

THOMSON REUTERS

# EDITED TRANSCRIPT

Qualys Inc Analyst & Investor Product Briefing on  
Groundbreaking Remote Endpoint Protection Offering

EVENT DATE/TIME: MARCH 26, 2020 / 6:30PM GMT



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

### CORPORATE PARTICIPANTS

**Philippe F. Courtot** *Qualys, Inc. - Chairman & CEO*

**Sumedh S. Thakar** *Qualys, Inc. - President & Chief Product Officer*

**Vinayak Rao** *Qualys, Inc. - VP of Corporate Development & IR*

### PRESENTATION

#### Operator

Good day, everyone, and welcome to Qualys analyst investor product briefing to discuss the groundbreaking free remote endpoint protection offering. This call is being recorded. (Operator Instructions) If you have any additional questions, you can submit them through the webcast portal or e-mail them to [ir.qualys.com](mailto:ir.qualys.com).

I would now like to turn the call over to Vinayak Rao, VP, Corporate Development, Investor Relations. Please go ahead, sir.

---

#### **Vinayak Rao** *Qualys, Inc. - VP of Corporate Development & IR*

Good day, and welcome to our product briefing to discuss our new groundbreaking remote endpoint protection solution. Joining me today are Philippe Courtot, our Chairman and CEO; and Sumedh Thakar, our President and Chief Product Officer.

Before we get started, I would like to remind you that the remarks today might 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 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. Our non-GAAP to GAAP reconciliation can also be found in the Q4 earnings press release.

With that, I'd like to turn the call over to Philippe.

---

#### **Philippe F. Courtot** *Qualys, Inc. - Chairman & CEO*

Thank you, Vin, and good day, and thanks to you all for attending our webcast. We all can see and anticipate that COVID-19 will bring major societal and business changes. Companies of all sizes are going to have to: one, rethink their business continuity plans to include remote connectivity, accelerate their migration plans to the cloud, streamline, if not, reinvent their supply and delivery chains. This is also going to have a profound impact on our industry. As it became crystal clear during this crisis, that current security solutions were not designed for an online world. This was quite apparent for us as a company, as like everybody else, we have suddenly [stuffed] our workforce working from home and we were not prepared for it.

Fortunately, because of the many years of architectural and foundational work at expanding our cloud platform, we could, in a very short period of time, ensure that our remote workers -- that our remote worker computers could be secured and properly touched. From there, we then build overnight the free service that could scale to first our customers so they could do the same. Now let me take the opportunity of this webcast to thank our engineers who worked relentlessly, burning the midnight hour to make this happen.

And with that, let me introduce our President and Chief Product Officer, Sumedh Thakar, who spearheaded such a critical initiative. Sumedh?

---

#### **Sumedh S. Thakar** *Qualys, Inc. - President & Chief Product Officer*

Thank you, Philippe. So while Qualys pioneered the cloud platform for security for almost the last 20 years, we also strongly embraced the SaaS model for our own internal usage, replacing on-prem solutions in favor of SaaS solutions. And this is really what all the customers today are trying to see, how we actually have been able to really seamlessly move to a remote working model because for us, all of our own employees are completely 100% remote. And so because of our embracing the cloud and the SaaS model, we've really reduced our reliance on internally hosted VPN connectivity. So our ability to collaborate across our worldwide workforce, which is now, like I said, 100% remote across the globe, has been pretty much unaffected with the use of cloud-based e-mail, chat, video conferencing,



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

et cetera. And of course, from a security perspective, we doubt for our own solution. So talking about our own experience, we already have Qualys deployed across our entire platform as well as our remote corporate IT endpoints.

And since we already have the Cloud Agent installed and deployed on every single laptop, already doing asset inventory, vulnerability management and Indication of Compromise detection, we have a very comprehensive view of all of the security and configuration posture of every single remote endpoint, whether it's with our employee in Japan, India or Central Europe. And we know exactly what are the critical missing patches on these systems, which systems are misconfigured, down to the level of which systems are missing an automatic screen lock, which systems are not enabled for screensaver, those that don't have antivirus running, et cetera. All of these are very important today when you have a 100% remote workforce that is leveraging home networks or unsecured Wi-Fi networks in public places.

