Qualys Q2 FY2026 Earnings Prepared Remarks

Foster City, Calif., – August 4, 2026 – 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, 2026.

Blair King, Investor Relations

Good afternoon, and welcome to Qualys' second quarter 2026 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 product capabilities, 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.

The adversary's playbook has been fundamentally rewritten by AI, collapsing exploit timelines, and making one thing undeniably clear. Durable pre-breach risk management increasingly requires a vendor-neutral, agentic AI risk fabric that moves beyond theoretical exposure to autonomous quantification of actual exploitable risk and remediation. Demonstrating this conviction, we delivered another quarter of strong revenue growth and profitability.

Platform Innovation:

The urgency behind that conviction continues to intensify. Frontier and open-source AI models are capable of discovering and weaponizing vulnerabilities faster than any human team can triage them, compressing exploit timelines to hours and, in some cases, turning disclosure into compromise before a patch even exists. AI is simultaneously becoming the greatest force multiplier and the most formidable challenge cybersecurity has ever faced. Where we part ways with Continuous Threat Exposure Management (CTEM) solutions is how we respond to it. CTEM solutions today respond by generating more findings, more theoretical risk scores, and more

dashboards, and then pass those findings off to siloed solutions that collect data and do the patching, while losing critical time at every handoff. That approach was already failing before AI accelerated the threat landscape, and it is fundamentally inadequate now. We believe the defenders who win in this new era of AI will not be the ones who simply detect more and more vulnerabilities and produce dashboard tourism. They will be the ones who can autonomously detect vulnerabilities at AI-speed, validate actual exploitability in production, quantify that risk in dollar terms, remediate it, and then prove the exposure is closed in multi-vendor environments, all before an adversary gets there first. That is the designed outcome of the AI-native Risk Operations Center (ROC) powered by our Enterprise TruRisk Management (ETM) solution, and it is where nearly every customer conversation we're having is heading.

Against this backdrop, I'm pleased to announce major new capabilities on the platform we'll be showcasing at Black Hat later this week, spanning both AI for security and security for AI to address the post-Mythos threat landscape head-on.

First, with respect to AI for security, we are pleased to introduce InstaScan, powered by Agent Insta, the newest addition to our agentic AI marketplace and ETM solution for AI-speed detection that is continuous, instantaneous, and scanless. Today, when a new vulnerability advisory is released, it can take 24 hours to a week for organizations to detect it through traditional scan cycles, while adversaries weaponize that same vulnerability in minutes. Agent Insta is designed to collapse that timeline. By converting the asset inventory, software paths, and advisory intelligence our customers already collect with Qualys sensors into high-confidence exposure findings without a scan, new detections appear within minutes of disclosure with no re-scan required and no agent disruption. The finding is then handed to Agent Val for instant exploit validation, and the risk impact is determined and quantified immediately. When competitors are still processing an advisory, writing signatures, and waiting for a scan to complete, our customers already know whether they are exposed and are taking action before a vendor patch exists.

Because the finding flows straight into validation and remediation, detection is not a report. It is the first step of a continuous closed loop. With last quarter's launch of TruConfirm and Agent Val safely validating actual exploitability across chained attack paths in live production environments and hyper-prioritizing millions of findings to the fewer than one percent that require immediate action, the bottleneck is now shifting from identifying what to fix to actually fixing it before adversaries can act.

This leads me to the next phase of our TruRisk Eliminate agenda, autonomous zero-day remediation at scale. Through AI-scored autonomous remediation waves, the AI-native ROC now determines the right action for every asset in multi-vendor environments, deploying a patch where confidence is high, staging a controlled rollout where caution is warranted, or applying a compensating control when operational risk demands it. Every action is gated by our AI driven Patch Reliability Score and resiliency snapshots, delivering rollback rates below one half of one percent. The most critical assets retain human-in-the-loop oversight while the platform autonomously remediates the rest. Orchestrating the cycle is Agent Sara, which prioritizes exploitable risk, quantifies it in dollar terms, sequences continuous waves, and revalidates closure with Agent Val, all without proportional headcount. Furthermore, with the introduction of peer-to-peer patching, we are accelerating the delivery across distributed environments while removing the dependencies on centralized infrastructure. Put simply, these newest innovations make autonomous zero-day remediation wave-driven, vendor agnostic, safe, and provable. In live benchmarking, this collapsed the window of exposure from 21 days to minutes and auto-patched 60 percent of vulnerabilities. That is not incremental. It turns a 6.5x surge in exploitable

vulnerability volume from an impossible backlog into a continuously cleared queue at the speed of modern attacks. You cannot solve a minute's problem with a month-long solution, and that's the gap the AI-native ROC was designed to solve with Agent Insta providing AI-speed detection, Agent Val hyper-prioritizing validated exposures, and Agent Sarah performing autonomous remediation in a continuous closed loop.

