FORTINET | WIZ

SOLUTION BRIEF

Fortinet and Wiz Automate Seamless Protection for Cloud Environments

Protecting Cloud Environments with Deep Visibility and Automated Remediation

Executive Summary

The Wiz and Fortinet integration provides customers with complete protection of cloud resources by detecting network exposure risks, understanding the context around them, and automatically remediating them. The integration takes advantage of the deep visibility that Wiz has into cloud environments and context of which exposures lead to critical attack paths and allows the Fortinet Security Fabric to ingest these insights to automate security enforcement to seamlessly protect cloud environments for joint customers. As a result, joint customers can now use FortiGate VM and FortiGate CNF to block or allow certain traffic to and from virtual machines (VMs) based on attack paths identified by Wiz or suspicious cloud events.

Expanding Cloud Footprint Brings Expanding Risk Exposure

As organizations continue to expand their cloud footprint in pursuit of their digital acceleration objectives, they inadvertently are also expanding their risk profile and operational complexity as a trade-off. According to the 2023 Cloud Security Report conducted by Cybersecurity Insiders and sponsored by Fortinet, some of the top challenges faced by organizations are lack of qualified staff (43%), lack of visibility (32%), and difficulty in setting consistent policies (32%).

In light of these operational challenges and the expansive yet porous cloud environments most organizations operate in, organizations cannot identify all instances of exposures within and across their multi-cloud environments, leaving the potential for critical risks to remain unnoticed until it is too late. At this point, organizations can face consequences that include data exposure, reputation loss, and business disruption.

In fact, the 2023 Cloud Security Report also uncovered that misconfiguration (59%) is the top cloud threat, followed by exfiltration of sensitive data (51%), insecure interfaces/APIs (51%), and unauthorized access (49%).

To proactively protect against threats, organizations need to deploy solutions to help them detect all public exposures, understand their business impact, and automatically remediate them to protect their workloads in the cloud.

Joint Solution

The Wiz and Fortinet integration enables mutual customers to benefit from end-to-end visibility and protection against network exposures in the cloud. Customers start by identifying public exposures in Wiz, understand cloud context from Wiz enhanced with network context from Fortinet, and automatically respond to and remediate any exposures with the Fortinet Security Fabric and Fortinet FortiGate VM and FortiGate CNF.

WIZ

Certified Wiz Integration

Solution Components

- Wiz Cloud-Native Application Protection Platform (CNAPP)
- Fortinet FortiGate VM Virtual Next-Generation Firewall
- FortiGate CNF Cloud-Native Firewall

Solution Benefits

- Automatically identify and remove unwanted public exposure
- Detect and respond to threats in real time
- Remove public exposure based on business impact

FORTINET FABRIC-READY

- **Automatically identify and remove unwanted public exposure**
  - Identify and validate publicly exposed virtual machines with Wiz, validate with Wiz's Dynamic Scanner, and automate remediation of external exposure by blocking internet traffic on Fortinet using the FortiGate VM and FortiGate CNF.
- **Detect and respond to public exposure in real time**
  - Detect suspicious behavior related to exposure with Wiz's threat detection rules, and quickly respond by automatically blocking traffic to the virtual machine with FortiGate.
- **Reduce exposure based on business impact**
  - Understand the business impact of an exposure with Wiz, such as a publicly exposed VM with a known vulnerability that has access to sensitive data, and automatically remove exposures based on criticality with Fortinet.

Solution Components

The Wiz Cloud-Native Application Protection Platform (CNAPP) enables organizations to secure everything they build and run in the cloud. It provides 100% full-stack visibility into every technology running in your public clouds across virtual machines, containers, serverless applications, and datastores without agents in minutes. Wiz builds a single prioritized queue of risks and attack paths so you can proactively reduce your attack surface. Wiz enables security, development, and operations teams to understand and control risks together across the pipeline, effectively scaling cloud security from build to runtime. Wiz unified cloud security platform enables organizations adopt a defense-in-depth strategy that enables prevention, detection, and response to cloud threats. Wiz's capabilities include:

1. Cloud security posture management (CSPM)
2. Cloud workload protection platform (CWPP)
3. Vulnerability management
4. Cloud infrastructure entitlement management (CIEM)
5. Container and Kubernetes security
6. CI/CD security (Infrastructure-as-Code scanning)
7. Data security posture management (DSPM)
8. Cloud detection and response (CDR)

Fortinet FortiGate VM virtual appliances offer protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating system, the foundation of the Fortinet Security Fabric, the industry's highest-performing and most expansive cybersecurity platform, organically built on a common management and security framework. Application control, antivirus, IPS, web filtering, and VPN along with advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, work in concert to identify and mitigate the latest complex security threats. Benefits include:

- End-to-end security across the full attack cycle
- Top-rated security validated by third-party testing
- Tight integration and multitenancy with Azure
- Centralized management across physical, virtual, and cloud deployments
- Automation templates for rapid deployment

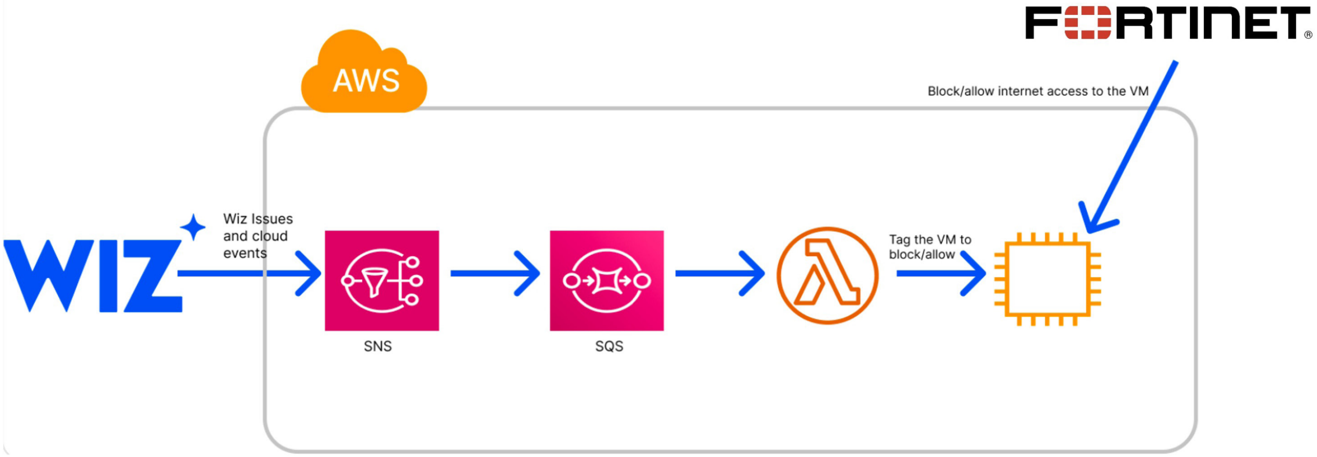
Fortinet FortiGate Cloud-Native Firewall (CNF) is a highly available SaaS service that simplifies network security while seamlessly scaling and integrating with AWS services such as AWS Gateway Load balancer and AWS Firewall Manager. FortiGate CNF reduces network security operations workloads by eliminating the need to configure, provision, and maintain any firewall software infrastructure while allowing security teams to focus on security policy management. FortiGate CNF can be billed based on consumption or purchased through annual contracts.

Joint Solution Integration

The Fortinet-Wiz integrated solution helps joint enterprise customers seamlessly protect cloud workloads with leading network security from Fortinet and leading cloud-native application protection platform from Wiz.

Wiz customers can leverage FortiGate VM and FortiGate CNF to seamlessly protect their cloud infrastructure and workloads on AWS whenever Wiz Issues are generated. Wiz Issues identify toxic combinations that result from multiple risk factors, such as a publicly exposed machine that has an exploitable vulnerability and an exposed secret allowing lateral movement in the environment.

Wiz sends the issue information (automatically or manually, depending on customer requirements) to the FortiGate VM and FortiGate CNF to either allow or block traffic going to and from protected VMs running in AWS based on FortiGate policies defined by the customer. As a result, this integration empowers customers to extend automated remediation to prevent exposure and threats at the cloud network level using Fortinet's leading network security solutions running in cloud environments.


FORTINET
AWS
Block/allow internet access to the VM
WIZ
Wiz Issues and cloud events
SNS
SQS
Tag the VM to block/allow

Joint Use Cases

Integrate Fortinet with Wiz Issues

- Identify publicly exposed VMs verified to be exposed by Wiz
- Identify the business impact of publicly exposed VMs with Wiz's Issues to find toxic combinations that can lead to an attack path (such as vulnerabilities, access to sensitive data, high privileges) and set up Fortinet remediation based on business impact

Integrate Fortinet with Wiz threat detection rules

- Detect threats in real time with Wiz's runtime sensor and threat detection rules, and automate remediation to update FortiGate when a suspicious event is detected

About Wiz

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 35 percent of the Fortune 100, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks, Lightspeed and Aglaé.
Visit https://www.wiz.io/ for more information.

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

September 11, 2023 2:16 PM