And as the agent for us was already active, even if these endpoints were all remote for us, enabling the patch management capability was literally a single click process that took us only a few minutes to enable. All the agents that we had globally to be able to immediately be ready to start accepting patch jobs. From thereon, our security team was able to use our cloud-based UI to assign critical patches to be deployed to the asset tag call laptops and head go. And from that point on, they did not really have to do anything because as these remote agents connected back to our platform, where we really have a highly scalable system, they received the patch jobs and immediately started downloading and installing these patches directly from the vendor CDNs, completely bypassing any usage of our VPN bandwidth, which is, of course, a very big relief for our network. And this is a very important point as part of this remote service, which is the fact that the remote endpoint service from Qualys leverages the cloud-based architecture, which is downloading the required updates and patches directly from the vendors and not going through the VPN and tunnels that the customers have.

Now for an organization, why is this is important? Just to take an example of our own network, the recently released SMBGhost Vulnerability for Windows, the patch size is about 350 megabytes. Imagine even with 1,000 laptops, trying to download this patch at the same time over VPN, using a traditional on-prem tools like SCCM, BigFix, Tanium, et cetera, that's about 350 gigabyte bandwidth needed just for 1,000 systems for a single patch. This is pretty much going to kill any VPN gateway. And for us, by being able to leverage that architecture where our agents are directly connected to the cloud, we were able to really get that scalability and that quick speed of deployment of these patches, even for about 800 remote endpoints, we were able to get those down to less than 100 in just under 5 days even though none of them were on our VPN network at that point of time.

And of course, this is possible mainly because of the unique architecture of the Qualys Cloud Agent and the platform itself, which we have -- where we have a very lightweight agent. And as you know, we have over 30 million of those now. That is able to connect to a highly scalable cloud platform and the single agent is able to perform multiple functions given that we do all the processing and analysis on our platform. While the single agent is able to do everything from asset inventory to configuration to vulnerability assessment, File Integrity Monitoring and detecting Indication of Compromise as well, it gives a complete always up-to-date, real-time view of all of the security and compliance aspects of these remote endpoints in a single cloud-based console with the ability to respond by pushing patches. And soon, we will be performing -- that agent will be performing other additional actions like removing files, scaling network connections, uninstalling software, et cetera.

What we have done is because of this architecture and because of the ability that we have, we've created this -- we have taken this platform, and we have actively expanded the platform to -- very quickly in less than a week to be able to offer a 360-day patching service to all of our customers. And they can leverage this for getting a full inventory of all of their assets, getting a full visibility into all the misconfigurations, all the critical vulnerabilities and the ability to deploy the patching for 60 days so that they can immediately get started with securing these end points that are already out of their network and the traditional tools that a lot of our customers have are not able to address this situation.

We are also working to actively expand this 60-day free service to also include the ability to detect malware compromises on remote endpoints by leveraging the same agent with absolutely nothing else to install and leveraging our IOC capability in the back end, and we will make an announcement about that.

The dashboard UI, which essentially is bringing together the complete visibility of what traditionally needs multiple tools to get that



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

visibility in the platform. The unified dashboard brings together the ability to see this complete remote inventory. A lot of customers now have people who are leveraging home systems so that they can continue work. And being able to bring those home systems into some level of ability to view their security posture can be done through that single dashboard. So all of the inventory of every single remote endpoint, the critical vulnerabilities and misconfigurations and all of them patches that need to be deployed can be done with this service. And we have put a lot of effort to prioritize this capability for our existing customers so that they can immediately get to start securing these remote endpoints.

And then we will also be adding additional new companies that are interested in leveraging this service. We will be looking at adding those on to the platform as soon as we have helped our existing customers to really get started with this patching process. And so for that, we have worked pretty diligently to create capacity on our back-end very quickly, so we can continue to do that.

This service is initially focused on remote endpoints, which for the bulk -- which is basically the bulk of the remote systems that we see, and this is focused on Windows initially. But then we are also actively working on the ability to bring the same service to Mac and Linux systems. And very soon, we will be publishing the time lines for those as well.

Vinayak, I wanted to see if you had any questions that were coming in. Or Philippe, do you have any comments on -- additional comments?

---

**Philippe F. Courtot** *Qualys, Inc. - Chairman & CEO*

Yes. No, I think this is very well said, Sumedh. So Vinayak, I think you can go and read the questions, and then we'll address them. Okay.

