Qualys

Cloud Agent

Real-time assessment of millions of global IT assets on-premises, mobile, or in the cloud

Qualys Cloud Agent enables instant, global visibility of IT assets—even occasionally-connected mobile and virtual devices, with up-to-date asset configuration data for security and compliance. A low-footprint agent installed on endpoints, Cloud Agent brings the high-performance functionality of all Qualys Cloud Platform services to all IT assets in the global enterprise.

Why You Need Cloud Agent

The lack of visibility into risks affecting global enterprise IT assets is a major challenge to securing an organization of any size. Scanning performance is a significant factor, especially when scanning hundreds of thousands of assets, and results in the identification of millions of potential issues that each require prioritization and remediation. However, the biggest challenge with occasionally connected devices is that traditional scanning solutions need systems to be accessible when the scan is executed. Otherwise, they're invisible, and no relevant data about those assets is collected. Using the Qualys Cloud Agent solves these problems, helping your organization to stay on top of enterprise security and compliance.

Broad OS support includes Windows, Linux, macOS, BSD, IBM AIX, Solaris, ChromeOS, Linux on zSystems, and public cloud platforms such as AWS, Azure, OCI, IBM, Alibaba, and Google Cloud. It works on-premise in clouds, and on remote endpoints. Cloud Agents work in concert with the Qualys Cloud Platform, so customers can easily add security and compliance capabilities. Multiple functions delivered by a single agent change how security leaders create and manage their security programmes across their hybrid IT enterprise.

THE BENEFITS OF USING A SINGLE AGENT FOR SECURING HYBRID ENVIRONMENTS INCLUDE THE FOLLOWING:

1. No scan windows are needed. Cloud agents continuously collect data about the assets they are installed on, even when they are offline.
2. Constant monitoring yields faster vulnerability discovery and patch confirmation.
3. No need for complex credentials and firewall management. Cloud Agent only communicates outbound to the Qualys platform.
4. The fact that Cloud Agent supports multiple Qualys apps lets users consolidate their security tools, reducing costs and complexity.
5. Supports assets that are difficult or impossible to monitor with network scanners, including:
   - Remote systems in branch offices
   - Roaming user devices
   - Ephemeral public cloud workloads

KEY FEATURES

Light Weight, Extensible, Self-updating & Centrally Managed

The Qualys Cloud Agent can be installed anywhere — including any host such as a laptop, desktop, server, or virtual machine — and can be deployed via a compact, silent installer, which can be embedded in system images, deployed via standard software management automation most organizations have in place, or run from the command line.

The Cloud Agent is designed to have minimal impact on the system and the network, typically consuming less than 1% of CPU resources with peaks of < 5% during scanning operations. Once installed, the agent will make a full configuration assessment, including Cloud Provider metadata, of its host while running in the background and uploading that snapshot (few KBs only) to the Qualys Cloud Platform. The agent is self-updating and self-healing, keeping itself up to date with no need to reboot.

Real-time Actionable Delta Collection with Customizable Configuration Profile

Agents check-in with the Cloud Platform and update the snapshot with new information as changes occur, removing the need to poll the system to update asset inventory data. Having an always-current picture of the system configuration allows inquiries even when the endpoint is offline or unreachable. Continuous evaluation and data enrichment happens on Qualys platform.

The Cloud Agent comes with flexible and granular performance configuration and scanning controls, allowing organizations to tune agent performance and bandwidth usage for specific environmental requirements. You can control a tiny memory footprint and minimal network bandwidth. Each Configuration Profile contains settings for:

- Agent performance
- Assigned hosts
- Agent scan interval
- Data collection options
- Blackout windows
- Suspending data collection
- Preventing auto-updating of agent binaries

Dynamic Tagging

Agent-based dynamic asset tagging provides a consistent, continuous view of your network and how each asset relates to your business. By automatically organizing assets in different ways, the platform lets you efficiently align the operations of your scanning, reporting, and remediation tracking with the way you view your business. The result: your IT, security, and compliance teams are informed quickly and effectively about the most important issues.

One Agent, Many Supported Qualys Applications

Cloud Agent for Asset Management

Cloud CyberSecurity Asset Management (CSAM) provides accessible, always-available access to the inventory data collected by the Qualys Cloud Agents and data collected by optional Vulnerability Management, Detection, and Response (VMDR) and Policy Compliance (PC) modules. CSAM scales to millions of assets, making it scalable for the largest global enterprise environments. It provides a new layer of intelligence into the current state of endpoints — including mobile and virtual — cataloging details about services, file systems, configuration files and the registry. As well as a wealth of additional information to manage and secure systems, the Qualys Cloud Agent requires no expensive asset management infrastructure.

Cloud Agent for Vulnerability Management (VMDR)

Cloud Agent for VMDR eliminates the need for establishing scanning windows or integrating with credential vaults for gaining access to systems — or to know where a particular asset resides. With agent-based vulnerability assessment, you can provide 100 percent coverage of your installed infrastructure. Unlike remote scanning, which requires credential management and complex firewall profiles to permit scans to pass through, agent-based VMDR runs locally with the correct privileges to do its work and only requires outbound encrypted communications over a single port to the Qualys Cloud Platform. With accurate, instantly updated information from the Cloud Agent, you will always know what vulnerabilities are on difficult-to-assess targets and, with TruRisk™, how to prioritize them for remediation. Qualys TruRisk™ quantifies security risk by workload criticality, vulnerability detections and correlates it with ransomware, malware, and exploitation threat intelligence to prioritize, trace and reduce risk.

