EXHIBIT 7

Cloud Agent Platform Technical White Paper

April 2017

Affected Versions: Cloud Agent Windows 1.5.6, Linux 1.6.0, Mac 1.6.0

Overview

This Technical White Paper documents the system design, functionality, communication protocols, lifecycle, configuration, deployment, and best practices of the Qualys Cloud Agent Platform.

The Cloud Agent provides a continuous view of assets for vulnerability management, policy compliance, and asset inventory without the need for credential management, scan windows, and firewall changes required by network scanner deployments. The Cloud Agent delivers visibility and security solutions for assets that are not able or not easily scanned from the network including remote/roaming users, distributed offices, and cloud server instances.

System Design and Functional Approach

The Cloud Agent Platform is designed for the agent and platform to work in concert to provide a high level of accuracy and fidelity, low end-to-end processing times, and minimal resource impact on the asset.

The agent is designed to capture the metadata of the operating system, installed applications, and system configurations as needed by the different activated service modules, and upload the metadata to the platform for analysis, correlation, reporting, and alerting. The agent does not perform local processing or analysis; it only performs metadata collection which keeps resource usage extremely low with 5 MB RAM, 0.01% CPU at idle, and peak usage and network bandwidth tunable using comprehensive configuration performance parameters.

The Cloud Agent supports Vulnerability Management QIDs and Policy Compliance CIDs similar to the authenticated local checks performed by the network scanner, with some current limitations. The agent does not have the ability to perform active networking checks against ports or log into applications with credentials. The agent does not currently support Policy Compliance User Defined Controls (UDCs) or technologies that require credentials to log into the instance such as databases. Qualys recommends using the Cloud Agent in conjunction with the network scanner for on-premise deployments to give a unified view of the asset, where the agent provides an internal view without requiring authentication credentials and the scanner provides an external view.

The Cloud Agent is the preferred method for assets like dynamic IP client machines, remote/roaming users, static and ephemeral cloud instances, and systems sensitive to external scanning where it's not possible or practical to do network scanning.

Asset Metadata Collected by Cloud Agent

The Cloud Agent design differs from the Qualys Scanner approach in that the agent does not perform vulnerability management and policy compliance processing in the agent itself. Rather, the Cloud Agent simply collects metadata on certain files, processes, and registry keys to find installed software, configuration settings, and environmental variables and securely transmits the metadata to the Qualys Platform for processing on the platform. The specifications of what the agent collects are defined in a configuration file called a "manifest" that is dynamically generated on the platform and downloaded by the agent when new vulnerability management QIDs and policy compliance CIDs are created by the Qualys content teams.

The specific metadata collected by the agent changes over time as new QIDs and CIDs are created and as some older QIDs or CIDs are deprecated or superseded. Some examples of metadata collected include:

- Files

```
%ProgramFiles(x86)%\Google\Chrome\Application\56.0.2924.87\chrome.dll file
version is 56.0.2924.87

%windir%\System32\ntdll.dll Version is 6.1.7601.23677

KERNEL version="2.6.32-642.6.1.el6" package="kernel-2.6.32-642.6.1.el6"
```

- Registry

```
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
PendingFileRenameOperations exists

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters DisabledComponents is
missing
```

- Configuration Settings

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SeCEdit\Reg
Values\MACHINE/Software/Microsoft/Windows
NT/CurrentVersion/Winlogon/PasswordExpiryWarning/ValueType is 4

