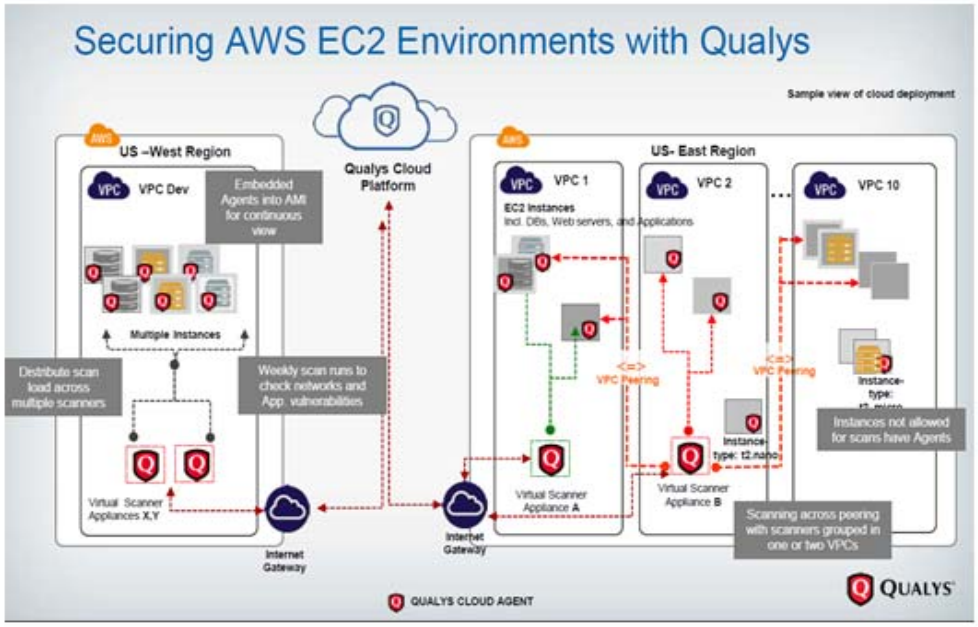
EXHIBIT 1

APPENDIX E

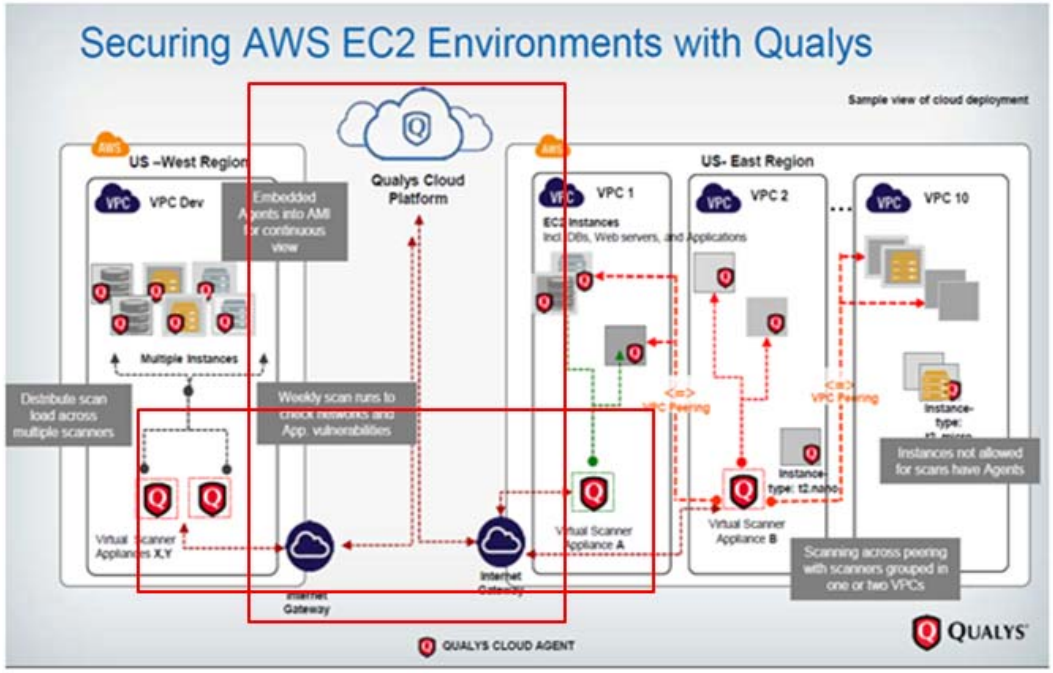
US Patent No. 8,141,154
Inspecting Dynamically Generated Executable Code

Claim 1	
1a. A system for protecting a computer from dynamically generated malicious content, comprising: 1b. a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe: 1c. a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and 1d. a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.	**1a. All Contentions – "A system for protecting a computer…":** Qualys Accused Products, including Vulnerability Management, Threat Protection, Continuous Monitoring, Indication of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring provide computer security functionality that will protect against dynamically generated malicious content.  qsc18-day1-03-cloud-platform.pdf at page 15.

US Patent No. 8,141,154
Inspecting Dynamically Generated Executable Code

Claim 1	
1a. A system for protecting a computer from dynamically generated malicious content, comprising: 1b. a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe: 1c. a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and 1d. a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.	Qualys Accused Products include a content processor that processes downloaded web and email content that they receive to identify function calls that include an input that is suspicious or malicious, and therefore should be submitted to a security computer for emulation / scanning. The emulation/scanning technology can be deployed in different configurations and receives content to process. The content processors will identify the functions that are attempting to download potentially malicious files as an input to those functions or access URLs, and will send the files to be emulated /scanned in the security computer. The security computer will return a verdict on whether the file is safe to be transmitted to the end user according to the returned verdict and security policy. Further explanation of the first and second function and input is provided below.  QualysCloud.pdf at p.29.

US Patent No. 8,141,154
Inspecting Dynamically Generated Executable Code

Claim 1	
1a. A system for protecting a computer from dynamically generated malicious content, comprising: 1b. a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe: 1c. a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and 1d. a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.	**1b. Contention 1 – Internet Gateway is the Content processor and the Qualys Cloud Platform and/or Virtual Scanner Appliances are the security computers** The Internet Gateway is a processor of content received over a network that includes a call to a function. To determine whether the content is safe to invoke, it transmits the content to a security computer (Qualys Cloud Platform and/or Virtual Scanner Appliances) for inspection and awaits a determination whether invoking functions within that content is safe. The Qualys Cloud Platform and Virtual Scanner Appliances comprise Vulnerability Management, Threat Protection, Continuous Monitoring, Indication of Compromise, Container Security, Web App Firewall, Web App Scanning, and Compliance Monitoring. See analysis for Claim 1a. above.  QualysCloud.pdf at p.29.

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.