Qualys.

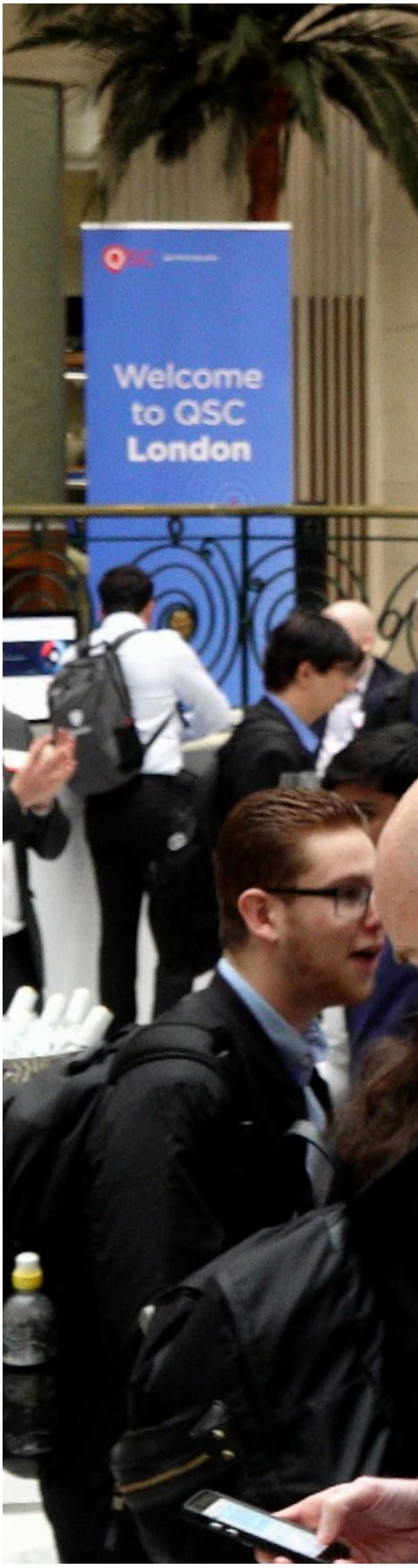
QSC

Introducing
QSC 2022

The Qualys Security Conference is a roadshow with 10 locations across the globe. The event showcases best practices through customer, technical, and thought leader sessions – with plenty of time to network with peers and Qualys experts.

