Qualys Q2 FY2025 Earnings Prepared Remarks

Foster City, Calif., – August 5, 2025 – Qualys, Inc. (NASDAQ: QLYS), a leading provider of disruptive cloud-based IT, security, and compliance solutions, today announced financial results for the second quarter ended June 30, 2025.

Blair King, Investor Relations

Good afternoon and welcome to Qualys' second 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 second quarter earnings call.

In Q2, we continued to execute well, resulting in another quarter of solid revenue growth and profitability.

Platform Innovation:

In this new era of cybersecurity driven by advanced data analytics, automation, and AI, Qualys is pioneering a new Risk Operations Center (ROC) category in cybersecurity and redefining how organizations manage cyber risk. While traditional Security Operations Centers (SOC) focus on detecting breaches after they happen, the ROC is built for prevention. Qualys' cloud-native Enterprise TruRisk Management (ETM) solution powers this transformation. With over 18 trillion data points processed in real-time, we have unleashed the power of our platform to integrate and normalize signals from both Qualys and third-party tools, including CrowdStrike, SecurityScorecard, Tenable, and Wiz. Unlike other Continuous Threat Expose Management (CTEM) solutions that simply highlight exposures and lack effective remediation or business context, Qualys' ETM solution is a powerful orchestration layer aggregating both Qualys and non-Qualys security findings, applying threat intelligence, and delivering a unified business-contextual

view of risk with holistic prioritization and automated remediation. This business-aligned approach to pre-breach cyber risk management continues to resonate strongly with customers and boards, and positions Qualys at the forefront of a paradigm shift in cybersecurity - one defined not just by the detection of vulnerabilities, but by measurable, proactive, automated risk reduction at scale. With active POCs already converting after announcing GA just a short time ago, we continue to see many parallels between this new market opportunity and the early days of our Vulnerability Management, Detection, and Response (VMDR®) launch, including a significant greenfield opportunity, and growing demand.

With our latest announcement yesterday, we are excited to introduce Qualys' latest game changing vision for the future of cyber risk management with the launch of a fully reimagined Agentic AI platform built on a unified fabric to seamlessly manage cyber risk across multi-vendor environments. At its core, every cyber risk AI agent represents a specialized autonomous AI fabric, equipped to automate complex business processes and autonomously adapt to customer environments by accessing diverse internal and external data sources, applications, and machines. These agents achieve complete end-to-end outcomes for cybersecurity teams. Available in a first-of-its-kind Agentic AI marketplace for risk management, CISOs can now quickly augment their teams with highly specialized autonomous experts that can bring down the time to remediation, increase accuracy, and reduce cost. Users can use out-of-the-box cyber risk agents available in the marketplace, interactively create their own specialist agents, or leverage 3rd party agents from our partners that can be added to the marketplace in the future.

Further advancing our remediation focus beyond patching, we are also introducing new capabilities into our TruRisk Eliminate umbrella of remediation solutions. Now, organizations can quickly determine trending risks to their environments, the estimated impact of a breach on any particular asset, and the probability of successfully applying a patch. If applying a patch is deemed a significant operational risk to the business, security and IT teams can alternatively choose to automate an array of compensating controls to prevent an incident from occurring. Embedding Qualys' AI-assistance directly into remediation workflows is a significant adoption lever, a strong competitive differentiator, and opens new market opportunities well beyond patch management.

Continuing this rapid pace of innovation, we are further broadening our ETM solution and bringing natively integrated Identity Security Posture Management (ISPM) to market at a time when identities have become part of the new perimeter. Compromised credentials are central to nearly every major cyber attack today, and Qualys' solution is aimed at helping organizations stay in front of adversaries by continuously analyzing identity systems for misconfigurations, excessive privileges, and toxic combinations. By unifying the identity risk surface, we eliminate silos and help security teams visualize identity exposure and remediate risks before attackers escalate privileges or move laterally. Spanning devices, cloud workloads, and applications, Qualys now provides holistic protection using Qualys and non-Qualys data sources across key identity touchpoints mapped to asset criticality and backed by real-time remediation through a single, natively integrated platform.

These innovative new approaches to cybersecurity risk management, along with several others we are showcasing at Black Hat this week allow our customers to reduce complexity and cost, achieve better outcomes, and create multidimensional paths for durable long-term growth in our business.

