SOLUTION BRIEF

FortiCWP Protects Data in the Public Cloud

Executive Summary

As organizations increase the amount of data stored in public clouds, they increase their exposure to the risk of storage misconfigurations, data leaks, and malware intrusions. FortiCWP cloud workload protection (CWP) mitigates these risks with centralized security monitoring and management that detects misconfigurations, identifies sensitive data, and protects against leaks and malware across multiple clouds.

FortiCWP Protects Sensitive Data in the Cloud

- Centralize multi-cloud data security
- Identify storage misconfigurations
- Map sensitive data
- Protect against data leakage
- Detect malware and threats

Protecting Cloud Data Requires a Unified Security Approach

Organizations are rapidly adopting public cloud services. Gartner predicts that spending on public cloud services will reach $482 billion in 2022, and by 2026, public cloud spending will exceed 45% of all enterprise IT spending.[1]

But the emergence of new regulatory requirements, such as the European Union's General Data Protection Regulation (GDPR) and the evolution of existing ones such as the Payment Card Industry Data Security Standard (PCI DSS) around personally identifiable information (PII), complicates public cloud usage for certain applications and data.

Traditional public cloud security solutions—whether those developed and maintained by cloud providers or point security solutions—provide inadequate data protection. A common strategy is to deploy multiple siloed cloud security solutions that address individual risks. However, the risk of having multiple security products in an organization increases complexity that can lead to security gaps and the inability to effectively respond to threats and attacks. In a recent survey, 78% of CISOs indicated they have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more. Consequently, most organizations recognize the benefits of vendor consolidation, with 80% of organizations interested in a vendor-consolidation strategy.[2]

The most effective security solution is to implement a unified security strategy. And a unified cloud security approach must address the following challenges:

- **Provide complete, real-time visibility** of multiple files across different public clouds. Many organizations make the mistake of using different point security tools across each of their cloud deployments, which creates a fragmented architecture and disaggregated visibility.
- **Identify misconfigured cloud storage.** The majority of cloud breaches are the result of misconfigurations. In 2021, more than 1 billion records for CVS Health customers were exposed, likely because of a cloud-storage misconfiguration.[3] And it is predicted that through 2023, at least 99% of cloud security failures will be the customer's fault, mainly in the form of cloud resource misconfiguration.[4]
- **Prevent data leaks from the cloud.** Organizations must have the ability to monitor and report on data leakage in their public clouds using unified, centralized tracking and reporting. This requires constant data monitoring—both that at rest and in motion. Without these controls in place, organizations place themselves at risk. For example, an employee shared a spreadsheet with his wife in hopes that she could help solve formatting issues, not realizing that the personal information of 36,000 employees was exposed, including employee ID data and places of birth.[5]
- **Detect and mitigate cloud-based malware.** The volume, velocity, and sophistication of malware makes it increasingly difficult for organizations to protect against attacks. The ability to store any file, unsupervised on any cloud storage, magnifies this risk. A recent report states: "Cloud-delivered malware has increased to an all-time high of 68% with cloud storage apps accounting for 66.4% of cloud malware delivery and malicious Office docs now accounting for 43% of all malware downloads."[6]

FortiCWP Delivers Centralized Visibility and Control

FortiCWP, the Fortinet Cloud Security Posture Management and Workload Protection solution, helps organizations tackle these challenges by providing:

- **Comprehensive configuration assessment** to ensure security of stored data. FortiCWP evaluates cloud storage service configurations in order to enable teams to identify misconfigurations and vulnerabilities in public clouds that could lead to the compromise of data

and the introduction of undesired risk through the storage of malicious data or downloading of sensitive information. In this case, FortiCWP evaluates storage service configurations against best practices and enables custom storage configuration policies.