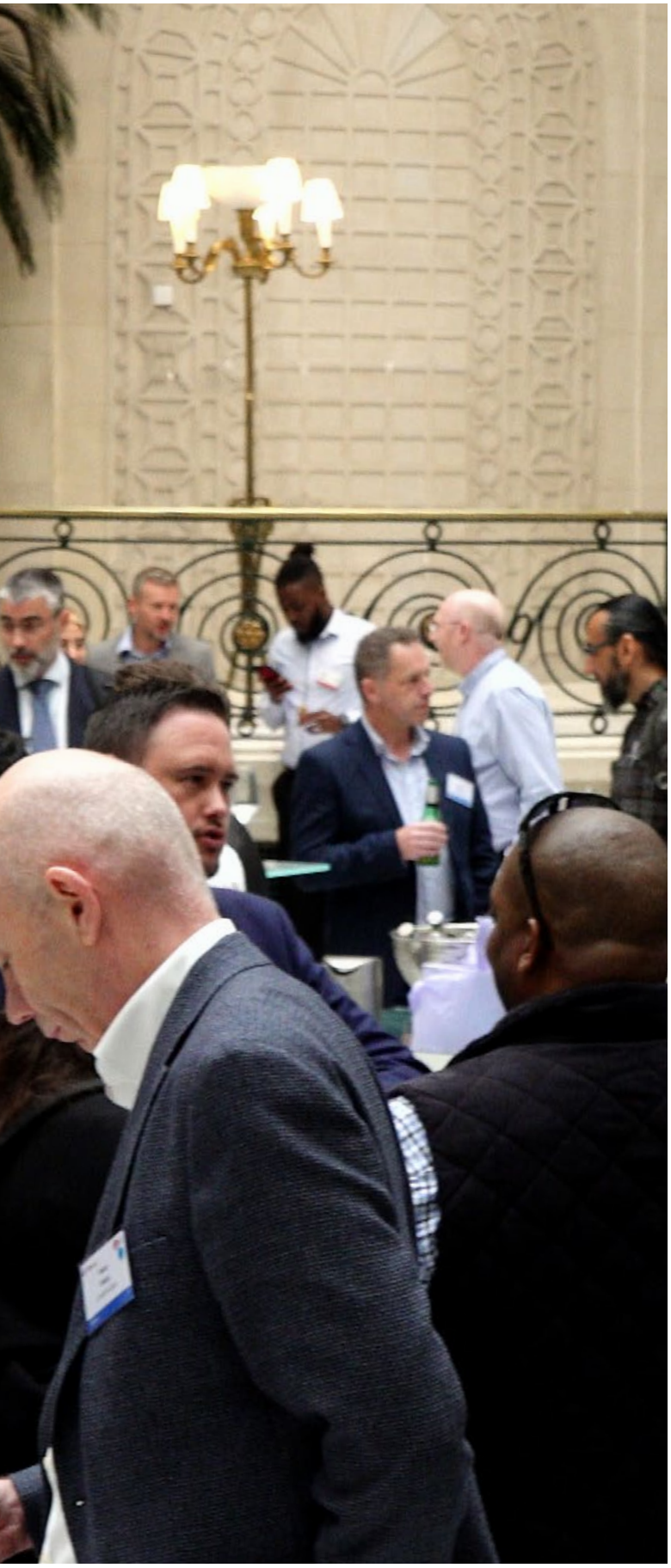
We're back in London, and welcome, everyone

Thank you for joining us at the Qualys Security Conference (QSC) 2022 in London. Approximately 300 cybersecurity professionals from around the world gathered at the Waldorf Hilton for a very special QSC, the first since the start of the coronavirus pandemic.



They are joining our CEO and other top executives to talk about cybersecurity challenges faced by organizations, as well as the solutions Qualys provides. The California company counts 66% of the Forbes Global 50 and 46% of the Forbes Global 500 as customers.

The day-long conference was prefaced by a training day, during which attendees were invited to hone their skills on Qualys programs. During the event, Qualys leaders outlined their vision and unveiled upcoming product updates. Representatives from organizations including bp, Cargotec, the University of Westminster, Anglo American, Sky Betting & Gaming, Endpoint Remediation, and Parity Technologies took the stage to reveal their experiences with Qualys products, and post-lunch, the CISO Exchange (powered by Pulse Conferences) encouraged guests to be honest about their challenges and swap ideas.



“

It was fantastic to have so many people attend. The conference provided the opportunity to learn from one another, share problems, find solutions, and determine industry trends. For example, there was a lot more interest in automation from CISO than I expected. In cyber security, there is no destination – it’s a journey. We are moving in the right direction regarding how we can simplify security and reduce costs. Qualys is leading the way with innovation and solving problems. We’re hoping to continue and strengthen our association with our customers and be there alongside them on this journey.

Sumedh Thakar
President and CEO, Qualys

Qualys.

Analysing the cyber threat landscape in 2022

Qualys continues to strengthen association with our customers and be alongside them on the journey to better secure business assets on the digital journey. Our continuous security intelligence platform mitigates risk, detects and responds to threats, and improves compliance posture.

