SOLUTION BRIEF

Dynamic Cloud Security: A Strategic Imperative for Feds' Dynamic, Multi-Cloud Environment

The Federal government's move to the cloud continues apace, as agencies seek to take advantage of the agility, efficiencies, and innovation it can deliver. Federal agencies were expected to spend $7.1 billion on cloud computing in 2020, according to a Bloomberg Government report[1] issued before the COVID-19 pandemic. Given the need to pivot to mass telework beginning in March, that figure is likely higher.

More than three-quarters of Federal IT decision makers responding to a GDIT survey[2] in May and June 2020 said their agencies had begun moving critical services to the cloud to address telework-related availability issues, and 83 percent of the cyber leaders responding to the survey said their agency increased multi-cloud adoption to support telework and mission needs related to COVID-19. At the same time, agencies needed to remain resilient against increasing cyberattacks and adhere to compliance requirements.

As cloud adoption accelerates, it facilitates cost optimization, agility, and productivity outside of the traditional office, among other benefits.

Cloud acceleration also means more applications, data, and users are exposed to security threats. Here's one example: By 2021, 90 percent of web-enabled applications will have more surface area for attack due to exposed application programming interfaces (APIs), rather than just the user interface, according to Gartner.[3]

Cloud Expands the Attack Surface

As cloud adoption accelerates, it facilitates cost optimization, agility, and productivity outside of the traditional office, among other benefits. However, cloud acceleration also means more applications, data, and users are exposed to security threats. Here's one example: By 2021, 90 percent of web-enabled applications will have more surface area for attack due to exposed application programming interfaces (APIs), rather than just the user interface, according to Gartner.[3] Similarly, the wider footprint of the multi-cloud environment can introduce security weaknesses if not managed holistically.

Overall, agencies are optimistic about multi-cloud, which helps them avoid vendor lock-in and take advantage of best-of-breed offerings. Most say multi-cloud will ultimately strengthen their security posture. At the same time, however, managing a multi-cloud environment is one of their top challenges over the next five years, according to GDIT's survey. Agencies must ensure workflows and applications can securely travel across and between different clouds, data centers, and devices, and that their security can scale as cloud use grows.

Multi-Cloud Brings Multiple Challenges

In a dynamic multi-cloud environment, agencies can pick and choose cloud platforms to meet their unique needs, and move applications and data into and out of the cloud and from one cloud to another as mission requirements change. These moves may be temporary or permanent, and due to factors such as performance, changes in cost or regulations, or changes in underlying technology. Cloud choice and movement flexibility are essential to agency innovation and agility.

Along with well-recognized benefits, the multi-cloud environment brings serious challenges, including:

- Disparate security controls applied to various cloud environments, which add, rather than reduce, security complexity
- Shortage of staff who are skilled in securing and managing multi-cloud infrastructures
- Achieving compliance within and across each cloud deployment

Gartner illustrates the importance of broad and deep cloud visibility with one striking statistic: Through 2025, 99 percent of cloud misconfigurations and security breaches will be the customer's fault.

A Unified System Enables Dynamic Multi-Cloud Security

Agencies using multiple cloud platforms, migrating or extending data and other resources from one cloud to another, and implementing software-as-a-service solutions, such as productivity and collaboration applications, need a consistent and easy-to-manage cloud security strategy that brings together network and application security solutions in a unified system.

Fortinet's Dynamic Cloud Security does just that, enabling secure applications and connectivity from data center to cloud, along with visibility and control spanning the entire multi-cloud infrastructure. Gartner illustrates the importance of broad and deep visibility with one striking statistic: Through 2025, 99 percent of cloud misconfigurations and security breaches will be the customer's fault.[4] Agencies with visibility across their entire cloud infrastructure are well-positioned to ensure they're not the latest cloud security statistic.

The backbone of Dynamic Cloud Security is Fortinet's market-leading security platform – the Fortinet Security Fabric – which offers a full range of essential security tools built on a common operating system. Fortinet's unique single-pane-of-glass management ties the tools together, alleviating the management burden on IT staff that results from a proliferation of disconnected platforms and point solutions. Fortinet's single-pane-of-glass management helps IT departments see every deployment, streamlining operations; uses unified workflows, ensuring consistent policy enforcement; standardizes configurations, guaranteeing uniform compliance; and maintains deep visibility, enabling threat detection and coordinated threat response.

Agencies Achieve Compliance and Go Beyond It

Achieving compliance with guidance and regulatory mandates such as HIPAA, NIST Special Publication 800-Series, and PCI DSS can be a time-consuming burden, especially if agencies take a piecemeal approach across cloud silos and security tools. They need a security architecture that spans the entire attack surface and integrates data aggregation and information sharing between each security tool. Automation of security and compliance tasks is also needed, so that staff can focus on threat-intelligence sharing and management.

Compliance isn't the end goal, however. It is a programmatic approach to security, but it doesn't guarantee security. Agencies need to evaluate and deploy tools that go beyond standard capabilities. For example, agencies can provide granular protection for cloud applications with cloud-native variants of tools such as web application firewalls that integrate with cloud APIs.

The Fortinet Security Fabric[5] integrates a range of cloud-native solutions to provide security for any application and deployment environment. These solutions include:

- FortiGate next-generation firewalls, which are available as a virtual appliance, enabling cloud-native security automation, VPN connectivity, network segmentation, intrusion prevention, and a secure web gateway
- FortiWeb, which protects web applications from known and unknown threats using signature detection, machine learning, and artificial intelligence. FortiWeb also protects web APIs using schema validation and OpenAPI security
- FortiCWP, which uses public cloud management APIs to continuously monitor configurations, user activity, and traffic logs across public cloud platforms. This visibility facilitates consistent compliance reporting across multiple clouds, as well as streamlined incident investigation and remediation
- FortiCASB, which enables data security in SaaS applications and ensures that SaaS application configurations maintain regulatory compliance
- FortiMail, a secure email gateway that helps agencies close gaps between their security requirements and the default security parameters of email applications

Agencies using security tools from more than 70 Fortinet partners can add them to the Security Fabric by leveraging prebuilt API connections, and they can add products that are not part of the partner ecosystem via REST APIs and DevOps scripts.

The Fortinet Security Fabric is available in a variety of virtual form factors, including versions designed to run as cloud native and containerized solutions, to ensure the broadest possible deployment. These various platform configurations leverage Fortinet's cloud connector technologies for tight integration in the unified Fortinet security platform.

Mission Agility is Enabled by Secure Multi-Cloud

To secure the multi-cloud, agencies need cloud security that follows applications and data across every cloud, platform, and network, coupled with a single-pane-of-glass dashboard that provides automation, deep visibility, and simplified management. This dynamic cloud security frees overburdened staff to focus on threat intelligence and moves agencies beyond compliance to a deeply secure cloud environment. The end result is mission agility without exposure to additional risks inherent in an expanding attack surface.

For more information, visit: https://www.fortinet.com/products/public-cloud-security.

[1] https://data.bloomberglp.com/bna/sites/3/2019/12/BGOV-The-State-of-Federal-Cloud-Report-2020.pdf
[2] https://www.meritalk.com/study/multi-cloud-defense/
[3] https://www.datacenterknowledge.com/security/what-data-center-managers-can-do-secure-apis-new-perimeter
[4] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
[5] https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-security-fabric.pdf