---

### QUESTIONS AND ANSWERS

**Vinayak Rao** *Qualys, Inc. - VP of Corporate Development & IR*

Great. We have questions on the line. The first one is, can you please explain how this product differs from your existing Cloud Agent, vulnerability management and patch management offering? And also, does this service only cover patching? Or does it provide additional insight as well?

---

**Sumedh S. Thakar** *Qualys, Inc. - President & Chief Product Officer*

I'll take that question. So thank you. So if we didn't go in and kind of create some sort of quickly put together a hacked-up service. Essentially, what we have done is combined the various capabilities that are already built in a single platform with asset inventory, leveraging the Cloud Agent, vulnerability management, configuration assessment and patching together into a seamless offering. And as some of you who have already seen this work that we have done with VMMDR really has made it extremely easy for us to package these capabilities together into a single unified dashboard so that the customers can keep track of all of the remote endpoints in one place. And so it goes beyond patching and vulnerability management. It also does configuration assessment, which is very important because even if you have a system that is patched for the software, but its password is ABC123 or the screensaver is not enabled or the Wi-Fi is connecting to secure Wi-Fi -- unsecured Wi-Fi networks, it is a challenge. So it provides a pretty comprehensive ability to work on protecting that machine so that it can be -- you can stop the compromises potentially.

And as I mentioned earlier, we are also working quickly to expand that service to be able to detect any potential compromise or attempt to compromise with our IOC solution, which will be coming very soon as well.

---

**Vinayak Rao** *Qualys, Inc. - VP of Corporate Development & IR*

Great. Moving on to the second question. What's the rollout plan for this service to existing customers versus trying to get new customers for the service?

---

**Philippe F. Courtot** *Qualys, Inc. - Chairman & CEO*

I will take this one. So in fact, we're starting the rollout now to our existing customers, and we wanted to give them priority first. While we are expanding the resources of our platform to support an extremely large number of companies, both large and small. So next question, unless you have to add something, Sumedh.



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

**Sumedh S. Thakar** *Qualys, Inc. - President & Chief Product Officer*

Yes, I think the focus right now is to -- because we have the visibility into what our customers are demanding, existing customers, we're really able to create an ability for them to scale this to their endpoints. But once we have some of those onboard pretty shortly starting next week or so, we will also be starting to onboard new customers. We already have a pretty good number of them who are -- who have shown interest in that new -- who has shown interest in the service.

**Philippe F. Courtot** *Qualys, Inc. - Chairman & CEO*

Yes. And we have created a wait list. So those which are not Qualys customers, we'll serve them on the first in, first out basis.

**Vinayak Rao** *Qualys, Inc. - VP of Corporate Development & IR*

Got it. Moving on to the next question. How can customers who haven't deployed Cloud Agents on the endpoint take advantage of the service? Can you also touch upon the implementation process for such customers?

**Sumedh S. Thakar** *Qualys, Inc. - President & Chief Product Officer*

Yes. I mean, the bigger cloud-based service deployment is actually very straightforward, and we already have a lot of customers who have the Cloud Agent deployed. And for them, enabling the patch capability is just a flip of a switch on the backend for us. There is absolutely nothing else to install. For those who don't have the agent installed on the remote endpoints, there are multiple ways. So in fact, we have written a very technical blog and published it. That goes into essentially leveraging existing tools as well as using cloud-based services like Microsoft Intune, et cetera, to get the agent deployed.

Now the advantage is that because the agent is so lightweight, it's just 3 megabytes, we've also had customers who are able to just e-mail their employees with attachment of the agent binary to install or in some cases, we're going to have customers for hosting the agent package on a simple S3 bucket and sending a link to that remote and is to download and install. And then after that, once it gets installed, all the updates and the connectivity to the platform and all of that is completely automated. That customers never really have to go and ask -- go and manually update those agents. So the deployment is actually and the implementation is pretty straightforward. Once they are brought up, they just connect back to a single cloud-based UI and the customers can see the progress pretty quickly.

**Vinayak Rao** *Qualys, Inc. - VP of Corporate Development & IR*

Got it. Next one. Who is the ideal customer for this solution? And what does the solution offer if a customer is already deploying CrowdStrike at the endpoint?

**Sumedh S. Thakar** *Qualys, Inc. - President & Chief Product Officer*

I mean, I think, today, pretty much any organization which is -- pretty much every organization out there who has a mandate or who has workers who are working remotely and taken their endpoints at home actually are -- is the right customer. As I said today, majority of the endpoints we see today are Windows, so those who are focused on Windows endpoints are the ideal customers here.