Qualys in action

More than

6bn

IP scans / audits undertaken a year

More than

50k

scanner appliances

77m

Cloud agents across servers, endpoints, clouds and containers

More than

2trn

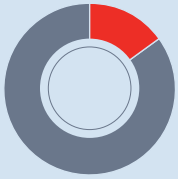
security events collected in real-time

More than

10trn

data points scanned – providing two-second visibility

Conti ransomware group focus

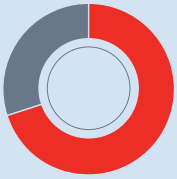


15%

Responsible for an estimated 15% of ransomware attacks

$175m

Generated approximately US$175 million income in 2021

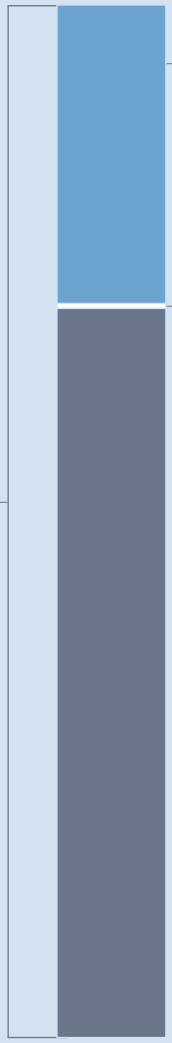


Up to

70%

of organisations compromised by ransomware pay

Vulnerabilities in numbers



185,446

Universe of **all known** vulnerabilities

29%

Vulnerabilities with **exploit available**

0.4%

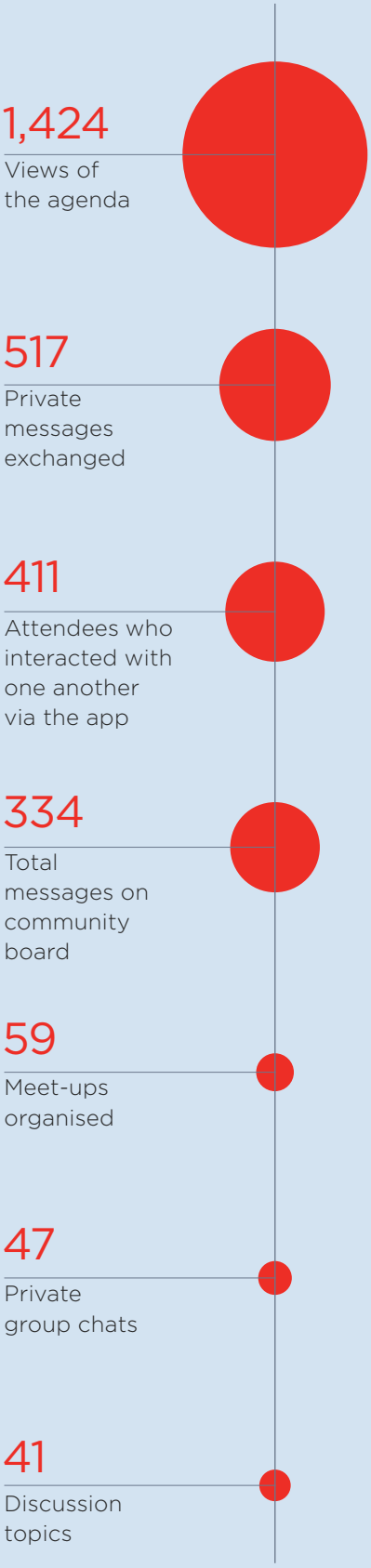
Number of vulnerabilities that cause **the most risk**

37 min

The **average time to remediation** for all compromised assets

Networking in action

Whova event app usage highlights



1,424

Views of the agenda

517

Private messages exchanged

411

Attendees who interacted with one another via the app

334

Total messages on community board

59

Meet-ups organised

47

Private group chats

41

Discussion topics

Why cybersecurity is more important now than ever

John Noble CBE was the keynote speaker. Mr Noble has extensive experience countering cyberthreats: as Director of Incident Management at the UK National Cyber Security Centre in a prior role, he oversaw the response to almost 800 severe cybersecurity incidents.

Mr Noble pointed to changes in our world over the last two years, and how that has made cybersecurity professionals more important. Mobile phones are increasingly coming under attack, cloud-related breaches are on the rise, and cyberattack tools have becoming more accessible, which means sophisticated ransomware attacks are becoming endemic.

