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 FortiCWP cloud workload protection (CWP) present actionable information for security teams. This enables them to focus on the highest priority issues, take quick remedial actions, and automatically fix well-known configuration errors to effectively manage and mitigate risk. 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:

- Reduce risk with centralized visibility and control
- Help prioritize remediation actions based on a risk score
- Streamline risk management across multi-cloud infrastructures
- Integrate with the configuration management life cycle in DevOps for continuous integration and continuous delivery (CI/CD)

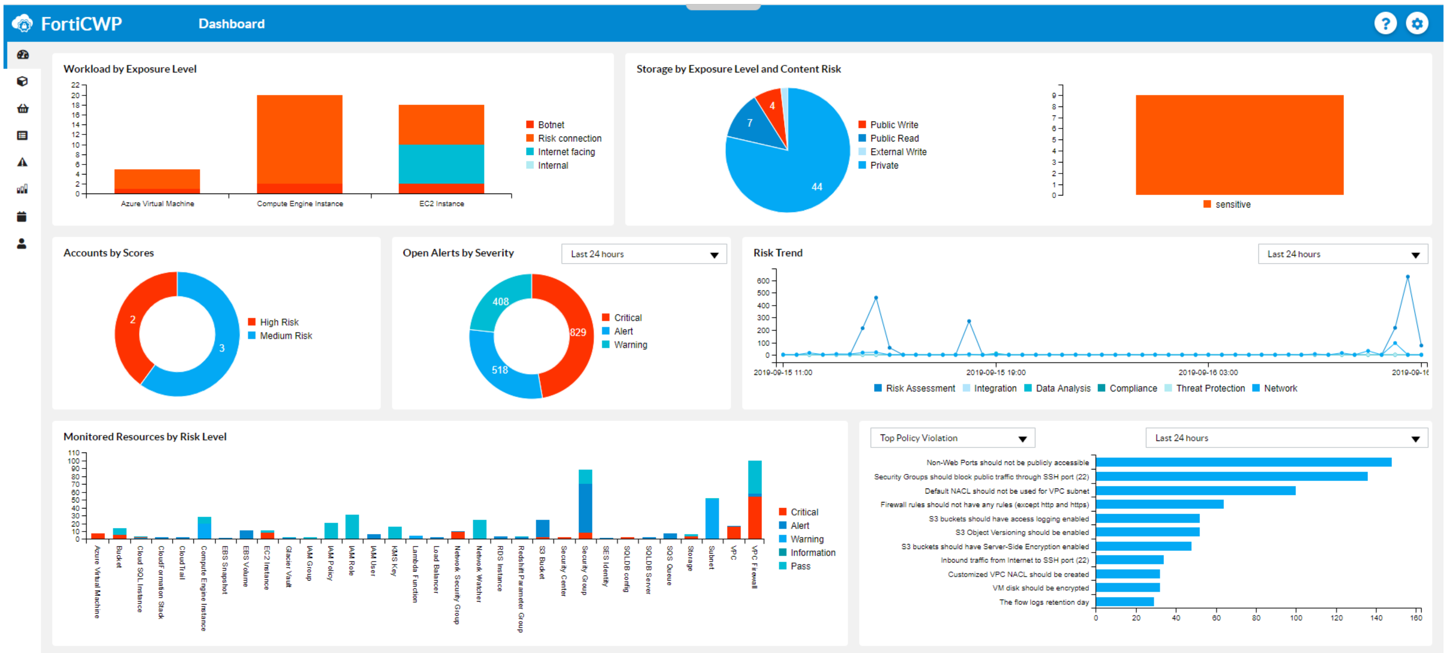

Figure 1: Ongoing risk assessment in FortiCWP helps prioritize security issues across public clouds.

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. 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. Further, when the process is finally complete, the data would be obsolete because of frequent configuration changes by the cloud and application teams.

In a fragmented public cloud infrastructure with multiple clouds and regions, configuration issues—and sophisticated attacks—are far more likely.

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. An auto-fixing option can automatically address certain issues without human involvement if enabled, 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. This enables custom notifications that may be integrated into the DevOps CI/CD pipeline.

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] Asher Benbenisty, "Don't Go Once More Unto the Breach: Fix Those Policy Configuration Mistakes," Infosecurity, October 30, 2018.

September20,201910:33AM

Mac:Users:susiehwang:Desktop:ATSK2235533154672151877:sb-forticwp-risk-management Folder:sb-forticwp-risk-management