And I guess, the other question is from -- compared to CrowdStrike. So I mean, CrowdStrike talked about the burst more for their offering to be able to provide their customers some additional services still, I think, May 16 or something like that. What that does not offer right now is a detailed patching plan and ability to patch the system. So it's, of course, a lot more focus on malware and compromise detection, which is helpful. But customers still need to have a way to patch these remote systems, and that's really where the Qualys service is going to be a lot more beneficial. And for us, we have not restricted it to mid-May or any date like that. What we have done is that we have done 60-day. From whenever they decide to start leveraging it, they get 60 days to be able to use the service. And so as -- depending on how this whole thing is going to progress, it offers additional flexibility for those customers.

**Vinayak Rao** *Qualys, Inc. - VP of Corporate Development & IR*

Got it. What are the driving force behind launching this service? And what do you expect to achieve out of this?

**Philippe F. Courtot** *Qualys, Inc. - Chairman & CEO*

I'll take this one. So yes, in fact -- this is a great question. In fact, as I mentioned in my brief introduction, we needed to show the product out. And then of course, bring it to our customers first. We decided to make it free, as Sumedh explained, from the date of deployment.



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

And also, time is at the asset. I mean this is something that customers need to do now. And this initiative, in fact, has been extremely well received by our customers. And as we mentioned earlier, the deployment has begun. And as well, we will, as we said, as well, we will shortly make it available for non-customers. And of course, this will help us advertise the ease of use, the scalability, the cost effectiveness and essentially the game-changing nature of our platform. It is also quite timely as the world would be different after COVID-19, as I mentioned again.

We believe that those using this free service would realize that the plethora of solution of security solution they have deployed over time in the golden networking era are antiquated and can be easily replaced by our integrated cloud solutions, not to mention the visibility they will achieve across their entire hybrid and global computing environment. Next question?

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Next question from (inaudible). After the free period, is the functionality automatically turned off? What's the current plan beyond the free 60-day period?

---

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

I think from a technical perspective, we -- it's 60-day trial. But for us, we have the ability to really work with these customers. And again, we are in a period where there's no clarity on how long this is going to last. So fortunately, we are in a position to be able to work this with our customers and figure out what they need to do. But of course, after that 60-day trial, they always have the ability to purchase the solution for those devices or additional devices as they please. But just from an ability to help them with the current situation, we have a lot of flexibility in working to extend these dates and time lines as needed. So Philippe, I don't know if you want to add something to that.

---

### **Philippe F. Courtot Qualys, Inc. - Chairman & CEO**

Yes. So I think -- our philosophy here fundamentally is to really help our customers. This is a cause which is well above us. These times are very difficult for all of us. So I think this is our contribution to the cause, if I missed it so. And so we will continue to fundamentally provide the service as long as that situation remains.

And I would add, I think I'm optimistic. I don't know if some of you have already seen the data coming from the Bay Area, where the curves -- the curve have flattened. And so let's hope that this is happening in the U.S. as it has happened in China, in the South Korea, in Taiwan and in Japan. And so -- and again, we're working to add additional services. So ultimately, I think this is for the good. And of course, we believe ultimately, we'll get a significant benefit because of the quality of the service that we have and the fact that it does the job. Next question.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

How differentiated is this offering with what's already available in the market? How does this differ from what Tenable recently announced that they will be offering for the COVID situation? And also, doesn't Microsoft have a Windows patching solution that customers can use?

---

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

So yes. I'm getting some feedback, sorry. So it's -- from a -- as far as we can see right now in the market, this is the only cloud-based. So I mean, first of all, to address this remote work situation, you need a cloud-based solution and cloud-based platform. And as far as we can see, we're the only solution in the market that is combining the asset inventory, the vulnerability assessment, the configuration assessment as well as the ability to actually deploy these patches into a single platform and with a single agent. And we're -- and Tenable, they announce extension, I believe, of Tenable.io and licenses for 30 days or until the end of April or something like that, from how I understand it. And again, at the end that the agent is not the lightweight agent that Qualys has. It's a full-blown scanner. And at the end, it still does not do patch management. So for the most part, what it offers customers is to say, yes, you have these issues. But there is -- now that these workers are remote, there is really nothing that they can do to really fix the situation, which is different with Qualys that we're able to deployed. Now that we're able to deploy the actual fixes to these devices while sitting remote.