Ransomware itself is changing, having grown from a cottage industry to a corporatized group, with some cybercriminals even mirroring capabilities previously shown by state actors. Industry reports claim up to
70% of ransomware victims pay up. While this saves victims from consequences, it also ends up feeding the cycle. Conti, a ransomware group thought to be responsible for 15% of cyberattacks, is estimated to
have earned $175 million in 2021.

There are several reasons for organizational compromise, but the root cause remains poor foundational cybersecurity. Patching – keeping software up to date – is the single most important thing a business should focus on, with multi-factor authentication a close second.

> Events like this that allow those involved in cyber security work to discuss these new challenges are vital. How great to have these essential conversations face to face with an amazingly high-quality group of attendees. I have learnt a lot. I am very grateful to Qualys for the invitation to speak. Talking to attendees, I know that they appreciate the effort that has gone into organising this event. The timing has been perfect.

John Noble CBE
Non-Executive Director, NHS Digital (and former Director at the National Cyber Security Centre)

A unified platform to solve today's cybersecurity conundrum

Shailesh Athalye, Qualys' Senior Vice President for Product Management followed. He talked about upcoming launches and additions to Qualys products, including VMDR 2.0, updates to CAR, and improvements to TotalCloud that will offer greater security for open-source software and better management of external attack surface.

Shailesh said Qualys is building a unified platform for customers in an attempt to directly address challenges at the ground level. Customers want a comprehensive reduction in cyber risks within their limited resources. One way to achieve this is by gaining more context around asset criticality. In response, Qualys has created a solution that stitches all siloed data together to better understand asset criticality and realize true risk, while providing asset context across the board. Qualys has also automated as much of the process as possible, so that manual interventions – and dependency – are reduced.

This unified security platform considers an individual business' point of view and offers unifying foundational controls for asset context, therefore securing endpoints across the environment. The automation of complex and time-consuming jobs that inhibit deep dives is another positive which will enable better and quicker decision-making from security teams.

Qualys in action: Three case studies

University of Westminster is remediating faster

Thierry Delaitre, Head of IT Developments at the University of Westminster, has found Qualys VMDR especially useful in the last two years, during the pandemic when hybrid teaching was necessary. The university supports more than 19,000 students across four campuses, and the digital landscape comprises 6,500 assets, with mobile devices making up 45% of all endpoints.

"If we can't see all the IT assets we have, we can't effectively manage risk – so improving visibility was one of the key factors for moving to Qualys VMDR," said Delaitre. "By deploying lightweight Qualys Cloud Agents on our systems, we have an instant overview of the operating system and software deployed across our estate."

Since employing VMDR, Delaitre and his team have tracked improvements across various security metrics. And by moving from a reactive to a proactive approach, the organization has reduced its average time to remediate vulnerabilities by 85%.

"Qualys shows us exactly which assets and vulnerabilities are present and helps us prioritize our remediation work," he added.
"For example, using data from Patch Management has enabled us to reduce the average number of vulnerabilities per device
on our Windows 10 estate by 93%."

Cargotec found coverage of blind spots better

Global logistics specialist Cargotec employs more than 11,000 people in 138 countries, making cybersecurity a significant challenge. Having accelerated its digital transformation journey
by moving to the cloud, there was an urgent need to enable effective vulnerability management
for thousands of IT assets. The ultimate plan
was to empower business units to explore innovative, data-driven services without compromising security.

Kevin Williams, Technical Lead of Cyber Security at Cargotec, said Qualys was chosen because it understood the core challenge – shining a light on vulnerability blind spots – better than its competitors. "From the outset, we were impressed," he continued. "Qualys knew exactly what we were trying to achieve and suggested effective ways to reach our goals."
Williams saw the modularity of the Qualys offering as a "big benefit". He said: "With the Qualys Cloud Platform, we can start with Qualys VMDR for vulnerability management and add new capabilities, from automated patching to cloud security assessments and more."

