

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)  
Tasha M. Thomas (tthomas@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 IPR2024-01190  
Patent No. 11,740,926

---

**PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 11,740,926**

## TABLE OF CONTENTS

I.	INTRODUCTION .....	1
II.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	1
III.	CERTIFICATIONS.....	3
IV.	IDENTIFICATION OF CHALLENGE; STATEMENT OF PRECISE RELIEF REQUESTED .....	3
V.	THE '926 PATENT.....	4
	A. Prosecution History .....	5
VI.	NO BASIS EXISTS FOR DISCRETIONARY DENIAL .....	5
	A. <i>Fintiv</i> .....	5
	B. Discretionary Denial Is Not Warranted under 35 U.S.C. §325(d) .....	6
VII.	LEVEL OF ORDINARY SKILL .....	8
VIII.	CLAIM CONSTRUCTION .....	8
	A. “Locating” a Snapshot.....	9
	B. “[Analyze/Analyzing] the Snapshot” .....	10
IX.	BACKGROUND .....	11
	A. Cloud Computing, Virtualization, and Snapshots.....	11
	B. Cyber Security .....	13
X.	PRIOR ART.....	15
	A. Veselov (U.S. Patent. No. 11,216,563; EX1007) .....	15
	B. Mohanty (U.S. Patent No. 9,692,778; EX1075) .....	19
	C. Ranum (U.S. Patent No. 9,088,606; EX1093).....	19
	D. Seo (U.S. Publication No. US 2019/0180028; EX1094) .....	20
	E. Hutchins (U.S. Publication No. US 2013/0024940; EX1070) .....	21
XI.	GROUND 1: CLAIMS 1, 5-10, AND 12-15 WERE OBVIOUS OVER VESELOV AND MOHANTY .....	21
	A. Reasons to Combine Veselov and Mohanty .....	22

B.	Independent Claims 1, 14, and 15 .....	26
1.	Preambles .....	26
2.	Element 15.i .....	28
3.	Elements 1.1, 14.1, and 15.1 .....	28
4.	Elements 1.2, 14.2, and 15.2 .....	29
5.	Elements 1.3, 14.3, and 15.3 .....	33
6.	Elements 1.4, 14.4, and 15.4 .....	34
7.	Elements 1.5, 14.5, and 15.5 .....	41
8.	Elements 1.6, 14.6, and 15.6 .....	41
9.	Elements 1.7, 14.7, and 15.7 .....	42
C.	Dependent Claims .....	45
1.	Claim 5 .....	45
2.	Claim 6 .....	45
3.	Claim 7 .....	46
4.	Claim 8 .....	48
5.	Claim 9 .....	50
6.	Claim 10 .....	51
7.	Claim 12 .....	52
8.	Claims 13 .....	53
XII.	GROUND 2: CLAIMS 1-10 AND 12-15 WERE OBVIOUS OVER VESELOV, MOHANTY, AND RANUM .....	57
A.	Reasons to Combine Veselov, Mohanty, and Ranum .....	57
B.	Claims 1, 14, and 15 .....	61
1.	Elements 1.4, 14.4, and 15.4 .....	61
2.	Elements 1.7, 14.7, and 15.7 .....	62
C.	Claim 2 .....	63
D.	Claim 4 .....	64
1.	Element 4.1 .....	64

2.	Element 4.2 .....	65
XIII.	GROUND 3-4: CLAIM 3 WAS OBVIOUS OVER VESELOV, MOHANTY, AND SEO (WITH OR WITHOUT RANUM) .....	66
A.	Reasons to Combine Veselov, Mohanty, and Seo (with or without Ranum) .....	66
B.	Claim 3 .....	69
XIV.	GROUND 5-6: CLAIM 11 WAS OBVIOUS OVER VESELOV, MOHANTY, AND HUTCHINS (WITH OR WITHOUT RANUM) .....	70
A.	Reasons to Combine Veselov, Mohanty, and Hutchins (with or without Ranum) .....	71
B.	Claim 11 .....	72
XV.	CONCLUSION.....	73

## LISTING OF CHALLENGED CLAIMS

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

[1.1] receiving a request to scan a protected virtual cloud asset in the cloud computing environment;

[1.2] locating, using an API or service provided by the cloud computing environment, a snapshot of at least one virtual disk of the protected virtual cloud asset;

[1.3] accessing, using an API or service provided by the cloud computing environment, the snapshot of the at least one virtual disk;

[1.4] analyzing the snapshot of the at least one virtual disk to determine the existence of a plurality of potential cyber threats, each cyber threat based on data stored on the virtual disk, wherein the data includes at least one of: unencrypted sensitive data, unencrypted system credentials, weak passwords, weak encryption schemes, disabled Address Space Layout Randomization, boot record manipulation, suspicious definitions, services to be run on startup, personally identifiable information, data in application logs indicating that the protected virtual cloud asset accessed personally identifiable information, data in application logs indicating that the protected virtual cloud asset accessed a computer containing personally identifiable information, or at least one change in at least one area of the virtual disk, as compared to an earlier point in time;

[1.5] determining a risk associated with each of the determined plurality of potential cyber threats;

[1.6] prioritizing the potential cyber threats associated with the protected virtual cloud asset based on the determined risk associated with each of the plurality of potential cyber threats; and

[1.7] reporting at least some of the determined plurality of potential cyber threats as alerts prioritized according to their associated risks.

# 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.