Cloud Agent for Policy Compliance (PC)

Cloud Agent for Policy Compliance turns Qualys' PC offering into a real-time compliance assessment solution. You can continuously evaluate configurations of all relevant assets (including mobile and virtual) against standards and benchmarks such as PCI-DSS, CIS, ISO, HIPAA, and many others. The Cloud Agent facilitates simple maintenance; the agents are always kept up to date and require no credential management or complex remote access through the firewall.

Cloud Agent for Cloud Environments

Cloud Agent works with VMDR and TotalCloud to simplify asset discovery, tracking, security, compliance, and remediation in dynamic cloud environments like AWS, Azure, Google Cloud, OCI, Alibaba and IBM. Visibility is enabled by embedding the agent into the master images of your cloud servers. When a new instance is created from the master image, it automatically activates the agent, which instantly registers with the platform. This functionality eliminates the need to implement a separate discovery mechanism or to build automation around spawning new scanners to scan any new instances.

Additionally, the information is always up to date, even when your virtual workloads are offline, to free up computing resources. When an image is returned online, it updates the snapshot, keeping your information current. Qualys also supports BYOL with OCI and Azure cloud. Sysadmins will get a comprehensive view of the instance's vulnerabilities, context around severity and risk, and the ability to drill-down into details. With these insights, sysadmins can programmatically prevent instances with high-severity vulnerabilities from launching in a production environment.

Cloud Agent for Patch Management (PM)

No need to install software on-premises or configure open ports and VPNs. Any workstation, server, or work-from-home (WFH) device installed with the Qualys Cloud Agent can be immediately scanned for missing patches and patched. Anywhere you can put the Qualys Cloud Agent, you can run Qualys Patch Management. When Qualys Patch Management is used with the Qualys Gateway Service, you can significantly optimize bandwidth usage by caching patches and other files locally on your network.

Qualys Patch Management can patch and apply post-patch configuration changes to operating systems, mobile devices, and 3rd-party applications from a large variety of vendors, all from a central dashboard. With Patch Management, you don't have to manage patches in silos via multiple vendor-specific consoles.

Cloud Agent for File Integrity Monitoring (FIM)

Qualys Cloud Agent continuously monitors the system files and registries specified in the monitoring profile and captures critical events, which are sent to the Qualys Cloud Platform, where it enriches the event data with threat intelligence by adding trusted source and file reputation context that control noise and prioritize events as either malicious or suspicious.

Runtime Software Composition Analysis (Runtime SCA)

Discover and report on vulnerabilities associated with the third-party or open-source software using the Cloud Agent to crawl in standard, non-standard directories such as Log4j, Java and Python

Cloud Agent for Endpoint Detection and Response (EDR)

With Qualys Multi-Vector EDR, security practitioners achieve advanced endpoint threat protection, improved threat context, and alert prioritization at a lower total cost of ownership than traditional EDR. With Cloud Agent and a single dashboard, gain orchestrated prediction, prevention, detection, and response with Qualys EDR.

Cloud Agent for Custom Assessment and Remediation (CAR)

Qualys Custom Assessment and Remediation allows security practitioners to create and execute custom scripts and controls quickly. Scripts are centrally managed and executed anywhere a Qualys Cloud Agent exists. The service creates a library of reusable scripts and security controls using the preferred scripting language for the task.

Extensible Data Sharing with Third-Party Tools

All the data collected by the Qualys Cloud Agent installed in an IT environment resides within the Qualys Cloud Platform. Qualys' extensive and easy-to-use API makes it easy to integrate your data with third-party tools, including Security Incident and Event Management (SIEM) platforms such as Splunk & QRadar, Big Data analytics and ITSM help desk systems, such as ServiceNow.

Cloud Agent Passive Sensor (CAPS)

Discover 100% device traffic and gain control over unmanaged assets by passively sensing in the network the Cloud Agent is installed. No network taps, span ports, or active probing necessary

Qualys Integrated Solutions Suite

The Qualys Cloud Platform and Qualys Cloud Agent support the Qualys Integrated Solutions Suite. The integrated suite of IT security and compliance solutions includes:

- CSAM — Cyber Security Asset Management
- VMDR — Vulnerability, Detection, Management, and Response
- PC — Policy Compliance
- PCI — PCI Compliance
- CERT — Certificate View
- PM — Patch Management
- EDR — Endpoint Detection and Response
- FIM — File Integrity Monitoring
- MD — Malware Detection
- PM — Patch Management
- SQA — Security Assessment Questionnaire Service
- SCA — Runtime Software Composition Analysis
- TC — Cloud Native Application Security
- CS — Container Security
- CV — Cloud View
- TP — Threat protection
- WAS — Web Application Scanning
- WAF — Web Application Firewall
- CM — Continuous Monitoring
- SAQ — Security Assessment Questionnaire
- CAR — Custom Assessment and Remediation
- PS — Network Passive Sensor
- QGS — Qualys Gateway Service
- CAPS — Cloud Agent Passive Sensor

Try any of these supported solutions and see how the Cloud Agent works for you!

For a free trial of Qualys Cloud Agent, visit qualys.com/forms/cloud-agent/

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance, and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR®, and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit **qualys.com**

v230928