SOLUTION BRIEF

FortiCWP Simplifies Compliance in the Public Cloud

Executive Summary

Especially for organizations operating in highly regulated industries, maintaining compliance across multiple public cloud environments is a key business requirement. However, the dynamic nature of the cloud can make it challenging to continually monitor and report on compliance with both regulatory requirements and security standards—not to mention detect violations of those. FortiCWP cloud workload protection (CWP) provides a consistent view for compliance across multiple public clouds, enabling organizations to more easily meet regulatory compliance requirements when leveraging the public cloud.

Fragmented, Time-Consuming Compliance for Public Clouds

Public cloud configurations include thousands if not millions of settings that make it extremely time-consuming to manually review configurations against compliance requirements. Further, most companies operate multiple public clouds. For many of these organizations, achieving security compliance visibility and control across all these environments is an impractical task.

Staff use siloed reporting tools and manually aggregate and reconcile event data to monitor each technology stack. The ability to interpret compliance and its implications to the ever-changing public cloud landscape is extremely difficult. Thus, organizations must always be on top of cloud changes and verify that all cloud deployments are compliant.

FortiCWP Enables Public Cloud Compliance

FortiCWP helps solve these compliance challenges by automating the evaluation of compliance-related configurations across an organization's public cloud infrastructures and different accounts. FortiCWP currently supports public cloud platforms including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Fortinet FortiCWP is a cloud security management solution that provides comprehensive compliance reporting for Infrastructure-as-a-Service (IaaS) instances across major public clouds. It simplifies compliance reporting, both scheduled on-demand, for regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and the European Union's General Data Protection Regulation (GDPR). FortiCWP also enables organizations to proactively manage their risk posture based on security standards from the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST), among others.

Key Benefits of FortiCWP for Compliance:

- Continuous compliance monitoring and reporting
- Consistent visibility across multiple public cloud IaaS environments
- Simplified compliance reporting for various regulations
- Proactive management of security standards
- Identification and remediation of unsecure provisioning and configurations

Companies use, on average, 4.9 cloud deployments today—a number that continues to increase annually.[1]

41% of security problems in the cloud are related to governance and legal issues.[2]

For IT and security staff, FortiCWP transforms tedious, time-consuming data aggregation and reconciliation into automated workflows. Specifically, FortiCWP provides out-of-the-box policies and predefined reports related to regulatory mandates and security standards.

Based on an organization's compliance requirements, FortiCWP performs hundreds of configuration assessments across its global public cloud deployments (see Figure 1). It then identifies risks associated with any unsecure provisioning or configuration detected in those public clouds.

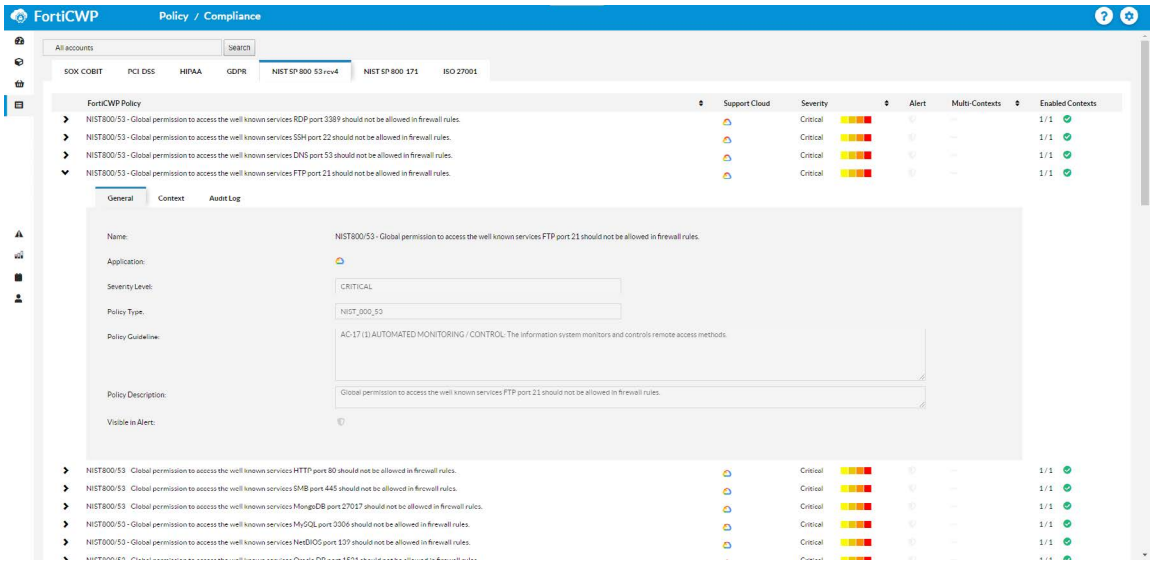

Figure 1: FortiCWP improves visibility and enhances compliance for public cloud platforms.

Unified Tracking and Reporting Leads to More Business Opportunities

Due to the steep penalties and fines attached to noncompliance with industry and government regulations like GDPR, HIPAA, and PCI DSS, compliance has become top of mind for multiple companies running applications in the public cloud. When the potential impact that breaches of confidential data like personally identifiable information (PII) can have on an organization's brand is considered, the implications of compliance are magnified even further.

At the same time, security standards like CIS and NIST provide a proven framework that enables organizations to proactively identify vulnerabilities that pose the greatest risk and remediate them before successful intrusions and breaches occur. FortiCWP breaks down the silos separating an organization's different public cloud deployments, providing a unified view across and between each cloud and the ability to generate corresponding reports matched to specific business requirements.

FortiCWP reporting capabilities include historical snapshots and real-time visualizations of each cloud deployment and potential misconfigurations. Armed with this information, audit teams can quickly identify policy violations and take the necessary remediation actions.

Reaping the Rewards of Proactive Cloud Compliance

Proactive compliance management requires transparent visibility and unified controls across and between each cloud deployment. FortiCWP enables organizations to streamline compliance workflows and to deliver continual, real-time compliance snapshots of their public cloud environments. Able to embrace a proactive cloud security posture, organizations can improve their risk postures while increasing operational efficiencies.

[1] "2019 State of the Cloud Report," RightScale from Flexera, February 2019.

[2] Ryan K.L. Ko, et al., "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," Proceedings of the 2011 IEEE World Congress on Services, Washington DC, USA, July 4-9, 2011.

September 21, 2019 6:51 AM

377363-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiCWP Compliance Solution\sb-forticwp-simplifies-compliance-in-the-public-cloud-v2.1