EXHIBIT A

US Patent No. 8,225,408

Method and System for Adaptive Rule-based Content Scanners

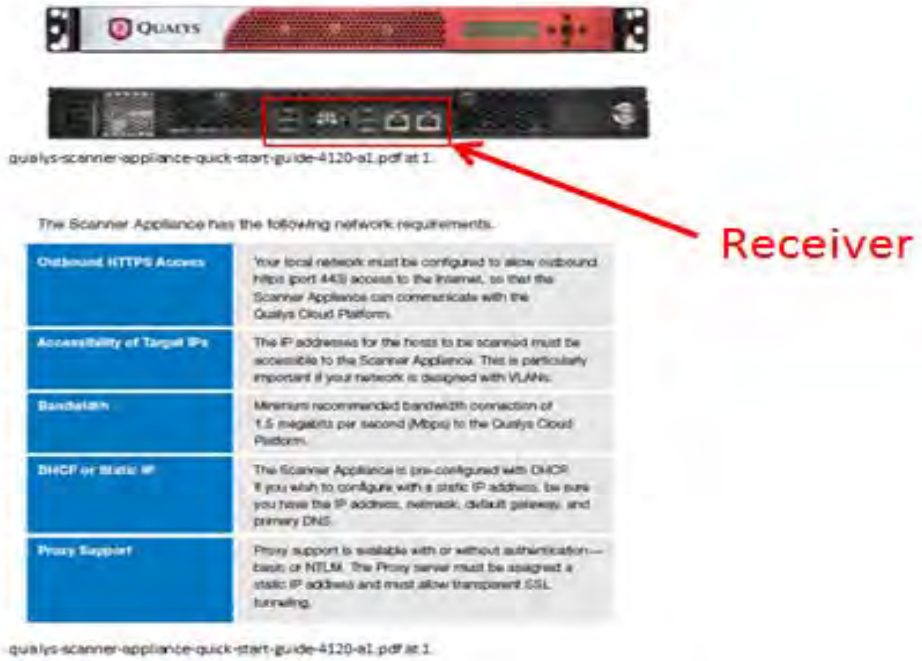
Claim 1	
1a. A computer processor-based multi-lingual method for scanning incoming program code, comprising: 1b. receiving, by a computer, an incoming stream of program code; 1c. determining, by the computer, any specific one of a plurality of programming languages in which the incoming stream is written; 1d. instantiating, by the computer, a scanner for the specific programming language, in response to said determining, the scanner comprising parser rules and analyzer rules for the specific programming language, wherein the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and wherein the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious; 1e. identifying, by the computer, individual tokens within the incoming stream; 1f. dynamically building, by the computer while said receiving receives the incoming stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules; 1g. dynamically detecting, by the computer while said dynamically building builds the parse tree, combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules; and 1h. indicating, by the computer, the presence of potential exploits within the incoming stream, based on said dynamically detecting.	The Qualys Accused Products perform a multi-lingual method for scanning incoming program code that a user attempts to download from the Internet. The program code is diverted to the Accused Products for analysis if the program code appears suspicious or is of a certain file type. Each Accused Product performs static, dynamic and behavioral analysis of received downloaded program code to identify exploits, and uses internal databases (as described below) to parse and analyze program code to detect exploits indicating that the program code is suspicious or malicious.

US Patent No. 8,225,408

Method and System for Adaptive Rule-based Content Scanners

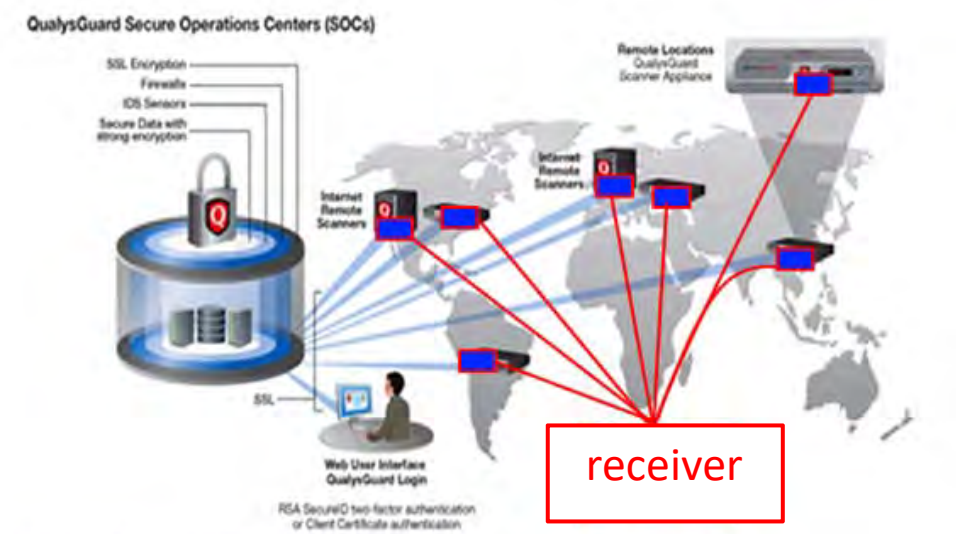
Claim 1	
1a. A computer processor-based multi-lingual method for scanning incoming program code, comprising: 1b. receiving, by a computer, an incoming stream of program code; 1c. determining, by the computer, any specific one of a plurality of programming languages in which the incoming stream is written; 1d. instantiating, by the computer, a scanner for the specific programming language, in response to said determining, the scanner comprising parser rules and analyzer rules for the specific programming language, wherein the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and wherein the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious; 1e. identifying, by the computer, individual tokens within the incoming stream; 1f. dynamically building, by the computer while said receiving receives the incoming stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules; 1g. dynamically detecting, by the computer while said dynamically building builds the parse tree, combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules; and 1h. indicating, by the computer, the presence of potential exploits within the incoming stream, based on said dynamically detecting.	**1b. Contention 1 – The Accused Products, each resident on the Qualys Cloud, receive an incoming stream of computer code** Each of the Accused Products, executed on a node that is part of the Qualys Cloud computing environment, includes a receiver component on a node that receives content based on a client device requesting the content from a source computer, such as the Internet. As shown below, the content is received by each Accused Product, (via the receiver) when a particular client device requests content provided by a source computer.  http://www.brsec.com.br/eng/int_qualysguard.asp

