EXHIBIT 6

HIGHLY CONFIDENTIAL – ATTORNEYS EYES' ONLY – SOURCE CODE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

FINJAN LLC, a Delaware Limited Liability Company,

Plaintiff,

v.

QUALYS INC., a Delaware Corporation,

Defendant.

Case No. No. 4:18-cv-07229-YGR (TSH)

OPENING EXPERT REPORT OF ERIC COLE, PH.D. REGARDING INFRINGEMENT BY QUALYS INC. OF PATENT NOS. 6,154,844; 8,677,494; AND 7,418,731
[HC-AEO]

Date: December 1, 2020

Eric Cole, PH.D.
Ashburn, Virginia

network security, Finjan submitted and was awarded multiple patents, including the patents involved in this case.

1. The '844 Patent

86. The '844 Patent focuses on inspecting files that are downloaded onto a computer and verifying that the code is not suspicious and will not cause any harm before it is allowed to run on a client, like a web browser. '844 Patent, 1:20-2:2. This is generally performed by looking at the content of the files, generating a profile and linking it to the content. This profile can be used in a number of ways to protect against threats. In one example, the profile may be used in real-time to decide what action would be allowed to be taken. '844 Patent, 2:3-3:7. In other instances, the profile could be analyzed by other processes as part of a backend security system used to classify malicious content and push out updates to other systems.

87. More specifically, the technology focuses on protecting a system against a potentially malicious Downloadable. A Downloadable is any code that would get delivered to a computer from a third-party site, in which can have no level of trust to the validity of the code that is going to run on their system. '844 Patent, 1:20-3:7. This code often comes from untrusted sites on the Internet and could run without the user's knowledge or permission. The Downloadable is often in the form of Executables, Java applets, ActiveX controls, JavaScript, Visual Basic scripts, HTML, PDFs, etc. '844 Patent, 1:60-2:2. Users often visit websites that they believe are legitimate and are inadvertently tricked into having code downloaded to their system that causes harm. Since the code can be very stealthy and bypass traditional security controls, additional protection that is provided in the '844 Patent is needed in order to minimize that damage that can be caused by this code. '844 Patent, 1:20-59.

88. The technology protects a computer system using an inspector. '844 Patent, 1:60-3:7. The inspector would review the Downloadable and create a security profile (also referred to as a "DSP") that verifies and validates the actions that the code is going to take on the system. '844 Patent, 1:60-3:7 and 3:66-5:13. The system can use the results of the analysis to allow code

to run or preventing it from running on the system. '844 Patent, 2:20-3:7. The security profile that is created is based off code that is identified to be suspicious. '844 Patent, 2:3-3:7. This is significant because this would allow the invention to be able to detect both known attack vectors and unknown (zero-day attacks). The term zero day or 0-day attack was coined to refer to cases where the adversary knew about a vulnerability and released malicious code weeks or months before the software vendors had a chance to develop/release a patch and a signature.

