Qualys Q3 FY2026 Earnings Prepared Remarks

Foster City, Calif., – November 9, 2026 – Qualys, Inc. (NASDAQ: QLYS), a leader in cloud-native cyber risk management, today announced financial results for the third quarter ended September 30, 2026.

Blair King, Investor Relations

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

AI has fundamentally transformed the adversary's playbook, graduating from accelerating existing attack techniques to autonomously operating inside live production environments. To put the scale of that shift in perspective, Microsoft's recent Patch Tuesday disclosed 1,414 new vulnerabilities in a single release compared to 93 before the advent of frontier AI models. That's a 15-fold increase in exposure volume within the last seven months alone that every enterprise must now absorb in real time. Within 10 minutes of Microsoft publishing that advisory, Agent Insta, powered by InstaScan, posted scanless detections in a customer's environment, giving them an immediate view of their exposure. No scan cycle. No agent disruption. No days-long wait. That's detection at AI-speed. But detection alone changes nothing if what follows still takes weeks, still relies on manual handoffs, and still can't prove the exposure is closed. Events like the PHP2Shell disclosure, and others are just a warning of what lies ahead, and the need for speed from disclosure to remediation is clear. Durable pre-breach risk management requires a vendor-neutral, agentic AI risk fabric that can autonomously transform detection into proven remediation of actual exploitable risk at the speed of modern attacks. Against this backdrop, we delivered another strong quarter of revenue growth and profitability alongside one of our most

meaningful quarters of platform innovation to date.

Platform Innovation:

That execution reflects a clear shift in how customers evaluate and select their security platforms. The traditional Continuous Threat Exposure Management (CTEM) model wasn't built for this moment, and it shows. More findings, more theoretical risk scores, more dashboards, and more handoffs, each one a gift of time to an adversary that now operates at machine speed. When customers can't patch fast enough to outrun autonomous exploitation, the last thing they need is another tool that tells them what's wrong and passes the problem to someone else to fix. CISOs are looking to update their boards with a plan of action against autonomous exploitation, including a roadmap for autonomous remediation instead of more manual tools and processes. That architecture was already losing before the frontier AI era. Today, against an AI-powered adversary, it's indefensible. We developed the vision and built the AI-native Risk Operations Center (ROC), powered by our Enterprise TruRisk Management (ETM) solution over three years ago, to end that cycle entirely. Today, Agent Insta, powered by InstaScan, is detecting newly exposed vulnerabilities on customer systems in less than 60 minutes after disclosure on average. Agent Val, powered by TruConfirm, has already performed approximately 9 million exploit validations across customer environments, and just 11% of those confirmed actual exploitability, eliminating 89% of the noise that would have otherwise consumed security and IT resources. And, TruRisk Eliminate with Agent Sara has helped customers deploy over 180 million patches in the last twelve months alone, with 60% of those running autonomously, doubling from 30% a year ago, at a rollback rate of fewer than 1 in 8,000. Together, they operate natively in a continuous closed-loop that proves autonomous closure within hours, not weeks. The AI-native ROC isn't a roadmap. It's not a vision slide. It's operational, measurable, and provable, and it's where nearly all enterprise and federal customer conversations are centered.

Carrying this momentum forward, we're further evolving our ETM and TruRisk Eliminate capabilities through an expanding ecosystem of remediation solutions. Over the last two quarters, we introduced our AI-powered Patch Reliability Score, Agent Sara's wave-based remediation, peer-to-peer patching, and AI-guided rollbacks. The cumulative effect of our TruRisk Eliminate agenda gives organizations confidence to deploy in production environments with rollback rates below one-tenth of one percent across well over half a billion patches delivered to date, including more than 200 million executed autonomously. That customer confidence is translating into accelerating adoption, with patch deployments up 47% from the advent of frontier models in early April of this year and autonomous deployments growing even faster.

The biggest blocker to faster patching is a lack of confidence in operational outcomes. At our recent ROCon conference in Austin, we built on this foundation by announcing what we call Autonomous RemOps, brought to life through TruRisk Eliminate 2.0 with TruConfidence. TruConfidence is a remediation and orchestration intelligence engine delivered on a straightforward operating principle: fix the minimum, credit existing controls, choose the right remediation path, control the rollout, and prove that it held. Three new capabilities represent meaningful new ground for Qualys. First, before a corrective action is raised, TruConfidence assesses the protection already provided by third-party security controls, so customers don't duplicate efforts. Second, it extends coverage beyond endpoints to cloud, applications, perimeter, and edge assets, including routers, switches, firewalls, and air-gapped infrastructure that historically sat outside response workflows because they can't run an agent. And third, building on the rollback capabilities we introduced last quarter, post-deployment operational resiliency monitoring through partners like Dynatrace now tracks system health to confirm the environment

