Secure Cloud Infrastructure Patent Portfolio Opportunity

1 Patent Family Comprising 3 Patents

Contact: gustavo@rzv-ip.com

More information is available upon request and under NDA.
Contact Gustavo Aray at gustavo@rzv-ip.com.

RZV International IP Transactions

Executive Summary

- RZV has been exclusively retained to monetize an innovative portfolio relevant to hardened cloud computing developed by a DevOps professional with a background in government and defense industry deployments.
- The portfolio discloses methods related to creating hardened (secure) virtualized computing resources. These methods enable the creation of cloud infrastructure that is compliant with government and industry security standards, such as those defined by CIS, NIST, FedRAMP, PCI DSS, and HIPAA. Additionally, they detail how to integrate Infrastructure-as-Code, Continuous Integration/Continuous Deployment, monitoring, and notifications to ensure the repeatable deployment and maintenance of secure resources.
- The key asset US11216265 is applicable to cloud computing providers that support hardened, secure infrastructure.
- Companies that may have an interest in the portfolio include:

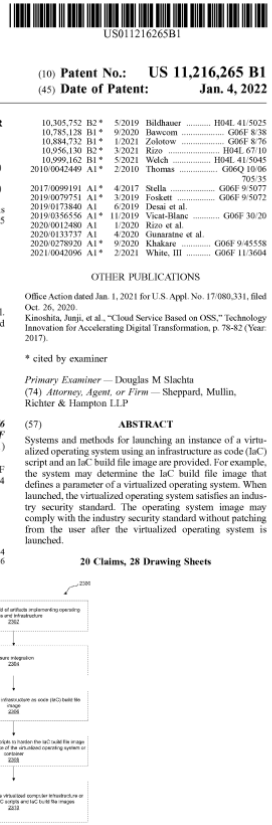
Portfolio:
3 US patents
Earliest Priority:
July 2020
Est. Avg. Expiry:
October 2040
Evidence of Use:
Claim charts available under NDA
Encumbrances:
None
Price Expectations:
Consistent with current market prices
Deal Structure:
We will consider all proposals
Deadlines:
All offers considered in the order received

RZV International IP Transactions

Secure Cloud Infrastructure US Patent Portfolio

Family	Patent #	Application #	Title	Priority Date	File Date	Pub. Date	Est. Expiry
1	US11216265	US17080289	Repeatable security hardening for virtualized hardware and infrastructure	2020-07-02	2020-10-26	2022-01-04	2040-10-26
	US11010191	US17080246	Platform-independent interface for generating virtualized multi-service hardware systems and infrastructure	2020-07-02	2020-10-26	2021-05-18	2040-10-26
	US11023301	US17080331	Unified api platform	2020-07-02	2020-10-26	2021-06-01	2040-10-26

Key Patent – US11216265B2



US011216265B1

(12) **United States Patent**
Hornbeck

(10) **Patent No.: US 11,216,265 B1**
(45) **Date of Patent: Jan. 4, 2022**

(54) **REPEATABLE SECURITY HARDENING FOR VIRTUALIZED HARDWARE AND INFRASTRUCTURE**

(71) Applicant: **Ryan L. Hornbeck**, Burbank, CA (US)

(72) Inventor: **Ryan L. Hornbeck**, Burbank, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **17/080,289**

(22) Filed: **Oct. 26, 2020**

Related U.S. Application Data

(60) Provisional application No. 63/047,532, filed on Jul. 2, 2020, provisional application No. 63/085,047, filed on Sep. 29, 2020.