2. The '494 Patent

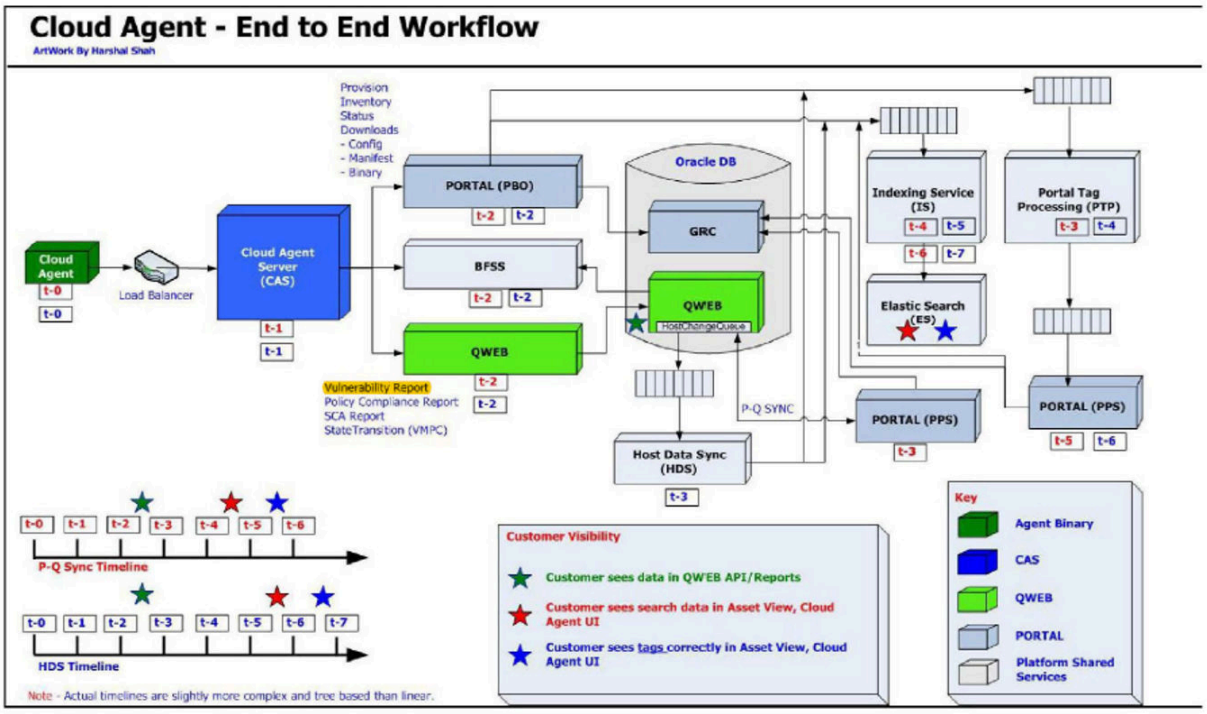
89. The technology of the '494 Patent (including through its incorporation of the '780 Patent as a parent application) generally relates to protecting against a potentially malicious "Downloadable." '780 Patent, 1:30-63; '494 Patent, 1:60-63. At the time of the invention claimed in the '494 Patent, a Downloadable was a new type threat in the form of executables, JavaScript, PDFs, etc. '780 Patent, 1:30-63; '494 Patent, 2:59-64. In a typical scenario, a Downloadable is delivered to a computer from another computer on the Internet (sometimes called a server) where there is not a sufficient level of trust and is a common avenue for adversaries to deliver malicious code to a system. '780 Patent, 1:30-2:44; '494 Patent, 2:51-3:2. This code often comes from untrusted sites or persons on the Internet and could run without the user's knowledge or permission. '780 Patent, 1:30-2:44; '494 Patent, 2:51-3:2. Claim 10 of the '494 Patent describes a system addressing this problem, and which downloads content, inspects content that is downloaded, determines if the downloaded content may perform malicious or suspicious operations, and stores this security profile in a database. '494 Patent, Claim 10. The '494 Patent, includes a description of the operations that are "suspicious." '780 Patent, 6:1-16. Suspicious operations described include operations for reading and writing files, sending or sending data over a network, and changing the registry.

90. The '494 Patent uses a malware scanning approach that was pioneered by Finjan. Deriving or generating Downloadable security profile data is quite different than the traditional signature based detection that was used before Finjan's inventions. The traditional signature

Cloud Agent Architecture

Cloud Agent End-to-End workflow

Cloud Agent End-to-End workflow
Cloud Agent Logical System Components Environment



QUALYS01994509.

159. Qualys Cloud Agents collect and upload data. Qualy Cloud Agents operate "in concert with the platform to optimize the discovery, classification, and reporting of vulnerabilities, compliance violations, and asset inventory. The agent uses a lightweight data collection mechanism to simply capture the version numbers and other metadata about the operating system and installed applications and sends the data to the platform for analysis and reporting." QUALYS00325126.

160. According to Qualys, Cloud Agents are the preferred scanning "method for assets like dynamic IP client machines, remote/roaming users, static and ephemeral cloud instances, and systems sensitive to external scanning. After their initial deployment, Cloud Agents run a full configuration assessment of their host in the background and upload the collected data to the Qualys Cloud Platform for analysis. Then, as soon as changes occur, Cloud Agents push updates

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.