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.

Protect 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. As of next year, 95% of organizations indicate they will rely on Software-as-a-Service (SaaS) applications, with adoption of Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) not far behind at 83% and 74%, respectively.[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. But these rarely work together, and moreover they create blind spots, security gaps, less accurate threat intelligence, and an inability to respond to attacks and breaches in a coordinated fashion.[2]

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. For example, researchers, scanning the internet for just three months, discovered 1.5 billion sensitive files—including payroll information, credit card details, medical data, and patents for intellectual property—that were stored in misconfigured, publicly available public clouds such as Amazon Simple Storage Service (Amazon S3) buckets.[3]
- **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, more than 90 companies were inadvertently leaking sensitive corporate and customer data because their employees were sharing public links to files in their enterprise cloud storage accounts.[4]
- **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. And there are serious security gaps. For example, researchers find that 10% of repositories hosted by cloud providers are compromised by malware.[5]

FortiCWP Delivers Centralized Visibility and Control

FortiCWP, a cloud security management product, 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. Integration with FortiSandbox-Cloud provides additional protection from zero-day malware threats. Both of these services are included at no extra cost as part of the FortiGate Enterprise Protection Bundle and Fortinet 360 Protection Bundle subscription services.

When it comes to threat detection and malware scanning, Fortinet received AV-Comparatives' highest award, the Advanced+ rating, for file detection and real-world protection.[6]

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.

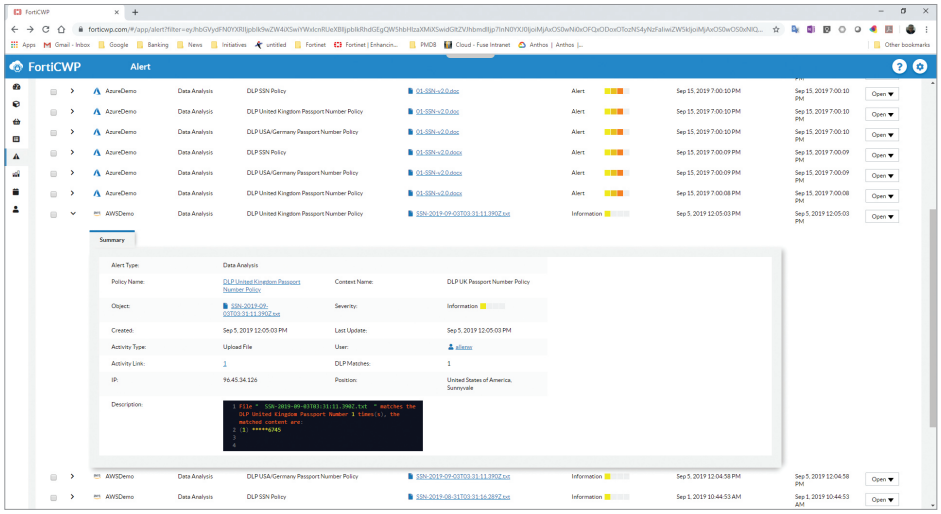

Figure 1: Unifying multi-cloud security.

[1] Louis Columbus, "State Of Enterprise Cloud Computing, 2018," Forbes, August 30, 2018.

[2] Bill Hogan, "Benefits of Using CASBs in Financial Services," Fortinet, September 26, 2017.

[3] Danny Palmer, "1.5 billion sensitive files exposed by misconfigured servers, storage and cloud services," ZDNet, April 5, 2018.

[4] Zack Whittaker, "Dozens of companies leaked sensitive data thanks to misconfigured Box accounts," TechCrunch, March 11, 2019.

[5] Patrick Nelson, "Major cloud is infested with malware, researchers say," Network World, November 10, 2016.

[6] "Anti-Virus," FortiGuard Labs, accessed March 18, 2019.

FORTINET®

www.fortinet.com

September 20, 2019 8:32 PM

488577-0-0-EN

D:\Fortinet\Work\2019\September\092019\sb-forticwp-protects data-in-public-cloud