In the first four months, Cargotec reduced the number of active vulnerabilities by over 60% and cut the average number of issues detected per asset from 100 down to 35. "We are still in the early stages with Qualys and have already identified 1.1 million vulnerabilities," Williams added.

Sky Betting & Gaming gained scale, not headcount

Glenn Pegden, Security Vulnerability Manager at Sky Betting & Gaming, engaged Qualys in 2017, on the eve of the General Data Protection Regulation (GDPR) being introduced. His organization's goal has been to create compelling customer experiences, but compliance and information security are key focus areas in such a heavily regulated industry. He needed an accurate overview of all assets and system owners across the estate.

"First, we rationalized six separate configuration management databases (CMDBs) down to just one, wanting a single source of truth," he said. "As the business prepared for GDPR, we seized the opportunity to ask all teams to populate the new CMDB with up-to-date system ownership information." There were 8,000 assets across two production data centers, plus around 1,000 assets in the office and cloud locations.

"Today, 99% of our remediation work is handled automatically, which means we can spend our time investigating the edge cases," Pegden continued. "Thanks to the efficiencies we've gained with Qualys, we can keep our headcount flat, even as the IT landscape grows. For example, I can manage 10,000 [assets] today in less time than it took me to manage 2,300 assets five years ago." He concluded: "Qualys is an immeasurable benefit to Sky Betting & Gaming, and VMDR has been at the heart of my role for the last five years. We look forward to working with Qualys for years to come."

> It was good to be on stage, and the feedback from the case-study session was brilliant. Lots of people have asked me lots of questions. I attended the conference and also the superb training day. For somebody who considers themselves quite a competent Qualys user, I learnt an awful lot about some of the newer stuff that I had never really investigated. At the event, the contact building was terrific.

Glenn Pegden
Security Vulnerability Manager,
Sky Betting & Gaming

Reflections on the fireside chats at CISO Exchange at QSC London

A selected group of cybersecurity leaders shared ideas and strategies to protect the organisations we work in, presented through a blend of case studies and fireside chats. Powered by Pulse Conferences, the CISO Exchange was a roundtable unique to the QSC hosted in London. In a CISO-driven agenda led by with and for CISOs, this was a unique opportunity to learn from one another, share problems, find solutions, and determine industry trends.

Are we playing an unfair squid game?

Craig McEwan, CISO of Anglo American, spoke about how cyber gangs have an unfair advantage: they don't play by the rules, are armed to the teeth, and – most critically – work together.

"While automation has its place in the fight against cybercriminals, it is not a silver bullet that can solve all cyber security problems. It means cyber security professionals don't need to trudge through mundane tasks and be freed up for more important work. Still, we need to realise that automation and artificial intelligence is not enough.

"It's clear that access to cyber weapons is easier for bad actors than ever before. It's wide open for those looking to obtain destructive cyber capabilities. At a time when the cost of living is surging, the worry is more people will tread this path and quite easily launch their ransomware attacks. It's a perfect storm.

"More than that, though, criminals share attack knowledge and tools. Businesses are trying to stop and defend against this collective, deeply collaborative entity, yet we still work in silos. As an industry, to tip the scales back in our favour, it is imperative to improve collaboration and pool our knowledge and capabilities, and quickly."

> In-person events like this are important because we are fighting against groups working together, sharing all that information. We need to do the same. While events like this are not the silver bullet to sharing, they will help build trust. I'm happy to share my thoughts, learnings and challenges, and I'm also happy to receive knowledge from and engage other companies, so events like this are crucial to help start those conversations.

Craig McEwan
CISO, Anglo American

The 48-hour window: managing the new normal

Ritesh Patel, BP's Digital Security Principal, was interviewed by the EMEA CISO of Qualys, Giuseppe Brizio about resolving the conflict between identifying and remediating risk, educating various stakeholders, and reducing the time to mitigate vulnerabilities in today's heightened threat environment.

