Filed on behalf of: Wiz, Inc.
By: Matthew A. Argenti (margenti@wsgr.com)
Michael T. Rosato (mrosato@wsgr.com)
Wesley E. Derryberry (wderryberry@wsgr.com)
Joseph M. Baillargeon (jbaillargeon@wsgr.com)
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, CA 94304

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WIZ, INC.,
Petitioner,

v.

ORCA SECURITY LTD.,
Patent Owner.

Case IPR2024-01109
Patent No. 11,726,809

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,726,809

TABLE OF CONTENTS

Listing of Challenged Claims

1. A method for securing virtual cloud assets against cyber vulnerabilities in a cloud computing environment, the method comprising:

[1.1] determining, using an API or service provided by the cloud computing environment, a location of a snapshot of at least one virtual disk of a protected virtual cloud asset, wherein the protected virtual cloud asset is instantiated in the cloud computing environment;

[1.2] accessing, based on the determined location and using an API or service provided by the cloud computing environment, the snapshot of the virtual disk;

[1.3] analyzing the snapshot of the at least one virtual disk by matching installed applications with applications on a known list of vulnerable applications;

[1.4] determining, based on the matching, an existence of a plurality of potential cyber vulnerabilities;

[1.5] correlating the determined potential cyber vulnerabilities with a network location of the protected virtual cloud asset;

[1.6] using the determined plurality of potential cyber vulnerabilities and the network location of the protected virtual cloud asset to determine a risk of the protected virtual cloud asset to the cloud computing environment;

[1.7] prioritizing, by the determined risk, the plurality of potential cyber vulnerabilities; and

[1.8] reporting the determined plurality of potential cyber vulnerabilities as alerts prioritized according to the determined risk

2. The method of claim 1, wherein reporting the determined potential cyber vulnerabilities includes communicating the prioritized alerts to a user console or a security information and event management (SIEM) system.

3. The method of claim 2, further comprising filtering the determined potential cyber vulnerabilities based on a determined risk level associated with each

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.