US Patent No. 8,225,408
Method and System for Adaptive Rule-based Content Scanners

Claim 1	
1a. A computer processor-based multi-lingual method for scanning incoming program code, comprising: 1b. receiving, by a computer, an incoming stream of program code; 1c. determining, by the computer, any specific one of a plurality of programming languages in which the incoming stream is written; 1d. instantiating, by the computer, a scanner for the specific programming language, in response to said determining, the scanner comprising parser rules and analyzer rules for the specific programming language, wherein the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and wherein the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious; 1e. identifying, by the computer, individual tokens within the incoming stream; 1f. dynamically building, by the computer while said receiving receives the incoming stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules; 1g. dynamically detecting, by the computer while said dynamically building builds the parse tree, combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules; and 1h. indicating, by the computer, the presence of potential exploits within the incoming stream, based on said dynamically detecting.	**1b. Contention 2 – The Accused Products, each resident on Appliance Scanners, receive an incoming stream of computer code** Each of the Accused Products executed on Appliance Scanners, dispersed over a computer network, includes a receiver component that receives content based on a client device requesting the content from a source computer, such as the Internet. As shown below, the content is received by each Accused Product (via the receiver of the Appliance Scanner) when a particular client device requests content provided by a source computer.  quialys-scanner-appliance-quick-start-guide-4120-a1.pdf at 1. The Scanner Appliance has the following network requirements. Outbound HTTPS Access Your local network must be configured to allow outbound https (port 443) access to the Internet, so that the Scanner Appliance can communicate with the Qualys Cloud Platform. Accessibility of Target IPs The IP addresses for the hosts to be scanned must be accessible to the Scanner Appliance. This is particularly important if your network is designed with VLANs. Bandwidth Minimum recommended bandwidth connection of 1.5 megabits per second (Mbps) to the Qualys Cloud Platform. DHCP or Static IP The Scanner Appliance is pre-configured with DHCP. If you wish to configure with a static IP address, be sure you have the IP address, netmask, default gateway, and primary DNS. Proxy Support Proxy support is available with or without authentication—basic or NTLM. The Proxy server must be assigned a static IP address and must allow transparent SSL tunneling. quialys-scanner-appliance-quick-start-guide-4120-a1.pdf at 1.

US Patent No. 8,225,408

Method and System for Adaptive Rule-based Content Scanners

Claim 1	
1a. A computer processor-based multi-lingual method for scanning incoming program code, comprising: 1b. receiving, by a computer, an incoming stream of program code; 1c. determining, by the computer, any specific one of a plurality of programming languages in which the incoming stream is written; 1d. instantiating, by the computer, a scanner for the specific programming language, in response to said determining, the scanner comprising parser rules and analyzer rules for the specific programming language, wherein the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and wherein the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious; 1e. identifying, by the computer, individual tokens within the incoming stream; 1f. dynamically building, by the computer while said receiving receives the incoming stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules; 1g. dynamically detecting, by the computer while said dynamically building builds the parse tree, combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules; and 1h. indicating, by the computer, the presence of potential exploits within the incoming stream, based on said dynamically detecting.	**1b. Contention 2 – The Accused Products, each resident on Appliance Scanners, receive an incoming stream of computer code (continued)** As shown below, Scanner Appliances dispersed as endpoints throughout a computer network, receive content based on a client device requesting the content from a source computer, such as the Internet.  http://www.brsec.com.br/eng/int_qualysguard.asp

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.