remained stable post-patch. When a patch doesn't hold, AI-powered Patch Failure Analysis explains root causes in plain language and recommends corrective action. The result is an AI-native ROC that serves as both the system of record and the system of action for cyber risk reduction. Other vendors entering the mitigation conversation are orchestrating a handoff on agent-based endpoints and passing a patching recommendation to a third-party tool, without giving the operational confidence and no verification that the fix was successfully applied or that the environment remained stable afterward. The Qualys platform was purpose-built to eliminate that handoff entirely and delivers natively integrated Autonomous RemOps with TruConfidence at scale, rapidly proving closure across every domain and asset type. With Qualys, no asset, whether it runs an agent or not, and no exposure, whether a patch exists or not, will be left without an immediate path to closure.

Our continuous innovation and industry-leading capabilities are now garnering significant recognition from customers, partners, and independent analysts. In the 2026 Forrester Wave for Proactive Security Platforms, Qualys received the highest rating among all evaluated vendors on key criteria, including network visibility, exposure, business-driven prioritization, and remediation. Additionally, KuppingerCole named Qualys the highest-rated leader in its 2026 Leadership Compass for Attack Surface Management, earning the top position in both Product and Market Leadership. Both underscore our customer-driven engineering and growing competitive differentiation across the platform.

Q3 Business Update:

Moving to our business update, the number of customers spending $500,000 or more with us grew 15% from a year ago to 243. Let me now share a couple of recent wins, which illustrate why organizations are turning to Qualys to help unify their security stacks, operationalize the ROC, and put autonomous remediation to work.

First, we closed a new low seven-figure annual bookings deal with a large government agency. This agency had been running an on-prem vulnerability management program for years, scanning with one vendor, manually triaging across disconnected dashboards, and handing patch cycles off to yet another vendor. As detection volumes surged, the model was breaking down. Response backlogs were growing, and the agency kept falling further behind. Seeking to streamline operations, this agency ran a highly competitive process and selected Qualys to help activate its ROC on a single, FedRAMP High authorized platform. In doing so, it landed with seven Qualys modules right out of the gate, including ETM, ETM Identity, VMDR, TruRisk Eliminate, Policy Audit, TotalCloud, and TotalAppSec. The net result is that this agency has now consolidated a fragmented, multi-vendor workflow onto a unified AI-powered risk fabric. A fabric that detects exposures within minutes of disclosure, validates actual exploitability so teams can act on real risk rather than theoretical scores, and automates response by natively applying patches and other compensating controls when patches are too risky to deploy or unavailable. What used to take weeks from detection to confirmed fix now takes hours, and a patch backlog that had been compounding security debt for years is now under control. Given the success of this deployment, this customer is also now actively evaluating TotalAI and planning to deploy agentic AI workflows across its operations.

The second was with an existing large federal agency, which had struggled to manage its cloud and infrastructure security using siloed tools, while manually consolidating findings with no unified view of risk. Prioritization relied on CVSS severity scores rather than validated exploitability, and their security and IT teams were making critical decisions on incomplete data. Threat response

had historically followed a pattern we hear all too often: security operations identified a vulnerability, opened a ticket, and handed it to an IT team running a third-party patching tool, a cycle that averaged weeks from identifying threats to assumed fix. With the advent of the Cybersecurity and Infrastructure Security Agency's (CISA) Binding Operational Directive (BOD) 26-04, which requires agencies to operationalize risk-based remediation and addresses AI-accelerated threats that compress exploit timelines to hours, that cycle was no longer sustainable. Our own Threat Research Unit's five-year analysis of more than 1.5 billion critical vulnerability instances shows that Qualys customers have already remediated approximately 173 million exposures before they ever entered CISA's Known Exploited Vulnerabilities (KEV) catalog, which is exactly the kind of proactive posture this directive now demands. In response, this customer evaluated several solutions and chose Qualys to operationalize its ROC automation. Where competing solutions aggregated data and continued to generate theoretical risk insights, Qualys was the only platform in this evaluation that could detect at AI-speed across hybrid environments, hyper-prioritize millions of findings to the exposures that genuinely required immediate action, and autonomously fix them. That translated into bringing third party data sources into the platform while consolidating several siloed tools into a seven-figure annual bookings upsell, adding ETM and TruRisk Eliminate while expanding its existing Qualys footprint. This customer is now aligning with the agency's risk tolerance across nine separate bureaus, unifying detection with Agent Insta, exploitability-based prioritization with Agent Val, and recognizing the operational efficiencies and speed of autonomous, wave-based zero-day remediation with Agent Sara.

These wins, alongside several other six and seven-figure federal and state wins in Q3, underscore the growing demand we see in our federal, state, and local government business, driven in part by agencies moving to meet these new operational requirements. They also reflect a consistent pattern we see across the business as more and more customers move from evaluating the AI-native ROC to operationalizing it.

