SOLUTION BRIEF

Fortinet Extends Compliance to the Cloud

Executive Summary

Multi-cloud adoption creates substantial business opportunities—greater agility, increased efficiencies, and expanded revenues. But managing multiple cloud deployments also introduces new challenges. Siloed cloud deployments obfuscate transparency and IT and security teams expend valuable time and resources aggregating data and managing controls across each cloud. These same challenges extend to compliance—from industrial and governmental regulations to security controls. Fortinet allows organizations to break down the barriers separating multi-cloud deployments, enabling them to automate compliance tracking and reporting—in the cloud and on-premises—while managing compliance and cybersecurity risks.

In addition to the sheer effort expended on compliance, many organizations have a difficult time demonstrating it. Digital transformation (DX) is fueling the rapid adoption of multiple clouds, which complicates compliance tracking and reporting and creates significant operational inefficiencies while ratcheting up cyber risks.

Multi-Cloud Adoption Complicates Compliance

Use of multiple clouds is now a mainstay with most enterprises: 84% indicate they have a multi-cloud strategy in place today.[1] But individual cloud providers maintain their own set of security and compliance tools and controls, which creates complexities for enterprises consuming the services. Each of them aggregates data and tracks and reports security and compliance differently. In addition, lack of security and compliance connectivity between and across cloud deployments creates additional complexities.

This disaggregation of compliance data and controls results in time-consuming, tedious workflows and processes for IT and security teams that are often are overburdened. Often, to address new security and compliance requirements, enterprises add new point products. However, as these do not integrate into legacy security and compliance controls, it simply exacerbates complexity. Unable to share information with other elements across the enterprise, these point products increase the amount of work for IT and security teams.

Headaches or Not, Compliance Is Required

Regardless of the complexity brought on by cloud computing, meeting and demonstrating compliance is not optional. DX is heightening the attention paid to data privacy by governmental and industrial regulatory bodies. The European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are recent responses to concerns about private consumer information and place significant responsibilities on businesses to demonstrate compliance. Additional compliance regulations are also under legislative consideration.[4] And of course, existing regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) also place significant compliance requirements on organizations.

Fortinet Key Compliance Capabilities:

- Automated compliance auditing and reporting for both cloud and on-premises environments
- Hundreds of built-in compliance reports across industries
- Customizable reports that include 400-plus charts and 35-plus templates
- Support for government and industry regulation mandates as well as security standards
- Targeted dashboards for key enterprise stakeholders (e.g., CIO, CISO, network architect, security architect)

56% of firms say they cannot determine compliance for their endpoint devices.[2]

Half of organizations are predicted to embrace the NIST Cybersecurity Framework as their security standard by 2020.[3]

Failure to demonstrate compliance with these regulations results in not only steep penalties and fines but also damage to brand reputation. But demonstrating compliance—whether in response to a data breach or internal or external audits—is not an easy undertaking. With cloud deployments proliferating and organizations embracing multiple clouds, this becomes increasingly difficult and time-consuming.

Organizations rely on an average of five clouds and run an average of 79% of their workloads in either the private or public cloud.[5]

Organizations are also embracing security standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) standards, and using them to prioritize security strategies and measure risks based on business objectives. Boards of directors and CEOs want to understand risks in terms of vulnerabilities—and how well the organization is doing in addressing them—and how these translate into implications to the business.

Unified Security with the Fortinet Security Fabric

Compliance cannot be achieved with a piecemeal approach across cloud silos and all security elements in general. Instead, organizations must embrace a security architecture that integrates transparency and controls within and across each cloud deployment. This integration must also extend to on-premises environments, resulting in single-pane-of-glass visibility and management.

But with IT and security teams stretched when it comes to staff and resources, and an advanced threat landscape that is increasing in volume, velocity, and sophistication, automation of compliance and security workflows and threat-intelligence protection, detection, and response is also critical.

The Fortinet Security Fabric addresses these requirements by enabling broad coverage of the entire attack surface and integrates data aggregation and information sharing between each of the security elements. With data at its core, this is a requisite for a successful compliance strategy. The Security Fabric also automates security and compliance tasks that consume valuable staff time to manage manually—from data aggregation, to notifications, to tracking and reporting—and place organizations at greater risk due to slow threat-intelligence sharing and management.

Integrated, Automated Compliance with Fortinet

To achieve end-to-end visibility and deliver comprehensive, automated compliance tracking and reporting covering both cloud and on-premises environments, Fortinet offers four products that integrate into the Fortinet Security Fabric. They support automated processes to facilitate compliance policy management and workflows, reducing risk when policies are changed.