(51) **Int. Cl.**
G06F 8/61 (2018.01)
G06F 21/50 (2013.01)
G06F 21/54 (2013.01)
G06F 8/76 (2018.01)

(52) **U.S. Cl.**
CPC ***G06F 8/63*** (2013.01); ***G06F 8/76*** (2013.01); ***G06F 21/50*** (2013.01); ***G06F 21/54*** (2013.01)

(58) **Field of Classification Search**
CPC ... G06F 8/63; G06F 8/76; G06F 21/50; G06F 21/54
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,255,370 B2 * 4/2019 Carpenter G06F 16/9024
10,291,466 B2 * 5/2019 Smartt H04L 41/0806
10,305,752 B2 * 5/2019 Bildhauer H04L 41/5025
10,785,128 B1 * 9/2020 Bawcom G06F 8/38
10,884,732 B1 * 1/2021 Zolotow G06F 8/76
10,956,130 B2 * 3/2021 Rizo H04L 67/10
10,999,162 B1 * 5/2021 Welch H04L 41/5045
2010/0042449 A1 * 2/2010 Thomas G06Q 10/06 705/35
2017/0099191 A1 * 4/2017 Stella G06F 9/5077
2019/0079751 A1 * 3/2019 Foskett G06F 9/5072
2019/0173840 A1 6/2019 Desai et al.
2019/0356556 A1 * 11/2019 Vicat-Blanc G06F 30/20
2020/0012480 A1 1/2020 Rizo et al.
2020/0133737 A1 4/2020 Gunaratne et al.
2020/0279020 A1 * 9/2020 Khakare G06F 9/45558
2021/0042096 A1 * 2/2021 White, III G06F 11/3604

OTHER PUBLICATIONS

Office Action dated Jan. 1, 2021 for U.S. Appl. No. 17/080,331, filed Oct. 26, 2020.
Kinoshita, Junji, et al., "Cloud Service Based on OSS," Technology Innovation for Accelerating Digital Transformation, p. 78-82 (Year: 2017).

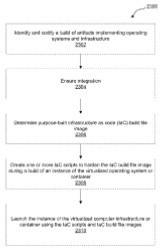
* cited by examiner

Primary Examiner — Douglas M Slachta
(74) *Attorney, Agent, or Firm* — Sheppard, Mullin, Richter & Hampton LLP

(57) **ABSTRACT**

Systems and methods for launching an instance of a virtualized operating system using an infrastructure as code (IaC) script and an IaC build file image are provided. For example, the system may determine the IaC build file image that defines a parameter of a virtualized operating system. When launched, the virtualized operating system satisfies an industry security standard. The operating system image may comply with the industry security standard without patching from the user after the virtualized operating system is launched.

20 Claims, 28 Drawing Sheets



Title:	Repeatable Security Hardening for Virtualized Hardware and Infrastructure
Assignee:	Ryan L. Hornbeck
Inventors:	Ryan L. Hornbeck
Priority Date:	July 2, 2020
Filing Date:	October 26, 2020
Issue Date:	January 4, 2022
Est. Expiration:	October 26, 2040

Key Claim 1

US11216265B2; Claim 1:

A method for creating a compute pipeline to define a new computer infrastructure component, the method comprising:

- identifying and codifying operating systems and infrastructure complying to hardened states defined by industry standards that ensure no compute resources are launched in an unsecured state, wherein the identifying and codifying is through scripting, automation, and scheduled builds of artifacts of the operating systems and the infrastructure;
- ensuring integration with enterprise monitoring and operation toolsets, audit capabilities, stateful management and compliance tools and services, and automation toolsets for the purpose of Continuous Integration and Continuous Delivery (CICD);
- determining purpose-built Infrastructure as Code (IaC) build file images, wherein the IaC build file image defines parameters of a virtualized operating system or container affected by Governance, Standards, and Security of a given Organization, and wherein the virtualized operating system or container, when launched, satisfies an industry security standard;
- creating IaC scripts to harden the IaC build file image during a build of an instance of the virtualized operating system or container defined by the Governance, Standards, and Security of the given Organization; and
- launching the instance of the virtualized operating system or container using the IaC scripts and purpose-built IaC build file images resulting in a stateful machine or container instance integrated with monitoring, logging, ChatOps, automation, and governance functions as deemed required by the Governance.

Thanks!

Contact: gustavo@rzv-ip.com