Complementing this momentum, QFlex is emerging as an effective lever for platform adoption and ETM expansion. In the first full quarter following General Availability, QFlex customers increased their average annual bookings by over 20% compared to their prior year annual bookings, while many added new modules to their subscriptions. Both wins I just described are direct examples of QFlex in action. The new federal agency customer consolidated onto a QFlex commitment spanning all seven modules from day one, while the existing agency added ETM and TruRisk Eliminate while expanding deployment on a footprint that already included seven Qualys modules. In both cases, QFlex gave them the flexibility to commit more extensively across the platform while preserving the ability to shift investment as their risk priorities evolve. That's the commercial pattern QFlex was designed to create. Customers commit at a higher level because the model removes the friction of predicting exactly which modules they might need twelve months from now, which, in turn, drives higher utilization across the platform and positions us for larger upsells over time.

Turning to our strategic alliances, I'm pleased to announce that we recently delivered several new technology integrations spanning mobile, identity, Internet of Things (IoT), and OT systems. As more organizations adopt the AI-native ROC as their autonomous risk fabric for pre-breach risk management, the value of that fabric grows with every new source of risk intelligence it can ingest, normalize, prioritize, and act on. These partnerships strengthen our multi-vendor architecture, extend the ROC's coverage, and serve as a key differentiator for Qualys.

In summary, over three years ago, we set out to transform Qualys from a company steeped in vulnerability management, detection, and response to a holistic, vendor-neutral pre-breach risk

management platform defined by measurable, proactive, and automated risk reduction at scale. This quarter, with the AI-native ROC operational and gaining customer momentum, TruRisk Eliminate with TruConfidence extending our reach to every asset type, a growing federal business, strong product roadmap, and early QFlex adoption broadening how customers commit to the platform, we are seeing the clearest evidence yet that organizations are choosing Qualys because we don't stop at just telling them what's wrong, we prove it's fixed. That's now driving larger commitments, deeper adoption, and stronger competitive differentiation while reinforcing our confidence in durable long-term growth.

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 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 third quarter results, revenues grew 11% to $188.0 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 55% of total revenues compared to 50% a year ago. Revenues from channel partners grew 24%, offsetting a 2% decline in direct. By geo, 15% growth outside the US was ahead of our domestic business, which grew 7%. US and international revenue mix was 54% and 46%, respectively.

In Q3, our overall net dollar expansion rate remained unchanged from last quarter's 105% but the net dollar expansion rate of customers with prior year purchase of ETM or CSAM subscriptions improved to 108%, up from 107% last quarter. Moving on to product mix, ETM/CSAM combined made up 12% of total bookings and 14% of new bookings on an LTM basis in Q3, up from last year's 10% and 11%, respectively. Next, Patch Management made up 9% of total bookings and 18% of new bookings on an LTM basis in Q3. This compares to 8% and 16%, respectively, in Q3 of last year. Lastly, TotalCloud made up 5% of total LTM bookings in Q3, unchanged from a year ago. ETM and CSAM, combined with Patch Management, are driving a meaningful shift in our bookings composition toward higher-value solutions, and we expect that trajectory to continue as customers deepen their engagement with the platform. TotalCloud remains an important growth lever for the business, and we are focused on improving adoption within our customer base.

Reflecting our scalable and sustainable business model, adjusted EBITDA for the third quarter of 2026 was $89.9 million, representing a 48% margin, compared to 49% last year. Operating expenses in Q3 increased by 11% to $72.2 million, driven by investments in Sales & Marketing, which grew 17%. With this strong performance, EPS for the third quarter of 2026 was $2.12 per diluted share, and our free cash flow was $100.0 million, representing a 53.2% margin, compared to 52.7% in the third quarter of last year. In Q3, we continued to invest the cash we generated from operations back into Qualys, including $1.8 million on capital expenditures and $53.6 million to repurchase 330 thousand of our outstanding shares. As of the end of the quarter, we had $176.1 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 $736.9 to $738.9 million, which represents a growth rate of 10%. This compares to prior guidance of $732.0 to $738.0 million. For the fourth quarter of 2026, we

expect revenues to be in the range of $191.0 to $193.0 million, representing a growth rate of 9% to 10%.

Shifting to profitability guidance, for the full year 2026, we expect 46% EBITDA margin with a low double-digit increase in operating expenses and free cash flow margin in the low 40s. We expect full year EPS to be in the range of $8.07 to $8.14, up from the prior range of $7.74 to $7.88. For the fourth quarter of 2026, we expect EPS to be in the range of $2.05 to $2.12. Our planned capital expenditures in 2026 are expected to be in the range of $9.5 to $11.5 million; and, for the fourth quarter of 2026, in the range of $2.3 to $4.3 million.

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