Turning to security for AI. As enterprises race AI workloads into production, the AI infrastructure they are building is already the next attack surface. With the introduction of TotalAI 2.0, organizations can now see their full AI estate from workforce to workloads and from code to runtime. Through new sensors that see AI activity at both the employee and workload level, security teams can now discover shadow AI activity across the organization, from what employees are doing with AI to which models, endpoints, and services are running in production across hybrid multi-cloud environments. We have also extended our posture management coverage to SaaS platforms, including Anthropic and OpenAI, to help organizations enforce security and compliance policies across the AI platforms their teams are already using. Additionally, they can now identify security gaps in code before deployment, remediate with guardrails at runtime, and test Model Context Protocol (MCP) tool exploits across over fifty adversarial scenarios. And, of equal importance, every AI risk across the entire stack, from GPUs to infrastructure to supply chain to the newest prompt injection-based attacks, is now scored and prioritized through the same TruRisk engine that powers the ROC. For organizations seeking to secure the infrastructure powering their AI future, these newest innovations become an increasingly strong differentiator for Qualys.

As ROC adoption accelerates and these capabilities continue to compound, we remain laser-focused on driving ETM adoption throughout our Vulnerability Management Detection and Response (VMDR®) customer base and positioning Qualys for larger upsell opportunities over time.

Q2 Business Update:

Moving to our business update. With customers spending $500,000 or more with us growing 8% from a year ago to 229, let me share a couple of recent wins, which illustrate why organizations are turning to Qualys to help unify their security stacks and operationalize the ROC.

The first is with an existing global 300 customer managing a complex, data-intensive environment spanning on-prem, multi-cloud, and a rapidly growing number of Large Language Models (LLMs) in production. As the volume and velocity of vulnerabilities across this environment accelerated, their teams recognized that prioritization based on theoretical risk scores couldn't deliver the business context needed to act decisively. With fragmented telemetry, disconnected tools, and little automation, their teams were spending more time documenting risk than reducing it, while unpatched assets and shadow IT were silently extending exposure windows by months. As a result, this customer chose Qualys to operationalize the ROC, adopting VMDR, ETM, TruRisk Eliminate, and TotalAI alongside several other modules in a low-seven-figure QFlex annual upsell. By consolidating Qualys and third-party data into a unified risk fabric, this customer has aligned risk reporting to the Board's tolerance level, shifted remediation from manual processes to autonomous workflows, and reduced its exposure window from months to hours while flattening the hiring curve and delivering better security outcomes. This is also an outstanding example of how we are leveraging our channel partners to activate the ROC and win new business.

The second is with a European healthcare company that had been a small existing scan on behalf

Qualys customer but was relying on a managed service provider to run its broader vulnerability management program across more than 140 locations. That model delivered people and process, but not autonomy. Scan operations, prioritization, and remediation guidance all flowed through the provider's team on the provider's timeline, leaving this customer dependent on external resources to understand and act on its own risk. As their environment grew more complex and vulnerability volumes surged, the limitations of that dependency became unsustainable. Costs were ballooning, remediation cycles were stretching longer, and the customer had limited visibility into the very data driving the decisions made on its behalf. This customer chose Qualys to consolidate its stack onto the Qualys platform by adopting VMDR, ETM, and TruRisk Eliminate in a six-figure QFlex upsell. ROC automation was the entry point, and remediation was the immediate proof of value. By unifying detection, prioritization, and autonomous remediation into a single AI-native workflow, this customer has replaced a manual people and process dependency with a platform that delivers significantly lower costs, less complexity, full control, and peace of mind for the CISO.

These wins reflect the broader ETM momentum we are starting to see as more and more customers recognize the efficiencies and scale of AI-native ROC automation.

Further supporting our growth trajectory, QFlex continues to gain traction as another strategic lever for accelerating ETM adoption. As you heard in the customer wins I described earlier, QFlex played a direct role in enabling significant upsells for Qualys by giving those customers the flexibility to commit broadly across the platform while preserving the ability to shift investment as their needs evolve. That’s precisely the value proposition our QFlex model was designed to deliver. Building on strong results from our initial rollout, we have now taken QFlex live for enterprise customers looking to expand with Qualys and believe it can become an increasingly important driver of platform expansion over time.