Q2 Business Update:

Moving to our business update. Over the past several months, I have personally met with many customers, prospects, and partners, and the message has remained resoundingly clear. Organizations are increasingly anchoring pre-breach cyber spend to solutions that articulate and demonstrate a measurable impact on business risk. Rather than consolidating around a single vendor, CISOs are seeking platforms that allow flexibility across their security stack while unifying risk through a common framework. This requires a centralized risk fabric, which brings together diverse tools and enables teams to uniformly assess, prioritize, and remediate risk.

With a 25 year track record of converting operational challenges for customers into strong competitive advantages, we are well positioned to capitalize on these evolving market opportunities. In Q2, this success was demonstrated by the number of customers spending $500,000 or more growing 7% from a year ago to 212. It was also evidenced by notable industry endorsements in markets we helped pioneer. Qualys' VMDR with TruRisk and TotalCloud were voted the best Vulnerability Management and Cloud Security solutions, respectively, at the 2024 SC Awards Europe. IDC named Qualys as a major player in Cloud Native Application Protection Platforms (CNAPP), and KuppingerCole recognized Qualys as a leader in CNAPP and the market leader in Attack Surface Management.

Let me share a couple of recent wins, which illustrate these accolades and reflect why companies 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 achieve better security outcomes.

First, a global FinTech company determined that managing siloed tools added complexity to their operations, lacked integration, and missed detections, which hindered their ability to assess risk and centralize remediation. This customer chose Qualys to transform siloed risk signals spanning code repositories, endpoints, identity, cloud, container, IT, and network assets into a cohesive, real-time risk management solution by consolidating Qualys and non-Qualys data. This included purchasing seven Qualys modules including ETM to begin operationalizing their ROC with ingested data from CrowdStrike, BitSight, and Wiz, resulting in a seven-figure annual bookings deal. By consolidating these data sources into the Qualys platform we are now 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.

Another marquee win was with a large federal government agency previously using 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 was frustrated with increasing costs associated with outdated on-prem deployments from years past. Looking to migrate to a cloud-native solution that meets the Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directives (BOD), they are now in the process of replacing two of their existing vendors in a high six-figure annual bookings deployment using ten Qualys modules including Cybersecurity Asset Management, VMDR with TruRisk, Patch Management, and TotalCloud. Through this highly strategic and competitive win, this customer is now able to leverage unified dashboards across nearly a dozen separate bureaus that provide them with greater insights and automation than any of the competitive products they evaluated, while taking full advantage of the speed and scale of an integrated platform. With out-of-the-box support for Continuous Diagnostics and Mitigation (CDM) within the CISA framework, we are now working toward a Phase Two agency wide roll-out of our Cybersecurity Asset Management solution, representing a significant upsell opportunity for us.

Beyond this win, we're pleased to announce Qualys has recently received agency authorization for FedRAMP High. With this authorization, Qualys is the only FedRAMP High platform offering inventory, vulnerability management, patch management, CSPM, container security, and endpoint detection and response (EDR) in a single unified workflow across hybrid environments. As government agencies increasingly transition workloads from on-prem environments to the cloud, this achievement marks a significant milestone and establishes Qualys as the only modern alternative to legacy scanners for federal, state, and local agencies. Our authorization, consolidated platform, and continued investment in public sector expansion underscore our commitment to this market and position Qualys well to drive long-term, incremental growth. That momentum was on full display at our second annual Public Sector Cyber Risk Conference in May where we were especially encouraged by the strong turnout and positive feedback to the concept of a Risk Operations Center to bring efficiency to government agencies instead of playing risk whack-a-mole with multiple siloed legacy solutions.

Investing in our partner ecosystem remains another key pilar of our growth agenda. Through our Strategic Technical Alliance Program, we are driving deep technology integrations, co-selling opportunities, and demand generation programs. We believe this expanding ecosystem bolsters our capacity, harnesses transformative solution sales, and brings new business to Qualys. Additionally, we have advanced our global ROC ecosystem by certifying three new strategic mROC partners who wanted to partner with Qualys to bring the ROC to their customer base. With growing channel momentum, and a growing pipeline of fresh new mROC services being offered to customers, we look forward to sharing some exciting new wins in the coming quarters.

With more and more customers and partners beginning to perceive Qualys as a leading pre-breach risk management platform that consolidates and orchestrates multiple security solutions and workflows, I'm pleased to announce May Mitchell as our newly appointed Chief Marketing Officer. Pipeline creation, growing module adoption, winning new business, and evangelizing the AI-native ROC are key priorities. With May at the helm, and her long experience in cyber security, we are intensifying our marketing activities and increasing focus on ramping top-of-funnel initiatives and enhancing brand awareness to help drive adoption of the Qualys platform to new heights.

