FORTINET

Cloud Security Analytics and Policy Management

What Security Architects Should Seek in a Solution

Table of Contents

Executive Overview

Organizations have embraced public cloud platforms of all kinds in a big way, but the result is increased security complexity. Built-in security tools for the various cloud providers are unique and incompatible. Consistently managing risk across all clouds renders security operations in a multi-cloud world time-consuming and ineffective. In addition, the expanded attack surface means that organizations must protect themselves from risks originating from both the application programming interface (API) and the user interface (UI) of cloud platforms. And these risks can result not only from configuration and management errors but also from the application elements themselves.

This eBook discusses five key use cases faced by security teams tasked with securing their public cloud infrastructure: (1) risk management, (2) data security, (3) traffic analysis and investigation, (4) threat detection and response, and (5) compliance. Each of these use cases outlines unique challenges in a multipublic cloud environment. For each, the top security priority is to integrate the security architecture for centralized visibility and control—something that cannot be done manually due to the differences in the public clouds. With an integrated architecture, organizations can address each of these challenges in a proactive, holistic way, improving operational efficiency and decreasing risk.

83%

of enterprise workloads will be in the cloud by 2020, and 63% of IT professionals see security as the most significant concern about this trend.[1]

Introduction: Dealing with Cloud Sprawl

Organizations have embraced public cloud computing in a big way: public cloud services are expected to grow by 17.3% in 2019 to a staggering $206 billion worldwide, with Infrastructure-as-a-Service (IaaS) as the fastest growing segment at 27.6%.[2] While the numbers are hard to fathom, the attractiveness of cloud platforms is not surprising. No matter what cloud-based service organizations are running—software, infrastructure, or platform—they enjoy the benefits of quick deployment, scalability on the fly, the ability to pay only for the capacity that is used, and the elimination of capital and human resources expenditures for the rollout.

However, after a decade or more of aggressively adding cloud resources, many organizations are suffering from what might be called cloud sprawl. Most organizations operate multiple clouds, and network security teams often struggle to keep track of assets and accurately identify risks in these dynamic environments. The decentralized nature of many cloud purchases exacerbates the problem, as IT is often not the final decision-maker. Another complication: the built-in security tools of the various public cloud providers work differently and track different sets of security data.

This eBook covers five key use cases for public cloud security and discusses the characteristics of an effective solution for each use case.

"This year, IaaS revenue is expected to grow 27.6%."[3]

Risk Management: An Enterprise View of Cloud Configurations

In today's rapidly evolving marketplace, complying with static regulations and standards is not enough. Each organization must assess its cyber-risk posture and map security programs to align with its risk tolerance. One key driver of risk for organizations is the misconfiguration of systems—both on the cloud management platform and in the application components themselves.[4] One report attributes 70% of cloud data breaches to misconfiguration, a number that jumped 424% year over year.[5]

With static, on-premises environments, these issues can be addressed using a configuration management database (CMDB). But rapid changes to cloud services and configurations introduce new challenges. Services on multiple clouds result in siloed visibility, and the dynamic nature of cloud deployments makes it difficult for an organization to consistently assess its security posture. This leads to the risk of misconfigurations in an increasingly complex infrastructure.

In addressing these issues, the first step should be to establish centralized visibility and track changes of configuration state and posture of the entire cloud infrastructure. With this broad view, a cloud security solution should be able to perform a comprehensive risk assessment, generating a risk score and offering best practice recommendations for improving it. With the assessment done, an organization's cloud infrastructure should be continually monitored to ensure that issues are flagged and resolved in a timely manner. Finally, analysis tools should be available to help security teams understand the life cycle of configuration changes across the multi-cloud environment.

“Cloud topped the list of digital-transformation initiatives targeted for development by enterprises in 2019.”[6]

Data Security: Constant Monitoring for Data Loss and Malware

A sprawling cloud infrastructure can mean that users store unsolicited datasets in an unorganized fashion across cloud infrastructures. This results in significant unknown risk from potentially malicious code embedded in files, as well as increased risk for data leakage. In the case of the latter, there is a need for a consolidated view of all files and storage throughout the cloud infrastructure. Anything but a comprehensive multi-cloud file scanning and monitoring solution falls short of identifying risky file transfer patterns.

This takes place in the context of increasingly numerous and costly threats. In the fourth quarter of 2018, FortiGuard Labs detected nearly 34,000 new malware variants—a 128% increase over the first quarter of the same year.[7] And new research pegs the cost of cyber crime in 2018 for the typical organization at $13 million—a 12% increase over 2017 and a 72% increase over five years.[8] Thus, the need to scan files in cloud storage is one of the only ways to prevent the propagation of high-risk content.

To secure critical data in a multi-cloud infrastructure, organizations need to be able to constantly monitor (1) stored documents to identify malware, and (2) activity with sensitive data to identify and investigate data leakage in the environment.

"As more devices and critical data is moved to the cloud, the types of malicious attacks don't necessarily change much, but how attacks are executed does."[9]

Traffic Analysis and Investigation: A Comprehensive View to Detect Attacks

There are two problems with cloud sprawl: the increased risk of network intrusions brought on by potential configuration errors, and the inability to adequately monitor network traffic. The root of these challenges rests with security team members, who often do not have a current inventory of assets and resources enabled in public clouds—and certainly cannot monitor changes in these resources over time.[10] Even with an accurate inventory, monitoring traffic within and between clouds and detecting suspicious activity within that traffic requires specific tools.