Turning to our executive team. With the recent departure of our CISO and General Manager of our ETM business, I want to address how we are positioning for continuity and acceleration. To lead product strategy and our ETM business going forward, I appointed Shailesh Athalye as our Chief Product Solutions Officer, a nearly 14 year Qualys veteran who has served as our Senior Vice President of Products for the last 5 years. Shailesh has been instrumental in shaping many of the platform innovations we discussed today, and his deep institutional knowledge of our technology, our customers, and our roadmap makes him the natural leader to drive the next phase of ETM adoption and our product-led growth strategy. Additionally, I am pleased to welcome Nathan Smolenski as our new Chief Information Security Officer. Nathan is a seasoned cybersecurity executive with over 24 years of experience driving security transformations across financial services, insurance, and high-growth SaaS environments, most recently serving as Global CISO at Cyera. We are excited to have both Shailesh and Nathan in these critical roles as we continue to scale our platform and accelerate ROC adoption.

In summary, Qualys’ continuous innovation spanning both AI for security and security for AI, growing AI-native ROC adoption powered by our ETM solution, a growing federal pipeline of new business opportunity, strong partner-led execution, and promising early QFlex engagement continue to reinforce the demand we’re seeing for a unified risk management platform that autonomously moves beyond theoretical exposure to validated, quantified, and remediated risk at the speed of modern attacks in multi-vendor environments. We believe these achievements not only advance our strong competitive differentiation but also sharpen the market opportunity ahead of us and bolster our confidence in reaccelerating 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 2026.

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 11% to $182.2 million. As a result of our strategic emphasis on leveraging our partner ecosystem to drive growth, the channel continued to increase its contribution, making up 54% of total revenues compared to 49% a year ago. Revenues from channel partners grew 22% with revenues from direct remaining largely unchanged from Q2 of last year. By geo, 15% growth outside the US was ahead of our domestic business, which grew 8%. US and international revenue mix was 55% and 45%, respectively.

In Q2, our overall upsell execution improved with our net dollar expansion rate at 105%, up from 104% last quarter. The net dollar expansion rate of customers with prior year purchase of ETM or CSAM subscriptions in Q2 was 107%, consistent to last quarter's. Moving on to product mix, our differentiated new products continued to drive growth. First, ETM/CSAM combined made up 12% of total bookings and 14% of new bookings on an LTM basis in Q2, up from last year's 9% and 10%, respectively. Next, Patch Management made up 9% of total bookings and 16% of new bookings on an LTM basis in Q2. This compares to 7% and 16%, respectively, in Q2 of last year. Lastly, TotalCloud made up 5% of total LTM bookings in Q2, unchanged from a year ago. We believe that these differentiated products combined will increase contribution to bookings in 2026, given our opportunity to increase market share and maximize share of wallet.

Reflecting our scalable and sustainable business model, adjusted EBITDA for the second quarter of 2026 was $83.8 million, representing a 46% margin, compared to 45% last year. Operating expenses in Q2 increased by 8% to $73.2 million, driven by investments in Sales & Marketing, which grew 14%. With this strong performance, EPS for the second quarter of 2026 was $1.98 per diluted share, and our free cash flow was $55.9 million, representing a 31% margin, compared to 20% in the prior year, due to fluctuations in working capital. Normalizing for this, first half 2026 margin was 42%, compared to 43% in the prior year. In Q2, we continued to invest the cash we generated from operations back into Qualys, including $3.7 million on capital expenditures and $76.8 million to repurchase 797 thousand of our outstanding shares. As of the end of the quarter, we had $229.8 million remaining in our share repurchase program.

With that, let us turn to guidance, starting with revenues: For the full year 2026, we now expect revenues to be in the range of $732.0 to $738.0 million, which represents a growth rate of 9% to 10%. This compares to prior guidance of $721.0 to $727.0 million. For the third quarter of 2026, we expect revenues to be in the range of $185.5 to $187.5 million, representing a growth rate of 9% to 10%. This guidance assumes our net dollar expansion rate remains at current levels, with moderate growth contribution from new business in 2026.

Shifting to profitability guidance, for the full year 2026, we expect EBITDA margin to be in the mid 40s with low-teens increase in operating expenses and free cash flow margin in the low 40s. We expect full year EPS to be in the range of $7.74 to $7.88, up from the prior range of $7.44 to $7.65. For the third quarter of 2026, we expect EPS to be in the range of $1.91 to $1.98. Our planned capital expenditures in 2026 are expected to be in the range of $8.0 to $12.0 million; and, for the third quarter of 2026, in the range of $1.0 to $2.5 million.

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