Now from a Microsoft perspective, of course, there's SCCM, which is an on-prem solution, and there's a few other solutions like that. But again, as I mentioned, with the VPN connectivity and the ability to download patches on VPN, that's, first of all, the big blocker.



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

Secondly, Microsoft solutions, of course, focused mainly on Microsoft products. And the third-party patching is always a challenge with being able to deploy patches for Adobe and other types of software, that's not the core Microsoft solution. And so for us, with our patching capability, we have an extremely strong coverage, not just of the Microsoft capabilities, but also the third-party vendors that are -- have Windows applications like Adobe. We have very, very in-depth coverage. And so I think that makes that solution pretty unique.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. Thanks, Sumedh. The next one is, do you anticipate after these couple of months, customers will go back to the existing model of on-prem patching solution? And do you foresee a bigger cultural shift?

---

### **Philippe F. Courtot Qualys, Inc. - Chairman & CEO**

Well, so this is -- as I mentioned earlier, I really believe the world after COVID-19 is going to be different. And if we look from the companies around us and our customers reducing costs, while increasing business flexibility is going to be a significant driver to essentially have companies moving much, much faster at adopting cloud-based solutions. So that's what I believe. And I think we'll start to see evidence of it. Next question.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. Next one. Will CIOs be willing to move to leverage a security room for performing patching function, which is more of an IT function than security?

---

### **Philippe F. Courtot Qualys, Inc. - Chairman & CEO**

Well, that's an interesting question as well. I think today, there is -- again, there's many changes which are mental changes which are taking place even before COVID-19. Whereby now, CIOs and CTOs and CISOs were now absolutely pushed to accelerate their digital transformation for business purposes. Again, COVID-19 is going to accelerate all of that. So the mind shift was already happening. So that doesn't mean by the way that certainly the people who are doing the patching are going to be replaced. No, what it means with our solution is that you could automate significantly that process, but you could also have the patching team being the one pushing the button. And so for us, it's not really -- we are not selling any more to 1 silo because we provide essentially an application that cuts across all the silos and streamline the operation as a result of that, significantly reduce the cost. Next question.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. Will the service help customers like financial entities demonstrate compliance for these remote endpoints?

---

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes. I think that's a really good question because no matter what the situation is, I think there's a lot of mandates, whether it's FedRAMP, whether it's ISO and others that actually do require that endpoints, remote endpoints also be configured, secured and patched to the latest patches at a -- on a regular basis. And I think the good part about our platform is that the ability to demonstrate the compliance is just a by-product of that capability. And so of course, those customers who are leveraging this will be able to pull the required compliance reports off of the platform to be able to demonstrate that even though their entire workforce is remote, that we're actually able to demonstrate the compliance because, again, the data collection, all of that is happening to the cloud. So you can really get an up-to-date inventory of the status of each and every device, no matter which country it is in as long as it's able to connect to the Internet.

---

### **Philippe F. Courtot Qualys, Inc. - Chairman & CEO**

And let me add one thing. What is also very unique with Qualys because essentially we're totally cloud-based that this -- we have essentially a third-party, an independent third-party auditor. So all these compliance reports are -- you cannot really change them because this is the platform which is performing these changes. So that's an additional benefit, again, of having essentially in one single platform, IT, security and compliance, all integrated as well. Next question.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Next question is, can the service cover devices that may not be issued by companies? Also, will the service cover nonsecurity patching as well?





## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes, that's a very important point. Actually, we do not restrict the usage of this service for only company-issued devices because we do understand and a lot of our customers are facing situations like that in certain cases, where maybe the company-provided device is not working or is not enough to be able to perform the functions because there was more of a laptop that was issued for e-mail. So we do have situations where customers are looking to have their users use systems that they already have at home. Maybe a power -- much more powerful desktop. And for us, again, being a very simple deployment that does not require any VPN tunneling and all of that, it's extremely easy. And so we do not restrict that license ability. In fact, we encourage customers to be able to deploy this service to noncompany-owned devices as well, because if you have a company-owned device that's sitting in a home network on an unsecured network, where the other devices may have some compromises, then you are still at risk. So overall, we're giving this ability to have this service be deployed on noncompany-owned devices as well.

