SOLUTION BRIEF

FortiCWP Simplifies Compliance in the Public Cloud

Executive Summary

For organizations operating in highly regulated industries, maintaining compliance across multiple public cloud environments is not only challenging, but is a critical business requirement. Failure to do so could lead to hefty penalties, brand damage, and lack of trust, and potential loss of business operations. In the ever-evolving regulatory environment, organizations can find it challenging to continually monitor and report on compliance with both regulatory requirements and security standards. The Fortinet FortiCWP Cloud Security Posture Management and Workload Protection solution 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. And with over 90% of organizations having adopted a multi-cloud strategy,[1] achieving security compliance visibility and control across all these environments can seem like an impractical task.

Combined with the dynamic changes in regulatory requirements, it is easy to see that organizations that manually aggregate and reconcile event data to monitor compliance and its implications, in a timely and effective way, will find it extremely difficult to manage. To stay compliant, organizations need an automated and simple way to validate, track, and report on compliance controls.

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

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.

Fortinet FortiCWP is a cloud security posture management (CSPM) and workload protection 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.

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 configuration assessments across its global public cloud deployments and identifies risks associated with any insecure provisioning or configurations detected in those public clouds.

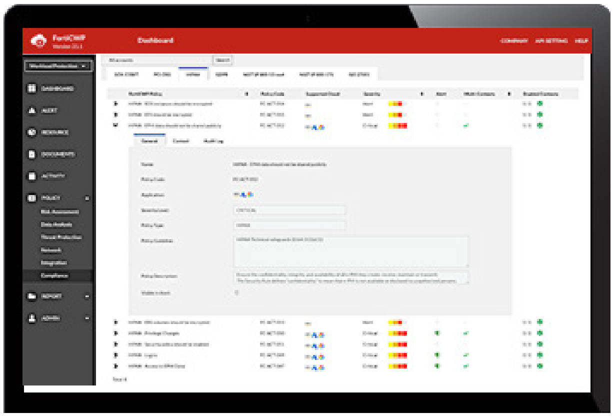

Figure 1: FortiCWP improves visibility and enhances compliance for public cloud platforms.

Unified Tracking and Reporting Leads to More Business Opportunities

Due to the steep penalties and fines attached to noncompliance with industry and government regulations, such as GDPR, compliance has become top of mind for multiple companies running applications in the public cloud. In these highly regulated industries, the average cost of a breach at organizations with high-level compliance failures in 2021 was $5.65 million.[2] So, when the potential impact of an organization's brand is considered, as a result of a breach in confidential data, such as personally identifiable information (PII), 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 to deliver continual, real-time compliance snapshots of their public cloud environments. Having this proactive cloud security posture allows organizations to have better insights into their business to improve their risk posture. This leads to better strategic alignment, increased operational efficiencies, and overall protection of an organization's brand and reputation.

[1] "2021 State of the Cloud Report," Flexera, 2021.

[2] "2021 Cost of Data Breach Report," IBM, July 2021.

Copyright © 2021 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.

November 9, 2021 7:57 AM
377363-A-0-EN