net.ipv4.conf.all.log_martians = 0
```

The Asset Inventory module collects hardware and software information, including but not limited to list of installed software and versions, IP address and MAC address, hardware information such as manufacturer and model, BIOS, installed CPUs and Volume information, local user accounts, open ports, and running services and their version information.

Agent – Platform Communication Design

Cloud Agent communication is optimized to support large scale agent deployments while providing flexible and granular performance configuration controls allowing organizations to tune agent performance and bandwidth usage for their specific environment requirements.

All communications are initiated by the agent outbound from the agent to the platform using REST over HTTPS/TLS on configurable intervals. (The platform does not initiate connections to the agent.) The agent and platform utilize SSL 3.0, TLS 1.2, SHA256 ciphers, and 2048-bit private key for the platform. Communications are encrypted using server certificates, with application-layer authentication, data security, and non-repudiation techniques. Agent communications are protocol compatible with stateful firewalls, application-aware firewalls, transparent and non-transparent web proxies, and NAT gateways.

Connections are transient and initiated from the agent on configurable intervals only for the duration of the session after which the session is terminated. Sessions are not persistent. Content downloads from the platform to the agent occur only through a request/reply method initiated by the agent outbound to the platform; the platform does not have the ability to initiate a connection to the agent.

Agents support HTTPS proxies with authentication using local configuration for all operating systems; PAC files and WPAD for Windows. The proxy configuration is configured using local command line tools (QualysProxy.exe on Windows and config-tool.sh on Linux and Mac), and can be scripted using software distribution tools. Windows agents configured with a PAC file check for a new PAC file at the start of each communication session initiated by the agent; this ensures that the agent will use the most recent file.

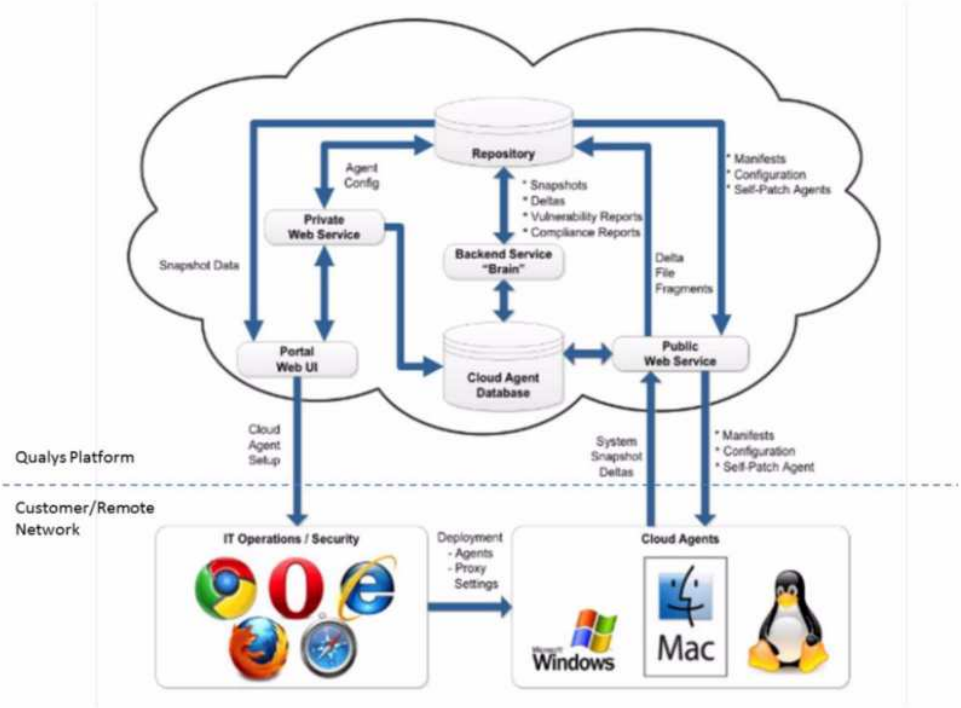

Figure: Qualys Cloud Agent Platform Communication

Configuration Profile Performance Parameters

The following table lists the pre-defined Configuration Profile performance parameters default values as of Portal 2.23. (Legacy performance parameters are still available to support older agent versions.)

Performance Parameters - Default	Low	Normal	High
Agent Status Interval	900 secs	900 secs	900 secs
Delta Upload Interval	60 secs	60 secs	60 secs
Chunk sizes for file fragment uploads	1024 KB	1024 KB	1024 KB
Upgrade Reattempt Interval	300 secs	300 secs	300 secs
Logging level for agent	Verbose	Verbose	Verbose
CPU Limit (Windows)	5 %	20 %	80 %
CPU Throttle (Linux/Mac)	20 ms	10 ms	0 ms

Based on real-world performance profiling, the recommended values for the new agent versions (Windows 1.5.6 and Linux/Mac 1.6.0) are listed in the table below for different performance profiles (Low, Normal, and High). Recommended values that are different from the default values are highlighted in *red italics*. It's not possible to edit the default performance profiles; one can create

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.