And as far as the patches go, we -- of course, the solution does have the ability to deploy nonsecurity patches. And we don't restrict that. But customers today are really focused on security patches. And you saw the recent announcement by Microsoft as well, where they are going to slow down a little bit on the nonsecurity related patches as well. So while our solution can do that, we do see customers really are more focused on the security patching for the next few weeks at least.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. Thanks, Sumedh. Next one is, do you need to make any changes or additional investments to your backend to support the additional load the uptake of this free service is going to cost?

---

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes. So I mean, we have done quite a bit of work the last few years to rearchitect the platform. And because of our overall rearchitecture moving to bare-metal Docker in certain cases, in cloud in other cases, we have a pretty hybrid and pretty scalable architecture. So for us, quite a few of our customers already have these agents, so it's just enabling another service. In other cases, we are deploying a whole bunch of new agents. But as of now, we really feel that the capacity that is needed to help our customers is there, and we continue to roll out additional capacity. So, so far, we don't necessarily see any big spend or any challenges to provide that additional service to our customers that's going to make any meaningful impact at this point of time.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. Can you also discuss the impact of the recent nationwide lockdown at India, on the employee based in Pune? Does that impact your product development plans in the near term?

---

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes, it's been very interesting. The whole 1.3 billion people are locked in at home and not able to leave at all. And so of course, fortunately, again, because of our reliance on SaaS-based and cloud-based solutions, overall, our workforce even in India, where we have about 800-plus employees, has remained fairly unaffected. Because -- and thankfully, over the last multiple years, there's been significant advancements in connectivity over there for people to be able to connect it from home with 4G networks and broadband and all of that. So again, we -- our employees have been able to be just as productive. We continue to work from home for everyone and leverage tools for videoconferencing and collaboration, which I think so far, we've really seen almost no impact at all, even though everybody is -- has this complete lockdown in Pune right now.

---

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. The next one is, can customers use this service for servers? Or does the solution work only at the endpoint?

---

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes. I mean for -- the agent is the same agent. And that's the beauty of the architecture, right? There's no different endpoint agent or remote agent. So, of course, the idea of the service, again, is to really help customers in this current period to do whatever it takes to get them more secure. So there's, again, no restriction, so to say, on them using it on the servers. And if that is something that is important





## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

for those customers at this point of time to leverage those agents on the servers in a given time frame again, because they may have some admins who are not able to come in to the office to do patching or do that over VPN or whatever it is. That's absolutely -- they are welcome to us the service in however, wherever they feel is going to be the most impact for them, and we are here to help.

---

**Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. Just an extension of the question, is there a limited number of assets a customer can deploy the service on?

---

**Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

No. We haven't really put any limit, so to say. So again, we're working with customers. Whatever is the right number of employees and the endpoints that they have. We are rolling this out and it's not a limited sort of a limited device trial or anything like that. So the idea is that if a company does have 1,000, 5,000, 10,000 endpoints, we should be able to enable this for all of them. Again, the platform already supports multiple millions of agents. So this is not something that we feel would be an issue, and so we are not limiting any numbers at this point.

---

**Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. The next one, which is coming out is, how will the remote protection solutions service evolve once VMDR is generally available?

---

**Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

This is the favorite question and all my engineers are asking right now because they are working on both of these aspects at the same time. And a great job that they have done to spin up the service. And essentially, the great part here is that when the VMDR is going to be launched end of this month and started rolling out early next month. All these customers who sign up for the remote protection solutions are just going to get an in-place upgrade of their service to the MDR experience UI and they always have the ability to sign up and purchase or get a trial for the VMDR prioritization capabilities that we are bringing as well. And that's, again, because of the cloud-based architecture, we are essentially able to push out this in-place upgrade so that they can try additional functionality and really leverage the prioritization capabilities if they choose to do that in addition to the patching of the remote endpoints, so they can actually do an even better job of prioritizing which patches need to be deployed on these remote endpoints as well.

---

**Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. When will the service support patches for non-Windows machines?

---

**Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

So we're actively working on that right now. I don't unfortunately have a date out of the -- out of my mind right now, but we will very soon, in a week or 2 be able to publish out a date when we can expand this service to Mac devices and Linux devices as well. But again, from a remote endpoint perspective, the majority of the devices that we see right now are all Windows devices and a very small number on Mac devices.

---

**Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. And if you're a current patch management customer, does this remote endpoint protection offering offer you any additional functionality?