- **Data leak protection (DLP) that enhances compliance.** FortiCWP offers dozens of predefined DLP policies that help organizations mitigate the risk of sensitive information exposed to unwanted parties and the resulting liability associated with this risk. This requires highly customizable DLP tools that identify and monitor sensitive data, defend against data leaks, and provide a set of predefined compliance reports pertaining to the security of sensitive information.
- **Award-winning threat detection and malware scanning.** FortiCWP addresses risks associated with ransomware and malware in the organization's cloud storage. The service automatically includes FortiGuard antivirus that scans files stored in the cloud.

Public Cloud Adoption With Confidence

There are no signs that public cloud adoption is slowing. As organizations deploy more applications and migrate more data to the cloud, their cyber risks will escalate without capabilities that provide transparent visibility and centralized controls across each of their cloud deployments. FortiCWP enables them to proactively manage public cloud risks—and specifically protect critical data—by breaking down silos separating clouds, which results in comprehensive visibility and unified policy management between and across cloud environments.

FortiCWP centralizes multi-cloud monitoring to find misconfigurations, protect sensitive data, defend against leaks, and provide predefined compliance reports.

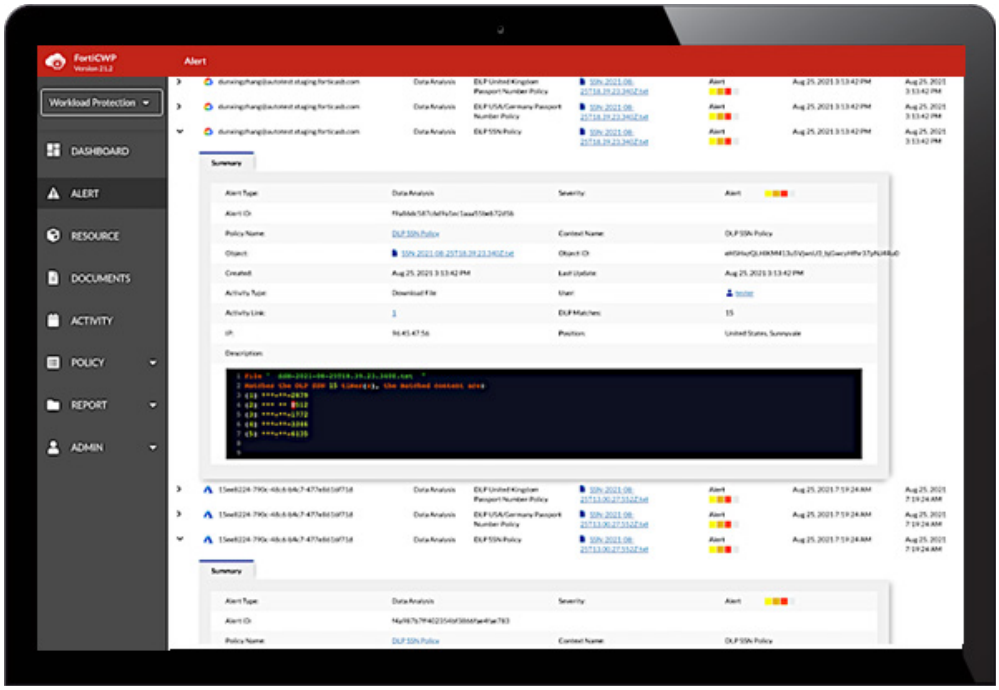

Figure 1: FortiCWP unifying multi-cloud security.

[1] "Gartner Says Four Trends Are Shaping the Future of Public Cloud," Gartner, August 2, 2021.

[2] Kasey Panetta, "Gartner Top Security and Risk Trends for 2021," Gartner, April 5, 2021.

[3] Lisa Vaas, "CVS Health Records for 1.1 Billion Customers Exposed," Threatpost, June 17, 2021.

[4] Kasey Panetta, "Is the Cloud Secure," Gartner, October 10, 2019.

[5] Maddie Rosenthal, "Insider Threats Examples: 17 Real Examples of Insider Threats," Tessian, July 21, 2021.

[6] "Cloud and Threat Report: July 2021 Edition," Netskope Threat Labs, July 2021.

November 13, 2021 2:31 AM
488577-A-0-EN