an existing large government agency. This customer had previously used multiple legacy and next-gen solutions to manage a variety of risk management use cases across their security, IT, and DevOps teams. In addition to the complexity of using multiple point products, this government agency had become increasingly frustrated with increasing costs associated with legacy on-prem deployments, the inefficiencies of operating siloed systems, and elongated remediation efforts. With a distinct need to shift several monolithic workloads to micro applications across its hybrid environment on a FedRAMP High Authorized solution, this customer accelerated the consolidation of its security stack across seventeen Qualys modules, including VMDR, Cybersecurity Asset Management, Total AppSec, TotalCloud, TruRisk Eliminate, and Total AI. Today, this customer is leveraging a unified dashboard that provides them with greater insights and automation than any of the competitive products they evaluated, while taking full advantage of the speed and scale of a cloud-native platform. This, alongside a significant seven-figure state win, are a testament to the strength we see in our federal, state, and local government business and the long-term growth potential of this market.

Beyond these wins, we're also increasingly gaining leverage from our partner ecosystem. In Q3, partner-led deal registration increased, demonstrating the success of our partner-first sales motion. In addition, we have now certified nearly a dozen partners who are actively launching mROC services, leveraging ETM to deliver centralized, automated, pre-breach risk management. Momentum is building toward a global ROC alliance, and we expect to certify additional strategic partners in the months ahead who are committed to positioning Qualys as their mROC partner of choice.

Further contributing to our platform growth is our flexible platform pricing model, which we're now calling QFlex. We beta tested QFlex in Q3 to help customers accelerate and maximize adoption of the Qualys Enterprise TruRisk Platform. In less than a quarter after introducing this model, we're seeing notable customer interest and tremendous success. To give you an example, an existing global 10 customer made a multi-year commitment under our QFlex program, increasing their annual bookings by over 50% while adding new modules to their subscription count with Qualys. This win reflects our growing capabilities in risk management, and we expect the contribution from QFlex to continue to grow.

In summary, our continuous innovation, early ROC deployments, strategic wins with major federal and state agencies, momentum in partner-led initiatives, and the initial adoption of QFlex collectively underscore Qualys' strength in unifying risk management workflows, reducing operational complexity for customers, and addressing today's toughest security challenges. We believe these achievements not only validate our ongoing investments but also position Qualys as a trusted leader in pre-breach cyber risk management, setting the stage for durable growth and long-term success.

With that, I'll turn the call over to Joo Mi to further discuss our third-quarter results and outlook for the fourth quarter and full year 2025.

Joo Mi Kim, Chief Financial Officer

Thanks, Sumedh, and good afternoon. Before I start, I'd like to note that, except for revenues, all financial figures are non-GAAP, and growth rates are based on comparisons to the prior year period, unless stated otherwise.

Turning to third quarter results, revenues grew 10% to $169.9 million. The channel continued to increase its contribution, making up 50% of total revenues compared to 47% a year ago. Revenues from channel partners grew 17%, outpacing direct, which grew 5%. As a result of our strategic emphasis on leveraging our partner ecosystem to drive growth, we expect this trend to continue. By geo, 15% growth outside the US was ahead of our domestic business, which grew 7%. US and international revenue mix was 56% and 44%, respectively.

In Q3, gross retention continued to improve; however, upsells remained challenging with our net dollar expansion rate at 104%, unchanged from last quarter.

In terms of product contribution to bookings, Patch Management and Cybersecurity Asset Management combined made up 17% of total bookings and 28% of new bookings on an LTM basis. Our Cloud Security solutions, TotalCloud CNAPP, made up 5% of LTM bookings.

Reflecting our scalable and sustainable business model, adjusted EBITDA for the third quarter of 2025 was $82.6 million, representing a 49% margin, compared to a 45% margin a year ago. Operating expenses in Q3 increased by 5% to $64.9 million, driven by investments in sales and marketing, which grew 9%. As we remain focused on driving growth, we are mindful of where to further increase investments while optimizing returns in others, which resulted in EBITDA margin exceeding our expectations in Q3. This demonstrates our ability to maintain high operating leverage and remain capital efficient while continuing to innovate and invest to support our long-term growth initiatives.

With this strong performance, EPS for the third quarter of 2025 grew 19% to $1.86. Our quarterly free cash flow was $89.5 million, representing a 53% margin, compared to 37% in the prior year. YTD free cash flow margin was 46%, compared to 42% in the prior year. In Q3, we continued to invest the cash we generated from operations back into Qualys, including $901 thousand on capital expenditures and $49.4 million to repurchase 366 thousand of our outstanding shares. Since commencing our share repurchase program in February of 2018, we’ve repurchased 10.4 million shares and returned $1.2 billion in cash to shareholders. As of the end of the quarter, we had $205.2 million remaining in our share repurchase program.

With that, let us turn to guidance, starting with revenues: For the full year 2025, we expect revenues to be in the range of $665.8 to $667.8 million, which represents a growth rate of 10%. This compares to prior guidance of $656 to $662 million. For the fourth quarter of 2025, we expect revenues to be in the range of $172.0 to $174.0 million, representing a growth rate of 8% to 9%. While we believe our platform approach to cyber risk management provides some insulation amidst macro volatility, this guidance assumes continued budget scrutiny and a challenging environment for new business growth in Q4.

Shifting to profitability guidance. We expect full year 2025 EBITDA margin in the mid-to-high 40s and a free cash flow margin in the low 40s. We expect full year EPS to be in the range of $6.93 to $7.00, up from the prior range of $6.20 to $6.50. For the fourth quarter of 2025, we expect EPS to be in the range of $1.73 to $1.80. Our planned capital expenditures in 2025 are expected to be in the range of $5.5 to $7.0 million; and, for the fourth quarter of 2025, in the range of $1.2 to $2.7 million.

With that, Sumedh and I would be happy to answer any of your questions.