---

**Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Well, I mean, if you are already paid patch management customer of Qualys, which we already have a bunch of them, hopefully, this service really help them, and they are already better and protected because of their ability to push out those patches pretty quickly. So from a functionality perspective, they already have everything that they need to be the first ones to secure the remote workforce.

---

**Philippe F. Courtot Qualys, Inc. - Chairman & CEO**

And Sumedh, and maybe would they -- I'm sure that they will get the new unified dashboard. But since we can put dashboards...

---

**Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes, of course. Yes, that's being pushed out to everybody as a service that they can use from a unified dashboard perspective. So yes, the existing patch management customers will get the unified dashboard, too.



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

### **Vinayak Rao Qualys, Inc. - VP of Corporate Development & IR**

Got it. And a couple of questions on (inaudible). This service helps with patch management. Does this it solve nonpatch issues as well? Is this a full-blown endpoint solution that covers [AV]. So what other services can you provide apart from patches?

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes. So I think I addressed some of that earlier. But -- so again, like I said, patching of software is one aspect. The service does provide complete visibility into configurations as well. So when you have your corporate devices that are out at home networks or shared networks or corporate -- outside of corporate networks, being able to ensure that the devices are configured correctly is also very important. Do they have antivirus running? Is the antivirus up to date? Is it able to pull the updates that are required directly from the cloud? Are those laptops enable for quick locking? And screen saver, is the password strong enough? I think all of those are capabilities that we have already part of this service that we'll be surfacing.

And as we have discussed, as we are adding additional ability for our agents in the next couple of months to be able to take sort of remediation actions to kill processes and uninstall software and all of that. That also will give us additional ability to also make changes to configurations on these devices, leveraging the same agent and the same platform and then make that solution even more comprehensive when you combine that with the ability that we are going to come up with to be able to detect malware as well. If any of these remote endpoints have malware, we will be able to detect that as well.

So the service that we are providing today is immediate focus on getting the devices patched to a good level. But very quickly, the same agent, same platform that they have deployed is getting additional updates that will enable more and more capabilities for them to be able to get a better picture of their security and compliance.

### **Philippe F. Courtot Qualys, Inc. - Chairman & CEO**

Vinayak, I'll put another question for -- we're almost getting at the end here, but I've got another question for Sumedh. So we have now our agents which are available for inventory for the mobile devices, the Android tablets, et cetera. What about the securities? So where are we on pushing additional capabilities to really not only know what you have, but do something about it on the mobile phones, on these mobile devices.

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Yes. So we've integrated that -- the acquisition of 1Mobility that we did. We've integrated already the agent as the Qualys Cloud Agent for mobile, Android and iOS devices, and that is being rolled out as part of VMMDR in the next few weeks. So which means customers can extend the ability to have this free inventory agent be deployed on any number of the remote endpoints, which are Android and iOS devices as well. And then over the next few months, we will also be adding vulnerability assessment, configuration assessment and ability to make changes from a response perspective on these devices as well. So over the next few months, we'll see more and more capabilities like we already have for Windows and Mac and Linux starting to roll out on the Android and iOS devices as well.

### **Philippe F. Courtot Qualys, Inc. - Chairman & CEO**

Okay. Thank you, Sumedh. So as you know, so we're just arriving at the end of the webcast here. So let me remind you that, first of all, we are registering and that is our webcast and that we will publish on our IR, on our Investor Relations web page. And if you have any -- if you have no answers to the top of your question we have not answered, we will answer in writing. And if you have any new questions that came up during this talk, please, you can send them at [ir@qualys.com](mailto:ir@qualys.com), and we will come back to you and we'll publish the response as well.

So with that, let me especially thank you very much to all of you for attending this webcast. These are obviously challenging times, but I have no doubt that we will probably bounce back stronger than ever. Stay safe and remain safe. And thank you very much. Okay. Goodbye.

### **Sumedh S. Thakar Qualys, Inc. - President & Chief Product Officer**

Thank you.



## MARCH 26, 2020 / 6:30PM GMT, Qualys Inc Analyst & Investor Product Briefing on Groundbreaking Remote Endpoint Protection Offering

### Operator

Ladies and gentlemen, that does conclude today's presentation. You may now disconnect, and have a wonderful day.

---

### DISCLAIMER

Thomson Reuters reserves the right to make changes to documents, content, or other information on this web site without obligation to notify any person of such changes.