Q **What are the main reasons it can be slow to remediate vulnerabilities, especially at larger organisations?**

A You have to start at the root cause of the problem. Sadly, many vulnerabilities are now very old. And I don't think bp is the only organisation in this situation. There are various reasons given for this, and the obvious one is when teams say "we needed down time to remediate the vulnerability". We need the business leaders to agree. Often the argument is that to take a server down for five minutes, it will cost us, say, £3 billion, without considering the impact of not patching a vulnerability. Another problem is surfacing the vulnerabilities. Historically we have not always known the vulnerabilities are there in the system. A scan of the server estate took so long. By the time you had finished the scan, you would have to start over again.

Q **Where does the risk lie with cyber vulnerabilities?**

A The risk has to sit somewhere, so who is on the hook? Previously, the person who owned and used the server would be responsible for the risk model. But if they don't know vulnerabilities are sitting and lurking on the server, it's a problem. No one is going to ask them. Every morning, I don't ask my car: "Are you OK?" I wait for a light to shine on the dashboard, which shows me there is an issue, and that I need to get the vehicle into the garage. It's the same in this situation.

The first thing is to surface the vulnerabilities across the organisation.

Q **Who decides when to break the glass in a 48-hour emergency?**

A It has got to be a joint conversation – no one can make that decision in isolation. We'll talk to everybody that will listen if we spot a vulnerability. We'll talk to the operations teams; we'll talk to businesses. If a zero-day, extinction-level attack happens in the early hours of Sunday morning and we can't reach anyone, then we'll probably have a narrower group.

Q **If you discover a vulnerability, which 48 hours do you pick to tackle it?**

A It depends. Sometimes we've done one over a weekend, just because the vulnerability landed on the weekend. It depends on the size of the business you're in as to whether you have an option to go for a weekend. If something happens on a Monday and there are business priorities that have got to be dealt with – in terms of the financial cycle or the end of the month – that may trump you being able to fix the problem. It is the business's call, it is their risk. If there is some reluctance because of timing, you might say: "We're just doing to do something with these boxes, or this application, to mitigate the vulnerability differently." It's not perfect, but it's better than nothing.

> It's been a very informative day. The highlights for me have been seeing a clear vision from Qualys, and a roadmap for its products. It's great to see some features in the works that we've wanted to produce. And then also talking to the product managers and almost challenging them. So that face-to-face interaction is central to the day's success.

Ritesh Patel
Digital Security Principal, BP

Key themes and takeaways from QSC 2022

1

Desire to increase security automation

Cyber security professionals have a clear appetite for dialing-up automated solutions, and with advancements in artificial intelligence, this area will develop at speed.

2

Power up patching capabilities and reducing risk

Ensuring that software is up to date remains the most essential foundational cyber security activity. Qualys Patch Management reduces risk by up to 60% faster.

3

Need to consolidate cyber security solutions

With hybrid working here to stay and new attack vectors to consider, simplifying technology and tools – preferably on one dashboard – is critical. Some 80% of CISOs are focused on vendor consolidation.

4

Greater collaboration and knowledge sharing are vital

Cybercriminals are joining forces, and ransomware-as-a-service has lowered the barrier to entry, so more effort must be made to work together to combat increasingly sophisticated attacks.

Qualys

Leading the industry for 20+ years

Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, and managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

Product Sales: **+44 (0) 118 913 1501**
Customer Support: **+44 (0) 118 913 1502**
Partner & Channel Development: **+44 (0) 118 913 1501**

Headquarters

USA
Qualys, Inc.
919 E Hillsdale Blvd,
4th Floor
Foster City,
CA 94404 USA
Tel: **+1 650 801 6100**
Fax: **+1 650 801 6101**
Email: **info@qualys.com**

United Kingdom (also supports South Africa)
Qualys Ltd
100 Brook Drive
Green Park
Reading, Berkshire
RG2 6UJ
United Kingdom
Tel: **+44 (0) 118 913 1500**
Email: **info-uk@qualys.com**