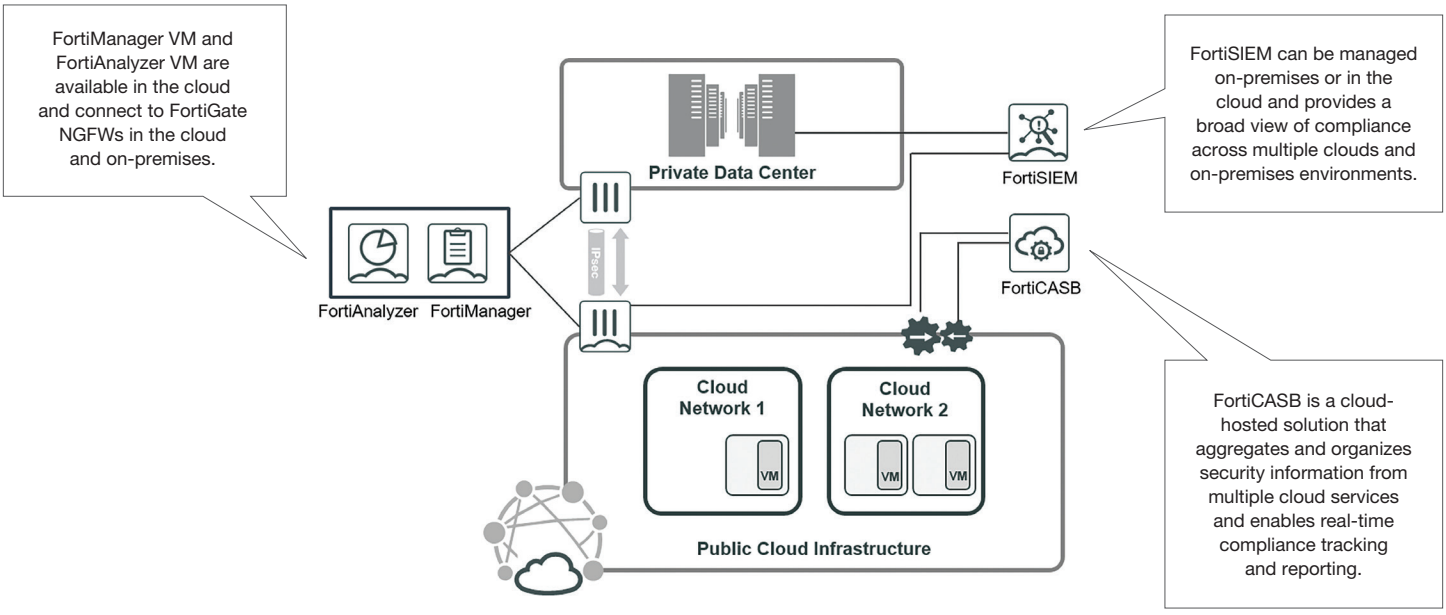

Figure 1. FortiAnalyzer, FortiManager, FortiSIEM, and FortiCASB integrate into the network, spanning multiple clouds and on-premises environments—from the campus to the network edge.

FortiCASB is a cloud-hosted service, while FortiSIEM, FortiAnalyzer, and FortiManager are available on-premises or as hosted cloud solutions.

- **FortiCASB** aggregates and organizes security information from multiple cloud services and APIs into meaningful compliance reports and live compliance dashboards that can be shared with different constituents—CIO, CISO, CEO, board of directors, among others.
- **FortiSIEM** provides a broader view of compliance across multiple clouds and on-premises environments. It aggregates data from Fortinet and non-Fortinet security tools and generates compliance reports with one click.
- **FortiAnalyzer** collects logs from Fortinet Security Fabric elements. Hundreds of prebuilt, regulation-specific reports make it extremely easy and fast for security teams to set up compliance tracking and reporting. This includes real-time reporting on industry standards such as PCI DSS and support for security standards such as NIST.
- **FortiManager** enables review, approval, and auditing of policy changes from a central location. It includes automated processes to facilitate policy compliance, policy life-cycle management, and enforced workflows to reduce risk for policy changes.

Fortinet Removes the Burden of Compliance

Compliance tracking and reporting is nonnegotiable. The Fortinet Security Fabric provides transparent visibility between and across multiple cloud deployments while automating data aggregation and compliance tracking and reporting. This saves IT and security staffs valuable time that can be reallocated to more strategic activities. It also enables organizations to quickly and easily demonstrate compliance with regulations and security standards. Additionally, organizations can proactively manage their risk postures via a comprehensive understanding of all vulnerabilities and threat measurements.

[1] "2019 RightScale State of the Cloud Report from Flexera: As Cloud Use Grows, Organizations Focus on Cloud Costs and Governance," RightScale from Flexera, accessed March 15, 2019.

[2] "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.

[3] "Developing the NIST Privacy Framework: How can a collaborative process help manage privacy risks?" NIST, September 24, 2018.

[4] Cynthia Brumfield, "The cybersecurity legislation agenda: 5 areas to watch," CSO Online, February 21, 2019.

[5] "2019 RightScale State of the Cloud Report from Flexera: As Cloud Use Grows, Organizations Focus on Cloud Costs and Governance," RightScale from Flexera, accessed March 15, 2019.

FORTINET

www.fortinet.com

July 24, 2019 8:53 AM

357865-0-0-EN

sb-compliance-in-the-cloud