In the conference calls upon which Event Briefs are based, companies may make projections or other forward-looking statements regarding a variety of items. Such forward-looking statements are based upon current expectations and involve risks and uncertainties. Actual results may differ materially from those stated in any forward-looking statement based on a number of important factors and risks, which are more specifically identified in the companies' most recent SEC filings. Although the companies may indicate and believe that the assumptions underlying the forward-looking statements are reasonable, any of the assumptions could prove inaccurate or incorrect and, therefore, there can be no assurance that the results contemplated in the forward-looking statements will be realized.

THE INFORMATION CONTAINED IN EVENT BRIEFS REFLECTS THOMSON REUTERS'S SUBJECTIVE CONDENSED PARAPHRASE OF THE APPLICABLE COMPANY'S CONFERENCE CALL AND THERE MAY BE MATERIAL ERRORS, OMISSIONS, OR INACCURACIES IN THE REPORTING OF THE SUBSTANCE OF THE CONFERENCE CALLS. IN NO WAY DOES THOMSON REUTERS OR THE APPLICABLE COMPANY ASSUME ANY RESPONSIBILITY FOR ANY INVESTMENT OR OTHER DECISIONS MADE BASED UPON THE INFORMATION PROVIDED ON THIS WEB SITE OR IN ANY EVENT BRIEF. USERS ARE ADVISED TO REVIEW THE APPLICABLE COMPANY'S CONFERENCE CALL ITSELF AND THE APPLICABLE COMPANY'S SEC FILINGS BEFORE MAKING ANY INVESTMENT OR OTHER DECISIONS.

©2020 Thomson Reuters. All Rights Reserved.



## Additional Analyst & Investor questions on our Remote Endpoint Protection Solution

- [How does the solution fit into the overall Qualys portfolio and is this first part of a broader strategy in endpoint protection?](#)

Qualys as you already know has been working on expanding the capabilities of its platform to the endpoint, including re-architecting the platform as well as the introduction of lightweight Cloud Agent and passive scanning, which give us additional telemetry.

We added Asset Inventory, Patch Management and Indication of Compromise detection capabilities to the agent last year with an eye towards endpoints and unlike most existing solutions, we are not just within the customer's network since our cloud model works and scales far better. It now happens that the current circumstances have suddenly pushed out all endpoints out of the customer environment and traditional on prem solutions are of no use. Because of the work we have already done, we were able to come out with a solution like this for endpoints almost overnight and soon with the introduction of malware detection and EDR capabilities, we believe we will be able to offer a comprehensive endpoint protection solution. This coupled with the information we can get from the traffic analysis our passive sensor provides will allow us to also eliminate many of the false positives that plague current solutions and as a result require heavy human intervention.

- [Do you anticipate resistance from your customer's employees who might resist having their personal computer activity monitored by their employer?](#)

Most of these devices are enterprise owned and have always had multiple security solutions on them to ensure security of the device but were more based on network installed on-prem model. COVID-19 has clearly shown with the influx of employees having to work from home that these on-prem solutions are not cutting it anymore even for corporate device as patching them remotely with existing solutions is extremely difficult.

A cloud-based approach is in fact the only efficient and cost-effective approach to patch such corporate devices and it does not add any additional activity monitoring that AV & EDR solutions weren't already doing.

It is also the only practical way to handle home devices and bring them in line with the same high level of security expected of any company owned device. Because our agent only monitors the device for activity related to the security of the system and does not extract any personal data of the user such as documents, pictures, videos etc. our approach makes it compatible with GDPR requirements and individual users can be reassured.

- [What is involved in installing the Qualys agent by admins and end-users, and are there any device platforms not supported \(Windows, macOS, Android, Chrome, iOS, Linux\)?](#)

Being a cloud based service our agents are extremely easy to deploy, extremely lightweight and very easy to distribute. Additionally once deployed they require "zero touch" as they configure themselves from the cloud and keep themselves up-to-date to the latest version with no user intervention.

Agent installation can be done using many methods starting all the way from using cloud-based service like Intune to using SharePoint / Google drive, S3 buckets or even emailing a 3 MB installer to the employees to do it themselves.

While the agents are available on many platforms like Windows, Mac, Linux, Android, iOS etc., the patch deployment functionality is currently available only for Windows which makes up the bulk of remote endpoints.

We are currently working to announce the date for Mac patch deployment, which should come out pretty soon and in future we will continue to enhance our android and iOS agents to have more response capabilities.