To further accelerate awareness and unleash new Qualys capabilities for customers, I'm also pleased to announce the launch of our Qualys platform pricing model, where we enable customers to purchase Qualys Units (QLUs) providing access to the entire platform and flexibly utilize the Qualys modules of their choice over the course of their subscription term. Instead of purchasing Qualys modules individually, organizations can now adopt the products they need today and in the future through a frictionless process designed to flexibly replace existing technologies and seamlessly switch between Qualys modules. Customers are expressing strong enthusiasm for this new pricing model, and we believe it will further enhance long-term customer loyalty, drive larger lands, reduce costs, and bolster cyber resilience over time with more customers adopting more Qualys solutions faster.

In summary, Qualys is well armed with fresh new capabilities, a new agency authorized FedRAMP High solution for government-wide use, strong channel momentum, and flexible platform pricing to help customers unify pre-breach risk management workflows, reduce costs, and address today's toughest security challenges. With trusted innovation and early ROC adoption, we're strengthening our position as the partner of choice for customers ready to centralize their response to cyber risk,

and believe we are poised to outpace our competitors, extend our thought leadership, and build upon an already strong foundation to drive durable long-term growth in the business.

With that, I'll turn the call over to Joo Mi to further discuss our second quarter results and outlook for the third 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 second quarter results, revenues grew 10% to $164.1 million. The channel continued to increase its contribution, making up 49% of total revenues compared to 46% a year ago. Revenues from channel partners grew 17%, outpacing direct, which grew 4%. 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 57% and 43%, respectively.

In Q2, despite ongoing macroeconomic uncertainty our gross retention rate and upsell execution improved with our net dollar expansion rate at 104%, up from 103% last quarter.

In terms of product contribution to bookings, Patch Management and Cybersecurity Asset Management combined made up 16% of total bookings and 26% of new bookings on an LTM basis. Our Cloud Security solutions, TotalCloud CNAPP, made up 5% of LTM bookings.

Turning to profitability, adjusted EBITDA for the second quarter of 2025 was $73.4 million, representing a 45% margin, compared to a 47% margin a year ago. Operating expenses in Q2 increased by 15% to $67.7 million driven by investments in sales and marketing and R&D.

Demonstrating our ability to innovate and invest in our long-term growth initiatives while remaining capital efficient, EPS for the second quarter of 2025 grew 11% to $1.68. Our free cash flow was $32.4 million, representing a 20% margin, compared to 33% in the prior year, due to fluctuations in working capital. Normalizing for this, first half 2025 margin was 43% compared to 45% in the prior year. In Q2, we continued to invest the cash we generated from operations back into Qualys, including $1.3 million on capital expenditures and $49.2 million to repurchase 375 thousand of our outstanding shares. Since commencing our share repurchase program in February of 2018, we've repurchased 10 million shares and returned over $1.1 billion in cash to shareholders. As of the end of the quarter, we had $254.6 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 $656 to $662 million, which represents a growth rate of 8% to 9%. This compares to prior guidance of $648 to $657 million. For the third quarter of 2025, we expect revenues to be in the range of $164.5 to $167.5 million, representing a growth rate of 7% 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 2025.

Shifting to profitability guidance. For the full year 2025, we expect an EBITDA margin in the range of low-to-mid 40s, implying a 15% to 17% increase in operating expenses and a free cash flow

margin in the mid 30s. We expect full year EPS to be in the range of $6.20 to $6.50, up from the prior range of $6.00 to $6.30. For the third quarter of 2025, we expect EPS to be in the range of $1.50 to $1.60. Our planned capital expenditures in 2025 are expected to be in the range of $7.0 to $9.0 million; and, for the third quarter of 2025, in the range of $1.0 to $3.0 million.

We continue to believe organizations will increasingly adopt cloud-native, full-stack security and compliance coverage to meet the demands of today's threat landscape and reduce costs. As the impact of the macro economy unfolds, we are closely monitoring the business environment and will continue to adjust our priorities accordingly. That said, considering the long-term growth opportunities ahead of us and our industry leading margins implying further room for investment, we intend to continue to responsibly align our product and marketing investments to focus on high-impact initiatives aimed at driving more pipeline, accelerating our partner program, and expanding our federal vertical. As a percentage of revenues, we expect to prioritize increased investment in S&M and engineering, with a more modest increase in G&A, consistent with our commitment to balance long-term growth and profitability.

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