SOLUTION BRIEF

FortiCWP Provides Risk Management for Public Clouds

Executive Summary

Building and operating applications using the public cloud introduces a new threat vector—the cloud management interface and application programming interface (API). Unlike static on-premises environments, public clouds dynamically change. This introduces the chance to make configuration mistakes or omit configuration updates that are needed. And when multiple public clouds are in use, different features, management tools, and interfaces lead to fragmented visibility. This makes it even harder for organizations to identify misconfigurations, detect sophisticated attacks, assess and mitigate resource risk in distributed environments, and ultimately ensure compliance and governance.

The continuous configuration assessments and risk analysis available in the Fortinet FortiCWP Cloud Security Posture Management and Workload Protection solution present actionable information for security teams. Organizations that have adopted containers for application development can leverage FortiCWP Container Guardian to achieve deeper insights into the security posture for their container workloads. This enables them to focus on the highest-priority issues, take quick remedial actions, and automatically fix well-known vulnerability and configuration errors to manage and mitigate risk effectively.

Actionable alerts allow organizations to prioritize response based on the severity of issues and protect the usage of various public cloud resources such as Amazon S3, EC2, and EKS using identity and access management (IAM) roles and other policies.

FortiCWP Risk Management Capabilities:

- Reduces risk with centralized visibility and control for workloads and containers
- Prioritizes remediation actions based on risk severity
- Streamlines risk management across multi-cloud environments
- Shift left security embeds security into software development life cycle

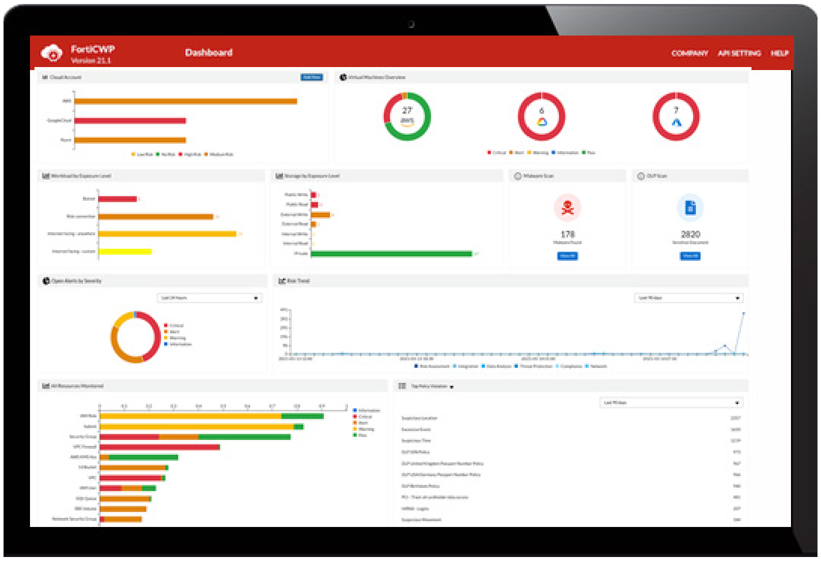

Figure 1: Continuous risk assessment in FortiCWP prioritizes security issues across public clouds.

Fragmented Cloud Infrastructures Inhibit Risk Management

In today's rapidly evolving IT environment, effectively managing a disparate set of tools to which multiple people in the organization have access is not enough. Each organization must continuously assess its IT risk posture and map security programs to align with its risk tolerance. One key driver of risk for organizations is the misconfiguration of cloud infrastructures.

Organizations with services in multiple clouds often leverage cloud-native security tools, increasing the likelihood of configuration problems—and the potential of sophisticated attacks that are not detected. In a recent survey by the Cloud Security Alliance, a key finding was that "Cloud providers' native security controls are not enough for many organizations."[1] And even if a security team were to spend hours of staff time manually checking configurations, the process would present the risk of human error—and prioritizing the most urgent fixes would be next to impossible. And even then, when the process is finally complete, the data would be obsolete because of frequent configuration changes by the cloud and application teams. So, many organizations have turned to additional and alternative security solutions to minimize their risk.

Containers Risk Management Requires a Different Approach

The adoption of cloud-native technologies to deliver new products and services has enabled organizations to rapidly transform key areas of their business. These technologies include the use of containers in microservices architectures, which have streamlined the way applications are built, tested, deployed, and redeployed.

A recent survey indicated the top security incidents that customers have experienced when using containers—67% of the incidents were the inability to detect misconfigurations, followed by the inability to remediate a major vulnerability.[2]

Traditional security tools lack the in-depth capabilities to secure container workloads. Container security requires visibility and protection during all stages of a container life cycle.