To effectively detect and remediate network intrusions and protect critical services, security teams need the ability to view the current topology of all cloud resources, monitor and analyze network traffic, and drill down on specific services and traffic patterns that are suspicious. Specifically, they need the ability to visualize network traffic in order to more effectively distinguish between misconfigurations and threatening traffic patterns.

Almost 45% of security architects believe their organizations are too reactive and need to become more proactive in how they approach security.[11]

Threat Detection and Response: Integrated Intelligence and Real-Time Sharing

As organizations move more applications to the public cloud and leverage more cloud-native services, complexity increases. With increased complexity comes a potential for configuration errors. This brings an even greater need for an integrated approach to threat detection and response—especially given the complexities of the current threat landscape. Threats in the public cloud can occur for various reasons, including misconfiguration of the cloud itself, the use of vulnerable software versions, and the implementation of insecure code in cloud applications.

The main priority should be to hamper the ability of cyber criminals to exploit these vulnerabilities. Security teams need the ability to identify and isolate threats—and effectively remediate them. With security teams overseeing security investigations, they require security tools that make it easier for them to provide meaningful and user-friendly insights to DevOps teams.

There are more than one million threat types today—up from 50 a decade ago.[12]

Compliance: Centralized Reporting for Quick Remediation and Audit Preparation

As more regulations are passed and media scrutiny of organizations' cybersecurity shortcomings intensifies, compliance is an increasingly important concern for almost every organization. Newer regulations such as the European Union's General Data Protection Regulation (GDPR) impose steep fines for noncompliance, and similar regulations are in the works in other jurisdictions.[13] And other regulations can create challenges, such as the Payment Card Industry Data Security Standard (PCI DSS) that can result in an inability to accept credit and debit cards—a devastating outcome for many businesses.

This patchwork of requirements makes compliance and preparation for audits a complex undertaking that consumes myriad hours of valuable staff time at many organizations. Compliance reporting can be even more complex in a multi-cloud infrastructure, with siloed reporting tools and event data for each cloud provider and IaaS solution. And since the public cloud increases the attack surface and introduces new threat vectors, it is required to be a part of compliance evaluations.

As with the other business needs we have described, efficient and effective compliance reporting requires an architecture that integrates the multi-cloud architecture for centralized visibility and policy management. This visibility should include the ability to maintain historical snapshots of public cloud environments. Security teams must look for robust reporting tools with out-of-the-box policies for a variety of regulations and standards. Reports need to be set to run on a regular basis, enabling security teams to quickly identify policy violations and take remedial actions. These processes also need to be automated to optimize overburdened security teams while minimizing risks.

“The amount of time legal and cybersecurity teams spent responding to intrusions increased 20% over the past year.”[14]

Conclusion: Integration Is Key

The consistent message repeated on every page of this eBook is that integration of the security controls of public cloud resources is one of the newest and most important priorities for securing the public cloud. Integration helps organizations protect data, prevent intrusions, fight advanced threats, and satisfy auditors. Because of the way public cloud infrastructures are configured outside of the application and network systems and since their built-in security tools use different methodologies, manual integration is virtually impossible—and certainly ineffective given the speed of today's advanced threats. As a result, there is a clear need for a dedicated tool that uniformly provides the visibility and control to secure the public cloud management interface and APIs.

Organizations leveraging a variety of services in multiple clouds must seek a unified security tool that has native integration with each major cloud platform, the ability to consolidate threat intelligence coming from each cloud in real time, intelligent monitoring of traffic within and between clouds, and robust reporting and analysis tools. With transparent visibility and centralized control across the entire infrastructure, organizations can fully leverage the immense benefits of cloud computing—without increasing risk.

"In the digital enterprise, the strategic fusion of former silos leads to richer customer experiences, business acceleration, and operational agility."[15]

[1] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

[2] Louis Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018," Forbes, September 23, 2018.

[3] Andy Patrizio, "Cloud Computing Companies," Datamation, January 9, 2019.

[4] Asher Benbenisty, "Don't Go Once More Unto the Breach: Fix Those Policy Configuration Mistakes," Infosecurity, October 30, 2018.

[5] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, April 6, 2018.

[6] "The future of cyber survey 2019," Deloitte, March 2019.

[7] "Threat Landscape Report Q4 2018," Fortinet, accessed March 12, 2019.

[8] "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, accessed March 12, 2019.

[9] Rich Campagna, "Malware's Journey Through the Cloud," Infosecurity, September 28, 2017.

[10] Chris Purcell, "Is Multi-Cloud Sprawl Causing Your Money to Fly Away?" CIO, September 17, 2018.

[11] "The Security Architect and the State of Cybersecurity," Fortinet, forthcoming.

[12] Dave DeWalt and David Petraeus, "The Cyber Security Mega Cycle Aftermath," Optiv, September 7, 2017.

[13] Kassidy Kelley, "CCPA compliance begins with data inventory assessment," TechTarget, December 2018.

[14] "2019 Scalar Security Study: The Cyber Resilience of Canadian Organizations," Scalar, February 2019.

[15] Benson Chan, "Digital transformation reimagines everything," Strategy of Things, September 7, 2017.

FORTINET

www.fortinet.com

377156-A-0-EN

September 21, 2019 10:54 AM

eb-fortiCWP-cloud-security-use-cases