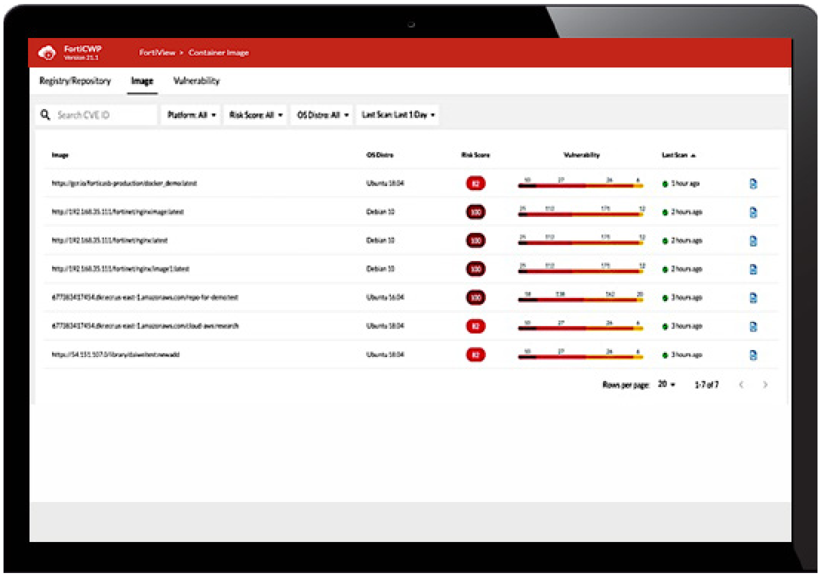

Image	OS Distro	Risk Score	Vulnerability	Last Scan
https://gcr.io/forticwb-production/docker_demo:latest	Ubuntu 18.04	82	10 27 26 6	1 hour ago
http://192.168.35.111/fortinet/nginx/image:latest	Debian 10	100	25 112 171 12	2 hours ago
http://192.168.35.111/fortinet/nginx:latest	Debian 10	100	25 112 171 12	2 hours ago
http://192.168.35.111/fortinet/nginx/image1:latest	Debian 10	100	25 112 171 12	2 hours ago
677083417454.dkr.ecr.us-east-1.amazonaws.com/repo-for-demo:test	Ubuntu 16.04	100	18 138 162 20	3 hours ago
677083417454.dkr.ecr.us-east-1.amazonaws.com/cloud-aws/research	Ubuntu 18.04	82	10 27 26 6	3 hours ago
https://54.151.107.0/library/daiwelnet:newadd	Ubuntu 18.04	82	10 27 26 6	3 hours ago

Rows per page: 20 1-7 of 7

Figure 2: FortiCWP Container Guardian monitors and detects vulnerabilities and misconfigurations in container workloads.

FortiCWP: Enabling Proactive Risk Management

The FortiCWP management solution performs thorough risk assessment and continuous analysis of the entire cloud infrastructure, including hundreds of configuration assessments for Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) settings. Administrators can enable auto-remediation actions for certain issues, and actionable alerts help security teams to identify and focus on the highest-priority issues with rapid remediation actions. Out-of-the-box configuration assessment policies are available for easy setup, and custom policy controls are available for advanced users.

FortiCWP also provides an overall risk score for the public cloud infrastructure through the Fortinet Security Rating Service, with higher scores indicating higher risk. The security team can view remediation guidelines for all items that increased the score and take proactive action. They can also drill down to resource profile details in order to understand how configurations changed over time to help with diagnosis and configuration life cycle-related recommendations. FortiCWP uses each cloud platform's API to gain full visibility of configurations, ensuring smooth operations and accurate assessments across multiple clouds.

Beyond the predefined configuration assessment policies used to manage organizational risk, FortiCWP allows organizations to create custom policies that can evaluate almost any part of the cloud configuration using advanced scripting capabilities.

And with FortiCWP Container Guardian, administrators gain deeper visibility into the security posture for container-based workloads so they can remediate risks earlier and ensure compliance to security best practices during the software development process. This capability integrates security into the DevOps continuous integration/continuous deployment (CI/CD) pipeline, so DevOps teams have increased confidence when deploying container workloads.

Managing Risk Proactively

An integrated security architecture across a multi-cloud environment enables consistency in policies and security practices companywide, improving an organization's security posture and reducing risk. FortiCWP enables security teams to be truly proactive with their risk management and offers actionable insights to different teams, helping bridge the gap between the security professional and the cloud architect.

[1] "State of Cloud Security Concerns, Challenges, and Incidents," Cloud Security Alliance, March 30, 2021.

[2] "State of Container and Kubernetes Security Report," StackRox, September 23, 2020.

FORTINET®

www.fortinet.com